Wprowadzenie

Niektóre aspekty bezpiecznej komunikacji

Przez co najmniej dwa tysiące lat byli ludzie, którzy chcieli wysyłać wiadomości, które mogły być odczytane tylko przez ludzi, dla których są przeznaczone. Kiedy wiadomość jest wysyłana ręcznie, przenoszona od nadawcy do odbiorcy, czy to przez niewolnika, jak w starożytnej Grecji czy w Rzymie, czy też przez pocztę dzisiaj, istnieje ryzyko, że zbłądzi. Niewolnik może zostać schwytany lub listonosz może dostarczyć na niewłaściwy adres. Jeśli wiadomość jest napisana w jasny sposób, to znaczy w języku naturalnym, bez jakiejkolwiek próby ukrywania się, każdy kto ją zdobędzie, będzie mógł ją przeczytać a jeśli zna ten język, zrozumie go. W nowszych czasach wiadomości mogą być wysyłane za pomocą telegrafu, radia, telefonu, faksu lub e-maila, ale możliwość ich przechwycenia jest nadal obecna i rzeczywiście wzrosła ogromnie, ponieważ, na przykład, transmisja radiowa może być słyszana przez każdego kto znajduje się w zasięgu i dostraja się do właściwej częstotliwości, podczas gdy wiadomość e-mail może trafić do niezamierzonych odbiorców, jeśli zostanie naciśnięty niewłaściwy przycisk na klawiaturze komputera lub jeśli "wirus" czai się w komputerze. Może wydawać się niesłusznie pesymistyczna, ale dobrą zasadą jest założenie, że każda wiadomość, która ma być poufna, wpadnie w ręce kogoś, kto nie powinien jej widzieć, i dlatego rozsądnie jest podjąć kroki, aby zapewnić, że co najmniej, mają duże trudności z jej odczytaniem i, korzystnie, nie będą w stanie go w ogóle przeczytać. Zakres szkód spowodowanych niezamierzonym ujawnieniem może zależeć w dużym stopniu od czasu, który upłynął między przechwyceniem a odczytaniem wiadomości. Są sytuacje, w których opóźnienie dnia lub nawet kilku godzin czytania wiadomości niweczy zadawane obrażenia; na przykład decyzja wspólnika o kupnie lub sprzedaży dużej liczby akcji na raz lub, na wojnie, przez dowódcę armii, aby zaatakować w określonym kierunku o świcie następnego dnia. Przy innych okazjach informacja może mieć wartość długoterminową i musi być utrzymywana w tajemnicy tak długo, jak to możliwe, na przykład komunikat odnoszący się do planowania operacji wojskowej na dużą skalę. Niezbędny jest zatem wysiłek wymagany do odczytania wiadomości przez rywala, przeciwnika lub wroga. Jeśli przy użyciu najbardziej znanych technik i najszybszych dostępnych komputerów, wiadomość nie może być odczytana przez nieautoryzowanego odbiorcę w czasie krótszym niż czas, w którym tajemnica lub poufność są niezbędne, a nadawca może być w miarę dobrze zadowolony. Nie może nigdy być całkowicie szczęśliwy, ponieważ sukces w czytaniu niektórych wcześniejszych wiadomości może umożliwić przeciwnikowi przyspieszenie procesu rozwiązywania kolejnych wiadomości. Możliwe jest również, że odkryto technikę, której nie jest świadomy i w związku z tym jego przeciwnik jest w stanie odczytać wiadomość w znacznie krótszym czasie, niż sądził, że jest to możliwe. Tak było w przypadku niemieckiej maszyny Enigma w wojnie 1939-1945.

Szyfr Juliusza Cezara

Problem zapewnienia bezpieczeństwa wiadomości rozważali m.in. starożytni Grecy i Juliusz Cezar. Grecy pomyśleli o dziwacznym rozwiązaniu: wzięli niewolnika, ogolili mu głowę i podrapali wiadomość. Kiedy urosły mu włosy, wysłały go, by przekazał wiadomość. Odbiorca ogolił głowę niewolnika i odczytał wiadomość. Jest to wyraźnie zarówno bardzo niepewna, jak i nieskuteczna metoda. Każdy, kto znał tę praktykę, kto przechwycił niewolnika, mógł również ogolić głowę i przeczytać wiadomość. Ponadto wysłanie wiadomości zajmie tygodnie, a otrzymasz odpowiedź w ten sposób. Juliusz Cezar miał lepszy pomysł. Napisał wiadomość i przesunął każdą literę o trzy kolejne miejsca w alfabecie, tak aby w alfabecie angielskim A został zastąpiony przez D, B przez E i tak dalej, aż do W, który zastąpiłby Z, a następnie X przez A, Y przez B, a na końcu Z przez C. Jeśli zrobił to ze swoją słynną wiadomością

VENI. VIDI. VICI.

(Przyszedłem, Zobaczyłem, Podbiłem.) Użyłem 26-literowego alfabetu używanego w krajach anglojęzycznych (który, oczywiście, nie chciał), zostałby wysłany jako

YHQL. YLGL. YLFL

Nie jest to bardzo wyrafinowana metoda, zwłaszcza, że ujawnia, że wiadomość składa się z trzech słów, każdej z czterech liter, z kilkoma powtórzonymi literami. Trudno jest przezwyciężyć takie słabości w systemie naiwnym, jak ten, chociaż rozszerzenie alfabetu z 26 liter na 29 lub więcej w celu umieszczenia symboli interpunkcyjnych i spacji spowodowałoby, że długości słów byłyby mniej oczywiste. Cezar zdobył jednak miejsce w historii kryptografii, a szyfr "Juliusza Cezara", jak jest jeszcze nazywany, jest wczesnym przykładem systemu szyfrowania i jest szczególnym przypadkiem prostego szyfru zastępczego, jak zobaczymy później.

Kilka podstawowych definicji

Ponieważ będziemy wielokrotnie używać słów takich jak digraf, kryptografia i szyfrowanie zdefiniujemy je teraz. Monografia to pojedyncza litera dowolnego alfabetu, którego używamy. Dwuznak jest dowolną parą sąsiednich liter, a więc AT jest digrafem. Trigraf składa się z trzech sąsiednich liter, więc jest to trigraf i tak dalej. Poligraf składa się z nieokreślonej liczby sąsiednich liter. Poligraf nie musi być rozpoznawany jako słowo w języku, ale jeśli próbujemy rozszyfrować wiadomość, która ma być po angielsku, a znajdziemy spotkanie heptograficzne, jest ono znacznie bardziej obiecujące, niż gdy znajdziemy heptrafę, taką jak DKRPIGX. Symbol to dowolna postać, w tym litery, cyfry i znaki interpunkcyjne, podczas gdy ciąg znaków jest dowolną sąsiednią kolekcją symboli. Długość łańcucha jest liczbą znaków, które zawiera. Tak więc A3 £% $ jest łańcuchem o długości 5. System szyfrowania lub system kryptograficzny to dowolny system, który może być użyty do zmiany tekstu wiadomości w celu uczynienia jej niezrozumiałym dla każdego innego niż zamierzony odbiorca. Proces stosowania systemu szyfrowania do wiadomości nazywa się szyfrowaniem lub szyfrowaniem. Pierwotny tekst wiadomości, zanim został zaszyfrowany, nazywany jest zwykłym tekstem; po zaszyfrowaniu jest nazywany tekstem zaszyfrowanym. Odwrotny proces szyfrowania, odzyskanie oryginalnego tekstu wiadomości z jej zaszyfrowanej wersji, nazywa się odszyfrowaniem lub odszyfrowaniem. Te dwa słowa nie są, być może, całkowicie synonimiczne. Zamierzony odbiorca wiadomości myślałby o sobie, że ją odszyfrowuje, podczas gdy niezamierzony odbiorca, który próbuje to zrozumieć, pomyślałby o sobie, że ją odszyfrowuje. Kryptografia to nauka o projektowaniu i używaniu systemów szyfrujących, w tym ich mocnych i słabych stron oraz podatności na różne metody ataku. Kryptografem jest każdy, kto zajmuje się kryptografią. Kryptoanaliza to nauka o metodach rozwiązywania układów szyfrów. Kryptoanalityk (często określany popularnie jako łamacz kodu) to każdy, kto jest zaangażowany w kryptoanalizie. Kryptografowie i kryptoanalitycy są przeciwnikami; każdy próbuje przechytrzyć drugiego. Każdy będzie starał się wyobrazić siebie na pozycji drugiej i zadać sobie takie pytania, jak: "Gdybym był nim, co bym zrobił, żeby mnie pokonać?" Obie strony, które prawdopodobnie nigdy się nie spotkają, są zaangażowane w fascynującą intelektualną bitwę i stawki może być naprawdę bardzo wysoki.

Trzy etapy odszyfrowywania: identyfikacja, zerwanie i ustawienie

Kiedy kryptoanalityk po raz pierwszy widzi komunikat zaszyfrowany, jego pierwszym problemem jest odkrycie, jaki rodzaj systemu szyfrowania został użyty. Być może był to już znany lub nowy. W obu przypadkach ma problem z identyfikacją. Aby to zrobić, powinien najpierw wziąć pod uwagę wszelkie dostępne informacje o zabezpieczeniach, takie jak typ systemu, który nadawca, o ile jest znany, używał poprzednio lub jakikolwiek nowy system, który pojawił się ostatnio w dowolnym miejscu. Potem przejrzy preambułę do wiadomości. Preambuła może zawierać informacje pomagające zamierzonemu odbiorcy, ale może również pomóc kryptoanalitykowi. W końcu przeanalizuje samą wiadomość. Jeśli

jest zbyt krótka, dalsze postępy mogą być niemożliwe i musi poczekać na więcej wiadomości. Jeśli wiadomość jest wystarczająco długa lub jeśli zebrał już kilka wystarczająco długich wiadomości, zastosowałby wiele testów matematycznych, które z pewnością powinny mu powiedzieć, czy używa się książki kodowej, względnie prostego systemu szyfrowania lub czegoś bardziej wyrafinowanego. Po zidentyfikowaniu systemu, kryptoanalityk może być w stanie oszacować, ile materiału (na przykład ile liter szyfrowych) będzie potrzebował, jeśli ma mieć uzasadnioną szansę na jego rozbicie, czyli dokładnie wiedzieć, w jaki sposób wiadomości są szyfrowane przez system. Jeśli system jest prosty, w którym nie ma większych zmian od jednej wiadomości do drugiej, takich jak książka kodowa, prosta zamiana lub transpozycja (patrz rozdziały od 2 do 6), może wtedy być w stanie odszyfrować wiadomość (y) bez wiele trudności. Jeśli, o ile jest to bardziej prawdopodobne, istnieją części systemu, które zostały zmienione z wiadomości na wiadomość, najpierw trzeba będzie określić części, które się nie zmieniają. Jako przykład, przewidując część 9, maszyna Enigma zawierała kilka kół; wewnątrz tych kół były druty; okablowanie wewnątrz kół nie zmieniło się, ale kolejność, w jakiej koła były umieszczane w maszynie, zmieniała się codziennie. Zatem okablowanie było częścią stałą, ale ich kolejność była zmienna. Problem łamania jest najtrudniejszy; może to zająć tygodnie lub miesiące i wymagać użycia technik matematycznych, wykorzystania błędów operatora, a nawet informacji dostarczonych przez szpiegów. Po ustaleniu wszystkich części stałych konieczne będzie ustalenie części zmiennych, takich jak pozycje początkowe kół Enigmy, które zmieniły się wraz z każdą wiadomością. To jest problem z ustawianiem. Po jej rozwiązaniu wiadomości mogą zostać odszyfrowane. Tak więc łamanie odnosi się ogólnie do systemu szyfrowania, podczas gdy ustawienie odnosi się do odszyfrowania poszczególnych wiadomości.

Kody i Szyfry

Chociaż słowa są często używane luźno, rozróżniamy kody i szyfry. W kodzie wspólne frazy, które mogą składać się z jednej lub więcej liter, cyfr lub słów, są zastąpione, zwykle, czterema lub pięcioma literami lub cyframi, zwanymi grupami kodów, pobranymi z książki kodów. W przypadku szczególnie typowych zwrotów lub liter może istnieć więcej niż jedna grupa kodowa pod warunkiem, że użytkownik zmieni swój wybór, aby utrudnić identyfikację typowych fraz. Na przykład w czterocyfrowym kodzie słowo "poniedziałek" może mieć trzy alternatywne grupy kodów, takie jak 1538 lub 2951 lub 7392. Zajmiemy się kodami w sekcji 6. Kody są szczególnym rodzajem systemu szyfrowania, ale nie wszystkimi szyframi systemy są kodami, więc użyjemy słowa "szyfr", aby odnieść się do metod szyfrowania, które nie używają kodów, ale wytwarzają zaszyfrowaną wiadomość z oryginalnego tekstu jawnego zgodnie z pewną regułą (algorytm słowa jest obecnie preferowany do "rządzenia", szczególnie gdy w grę wchodzą programy komputerowe). Rozróżnienie kodów i szyfrów może czasem być nieco rozmyte, szczególnie w przypadku prostych systemów. Szyfr Juliusza Cezara można uznać za wykorzystujący jednostronicowy kodeks, w którym naprzeciwko każdej litery alfabetu jest drukowana litera trzy kolejne pozycje w alfabecie. Jednak w przypadku większości systemów, którym będziemy się zajmować, rozróżnienie będzie wystarczająco jasne. W szczególności Enigma, często błędnie określana jako "kod Enigmy", jest z pewnością maszyną szyfrującą, a nie kodem. Historycznie, dwie podstawowe idee dominowały w kryptografii do stosunkowo niedawnych czasów i wielu systemów szyfrów. Pierwszym pomysłem jest przetasowanie liter alfabetu, tak jak tasuje się paczkę kart, której celem jest stworzenie czegoś, co można by nazwać przypadkowym uporządkowaniem, permutacją lub anagramem liter. Drugi pomysł polega na przekształceniu liter wiadomości w liczby, biorąc A = 0, B = 1, ..., Z = 25, a następnie dodaj kilka innych liczb, które same mogą być literami skonwertowanymi na liczby, znanymi jako " klucz ", do nich list po literze; jeśli dodawanie daje liczbę większą niż 25, odejmujemy od niej 26 (jest to tzw. arytmetyka (mod 26)). Otrzymane liczby są następnie przekształcane z powrotem w litery. Jeśli dodane liczby są tworzone przez wystarczająco nieprzewidywalny proces, wynikowy komunikat szyfrowania może być bardzo trudny, a nawet

niemożliwy, do odszyfrowania, chyba że dostaniemy klucz. Co ciekawe, szyfr Juliusza Cezara, choć skromny, może być uważany za przykład dowolnego typu. W pierwszym przypadku nasze "tasowanie" jest równoznaczne z przesunięciem trzech ostatnich kart z przodu paczki, tak aby wszystkie litery przesunęły się "w dół" o trzy miejsca, a X, Y i Z znajdują się na pierwszym planie. W drugim przypadku kluczem jest po prostu liczba 3 powtarzana w nieskończoność - jako "słaby" klucz, jaki można sobie wyobrazić. Przetłumaczenie wiadomości na inny język może być uznane za formę szyfrowania przy użyciu książki kodowej (tj. Słownika), ale wydaje się, że rozciąganie użycia słowa kodowego za daleko. Tłumaczenie na inny język poprzez wyszukiwanie każdego słowa w książce kodowej, działającej jak słownik, zdecydowanie nie jest zalecane, ponieważ wie każdy, kto próbował nauczyć się innego języka. Z drugiej strony używanie mało znanego języka do przekazywania wiadomości krótkoterminowe znaczenie może czasem być rozsądne. Mówi się na przykład, że w czasie II wojny światowej żołnierze indiańscy z plemienia Navajo byli czasami wykorzystywani przez siły amerykańskie na Pacyfiku do przekazywania wiadomości telefonicznie w ich własnym języku, na rozsądne założenie, że nawet gdyby wróg przechwycił rozmowy telefoniczne, prawdopodobnie nie mieliby nikogo dostępnego, który mógłby zrozumieć, co zostało powiedziane. Inną formą szyfrowania jest użycie osobistego skrótu. Taka metoda była stosowana od co najmniej średniowiecza przez ludzi, takich jak Samuel Pepys, którzy prowadzą pamiętniki. Biorąc pod uwagę wystarczającą liczbę wpisów, takie kody zazwyczaj nie są trudne do rozwiązania. Regularne pojawianie się symboli, takich jak te, które przedstawiają nazwy dni tygodnia, dostarczy dobrych wskazówek dla pewnych kłamstw. O wiele głębszy przykład daje odszyfrowanie starożytnego Mycenaena przez Ventris skrypt znany jako Linear B, oparty na symbolach reprezentujących greckie sylaby Dostępność komputerów i praktyczność budowania złożonych układów elektronicznych na chipie krzemowym przekształciły kryptografię i kryptoanalizę. W konsekwencji niektóre z najnowszych systemów szyfrowania opierają się na dość zaawansowanych matematycznych koncepcjach, które wymagają znacznych urządzeń obliczeniowych lub elektronicznych, a zatem były niewykonalne w erze przed komputerem.

Ocena siły systemu szyfrowania

Kiedy proponuje się nowy system szyfrowania, należy ocenić jego siłę w stosunku do wszystkich znanych ataków i przy założeniu, że kryptoanalityk wie, jaki rodzaj systemu szyfrowania, ale nie wszystkie szczegóły, są używane. Siła może być oceniona dla trzech różnych sytuacji:

(1) że kryptoanalityk ma dostępne tylko teksty szyfrów;

(2) że posiada zarówno teksty szyfrów, jak i ich oryginalny tekst jawny;

(3) że ma zarówno szyfr, jak i zwykły tekst, który sam wybrał.

Pierwsza sytuacja jest "normalna"; nie należy stosować systemu szyfrowania, który można rozwiązać w rozsądnym czasie w tym przypadku. Druga sytuacja może się pojawić, na przykład, jeśli identyczne wiadomości są wysyłane zarówno przy użyciu nowego szyfru, jak i przy użyciu "starego" szyfrowania, który może odczytać kryptoanalityk. Takie sytuacje, które stanowią poważne naruszenie bezpieczeństwa, nierzadko występują. Trzecia sytuacja powstaje głównie wtedy, gdy kryptolog, chcąc ocenić siłę proponowanego przez siebie systemu, rzuca wyzwanie kolegom, działającemu jako wróg, aby rozwiązać swój szyfr i pozwala mu dyktować, jakie teksty powinien zaszyfrować. Jest to standardowa procedura testowania nowych systemów. Bardzo interesującym problemem dla kryptoanalityka jest budowa tekstów, które po zaszyfrowaniu dostarczą mu maksymalnej informacji o szczegółach systemu. Format tych wiadomości zależy od sposobu przeprowadzenia szyfrowania. Druga i trzecia sytuacja może również powstać, jeśli kryptoanalityk ma dostęp do szpiega w organizacji kryptografa; tak było w latach 30. XX wieku kiedy polscy kryptoanalitycy otrzymywali tekstowe i szyfrowe wersje niemieckich wiadomości Enigmy. System szyfrów, który nie może być rozwiązany

nawet w tej trzeciej sytuacji, jest rzeczywiście silnym szyfrem; to jest to, czego chcą kryptografowie, a kryptoanalitycy się boją.

Błąd podczas wykrywania i korygowania kodów

Inną klasą kodów są te, które mają zapewnić dokładność przekazywanych informacji, a nie ukrywać ich zawartości. Takie kody są znane jako kody wykrywające błędy i korygujące i były przedmiotem wielu badań matematycznych. Zostały one użyte od najwcześniejszych dni komputerów, aby chronić się przed błędami w pamięci lub w danych przechowywanych na taśmie magnetycznej. Najstarsze wersje, takie jak kody Hamminga, mogą wykryć i skorygować pojedynczy błąd w postaci 6-bitowej. Nowszym przykładem jest kod, który został użyty do wysłania dane z Marsa ze statku kosmicznego Mariner, które mogłyby skorygować do 7 błędów w każdym 32-bitowym "słowie", co pozwoliło na znaczną ilość zepsucia sygnału podczas długiej podróży z powrotem na Ziemię. Na innym poziomie prostym przykładem kodu wykrywającego błąd, ale bez korekty błędów, jest ISBN (International Standard Book Number). Składa się z 10 cyfr lub 9 cyfr, po których następuje litera X (która jest interpretowana jako liczba 10) i zapewnia sprawdzenie, czy numer ISBN nie zawiera błędu. Kontrola jest przeprowadzana w następujący sposób: zsumować 1-krotność (pierwsza cyfra)? 2 razy (druga cyfra)? 3 razy (trzecia cyfra). . . i tak do? 10 razy (dziesiąta cyfra). Cyfry są zwykle drukowane w czterech grupach oddzielonych myślnikami lub miejsca dla wygody. Pierwsza grupa wskazuje obszar językowy, drugi identyfikuje wydawcę, trzeci to numer seryjny wydawcy, a ostatnia grupa to jednocyfrowy znak kontrolny. Suma (znana jako suma kontrolna) powinna dawać wielokrotność 11; jeśli nie, wystąpi błąd w ISBN. Na przykład:

1-234-56789-X daje sumę kontrolną

1 (1) + 2 (2) + 3 (3) + 4 (4) + 5 (5) + 6 (6) + 7 (7) + 8 (8) + 9 (9) + 10 (10)

który jest

1 +4+4 +4+9 +9+ 16 + 25 + 36 + 49 + 64 + 81 + 100 = 385 = 35 x 11

i tak jest ważne. Z drugiej strony

0-987-65432-1 daje sumę kontrolną

0+18+24+28+30+30+28+24+18+10 = 210 =19x11

i tak musi zawierać co najmniej jeden błąd.

Kod ISBN może wykryć pojedynczy błąd, ale nie może go skorygować, a jeśli tak są dwa lub więcej błędów, które mogą wskazywać, że numer ISBN jest poprawny, a kiedy nie jest. Temat poprawiania błędów i wykrywania kodów wymaga pewnych zaawansowanej matematyki i nie będą dalej rozważane w tej książce. Zainteresowani czytelnicy powinni zapoznać się z książkami takimi jak [1.1], [1.2], [1.3].

Inne metody ukrywania wiadomości

Istnieją inne metody ukrywania znaczenia lub treści komunikatu, które nie opierają się na kodach lub szyfrach. Dwa pierwsze nie są tutaj istotne, ale zasługują na to, aby je wspomnieć. Takie metody są

(1) użycie tajemnego lub "niewidocznego" atramentu,

(2) użycie mikrokropek, maleńkich zdjęć wiadomości na mikrofilmie, utkwiło w wiadomości w nieoczywistym miejscu,

(3) "osadzanie" wiadomości wewnątrz niewinnej wiadomości, w której słowa lub litery tajnej wiadomości są rozproszone, zgodnie z pewną zasadą, za pośrednictwem nie-tajnej wiadomości.

Pierwsze dwa z nich zostały wykorzystane przez szpiegów; wybitnie odnoszący sukcesy "podwójny agent" Juan Pujol, znany jako garbo, używał obu metod od 1942 do 1945 roku [1.5]. Trzecia metoda była również wykorzystywana przez szpiegów, ale mogła również zostać użyta przez jeńców wojennych w listach do domu, aby przekazać informacje o tym, gdzie się znajdowały lub o warunkach panujących w obozie; cenzorzy będą zwracać uwagę na takie próby. Przykłady w tej książce są prawie w całości oparte na tekstach angielskich, przy użyciu 26-literowego alfabetu lub jego rozszerzonej wersji, aby umożliwić włączenie symboli interpunkcyjnych, takich jak spacja, kropka i przecinek. Modyfikacja przykładów w celu dodania większej liczby symboli lub liczb lub do języków z różnymi alfabetami nie przedstawia żadnych trudności w teorii. Jeśli jednak system szyfrowania jest wdrażany na fizycznym urządzeniu, zmiana rozmiaru alfabetu może nie być możliwa bez jego przeprojektowania; dotyczy to maszyn Enigmy i Hagelin, tak jak my .Zobaczymy później. Języki inne niż alfabetyczne, takie jak japoński, musiałyby być "alfabetycznie" lub, być może, traktowane jako materiały nietekstowe, takie jak fotografie, mapy, diagramy itp., Które mogą być zaszyfrowane za pomocą specjalnie zaprojektowanych systemów typu stosowanego w szyfrowaniu. programy telewizji satelitarnej lub dane z pojazdów kosmicznych.

Arytmetyka modulo

W kryptografii i kryptoanalizie często konieczne jest dodanie dwóch strumieni liczb do siebie lub odjęcie jednego strumienia od drugiego, ale stosowana forma dodawania lub odejmowania zwykle nie jest zwykłą arytmetyką, lecz tzw. Arytmetyką modułową. W modułowej arytmetyki wszystkie dodatki i odejmowania są wykonywane w odniesieniu do ustalonej liczby, znanej jako moduł. Typowe wartości modułu w kryptografii to 2, 10 i 26. Bez względu na moduł, wszystkie liczby, które występują, są zastępowane przez ich resztki, gdy są one dzielone przez moduł. Jeżeli reszta jest ujemna, dodaje się moduł, aby pozostała część stała się nieujemna. Jeśli na przykład moduł wynosi 26, jedyne liczby, które mogą wystąpić, to od 0 do 25. Jeśli dodamy 17 do 19, wynik wynosi 10, ponieważ 17 + 19 =36 a 36 pozostawia resztę 10, podzielone przez 26. Aby to zaznaczyć, modulus 26 jest używany, pisaliśmy

17-19, 10 (mod 26).

Jeśli odejmujemy 19 od 17, wynik (- 2) jest ujemny, więc dodajemy 26, co daje 24 jako wynik. Symbol ≡ Jest odczytywany jako "jest przystający ", więc powiedzielibyśmy "36 jest zgodny z 10 (mod26)", a "-2 jest przystające 24 (mod26)". Kiedy dodawane są dwa strumienie liczb (mod 26), reguły odnoszą się do każdej pary liczb osobno, bez "przenoszenia" do następnej pary. Podobnie, gdy odejmujemy jeden strumień od drugiego (mod 26), reguły odnoszą się do każdej pary cyfr oddzielnie, bez "pożyczania" od następnej pary.

Przykład 1

Doadajemy stumień 15 11 23 06 11 do strumienia 17 04 14 19 23 (mod 26)

Rozwiązanie

$$\begin{array}{rccccc} & 15 & 11 & 23 & 06 & 11 \\ & \underline{17} & \underline{04} & \underline{14} & \underline{19} & \underline{23} \\ & 32 & 15 & 37 & 25 & 34 \\ (\text{mod } 26) & 06 & 15 & 11 & 25 & 08 \end{array}$$

a więc wynik to 06 15 11 25 08

Jeśli odejmujemy 19 od 17, wynik (? 2) jest ujemny, więc dodajemy 26, co daje 24 jako wynik. Symbol? Jest odczytywany jako "jest zgodny", więc powiedzielibyśmy "36 jest zgodny z 10 (mod26)", a "? 2 jest zgodny z 24 (mod26)". Kiedy dodawane są dwa strumienie liczb (mod 26), reguły odnoszą się do każdej pary liczb osobno, bez "przenoszenia" do następnej pary. Podobnie, gdy odejmujemy jeden strumień od drugiego (mod 26), reguły odnoszą się do każdej pary cyfr oddzielnie, bez "pożyczania" od następnej pary. Gdy moduł wynosi 10, pojawiają się tylko liczby od 0 do 9, a gdy moduł wynosi 2, widzimy jedynie 0 i 1. Arytmetyka (mod 2), lub arytmetyczna binarna, jak zwykle jest znana, jest szczególnie szczególna, ponieważ dodawanie i odejmowanie są identycznymi operacjami i tak zawsze wytwarzają ten sam wynik viz:

$$\begin{array}{cccc} 0 & 0 & 1 & 1 \\ +0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 2 \\ \equiv 0 & 1 & 1 & 0 \end{array} \qquad \begin{array}{cccc} 0 & 0 & 1 & 1 \\ -0 & 1 & 0 & 1 \\ \hline 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \pmod 2 \end{array}$$ i

Modułowe dodawanie i odejmowanie liter

Często konieczne jest również dodawanie lub odejmowanie strumieni liter przy użyciu 26 jako modułu. Aby to zrobić, konwertujemy każdą literę na dwucyfrowy numer, zaczynając od A = 00 i kończąc na Z = 25. Podobnie jak w przypadku liczb, każda para liter jest traktowana osobno (mod 26) bez "przeniesienia" lub "pożyczki" do lub z następnej pary. Po zakończeniu dodawania lub odejmowania liczby wypadkowe są zwykle przekształcane z powrotem w litery.

Przykład 2

(1) Dodajemu TODAY do NEVER(mod 26)

(2) Odejmujemy NEVER od TODAY(mod 26)

Rozwiązanie

(1) TODAY=19 14 03 00 24
NEVER=13 04 21 04 17
Dodajemy 32 18 24 04 41≡06 18 24 04 15=GSYEP.

(2) TODAY=19 14 03 00 24
NEVER=13 04 21 04 17
Odejmujemy 06 10–18–04 07≡06 10 08 22 07=GKIWH.

Od Juliusza Cezara do prostego podstawiania

Szyfry Juliusza Cezara i ich rozwiązanie

W szyfrze Juliusza Cezara każda litera alfabetu została przesunięta o 3 miejsca w kółko, czyli A zostało zastąpione przez D, B przez E ... przez Z, X przez A, Y przez B i Z przez C. Chociaż Juliusz Cezar przeniósł litery 3 miejsca, które mógł wybrać, aby przenieść je o dowolną liczbę miejsc od 1 do 25. Istnieje zatem 25 wersji szyfru Juliusza Cezara, a to wskazuje, w jaki sposób można rozwiązać taki szyfr: zanotuj komunikat szyfrowania i 25 linie pod nim napisz 25 wersji uzyskanych przez przesunięcie każdej litery 1, 2, 3, ..., 25 miejsc. Jedna z tych 25 linii będzie oryginalna

wiadomość.

Przykład 2.1

Tekst wiadomości zaszyfrowanej przez system Juliusza Cezara jest

VHFX TM HGVX

Odszyfruj wiadomość.

Rozwiązanie

Zapisujemy komunikat szyfrowania i 25 przesuniętych wersji, wskazujących przesunięcie po lewej stronie każdej linii (patrz tabela 2.1) i widzimy, że szyfr używał przesunięcia o wartości 19, ponieważ tekst szyfrowania został przesunięty o 7 miejsc, w stosunku do jawnego, a to oznacza, że tekst jawny musi zostać przesunięty (26 - 7) = 19 miejsc, aby dać szyfr. Wygląda bardzo prawdopodobne, przy założeniu, że żadna inna zmiana nie wytworzyłaby zrozumiałej wiadomości, że poprawnie odszyfrowaliśmy wiadomość i nie ma sensu wypisywać pozostałych linii. To założenie wyjątkowości jest sensowne, gdy szyfrujemy wiadomość ma więcej niż pięć lub sześć znaków, ale jest bardzo krótka

Tabela 2.1

Przesunięcie	Wiadomość
0	VHFX TM HGVX
1	WIGY UN IHWY
2	XJHZ VO JIXZ
3	YKIA WP KJYA
4	ZLJB XQ LKZB
5	AMKC YR MLAC
6	BNLD ZS NMBD
7	COME AT ONCE

wiadomości istnieje możliwość więcej niż jednego rozwiązania; na przykład, jeśli jest to wiadomość szyfrowana

DSP

istnieją trzy możliwe rozwiązania; jak pokazano w Tabeli 2.2.

Przesunięcie	Wiadomość
2	FUR
8	LAX
15	SHE

Nie są one bardzo znaczące jako "wiadomości", chociaż można sobie wyobrazić sytuacje, w których mogą przekazywać ważne informacje; na przykład mogą to być nazwy koni wyrzuconych w celu wygrania wyścigów. Przede wszystkim jednak służą one do zilustrowania ważnej kwestii, która często pojawia się: jak długo musi być komunikat szyfrowy, jeśli ma mieć unikalne rozwiązanie? Odpowiedź zależy od systemu szyfrowania i może być dowolna z "około czterech lub pięciu liter" (dla szyfru Juliusza Cezara) do "nieskończoności" . Przed opuszczeniem Juliusza Cezara jest tutaj raczej zabawny przypadek nietypowego rozwiązania. W przypadku szyfrowania "message"

MSG

(który wygląda jak skrót słowa "wiadomość") dwa możliwe rozwiązania są przedstawione w Tabeli 2.3

Przesunięcie	Wiadomość
2	OUI
12	YES

ale nie twierdzi się, że szyfr dostarcza prostego sposób tłumaczenia języka francuskiego na angielski.

Proste szyfry podstawieniowe

W prostym szyfrze podstawieniowym normalny alfabet zastąpiony jest permutacją (lub "tasowaniem") samego siebie. Każda litera normalnego alfabetu zostaje zastąpiona, ilekroć dojdzie do skutku, przez literę, która zajmuje tę samą pozycję w permutowany alfabet. Oto przykład permutowanego alfabetu z normalnym alfabetem napisane powyżej:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Y M I H B A W C X V D N O J K U Q P R Z P E L Z Z S

Jeżeli ten alfabet zastępczy jest używany zamiast normalnego alfabetu i używamy prostego szyfru zastępczego, a następnie wiadomości

COME AT ONCE

której użyliśmy wcześniej zostanie zakodowany jako

IKOB YT KJIB

próba rozwiązania tego jako szyfru Juliusza Cezara zakończyłaby się niepowodzeniem.

Przypuśćmy, że kryptoanalityk zdecydował się traktować to jako prostą zamianę czy szyfr byłby w stanie go rozwiązać? Zauważyłby to najwyraźniej , że składał się z trzech słów zawierających odpowiednio 4, 2 i 4 litery oraz że pierwsze i dziewiąte litery są identyczne, tak jak 2 i 7 litera oraz litery czwarte i dziesiąte tak, że chociaż jest 10 liter, istnieje tylko 7 różnych liter. Wynika z tego, że każdy zestaw trzech słów w język angielskim lub dowolny inny język, który spełnia te kryteria, jest możliwe rozwiązanie. Dlatego rozwiązaniem może być między innymi

GIVE TO INGE

lub

SECT IN EAST.

Żadne z nich nie wygląda na bardzo prawdopodobne, ale są one poprawne i pokazują, że krótki prosty szyfr zastępczy może nie mieć unikalnego rozwiązania. Prowadzi to, jak już wskazano, do oczywistego pytania: "Ile liter takiego szyfru potrzeba, aby móc znaleźć unikalne rozwiązanie?" Dla prostego szyfrowania substytucji może wystarczyć minimum 50 aby zapewnić wyjątkowość w większości przypadków, ale rozwiązywanie wiadomości o tak krótkim czasie nie byłoby zbyt łatwe. Doświadczenie wskazuje, że potrzeba około 200, aby rozwiązanie było łatwe i unikalne. Wrócimy do tego pytania później. Istnieją dwa inne punkty warte uwagi na temat powyższego przykładu i alfabetu zastępczego. Pierwszą kwestią jest to, że zadanie odszyfrowywania stało się łatwiejsze niż potrzeba, ponieważ słowa w szyfrze zostały oddzielone spacjami, oddając w ten sposób długość słów oryginalnej wiadomości. Istnieją dwa standardowe sposoby wyeliminowania tej słabości. Pierwszym sposobem jest zignorowanie spacji i innych znaków interpunkcyjnych i napisanie wiadomości w postaci ciągów znaków alfabetu. W ten sposób staje się komunikat i jego szyfrowanie

COMEATONCE

IKOBYTKJIB

Wynikiem tego jest to, że kryptoanalityk nie wie, czy wiadomość zawiera jedno słowo składające się z 10 liter lub kilku słów, każda z mniejszej liczby liter, a w konsekwencji liczba możliwych rozwiązań znacznie się zwiększa. Wadą tego podejścia jest to, że odbiorca wiadomości musi wstawiać przestrzenie itp. W miejsca, które uważa za odpowiednie, co może czasem prowadzić do niejednoznaczności. W ten sposób zadanie rozszyfrowania jest trudniejsze zarówno dla kryptoanalityka, jak i odbiorcy. Drugim sposobem, który jest częściej stosowany, jest użycie nieczęste litera taka jak X zamiast "spacji". W rzadkich przypadkach, gdy wymagany jest prawdziwy X, można go zastąpić inną kombinacją liter, na przykład KS. Jeśli zrobimy to za pomocą wiadomości w przykładzie, to wiadomość i jej szyfrowanie staną się (ponieważ X staje się G w alfabecie zastępczym, a X nie występuje w samym komunikacie)

COMEXATXONCE

IKOBGYTGKJIB

Kryptoanalityk może teraz przypuszczać, że G reprezentuje spację, a więc znajdzie długość słowa. W dłuższej wiadomości z pewnością to zrobi, jak się wkrótce przekonamy. Odbiorca nie będzie już miał wątpliwości, ale z drugiej strony zadanie dla kryptoanalityka jest łatwiejsze niż w poprzednim przypadku. Rozszerzeniem tego pomysłu jest umieszczenie dodatkowych znaków w alfabecie, aby zwolnić miejsce i niektóre symbole interpunkcyjne, takie jak kropka i przecinek. Jeśli to zrobimy, musimy użyć dodatkowych symboli dla alfabetu szyfrów. Pomogą w tym wszelkie symbole niebędące alfabetycznymi, typowe trio może być $,% i &. Może się więc zdarzyć, że, na przykład, w 29-literowym alfabecie szyfrowym D jest reprezentowane przez &, J przez $ i S przez% podczas "spacji", pełne zatrzymanie i przecinek staje się, na przykład, H, F i V. Cyfry są zwykle pisane w całości, ale alternatywnie alfabet może być dalej rozszerzany, aby poradzić sobie z nimi, gdyby było to pożądane. Takie dodatkowe znaki mogą sprawić, że tekst szyfru będzie wyglądał na trudniejszy, ale w praktyce bezpieczeństwo szyfru zostanie tylko nieznacznie zwiększone. Po drugie, należy zauważyć, że dwie litery w alfabecie podstawienia powyżej, Q i T, pozostają niezmienione. Studenci kryptografii często myślą, że należy tego unikać, ale nie ma takiej potrzeby, jeśli występują tylko jedna lub dwie litery tego

typu. Można matematycznie wykazać, że losowy alfabet substytucji ma około 63% szans na niezmienność co najmniej jednej litery w alfabecie szyfrowym (M1). Hazardziści byli znani z tego, że zarabiają pieniądze, ponieważ jeśli dwie osoby przetasują paczkę kart, a następnie porównają karty z paczek, to po 63% szans, że w pewnym momencie każdy z nich wylosuje tę samą kartę zanim dotrą do końca paczki. Gracz, który to wie, zasugeruje swojemu przeciwnikowi, że gra na równych stawkach, przy czym hazardzista obstawia, że dwie identyczne karty zostaną wylosowane kiedyś, a jego przeciwnik obstawi, że nie. Szanse sprzyjają hazardzistom o około 63: 37. (Może się wydawać zaskakujące, że szansa na porozumienie wynosi 63% zarówno dla 26-literowego alfabetu, jak i dla talii 52 kart, w rzeczywistości szanse nie są dokładnie takie same w dwóch przypadkach, ale są one takie same dla ponad 20 miejsc dziesiętnych.)

Jak rozwiązać prosty szyfr zastępczy

Najpierw zobaczymy, jak nie rozwiązać prostego szyfru zastępczego: próbując wszystkich możliwości. Ponieważ litera A w normalnym alfabecie może być zastąpiona przez dowolną z 26 liter i literę B dowolną z pozostałych 25 liter i literę C dowolną z pozostałych 24 liter, i tak dalej, widzimy, że liczba możliwe różne proste alfabety zastępcze

26 x 25 x 24 x 23 x … x 3 x 2? x 1

który jest napisany w matematyce, dla wygody, jako 26!, nazywany silnikiem 26. Jest to ogromna liczba, większa niż 10 do 26 potęgi (lub 1026 jak to jest powszechnie pisane), tak że nawet komputer zdolny do testowania tysiąca milion (tj. 109) alfabetów co sekundę zajęłoby kilkaset milionów lat, aby ukończyć zadanie. Najwyraźniej metoda próbowania wszystkich możliwości, która działa w zadowalający sposób z szyframi Juliusza Cezara, gdzie jest ich tylko 25, jest tu całkiem niepraktyczna.

Praktyczna metoda rozwiązania tego typu szyfrów jest następująca.

(1) Wykonaj liczbę częstotliwości liter występujących w szyfrze, tzn. Zlicz ile razy wystąpią A, B, C, ..., X, Y, Z.

(2) Próba zidentyfikowania, który znak szyfrowania reprezentuje "przestrzeń". To powinno być łatwe, chyba że komunikat szyfrowy jest bardzo krótki, ponieważ symbole "spacja" i znaki interpunkcyjne stanowią od 15% do 20% typowego tekstu w języku angielskim, a większość z nich to "przestrzeń". Jest wysoce prawdopodobne, że najczęściej występująca litera kodu jest "przestrzenią". Ponadto, jeśli to założenie jest poprawne, litera kodu, która reprezentuje "spację" pojawi się po każdych kilku znakach, bez naprawdę długich przerw.

(3) Po zidentyfikowaniu "spacji", przepisuj tekst spacjami zastępując znak szyfrujący go reprezentujący. Tekst pojawi się teraz jako zbiór oddzielnych "słów", które mają taką samą długość i strukturę jak słowa w postaci zwykłego tekstu. Na przykład, jeśli tekst w postaci zwykłego tekstu ma powtarzającą się literę, tak samo będzie w wersji szyfrowej.

(4) Próba identyfikacji reprezentacji szyfrów niektórych liter o wysokiej częstotliwości, takich jak E, T, A, I, O i N, które razem stanowią zazwyczaj ponad 40% całego tekstu, przy czym E jest zdecydowanie najbardziej wspólna litera w większości tekstów. Tabela typowych częstotliwości liter w języku angielskim jest bardzo pomocna w tym miejscu i taka tabela jest podana tu :

A	57	E	116	I	58	M	14	Q	3	U	25	Y	18
B	9	F	28	J	1	N	57	R	49	V	9	Z	1
C	17	G	14	K	5	O	53	S	55	W	11		
D	26	H	46	L	34	P	18	T	91	X	1		

druga tabela, oparta na dużo większej próbie, zostanie znaleziona w części 7; albo wystarczy do rozwiązania prostych szyfrów zastępczych. Tabele powinny być traktowane wyłącznie jako wskazówki; Częstotliwość wyższych liter jest rozsądnie zgodna z jednej próbki na drugą, ale niskie częstotliwości mają niewielką wartość. W tabeli podanej poniżej częstotliwości liter angielskich litery J, X i Z mają częstotliwość 1 na 1000, ale w każdej konkretnej próbce zawierającej 1000 liter jedna z nich może występować kilka razy lub wcale. Podobne uwagi dotyczą częstotliwości liter w większości języków.

(5) Przy niektórych częściach słów oznaczonych w ten sposób szukaj krótkich słów z jedną lub dwoma nieznanymi jeszcze literami, na przykład jeśli znamy T i E i widzimy trzyliterowe słowo z nieznaną literą między T i E, to jest to prawdopodobnie THE i nieznana litera to H. Odzyskiwanie słów takich jak THIS, THATE THEN i THEN będzie następowało, zapewniając więcej par połączeń szyfrowych.

(6) Uzupełnij rozwiązanie, używając informacji gramatycznych i kontekstowych.

Przykład 2

Wiadomość szyfrowana składająca się z 53 pięcio-literowych grup została przechwycona. Wiadomo, że system szyfrowania jest prostym podstawieniem, a spacje w oryginale reprezentowane są przez literę Z, a wszystkie pozostałe interpunkcje są ignorowane. Odzyskaj jawny tekst wiadomości. Komunikat szyfrowy to

```
MJZYB LGESE CNCMQ YGXYS PYZDZ PMYGI IRLLC
PAYCK YKGWZ MCWZK YFRCM ZYVCX XZLZP MYXLG
WYTJS MYGPZ YWCAJ MYCWS ACPZY XGLYZ HSWBN
ZYXZT YTGRN VYMJC POYMJ SMYCX YMJZL ZYSLZ
YMTZP MQYMJ LZZYB ZGBNZ YCPYS YLGGW YMJZP
YMJZL ZYCKY SPYZD ZPKYI JSPIZ YMJSM YMJZL
ZYSLZ YMTGY GXYMJ ZWYTC MJYMJ ZYKSW ZYECL
MJVSQ YERMY MJCKY CKYKG
```

Rozwiązanie

(1) Zaczynamy od zliczania częstotliwości liter:

A	3	E	4	I	4	M	27	Q	3	U	0	Y	49
B	4	F	1	J	17	N	4	R	4	V	3	Z	33
C	18	G	14	K	9	O	1	S	14	W	9		
D	2	H	1	L	14	P	13	T	6	X	8		

(2) Ponieważ Y, z 49 wystąpieniami na 265, jest zdecydowanie najczęstszą literą, co stanowi ponad 18% tekstu, dochodzimy do wniosku, że Y jest reprezentacją szyfru znaku spacji. Kolejne najczęstsze postacie to Z i M i zauważamy, że są to dobre kandydatury na E i T lub T i E.

(3) Zastąpimy teraz Y przez "spację" w tekście szyfrującym, ignorując spacje między pięcioliniowymi grupami, które nie mają znaczenia, a więc uzyskujemy tekst, który ujawnia długości słów. W wiadomości znajduje się 50 słów i numerujemy je, by można je było wykorzystać w przyszłości.

```
 1       2       3  4    5       6      7
MJZ BLGESECNCMQ GX SP ZDZPM GIIRLLCPA CK

    8       9       10      11    12   13    14
KGWZMCWZK FRCMZ VCXXZLZPM XLGW TJSM GPZ WCAJM

   15     16     17     18    19     20    21   22   23
CWSACPZ XGL ZHSWBNZ XZT TGRNV MJCPO MJSM CX MJZLZ

 24    25      26     27    28 29  30    31    32   33
SLZ MTZPMQ MJLZZ BZGBNZ CP S LGGW MJZP MJZLZ CK

34   35     36     37    38    39   40  41   42   43
SP ZDZPK IJSPIZ MJSM MJZLZ SLZ MTG GX MJZW TCMJ

 44   45      46     47   48   49 50
MJZ KSWZ ECLMJVSQ ERM MJCK CK KG
```

Istnieje dość wiele krótkich słów, średnia długość słowa wynosi od 4 do 5, a ogólnie rozkład długości słów wygląda dobrze dla języka naturalnego, tym samym wspierając nasze przekonanie, że Y reprezentuje znak "spacji".

(4) Patrząc na krótsze słowa, znajdziemy następujące.

Jedno słowo o długości 1: słowo 29, które jest S i domyślamy się, że S jest prawdopodobnie A lub I. Dziesięć słów o długości 2; jeden (CK) występuje trzy razy, w pozycjach 7, 33 i 49, a dwa występują dwukrotnie - GX w pozycjach 3 i 41 oraz SP w pozycje 4 i 34. Jedenaście słów o długości 3, z których dwie występują dwukrotnie: MJZ na pozycjach 1 oraz 44 i SLZ na pozycjach 24 i 39.

(5) Ponieważ już podejrzewamy, że M i Z są albo E i T, albo odwrotnie widzimy, że trigraf MJZ to E? T lub T? E, a ponieważ występuje dwa razy jest bardzo prawdopodobne, że to jest tak, że M, J i Z to odpowiednio T, H i E. Jest jeszcze kilka słów, w których znajdują się litery szyfrowe M, Z i J zaangażowane, w tym

(23) MJZLZ, który staje się? E, więc L jest R lub S,

(26) MJLZZ, który przechodzi w TH? EE, co daje L jako R,

(42) MJZW, który staje się THE? więc W jest M lub N,

(37) MJSM, który staje się TAK, jeśli S jest A i THIT, jeśli S jest I.

Na podstawie tych danych wyciągamy wniosek, że L oznacza R, a S oznacza A, a W oznacza M lub N. Ponieważ słowo 26 okazało się TRZY patrzymy na słowo 25, aby sprawdzić, czy może to być liczba; jego szyfrem jest MTZPMQ, o którym wiemy, że jest T? E? T? na gładko i wygląda na prawdopodobnie DWADZIEŚCIA, co jeśli jest poprawne, daje T, P i Q odpowiednio oznaczają W, N i Y, a zatem rozstrzygają niejednoznaczność na W który musi być M.

(6) Zidentyfikowaliśmy teraz odpowiedniki dziewięciu szyfrów w postaci zwykłego tekstu litery: J, L, M, P, Q, S, W, Y i Z, które są H, R, T, N, Y, A, M, "spacja" i E. Te dziewięć liter razem stanowi ponad 60% tekstu, więc my teraz wypisze tekst ponownie z odpowiednikami tekstowymi w formacie tekstowym litery szyfrów, gdy tylko są dostępne, w przeciwnym razie za pomocą kropki (.) gdzie list nie jest jeszcze znany. Po wykonaniu tej czynności będziemy mogli teraz dokonać większej liczby identyfikacji par szyfrowych. Słowo 30, które częściowo odczytaliśmy jako R..M, ma powtarzającą się literę w środku i

może być POKÓJ tak, że litera G to zwykła litera O. Word 50, KG w szyfrze jest więc .O w równina, która sugeruje, że K reprezentuje S, lub ewentualnie D, ponieważ my już wiem, że nie może to być N ani T. Słowa 48 i 49, MJCK i CK mają częściowo odszyfrowane jako TH.S i .S, co prowadzi do wniosku, że C to I. Ponieważ C i G występują odpowiednio 18 i 14 razy, powinny mieć wysoką częstotliwość litery, a ja i O jesteśmy dobrymi kandydatami, jak mogliśmy to zauważyć wcześniej. Wstawianie I, O i S dla C, G i K w częściowo odzyskanym tekście i mamy :

```
 1        2        3  4    5        6      7
MJZ BLGESECNCMQ GX SP ZDZPM GIIRLLCPA CK
THE .RO.A.I.IT.  O.  AN E.ENT O...RRIN.  IS

    8        9        10       11    12   13    14
KGWZMCWZK FRCMZ VCXXZLZPM XLGW TJSM GPZ WCAJM
SOMETIMES ..ITE .I..ERENT .ROM .HAT ONE MI.HT


   15     16     17      18    19     20     21   22   23
CWSACPZ XGL ZHSWBNZ XZT TGRNV MJCPO MJSM CX MJZLZ
IMA.INE .OR E.AM..E .E.  WO...  THIN.  THAT I.  THERE

 24     25      26      27    28 29  30    31     32   33
SLZ MTZPMQ MJLZZ BZGBNZ CP S LGGW MJZP MJZLZ CK
ARE TWENTY THREE .EO..E IN A ROOM THEN THERE IS

34   35      36     37    38    39   40  41   42    43
SP ZDZPK IJSPIZ MJSM MJZLZ SLZ MTG GX MJZW TCMJ
AN E.ENS ..AN.E THAT THERE ARE TWO O.  THEM .ITH

 44   45      46      47   48   49 50
MJZ KSWZ ECLMJVSQ ERM MJCK CK KG
THE SAME .IRTH.A.  ..T THIS IS SO
```

Pozostałe litery są teraz łatwo identyfikowane i cały deszyfrowany alfabet zastępczy, oznaczający "spację" przez ^, to

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G P I V B Q O X C H S R T L K N Y U A W . D M F ^ E

Alfabet szyfrowania, którego nadawca użyłby do wytworzenia tekst szyfrowany z równiny, jest oczywiście odwrotnością tego wywodu:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S E I V Z X A J C . O N W P G B F L K M R D T H Q Y

Ogólnie, alfabety szyfrowania i deszyfrowania będą różne w prostym podstawieniu lub systemie Juliusza Cezara; w tym ostatnim przypadku są one takie same tylko wtedy, gdy przesunięcie wynosi 13; w pierwszym przypadku można je ułożyć w taki sam sposób, układając większość, jeśli nie wszystkie, w pary tak, aby litery pary szyfrowały się nawzajem, pozostawiając pozostałe litery niezmienione. Niektóre maszyny szyfrujące, w tym zarówno maszyny Enigma, jak i Hagelin, automatycznie wytwarzają takie wzajemne alfabety, dzięki czemu procesy szyfrowania i deszyfrowania są takie same,

co stanowi wygodę dla użytkownika, ale także osłabia bezpieczeństwo. W prostym systemie podstawiania opartym na 26-literowym alfabecie liczba możliwych alfabetów substytucyjnych jest zmniejszona z więcej niż 10^{26} do mniej niż 10^{13}. Chociaż jest to nadal duża liczba, jest znacznie mniej groźna z punktu widzenia kryptoanalizy. Takie wzajemne proste szyfry zastępcze są jednak używane okazjonalnie, głównie przez osoby, które prowadzą dzienniki i chcą zrobić wpisy niezrozumiałe dla przypadkowego obserwatora. Filozof Ludwig Wittgenstein prowadził w ten sposób szyfr, w wojsku austriackim w wojnie 1914-18. Patrząc na przykład, widzimy, że litera U nie występuje w tekście szyfrującym, a litery J i Z nie występują w zwykłym tekście. Z został użyty zamiast "spacji" w zwykłym tekście i stał się literą y z szyfru Y, podczas gdy litera J była tekstem w postaci zwykłego tekstu litery C i nie ma litery J w oryginalnym zwykłym tekście, którym jest

THE PROBABILITY OF AN EVENT OCCURRING IS

SOMETIMES QUITE DIFFERENT FROM WHAT ONE MIGHT

IMAGINE FOR EXAMPLE FEW WOULD THINK THAT IF

THERE ARE TWENTY THREE PEOPLE IN A ROOM THEN

THERE IS AN EVENS CHANCE THAT THERE ARE TWO OF

THEM WITH THE SAME BIRTHDAY BUT THIS IS SO.

Rozwiązanie tego kryptogramu opierało się częściowo na założeniu, że częstotliwości jego poszczególnych liter, w szczególności "przestrzeń", E, T, A, O, I i N, byłyby takie, jakich można by się spodziewać w próbce o takim rozmiarze zapisanej w " typowym "angielskim. Czasami jednak fragment może pochodzić z "nietypowego" źródła, takiego jak wysoko wyspecjalizowana praca naukowa, a więc słowa, których nie można znaleźć w powieści lub gazecie, mogą występować wystarczająco często, by zniekształcić normalne częstotliwości liter. Przeprowadzono badania milionów znaków angielskich i innych języków, tekstów różnych gatunków, takich jak powieści, artykuły prasowe, piśmiennictwo naukowe, teksty religijne, traktaty filozoficzne itp. Oraz wynikowe słowo i litera opublikowane częstotliwości. Brown University w USA był pionierem tej pracy, a tabele podano w "Brown corpus" Takie dane są potrzebne do analizy stylistycznej (na przykład do ustalenia autorstwa anonimowych lub kwestionowanych tekstów) i innych badań literackich. Znajomość prawdopodobnego przedmiotu kryptogramu może być wielką pomocą dla kryptoanalityka. Jeśli wie, na przykład, że wiadomość od jednego fizyka wysokich energii do innych słów, takich jak PROTON, ELECTRON lub QUARK może być w tekście, a identyfikacja takich słów w szyfrach może zasadniczo zredukuj dzieło odszyfrowywania go. Używanie nietypowych słów lub unikanie popularnych słów może również wpływać na częstotliwości liter, co może okazać się pomocne lub utrudnić kryptoanalitykowi. W jednym skrajnym przypadku napisano powieść, która w ponad 50000 słowach nigdy nie używała litery E, ale robiono to celowo; autor, który związał literę E na swojej maszynie do pisania, aby nie można było jej użyć. To niezwykły wyczyn.

Częstotliwości liter w językach innych niż angielski

Prosty szyfr zastępczy w dowolnym języku alfabetycznym można rozwiązać za pomocą powyższej metody: liczba częstotliwości, po której następuje użycie samego języka. Oczywiście, kryptoanalityk musi mieć przynajmniej umiarkowaną znajomość języka, choć z prostym szyfrem zastępczym nie musi być biegły. Oczywiście liczba liter w typowej próbce będzie się różnić w zależności od języka, chociaż różnica między językami a wspólną podstawą, taką jak łacina, będzie mniejsza niż pomiędzy językami o zupełnie innych korzeniach. Nie wszystkie języki używają 26 liter; niektórzy używają mniej; Włoski zwykle używa tylko 22, a niektóre, takie jak rosyjski, używają więcej, podczas gdy inne (chińskie) wcale

nie mają alfabetu. Ponieważ Włosi zwykle nie używają K, W lub Y, litery te mają zerową częstotliwość, ale włoski tekst, który zawiera wzmiankę o Nowym Jorku, pokazuje, że nawet takie listy mogą się pojawić. W języku francuskim i niemieckim powinniśmy naprawdę rozróżnić samogłoski z różnymi akcentami lub umlautami, ale w celu uproszczenia tabel poniżej wszystkie formy tej samej litery zostały policzone razem. Tak więc w języku francuskim E, É, Ê i È były wszystkie uwzględnione w liczbie E. Ponadto liczby zostały wykluczone z liczenia, o ile nie zostały podane, a wszystkie symbole niealfabetyczne, takie jak spacja, przecinek, kropka, cytaty, średniki itp. zostały uznane za "inne ". Wielkie i małe litery były traktowane tak samo. Dzięki tym konwencjom w tabeli pokazano częstotliwość liter w próbkach 1000 w czterech językach europejskich. Tabela częstotliwości liter w języku angielskim podana powyżej została powtórzona dla wygody.

	Angielski	Francuski	Niemiecki	Włoski	Walijski
A	57	72	49	103	77
B	9	13	18	4	13
C	17	17	28	46	23
D	26	34	43	42	63
E	116	143	129	95	55
F	28	7	11	8	28
G	14	11	20	12	32
H	46	9	42	11	43
I	58	56	69	103	57
J	1	1	1	0	0
K	5	0	8	0	0
L	34	42	25	58	47
M	14	35	36	20	23
N	57	54	58	58	58
O	53	48	24	69	64
P	18	27	7	16	3
Q	3	5	0	3	0
R	49	51	69	55	52
S	55	64	54	38	20
T	91	64	64	52	31
U	25	42	28	21	17
V	9	10	8	14	0
W	11	0	12	0	31
X	1	3	0	0	0
Y	18	3	0	0	67
Z	1	1	11	7	0
Inne	184	188	186	165	196

Analiza statystyczna tych obliczeń pokazuje, że angielski, francuski i niemiecki oraz, w mniejszym stopniu, włoski, są bardzo blisko spokrewnione w odniesieniu do częstotliwości jednoliterowych, podczas gdy ich relacja z walijskim jest zauważalnie słabsza. Częściowym wyjaśnieniem jest to, że Y jest bardzo powszechne w języku walijskim, będąc samogłoską (z dwoma różnymi wymowy), ale znacznie mniej powszechne w języku angielskim i dość rzadkie w innych językach. Liczby pokazują również, że N można uznać za "najbardziej spójną literę", ponieważ występuje z praktycznie taką samą częstotliwością we wszystkich pięciu językach, co stanowi około 6% do 7% całego tekstu alfabetycznego.

Ile liter jest potrzebnych, aby rozwiązać prosty szyfr podstawieniowy?

W powyższym przykładzie dysponowaliśmy 265 literami i dość łatwo rozwiązaliśmy proste podstawienie. Moglibyśmy to zrobić, gdybyśmy mieli tylko, powiedzmy, 120 liter. Bardziej ogólnie, jak wcześniej, jak to może być wystarczające, aby kryptoanalityk rozwiązał taki szyfr? Jest to problem w

teorii informacji i wyprowadzono formułę, która obejmuje częstotliwości poszczególnych liter lub poligrafów w języku, co zapewnia oszacowanie. Dla prostego szyfrowania substytucji może wystarczyć 200 liter, jeśli skupimy naszą uwagę na pojedynczych literach, ale użycie dwuznaków (takich jak ON, INorAT) lub trigrafów (takich jak THORAND) ogromnie wzmaga atak i uważa się, że nawet 50 lub 60 liter może wtedy być dość.

Problem 2.1

Znaleziono zaszyfrowany tekst w języku angielskim składający się z 202 znaków. Wiadomo, że użyto prostego szyfru zastępczego i że spacje w jawnym tekście zostały zastąpione przez Z, a wszystkie pozostałe interpunkcje zostały zignorowane. Istnieją powody, by sądzić, że autor wolał używać "twoje" niż "twoje". Odszyfruj tekst.

VHEOC WZIHC BUUCW HDWZB IRWDH TDOZH VIHVI

YBWIU HQOWU HUFWH ZOXBI LHTBI LWDHG DBUWE

HVIRH FVXBI LHGDB UHZOX WEHOI HIODH VCCHU

FPHQB WUPHI ODHGB UHEFV CCHCN DWHBU HSVYJ

HUOHY VIYWC HFVCT HVHCB IWHIO DHVCC HUFPH

UWVDE HGVEF HONUH VHGOD RHOTH BU

Przykład 2 ilustruje, że proste szyfry zastępcze, choć o wiele trudniejsze do rozwiązania niż te z gatunku Juliusza Cezara, są nadal zbyt łatwo rozwiązywalne, aby mogły być przydatne. Dla takich szyfrów kryptoanalityk wymaga tylko wystarczającego tekstu szyfrowania, co odpowiada pierwszej sytuacji wspomnianej w poprzedniej części. Gdyby otrzymał odpowiedni tekst, podobnie jak w drugiej sytuacji, jego zadanie byłoby naprawdę trywialne, gdyby "wiadomość" nie zawierała kilku wyraźnych liter. W trzeciej sytuacji, w której kryptoanalityk może określić tekst, który ma być zaszyfrowany, zrobiłby to po prostu podaj "wiadomość"

ABCDEFGHIJKLMNOPQRSTU VWXYZ

i wtedy nie mieliby żadnej pracy do wykonania.

Dla niewtajemniczonych może się wydawać, że ponieważ istnieje ponad 1026 (czyli sto milionów milionów milionów) możliwości, zadanie rozwiązania prostego szyfru zastępczego z samego tekstu szyfrującego, które, jak wskazano wcześniej, zajęłoby komputer przy użyciu ". metoda brutalnej siły próbowania wszystkich milionów lat jest niemożliwa. Jednak właśnie widzieliśmy, jak można to zrobić ręcznie w ciągu godziny, wykorzystując znane, nie-losowe częstotliwości liter i gramatyczne zasady języka angielskiego lub cokolwiek jest odpowiednim językiem, wraz z wszelkimi informacjami kontekstowymi, które mogą być dostępne. Jest bardzo ważna lekcja:

bardzo niebezpieczne jest osądzenie bezpieczeństwa systemu szyfrowania wyłącznie na czas że najszybszym komputerem, jaki można sobie wyobrazić, byłoby rozwiązanie go za pomocą ataku brute force

Następnym krokiem jest zatem przyjrzenie się sposobom zwiększania bezpieczeństwa tych prostych metod i to robimy w następnej części

Systemy polialfabetyczne

Wzmocnienie Juliusza Cezara: Szyfr Vigenère'a

Słabością systemu Juliusza Cezara jest to, że istnieje tylko 25 możliwych odszyfrowań, więc kryptoanalityk może je wszystkie wypróbować. Życie może oczywiście być dla niego trudniejsze, jeśli zwiększymy liczbę spraw, które trzeba wypróbować, zanim uda się osiągnąć sukces. Możemy to zrobić, jeśli zamiast przesuwać każdą literę o stałą liczbę miejsc w alfabecie, przesuniemy litery o zmienną wielkość w zależności od ich pozycji w tekście. Oczywiście musi istnieć reguła decydująca o wysokości zmiany w każdym przypadku, w przeciwnym razie nawet upoważniony odbiorca nie będzie w stanie odszyfrować wiadomości. Prostą zasadą jest użycie kilku stałych przesunięć w sekwencji. Na przykład, jeśli zamiast stałej zmiany 19, jaka została użyta w komunikacie

COME AT ONCE

w ostatnim rozdziale i który został zakodowany

VHFX TM HGVX

używamy dwóch zmian, na przykład 19 i 5, na przemian, tak aby pierwsza, trzecia, piąta itd. litery zostały przesunięte o 19 miejsc, a druga, czwarta itd. zostały przesunięte o 5 miejsc, a następnie szyfr staje się teraz

VTFJ TY HSVJ.

Jeśli zastąpimy znak spacji przez Z w komunikacie i użyjemy trzech przesunięć, powiedzmy 19, 5 i 11, po kolei tekst jawny staje się

COMEZATZONCE.

Szyfr to teraz

VTXXELMEZGHP

a klucz, który zapewnia szyfrowanie, to 19-5-11. Aby odczytać komunikat, odbiorca musi użyć klucza rozszyfrowania, w którym każda z tych trzech liczb jest zastąpiona przez jego dopełnienie (mod 26), tj. 7-21-15. Nawet jeśli kryptoanalityk podejrzewał, że zastosowano system Juliusza Cezara z trzema zmianami, które były stosowane sekwencyjnie, musiałby wypróbować 75 lub więcej kombinacji (jedna z przesunięć może wynosić 0). W przypadku tak krótkiego komunikatu, jak to byłoby możliwe więcej niż jedno rozwiązanie. Jeśli przesłanie jest zbyt krótkie, aby zidentyfikować trzy zmiany niezależnie, tak jak zrobimy to w poniższym przykładzie, może trzeba będzie wypróbować metodę "brutalnej siły", ale ponieważ wiąże się to z 25x25x25=15625 próbami, byłby on stosowany jedynie w ostateczności. W skrajnym przypadku, w którym liczba użytych zmian była równa liczbie liter w komunikacie, wiadomość staje się "nietłukąca się", chyba że istnieje pewna nielosowa cecha sekwencji zmian. Tam, gdzie nie ma żadnej nielosowej cechy, np. Kiedy sekwencja zmian została wygenerowana przez jakiś proces "losowej liczby", mamy tzw. Szyfr jednorazowy, do którego dochodzimy w części 7. Takie podejście do wzmacniania szyfru Juliusza Cezara za pomocą kilku zmian było stosowane od setek lat. Takie systemy znane są pod nazwą szyfrów Vigenère. Ponieważ większość ludzi łatwiej zapamiętuje słowa niż arbitralne ciągi liter i cyfr, klucze Vigenère często przyjmują postać słowa kluczowego. Zmniejsza to oczywiście liczbę możliwych kluczy, ale jest to cena, którą kryptolog musi zapłacić za zmniejszenie obciążenia pamięci. Litery słowa kluczowego są interpretowane jako liczby w zwykły sposób (A = 0, B = 1, C = 2, ..., Z = 25), tak że na przykład słowo kluczowe CHAOS byłoby równoznaczne z użyciem pięciu słów kluczowych. przesuwa się kolejno o 2, 7, 0, 14 i 18. Słowo kluczowe lub klucz numeryczny byłyby

zapisywane wielokrotnie nad tekstem jawnym, a każda litera zwykłego tekstu przenosiła odpowiednią liczbę miejsc, aby nadać szyfrowi. Tak więc, jeśli zaszyfrujemy COMEZATZONCE przy użyciu Vigenère ze słowem kluczowym CHAOS, będzie to układ

CHAOSCHAOSCH

COMEZATZONCE

a wynikowy szyfr to

EVMSRCAZCFEL.

Szyfr Vigenère'a jest szczególnym, a raczej specjalnym przypadkiem systemu polialfabetycznego, w którym, jak sama nazwa wskazuje, stosuje się wiele różnych alfabetów substytucyjnych, a nie tylko jeden, jak w prostych systemach substytucji. Liczba użytych alfabetów substytucyjnych może wynosić od 2 do wielu tysięcy; w enigmie na przykład jest to 16900, a są to proste substytucje, a nie zmienione alfabetem Juliusza Cezara, jak w szyfrach Vigenère'a

Jak rozwiązać szyfr Vigenère'a

Pierwszym krokiem w rozwiązaniu szyfru Vigenère'a jest określenie długości i, zakładając, że jest dostępny wystarczający tekst szyfrowania, robimy to patrząc na powtarzające się kombinacje liter, poligrafy, takie jakie są zadzwonił i nie wiadomo, jak daleko są w tekście. Jeśli te powtórzenia są prawdziwe, to znaczy, jeśli są one wersjami szyfrów tego samego zwykłego tekstu, to one będą oddzielone wielokrotnościami długości klucza, który powinien wtedy być zidentyfikowane lub przynajmniej zredukowane do jednej z niewielkiej liczby możliwości. Im dłużej powtarzane poligrafy są lepsze dla sytuacji kryptoanalityka, ale pomocne mogą być nawet dwuznaczniki, kombinacje dwuliterowe.

Przykład 1

Wiadomość zaszyfrowana składająca się z 157 znaków zaszyfrowanych za pomocą szyfru Vigenère z literą Z używaną jako "przestrzeń" to

HQEOT FNMKP ELTEL UEZSI KTFYG STNME GNDGL

PUJCH QWFEX FEEPR PGKZY EHHQV PSRGN YGYSL

EDBRX LWKPE ZMYPU EWLFG LESVR PGJLY QJGNY

GYSLE XVWYP SRGFY KECVF XGFMV ZEGKT LQOZE

LUIKS FYLXK HQWGI LF

(1) Znajdź długość klucza.

(2) Znajdź klucz i odszyfruj wiadomość.

Rozwiązanie

(1) Badamy tekst i stwierdzamy, że sześć digrafów występuje trzy lub więcej razy, a mianowicie:

EL w pozycjach 11, 14 i 140;

FY w pozycjach 23, 119 i 146;

GN w pozycjach 31, 64 i 103;

HQ w pozycjach 1, 40, 58 i 151;

LE w pozycjach 70, 91 i 109;

YG w pozycjach 24, 66 i 105.

Dalsze badanie ujawnia, że digragram GN w pozycjach 64 i 103 jest w obu przypadkach początkiem powtórzenia ośmioliterowego ("oktografu"):

GNYGYSLE

Powtarzających się osiem liter jest bardzo mało prawdopodobne (ale doświadczenie Jacka Gooda, o którym mowa w dalszej części tego rozdziału, pokazuje, że czasami zdarzają się nawet "bardzo mało prawdopodobne" wydarzenia!), Więc zakładamy, że prawie na pewno jest to znaczące. W związku z tym znajdujemy odległość między oktografami, która wynosi (103? 64)? 39, a od 39? 3? 13 przypuszczamy, że klucz ma długość 3 lub 13. Patrzymy teraz na odległości między powtórzeniami innych dwuznaki, takie jak poniższe: EL w pozycjach 11, 14 i 140 daje interwały 3 i 126 (~ 3? 42); HQ w pozycjach 1, 40, 58 i 151 daje przedziały 39, 18 i 93, wszystkie wielokrotności 3. Wskazują, że 3 jest zdecydowanie najbardziej prawdopodobną długością słowa kluczowego. Zakładając, że tak jest, następnym krokiem jest znalezienie klucza. (2) Teraz uważamy, że zastosowano trzy zmiany; pierwsza zmiana dotyczy 1., 4., 7., ... liter; druga zmiana na 2, 5, 8, ... litery i trzecia zmiana na 3, 6, 9, ... litery. W związku z tym wypiszmy szyfr na szerokości trzech kolumn i zróbmy częstotliwość litery szyfrów w każdej z tych trzech kolumn i znajdujemy Tabela 3.1.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
First shift	0	1	0	0	0	3	13	4	0	0	1	7	1	2	1	5	0	0	2	2	4	4	0	0	2	1
Second shift	0	0	0	0	13	6	0	0	3	2	2	1	2	3	0	0	6	3	3	1	0	0	2	1	3	1
Third shift	0	0	2	2	4	1	1	1	0	1	5	5	1	0	1	4	0	2	3	2	0	1	3	4	6	3

Liczby w wierszach ogółem 53, 52 i 52. Jeśli częstotliwości były losowo rozdzielone, każda z liczb powinna wynosić około 2, ale możemy rozsądnie oczekiwać zakresu od 0 do około 5 lub 6. Oczywiście częstotliwości są dalekie od losowych ponieważ każda pojedyncza kolumna składa się z liter tekstowych, które zostały przesunięte o tę samą wartość. Linia ataku polega wówczas na szukaniu niezwykle dużych częstotliwości w nadziei, że zidentyfikuje się litery, które są zaszyfrowanymi wersjami Z, literą używaną do reprezentowania "przestrzeni" w trzech rzędach powyżej. W pierwszym rzędzie zauważamy, że G występuje 13 razy, a L, który występuje 7 razy, jest następnym najczęstszym. Jeśli G jest szyfrowaniem Z, wówczas przesunięcie w pierwszym wierszu wynosi 7, a L będzie szyfrowaniem E, literą 7 miejsc przed nią w alfabecie. Ponieważ E jest literą o wysokiej częstotliwości, to wspiera naszą wiarę, że pierwsza zmiana wynosi 7, tj. że pierwsza liczba w kluczu to 7. W drugim rzędzie widzimy, że E występuje 13 razy, co czyni go dobrym kandydatem do bycia szyfrem Z, a to sugerowałoby, że druga zmiana wynosi 5. W tym wierszu następnymi najczęstszymi literami szyfrującymi są F i Q zarówno które występują 6 razy i przesuwając je z powrotem o 5 miejsc, widzimy, że odpowiadałyby one odpowiednio literowym literom A i L, które wyglądają obiecująco. Z drugiej strony, szyfrowana wersja zwykłego tekstu E byłaby J, a ta litera szyfrowa pojawia się tylko dwa razy w drugim rzędzie, podczas gdy możemy się spodziewać, że wystąpi ona 5 razy, ponieważ E stanowi około 10% liter w typowych próbkach języka angielskiego. Dowody, choć nie do końca przekonywujące, wskazują na to, że druga cyfra klucza to prawdopodobnie 5. W trzecim rzędzie nie ma litery o wyjątkowo wysokiej częstotliwości, z Y, K i L, które występują odpowiednio 6, 5 i 5 razy jako najlepsi pretendenci jako odpowiednik szyfrów Z.

Możemy spróbować każdego z nich po kolei, ale alternatywnym podejściem jest napisanie początku tekstu zaszyfrowanego, ignorowanie spacji po każdej pięcioliterowej grupie i używanie założonych zmian 7 i 5, aby odszyfrować pierwszą i drugą literę każdego z nich grupa trzech. Trzecia litera w każdej grupie "odszyfrowujemy" jako "/" i sprawdzamy, czy potrafimy zidentyfikować niekompletne słowa i wyprowadzić trzecią liczbę klucza. Więc mamy

Szyfr: HQEOTFNMKPELTELUEZSIKTFYGSTNMEGNDGLPUJCHQWFEXFEEPR

Zwykły: AL / HO / GH / IE / ME / NE / LD / MA / EN / GH / EI / EG / NE / AL / YE / YE / IM

Pierwsze słowo wygląda tak, jakby to było JESZCZE, a jeśli tak, to zwykła litera T staje się literą E, co oznacza przesunięcie 11, ponieważ E jest 11 miejscami "włączonymi" od T (lub, co jest tym samym, 15 miejsc " za "T" w alfabecie. Przy przesunięciu 11 literą szyfrowania odpowiadającą "spacja" (to znaczy Z) będzie K, co było jedną z naszych możliwości. Doszliśmy do wniosku, że trzecia cyfra w kluczu to 11, więc kluczem do szyfrowania trzycyfrowego jest 7-5-11, a kluczem do rozszyfrowania jest 19-21-15, co potwierdza pełne odszyfrowanie, którym jest:

ALTHOUGH I AM AN OLD MAN NIGHT IS GENERALLY MY TIME
FOR WALKING IN THE SUMMER I OFTEN LEAVE HOME EARLY IN
THE MORNING AND ROAM ABOUT FIELDS AND LANES ALL DAY

Podczas gdy takie polialfabetyczne systemy Juliusza Cezara są trudniejsze do rozwiązania niż wersja prosta, wciąż mają wrodzoną słabość, że gdy już zidentyfikujemy literę szyfrowania dla "spacji" lub jakiejś innej litery o wysokiej częstotliwości, w przesuniętym alfabecie 25 innych liter tego alfabet następuje natychmiast. Następnie, jeśli nie mamy pewności co do litery szyfrowania dla "spacji" w jednym lub kilku alfabetach, znajomość niektórych liter w niekompletnych słowach może być wystarczająca, abyśmy mogli je wypełnić, a więc uzyskać pełne rozwiązanie, jak podano w przykładzie powyżej. Ta słabość znika, jeśli zamiast alfabetów w normalnej kolejności przesunąć o różne liczby według klucza, używamy zestawu alfabetów w różnych zamówieniach i niezależnie od siebie. Ta modyfikacja stwarza jednak dwa inne problemy:

(1) w jaki sposób uzyskujemy takie alfabety?

(2) w jaki sposób wytransformowany alfabet może zostać udostępniony zamierzonemu odbiorcy (odbiorcom) bez ujawniania ich nieuprawnionym przechwytującym?

Pytania te mają fundamentalne znaczenie dla tego, czy tasowane alfabety są uzyskiwane za pomocą jakiejś prostej metody, jak na przykład w Juliuszu Cezarze, kryptoanalityk wkrótce zauważy metodę i odszyfrowanie będzie znacznie łatwiejsze. Z drugiej strony zamierzony odbiorca musi wiedzieć, które alfabety są używane lub, alternatywnie, jak je uzyskać. Istnieje wiele sposobów rozwiązania obu tych problemów, z których niektóre podejdziemy później, ale dwa z możliwych rozwiązań (2) opiszemy poniżej. Najpierw jednak definiujemy dwa terminy, które są istotne dla systemów kryptograficznych.

Wskaźniki

Gdy twórca wiadomości ma do wyboru kilka parametrów związanych z jej szyfrowaniem, które musi udostępnić adresatowi (odbiorcom), prawdopodobnie przekaże te informacje, ewentualnie w postaci zaszyfrowanej, wskaźnikiem, który może poprzedzać lub śledzić wiadomość lub ukryć się w niej. Tak więc w powyższym przykładzie klucz, 7-5-11, musiałby być gdzieś dostarczony, albo w informacji wysłanej wcześniej, albo zaszyfrowany w zaaranżowanym szyfrze i być może ukryty w wiadomości w

określonym miejscu. W tym przypadku sam klucz, 7-5-11, może służyć jako wskaźnik, ale jest mało prawdopodobne, aby został wysłany w tej formie.

Głębia

Kiedy dwa lub więcej komunikatów jest szyfrowanych przez ten sam system z identycznymi parametrami (komponenty, klucze, części, ustawienia itp.), Mówi się, że są one dogłębne. Tak więc, jeśli dwa Vigenère wiadomości są wysyłane za pomocą tego samego słowa kluczowego, są one dogłębne; ale jeśli są wysyłane za pomocą różnych słów kluczowych, nawet jeśli słowa kluczowe mają tę samą długość, nie są one dogłębne. Jeżeli jednak dwie wiadomości Vigenère mają słowa kluczowe o tej samej długości i które mają identyczne litery w odpowiednich pozycjach komunikaty szyfrów będą miały częściową głębokość. To niekoniecznie musi być prawdziwe w przypadku innych systemów szyfrowania, w których najmniejsza zmiana wskaźnika powoduje, że komunikaty nie są wnikliwe. To, czy kryptoanalityk może wykorzystać znalezienie dwóch lub większej liczby komunikatów, zależy od systemu, który został użyty do ich szyfrowania. W niektórych przypadkach, takich jak proste systemy zastępcze lub Vigenère, z pewnością mógłby to zrobić, ale w innych, takich jak dwuliterowe systemy szyfrowania opisane w części 5, głębokości są znacznie mniej użyteczne. Mówiąc ogólnie, jeśli system szyfrowania jest wykonywany list po literach, to głębokości mogą być identyfikowalne i użyteczne dla kryptoanalityka, ale jeśli szyfrowanie obejmuje dwie lub więcej liter w tym samym czasie, głębokość, jeśli w ogóle rozpoznawalna, może nie być o dużym wykorzystaniu.

Rozpoznawanie "głębi"

W jaki sposób kryptoanalityk rozpozna głębokość? Jeśli dwie lub więcej wiadomości zostały wysłane w tym samym systemie i okazało się, że mają te same wskaźniki, prawdopodobnie są one dogłębne. Musimy powiedzieć "prawdopodobnie", a nie "na pewno", ponieważ przerwa między dwoma czasami transmisji mogła pokrywać się z czasem przejścia, gdy część systemu szyfrowania mogła zostać zmieniona. Taka sytuacja miałaby miejsce, na przykład, z dwoma wiadomościami Enigma wysłanymi tuż przed i tuż po północy. Jeśli wskaźniki są ukryte, może nie być żadnych zewnętrznych dowodów na to, że komunikaty są dogłębne. Jak więc kryptoanalityk może odkryć, że są? Zakładając, że system szyfrowania obejmuje tylko jedną literę na raz, najpierw napisałby wiadomości pod sobą, ustawiając początkowe litery szyfrów wiadomości, a następnie zastosował prosty test statystyczny. Jeżeli dwa komunikaty szyfru nie są dogłębnie, prawdopodobieństwo, że litera szyfrująca jednego komunikatu będzie taka sama jak odpowiadająca mu litera kodu w drugiej, tj. Pod nim, wynosi 1 na 26. Jeśli komunikaty są dogłębnie prawdopodobne, że odpowiedni szyfr litery będą takie same, jak prawdopodobieństwo, że odpowiednie litery w postaci zwykłego tekstu są takie same i okazuje się, że jest około dwa razy większe niż prawdopodobieństwo losowe, to jest około 1 na 13 dla języka angielskiego i dla większości języków używających alfabetu łacińskiego. Jest to szczególny przypadek bardziej ogólnej obserwacji, o której mowa w rozdziale 7; dla szczegółów matematycznych patrz M6. Wynika z tego, że jeśli wyrównaliśmy parę wiadomości, spodziewalibyśmy się około czterech przypadków identycznych par szyfrów na sto znaków szyfrowania, jeśli wiadomości są nie dogłębne, ale około siedmiu lub ośmiu identycznych par na sto znaków, jeśli komunikaty są dogłębne. Im dłuższe wiadomości, tym mocniejsze dowody za lub przeciw głębi. Obudowa dla głębokości jest znacznie wzmocniona, jeśli są jakieś zbiegi okoliczności na poligrafie, np. Umowy 2- lub 3-literowe, ponieważ są bardzo mało prawdopodobne w wiadomościach, które nie są dogłębnie. Oczywiście test ten nie jest nieomylny, przypadki poligraficzne mogą występować losowo w parach tekstów szyfrów. Jack Good w [3.1] odnotowuje, że kiedyś znalazł całkowicie fałszywego oktepta w parze wiadomości wojennych. Prawdopodobieństwo 8-krotnego zbiegu okoliczności, takiego jak ten, jest mniejsze niż 1 na 20000000000. Nawet uwzględnienie wszystkich wiadomości szyfrowych obserwowanych w czasie wojny wydaje się godne uwagi. Z drugiej strony Jack również odnotowuje [3.1], że znalazł także 22-

długie powtórzenie; to było prawdziwe! Decyzja, czy para wiadomości jest do głębi, staje się łatwiejsza niż długość krótszego komunikatu wzrasta. W ten sposób łatwiej jest określić głębokość za pomocą pary wiadomości, z których każda ma 500 liter długości, niż w parze wiadomości, z których jedna ma 2000 liter, a druga ma tylko 100 liter. Ważna jest długość nakładania się komunikatów.

Przykład 2

Trzy wiadomości zostały zaszyfrowane za pomocą systemu, który szyfruje jedną literę na raz. Najkrótsza wiadomość ma długość 500 znaków, a liczba umów na litery szyfru między trzema parami wiadomości wygląda następująco. Wiadomość 1 i wiadomość 2: 37.

Wiadomość 1 i wiadomość 3: 27.

Wiadomość 2 i wiadomość 3: 16.

Czy jakakolwiek para tych wiadomości może być głęboka?

Rozwiązanie

Przy nakładaniu się 500 liter oczekiwalibyśmy około 38 umów na szyfrogram, jeśli para wiadomości jest głęboka, a tylko około 19, jeśli nie są dogłębnie. Na tej podstawie dane z pewnością sugerują, że komunikaty 1 i 2 są dogłębne, a komunikaty 2 i 3 nie są dogłębne. Dowód na powiązanie komunikatów 1 i 3 jest anomalny i na pierwszy rzut oka jest niejednoznaczny, ponieważ prawdopodobieństwo obejrzenia 27 umów, gdy spodziewamy się 38, jest mniej więcej takie same, jak prawdopodobieństwo 27, gdy spodziewamy się 19. Jednakże, ponieważ jesteśmy dość pewni, że komunikaty 1 i 2 są dogłębne, a komunikaty 2 i 3 nie są możliwe, możemy rozsądnie stwierdzić, że komunikaty 1 i 3 nie są. Z punktu widzenia kryptoanalityka najcenniejszą głębią byłyby te, w których system szyfrowania polegał na dodawaniu strumienia klucza do tekstu jawnego, na przykład w szyfrach książkowych lub jednorazowej podkładce lub, na prostszym poziomie, Vigenère. W przeciwnym razie "niezniszczalny" jednorazowy pad stanie się łamliwy, gdy zostanie znaleziona głębia. Wiadomości wysyłane w systemach Vigenère z różnymi kluczami mogą czasami tworzyć niezwykłe funkcje, które pomogą kryptoanalitykowi w ich identyfikacji, co można zobaczyć na podstawie poniższych informacji.

Problem 1

Kochający muzykę spiker wysłał trzem swoim agentom identyczną wiadomość w postaci zwykłego tekstu z użyciem encyklopedii Vigenère ze słowami kluczowymi

(1) RHAPSODY, (2) SYMPHONY i (3) SCHUBERT.

Co powinien znaleźć kryptoanalityk w badaniu par szyfrów? Sprawdź swoje wnioski, szyfrując (używając X jako separatora) wiadomość

NOW IS THE TIME FOR ALL GOOD MEN TO COME TO THE AID OF THE PARTY

używając trzech słów kluczowych i porównując trzy komunikaty szyfrów w parach.

Problem 2

Wiadomość zawierająca 249 liter i Z użytą jako przestrzeń została zaszyfrowana przy użyciu szyfru Vigenère. Tekst to

GLEKR DAKRD SHZIZ MUIOK RQSSJ MOWA ZIESO

YMAHB PLZBF DSHMW HHEXZ TAHZX YIGTA XZMUE

TSVXZ LRIML MYNEV OEELD TANXZ TMFEM GIRSB

RESJM LEMIV XEDBX MJONA HZLHG HSVWZ MUIZV

NWESJ MTAMI UVYMD LMTRH BJZMU ETSGL EKRDA

KRDAG MMNYV RIMRD NNZFE KMSFS CVIFR WZMUM

SSCVO HSDIL MMNSG LESNT PXAHI QMMNS GLILM

FOHX.

Znajdź klucz i odszyfruj wiadomość

Ile tekstu potrzebujemy, aby rozwiązać szyfr Vigenère?

W przykładzie 1 mieliśmy 157 znaków szyfru i klucz o długości 3, więc mieliśmy ponad 50 znaków z każdego alfabetu szyfrów. Przy tak dużej ilości tekstu znaleźliśmy liczne powtarzające się dwuznaki, z których niektóre rozciągnęły się na trigrafy i, szczęśliwie, jeden oktograf. Z nich udało nam się znaleźć klucz i łatwo odszyfrować wiadomość. Tekst szyfrujący o długości równej 50-krotności długości klucza powinien być na ogół wystarczający do rozwiązania tego rodzaju szyfru. System Vigenère jest więc podatny na zagrożenia w ramach sytuacji (1) z części 1. W sytuacji (2), w której dostępne są teksty zwykłe i szyfrowane, wystarczający jest tekst o długości dwukrotnie większej niż długość klucza. Oczywiście nie można zalecać szyfrów Vigenère, chyba że wiadomości są bardzo krótkie lub klucze są bardzo długie.

Cylinder Jeffersona

Proste urządzenie, które dostarcza szeregu prostych alfabetów zastępczych, wydaje się być skonstruowane przez Thomasa Jeffersona pod koniec XVIII wieku, a następnie ponownie wynalezione przez innych. Urządzenie składa się z zestawu ponumerowanych, fizycznie identycznych dysków zamontowanych na wspólnej osi, wokół których można je niezależnie obracać. Każda płyta ma alfabet w jakiejś tasowanej kolejności, prawdopodobnie innej dla każdej płyty, wygrawerowanej na jej obrzeżach. Teoretycznie może być dowolna liczba dysków w zestawie, ale zwykle będzie to między 20 a 40. Jeśli na przykład w zestawie było 30 płyt, wiadomość, która ma zostać zaszyfrowana, została najpierw podzielona na bloki, z których każda zawierała 30 liter. 30 krążków na cylindrze zostanie następnie obróconych tak, aby pierwsze 30 liter wiadomości pojawiło się w poziomie linii, a następnie 30 liter dowolnej z pozostałych 25 linii poziomych zostanie wysłanych jako szyfr. Następnie krążki zostałyby obrócone tak, aby powstał drugi blok z 30 literami w postaci zwykłego tekstu i ponownie jedną z pozostałych 25 linii poziomych wybranych jako tekst szyfrujący. Rozszyfrowanie wymagałoby odseparowania dysków w celu pokazania 30 liter każdego bloku szyfru w linii poziomej, a następnie spojrzenia na pozostałe 25 linii poziomych i znalezienia tego, który miałby sens. Nasuwa się pytanie: "Czy to możliwe, że może istnieć więcej niż jedna linia, która ma sens?" Takiej sytuacji nie można uzyskać w przypadku większości systemów szyfrów, gdzie istnieje unikalny związek między tekstem jawnym a tekstem szyfrowania, ale cylinder Jeffersona jest wyjątek. Jeżeli wiadomość tekstowa jest w języku naturalnym, możliwość znalezienia więcej niż jednej rozsądnej linii wśród 25 jest znikoma. Z drugiej strony, jeśli składa się z wiadomości w postaci zwykłego tekstu grupy kodów, takie jak opisane w rozdziale 6, nie jest niemożliwe, aby znaleziono więcej niż jedno prawidłowe odszyfrowanie. Zależy to od tego, ile teoretycznie dostępnych grup kodu zostało faktycznie użytych w kodzie. Gdyby wszystkie możliwe grupy kodów były używane, każda z 25 linii wygenerowałaby prawidłowe odszyfrowanie, chociaż jest mało prawdopodobne, że więcej niż jeden z nich miałby sens po konwersji z powrotem na język naturalny. Zabezpieczenie cylindra Jeffersona zostałoby znacznie poprawione, gdyby kolejność,

w jakiej dyski zostały umieszczone na wspólnej osi, można było regularnie zmieniać, np. codziennie, ale wymagałoby to od nadawcy (-ów) i odbiorcy (-ów) uzgadniania zamówienia z wyprzedzeniem. W takim przypadku porządkowanie dysków będzie "wskaźnikiem" dla wiadomości, ale zamiast być podane w preambule lub osadzone w tekście wiadomości, będzie prawdopodobnie podane w wydrukowanym arkuszu, który został wytworzony i rozprowadzony jakiś czas przed rozpoczęciem okresu szyfrowania. Bez znajomości przetasowanych alfabetów na dyskach lub kolejności, w jakiej same dyski zostały umieszczone na wspólnej osi, kryptoanalityk miałby znaczną trudność w odszyfrowywaniu wiadomości i prawdopodobnie potrzebowałby wielu wiadomości wysłanych w tym samym okresie szyfrowania (tj. Przy użyciu tej samej kolejności dysków), aby osiągnąć sukces. Jeśli kolejność dysków nie może być zmieniona, okres szyfrowania jest nieskończony i wszystkie wiadomości wysyłane za pomocą tego systemu mogą być rozpatrywane łącznie, ale odszyfrowanie nadal nie będzie łatwe, ponieważ wiadomości mogą być wszystkie ułożone pionowo w blokach po 30 liter, nie są one ściśle określone, ponieważ ta sama litera w tej samej pozycji w bloku może być zaszyfrowana do jednej z 25 liter. Po odzyskaniu przetasowanych alfabetów, możliwe jest, że odszyfrowanie staje się trywialne przez nadawców, którzy popełniają błędy lub niektóre wiadomości w postaci zwykłego tekstu. Prosty w koncepcji, choć jest, cylinder Jeffersona zapewnił prawdziwie polialfabetyczny system szyfrowania i był genialną i skuteczną formą maszyny szyfrującej. Jako taki był prekursorem jednych z najczęściej używanych maszyn szyfrujących XX wieku, jak zobaczymy później.

Szyfry Jigsaw

Tu przyjrzymy się kilku systemom szyfrowania, które opierają się na innym pomyśle niż te, które spotkaliśmy do tej pory. W tych systemach każda litera zachowuje własną tożsamość, a więc częstotliwości poszczególnych liter wiadomości pozostają niezmienione, ale litery składowe dwuznaków i poligrafy wyższego rzędu są oddzielone, a w konsekwencji ich pierwotne częstotliwości tekstu jawnego są niszczone. Ponieważ metoda używana do ich rozwiązania przypomina raczej układanie układanki, którą zgrupowałem pod (nieoficjalną) nazwą "szyfry jigsaw". Najprostsze takie systemy są nazywane

Transpozycjami

Układy szyfrów, które zbadaliśmy we wcześniejszych częściach w oparciu o alfabety zastępcze, gdzie każda litera jest zastępowana inną literą, ale kolejność liter w alfabecie pozostaje niezmieniona. Alternatywnym podejściem jest pozostawienie liter w komunikacie niezmienionym, ale zmienić ich kolejność. Powoduje to, że wiadomość szyfrowana jest anagramem wiadomości w postaci zwykłego tekstu. Jakimś sposobem jest to, aby użyć systemu transpozycji.

Prosta transpozycja

W prostym systemie transpozycji wiadomość jest najpierw zapisywana w ramce, zwykle w prostokącie, który został podzielony na kwadraty za pomocą szeregu linii poziomych i pionowych. Liczba pionowych linii jest ustalana za pomocą klawisza numerycznego lub literalnego; liczba linii poziomych może być stała lub może być określona na podstawie długości wiadomości. Jeśli liczba wierszy jest ustalona, wiadomość jest dzielona na odcinki o odpowiedniej długości, pojemność pudełka. Wiadomość jest zapisywana w skrzynce wiersz po wierszu, zaczynając od góry, ale jest ona następnie usuwana z kolumny po kolumnie w kolejności określonej przez klucz. W wyniku tego litery pozostają niezmienione, ale są przesyłane w innej kolejności. Metoda szyfrowania jest bardzo prosta, jak pokazuje poniższy przykład.

Przykład 4.1

Użyj prostego systemu transpozycji za pomocą 5-cyfrowego klawisza 3-1-5-2-4, aby zaszyfrować wiadomość

MEETING WILL BE ON FRIDAY AT ELEVEN THIRTY

Szyfrowanie

Ignorując spacje między wyrazami, w wiadomości znajduje się 35 liter. Ponieważ klucz ma długość 5, będziemy potrzebować pudełka z 5 kolumnami i 7 rzędami. Dlatego zapisujemy klucz i pod nim rysujemy pudełko z 5 kolumnami i 7 rzędami, aby pomieścić wiadomość. Następnie piszemy wiadomość do pola po wierszu, zaczynając od górnego wiersza i ignorując spacje między wyrazami: patrz tabela 4.1.

Key	3	1	5	2	4
	M	E	E	T	I
	N	G	W	I	L
	L	B	E	O	N
	F	R	I	D	A
	Y	A	T	E	L
	E	V	E	N	T
	H	I	R	T	Y

Na koniec, zapisujemy wiadomość jako serię 5-literowych grup, pobierając tekst z kolumny po kolumnie w kolejności wskazanej przez klucz:

EGBRA VITIO DENTM NLFYE HILNA LTYEW EITER.

Oto, co zobaczy zarówno odbiorca, jak i kryptoanalityk. W jaki sposób odbiorca rozszyfruje wiadomość i jak może kryptoanalityk próbuje ją rozwiązać?

Rozszyfrowanie

Odbiorca zapisuje wiadomość szyfrowania w kolumnie prostokąta transpozycji za kolumną w porządku kolumny podanym przez klucz transpozycji, a następnie odczytuje wiersz wiadomości po wierszu, zaczynając od góry.

Atak kryptoanalityczny

Choć proste, szyfr transpozycji może nie być łatwy do rozwiązania. Częstotliwość liczba pojedynczych liter ("monografie") pokaże, że nie zostały one zmienione, ale częstotliwości par liter ("digrafy"), takie jak TH, HE i QU będą różne od tego, czego można by się spodziewać w tekście angielskim. Kryptoanalityk podejrzewałby zatem, że stosowany jest system transpozycji, a jego pierwszym zadaniem przy próbie rozwiązania byłoby określenie długości klucza. Ponieważ powyższy komunikat ma 35 liter, wszystkie 7 grup ma 5 liter. Kryptoanalityk nie wiedziałby, czy wiadomość ma rzeczywiście 35 liter, czy została "wyścielana" kilkoma "fałszywymi literami" w celu stworzenia pełnych grup szyfrów, z których wszystkie mają 5 liter. W obu przypadkach ma jednak możliwą wskazówkę co do długości klucza. Od 35? 5? 7 warto przyjrzeć się tekstowi zaszyfrowanemu przy założeniu, że klucz ma długość 5 lub 7. Zakłada on, że pole transpozycji jest "regularne", tj. Że wszystkie kolumny mają jednakową długość ; mogą nie być, ale jest to rozsądny pierwszy krok. Zakładając, że klucz ma długość 5, dwie litery sąsiadujące z oryginalną wiadomością będą miały 7, 14, 21 lub 28 pozycji w szyfrze tekst, chyba że jedna z pary znajdowała się na końcu jednego rzędu, a druga była na początku następnego. Kryptoanalityk wypisuje więc tekst zaszyfrowany w 5 kolumnach po 7 liter, co daje litery, które znajdowały się obok siebie w zwykłym tekście, z dużą szansą, że znajdą się w tym samym wierszu tekstu szyfrowania ułożonego w ten sposób. Przy użyciu tego układu tekst szyfrowania jest taki, jak pokazano w Tabeli 4.2.

E	T	M	I	E
G	I	N	L	W
B	O	L	N	E
R	D	F	A	I
A	E	Y	L	T
V	N	E	T	E
I	T	H	Y	R

Następnym krokiem jest spojrzenie na różne pary liter w każdym rzędzie, aby zobaczyć, które z nich wyglądają na najbardziej prawdopodobne dwuznaki. W tym celu pomoc w uzyskaniu dostępu do częstotliwości digrafów w języku angielskim, takich jak znajdujący się w korpusie Browna iw niektórych książkach o kryptografii. W pierwszym rzędzie powyżej, na przykład, stwierdziliśmy, że pary ME, TI i ET są częstsze niż pozostałe. Robimy to dla każdego rzędu i odnotowujemy implikacje; tak więc, jeśli w pierwszym rzędzie T rzeczywiście powinien znajdować się obok I, kolumna 2 powinna znajdować się na lewo od kolumny 4. Wykonując to ćwiczenie dla każdego wiersza, mamy nadzieję znaleźć potwierdzenia takich możliwości, a więc odzyskać prostokąt transpozycji i oryginalny tekst. Nie każda implikacja będzie prawidłowa, a niektóre będą sprzeczne z innymi, ale, miejmy nadzieję, wystarczająco

poprawne implikacje będą widoczne, aby umożliwić nam zastąpienie niewłaściwych. Dowody są przedstawione w tabeli 4.3.

Row	Digraphs	Implied adjacent columns
1	ME, TI, ET	3-1 or 3-5, 2-4, 1-2 or 5-2
2	IN, WI, NG	2-3, 5-2, 3-1
3	BE, ON, LE	1-5, 2-4, 3-5
4	RI, DA, ID	1-5, 2-4, 5-2
5	AT, ET, EA	1-5, 2-5, 2-1
6	VE, NT	1-3 or 1-5, 2-4
7	IT, TH, HI	1-2, 2-3, 3-1

Chociaż istnieją pewne sprzeczności, pewne implikacje zdarzają się wystarczająco często, aby zasługiwały na dalsze badanie, a mianowicie

1-5, 2-4, 3-1 i 5-2.

Jeśli teraz zmienimy układ kolumn szyfrujących w kolejności sugerowanej przez te pary, zobaczymy, gdy zaczniemy od kolumny 3 (musielibyśmy wypróbować inne kolumny na pierwszej pozycji), że tekst szyfru powinien zostać zmieniony tak, aby kolumny szyfrów

3-1-5-2-4

stają się kolumnami w postaci zwykłego tekstu

1-2-3-4-5

tak, że pierwszy rząd szyfrów

E T M I E

staje się wierszem tekstu jawnego

M E E T I.

Podobnie drugi rząd szyfrów

G I N L W

staje się

N G W I L

a reszta wiadomości potwierdza odszyfrowanie. Jest to bardzo prosty przykład, że klucz był krótki i jego długość była pierwszą oczywistą próbą, ale ilustruje metodę rozwiązania. Wskazuje również, że dostęp do tabeli częstotliwości digrafów, choć niekoniecznie niezbędny, znacznie uprości to zadanie. Miał tekst szyfrowania nie było wielokrotnością 5, nie byłoby tak prawdopodobne, że długość klucza może wynosić 5 (lub 7, w tym przypadku) i inne kluczowe długości mogą wymagać wypróbowania. W przypadku kluczy o długości nie przekraczającej 5, nawet brutalny atak siły jest możliwy, ponieważ istnieje tylko umiarkowana liczba możliwych kolejności kolumn (120, gdy kluczowa długość wynosi 5). Gdy długość klucza wzrasta powyżej 5, atak brutalnej siły staje się bardzo uciążliwy, a ostatecznie niepraktyczny ręcznie, podczas gdy metoda dwuwymiarowa stosowana powyżej jest realistyczna dla wszystkich kluczowych długości, które można napotkać w praktyce. Kryptograf, wiedząc o tym

wszystkim, starał się ukryć kluczową długość tak dalece, jak to możliwe, i mógł również użyć innych środków, takich jak

Podwójna transpozycja

Słabością prostej metody transpozycji jest to, że gdy wiadomość szyfrowania jest wypisywana kolumna po kolumnie "na szerokość klucza", tj. W wierszach zawierających tyle liter, ile wynosi długość klucza, litery, które były sąsiadujące z tekstem jawnym będą miały tendencję do mieszczą się w tym samym wierszu, a poszukiwanie "dobrych" dwuznak może ujawnić porządek transpozycji kolumn. Staje się to bardzo oczywiste, jeśli zastąpimy tekst zwykły w powyższym przykładzie liczbami 1, 2, 3, ..., 35, podkreślając pierwsze pięć liczb dla łatwościidentyfikacji i zastosowanie klucza transpozycji, który używaliśmy wcześniej, dzięki czemu (patrz Tabela 4.4)

Key	3	1	5	2	4
	1	2	3	4	5
	6	7	8	9	10
	11	12	13	14	15
	16	17	18	19	20
	21	22	23	24	25
	26	27	28	29	30
	31	32	33	34	35

otrzymujemy tekst zaszyfrowany

2 7 12 17 22 27 32 4 9 14 19 24 29 34 1 6 11 16 21 26
31 5 10 15 20 25 30 35 3 8 13 18 23 28 33

i jeśli spojrzymy na odstępy między podkreślonymi liczbami, znajdziemy to

1 i 2 są oddalone o 14 miejsc

2 i 3 są oddalone o 28 miejsc

3 i 4 są oddalone o 21 miejsc

i

4 i 5 są oddalone o 14 miejsc

tj. podkreślone liczby padają w odstępach wielokrotności 7, tak że gdy rozmieszczamy "tekst" w 7 rzędach po 5, to spadają one do tego samego rzędu. Jeśli jednak weźmiemy ten tekst "szyfrowania" i ponownie zastosujemy transpozycję (tabela 4.5)

Key	3	1	5	2	4
	2	7	12	17	22
	27	32	4	9	14
	19	24	29	34	1
	6	11	16	21	26
	31	5	10	15	20
	25	30	35	3	8
	13	18	23	28	33

tekst zaszyfrowany

7 32 24 11 5 30 18 17 9 34 21 15 3 28 2 27 19 6 31 25
13 22 14 1 26 20 8 33 12 4 29 16 10 35 23

i widzimy, że pary, które pierwotnie były sąsiadowały z "tekstem jawnym", są obecnie nierównomiernie rozmieszczone w tekście "zaszyfrowanym",

1 i 2 są oddalone o 9 miejsc

2 i 3 są oddalone o 2 miejsca

3 i 4 są oddalone o 17 miejsc

i

4 i 5 są oddalone o 25 miejsc

a atak dwuznakowy, który był wcześniej używany, przestanie działać. Bezpieczeństwo podwójnego szyfru transpozycji byłoby jeszcze większe, gdybyśmy użyli dwóch różnych słów kluczowych, zamiast używać tego samego dwa razy, szczególnie jeśli słowa kluczowe miały różną długość. W takim systemie istnieje jednak zwiększone ryzyko, że nadawca popełni błąd, używając dwóch słów kluczowych w niewłaściwej kolejności. Generalnie będzie to generować inny tekst szyfrowania, którego odbiorca nie będzie w stanie odcyfrować, a wiadomość będzie musiała zostać wysłana ponownie w poprawnej formie. Zapewniłoby to kryptoanalitykowi dwie wersje tego samego tekstu, zaszyfrowane tymi samymi kluczami, ale w przeciwnych zleceniach; sytuacja, którą może wykorzystać. Ten rodzaj błędu stanowi zagrożenie dla dowolnego systemu obejmującego podwójne szyfrowanie. Niektóre wiadomości Enigmy były szyfrowane dwukrotnie, w różnych ustawieniach, dla dodatkowego bezpieczeństwa i była przynajmniej jedna okazja, kiedy szyfrowanie zostało przeprowadzone w niewłaściwej kolejności.

Przykład 4.2

Zastosuj metodę podwójnej transpozycji do tekstu

A B C D E F G H I J K L M N O

za pomocą dwóch kluczy

3-1-5-2-4 i 3-1-2

(i) w podanej kolejności, (ii) w odwrotnej kolejności. Dlatego sprawdź, czy dwa teksty szyfrów są różne.

Weryfikacja

(i) Stosujemy 3-1-5-2-4 (patrz Tabela 4.6),

3	1	5	2	4
A	B	C	D	E
F	G	H	I	J
K	L	M	N	O

dający

B G L D I N A F K E J O C H M.

Teraz stosujemy 3-1-2 (patrz tabela 4.7),

3	1	2
B	G	L
D	I	N
A	F	K
E	J	O
C	H	M

a tekst zaszyfrowany to

G I F J H L L N K O M B D A E C.

(ii) stosujemy 3-1-2 (patrz Tabela 4.8),

3	1	2
A	B	C
D	E	F
G	H	I
J	K	L
M	N	O

dający

B E H K N C F I L O A D G J M.

Teraz stosujemy 3-1-5-2-4 (patrz Tabela 4.9),

3	1	5	2	4
B	E	H	K	N
C	F	I	L	O
A	D	G	J	M

a tekst zaszyfrowany to

E F D K L J B C A N O M H I G

co różni się od pierwszej wersji.

Inne formy transpozycji

Do tej pory napisaliśmy tekst w prostokącie, rząd po wierszu, ale są dostępne alternatywy, a niektóre z nich utrudniłyby kryptoanalitykowi rozwiązanie tego systemu. W każdym przypadku tekst wiadomości jest dzielony na bloki o odpowiedniej długości, aby pasowały do pola transpozycji.

Regularne pudełka do transpozycji

Przez regularne pole transpozycji rozumiemy pole z kolumnami o przewidywalnej długości. Tekst może być zapisany w pudełku na różne sposoby, ale należy zachować ostrożność, w przeciwnym razie można wprowadzić słabe punkty. Oto kilka przykładów, z których nie wszystkie mogą być zalecane.

(i) Możemy użyć prostokąta, ale piszemy tekst wokół prostokąta w sposób "spiralny" (tabela 4.10).

A	B	C	D	E
P	Q	R	S	F
O	X	Y	T	G
N	W	V	U	H
M	L	K	J	I

Niestety zdecydowanie nie jest to zalecane. Bez względu na to, jakie uporządkowanie kolumn zostanie użyte w transpozycji, pentagram EFGHI i trigraph STU pojawią się w postaci niezmienionej w "szyfrze". Na przykład, jeśli wiadomość jest

THISXMETHODXISXNOTXSECURE

a transpozycja to 3-1-5-2-4 to pudełko jest pokazane w Tabeli 4.11,

3	1	5	2	4
T	H	I	S	X
N	O	T	X	M
X	R	E	S	E
S	U	C	E	T
I	X	D	O	H

to jest tekst szyfrowania

HORUX SXSEO TNXSI XMETH ITECD

Pentagram, XMETH, wkrótce zostanie zauważony przez kryptoanalityka. Trigraph, XSE, choć autentyczny, nie jest tak oczywisty. Gdyby użyto prostokąta z większą liczbą rzędów niż kolumn, "dobre" poligrafy byłyby jeszcze bardziej oczywiste.

(ii) Użyj pola "w kształcie rombu". W tym polu wszystkie wiersze (i kolumny) zawierają nieparzystą liczbę liter, zaczynając od 1 i zwiększając każdorazowo o 2 do pewnej uprzednio określonej liczby, a następnie zmniejszając o 2 za każdym razem do 1. Pole jest oczywiście symetryczne względem centralny rząd i kolumna, a wszystkie kolumny są prawidłowo wyrównane w pionie (tabela 4.12).

			A			
		B	C	D		
	E	F	G	H	I	
J	K	L	M	N	O	P
	Q	R	S	T	U	
		V	W	X		
			Y			

Ma to tę zaletę, że długości kolumn są zmienne, co komplikuje atak digrafów. Jeśli użyjemy na przykład siedmiocyfrowego klucza transpozycji 3-1-7-5-2-4-6 (Tabela 4.13)

3	1	7	5	2	4	6
			A			
		B	C	D		
	E	F	G	H	I	
J	K	L	M	N	O	P
	Q	R	S	T	U	
		V	W	X		
			Y			

przesyłany tekst będzie

EKQDH NTXJI OUACG MSWYP BFLRV

litery, które były pierwotnie przyległe, będą teraz znajdować się w odległościach od 5 (na przykład H-I) do 21 (E-F) od siebie, zamiast wielokrotności 5 jak przy normalnym kwadracie 5x5

(iii) Użyj sześciokąta. W przykładzie w tabeli 4.14

		A	B		
	C	D	E	F	
G	H	I	J	K	L
M	N	O	P	Q	R
	S	T	U	V	
		W	X		

każdy wiersz lub kolumna zawiera parzystą liczbę liter zaczynającą się od 2 i rosnącą o 2 za każdym razem, aż do pewnego limitu. Długość najdłuższego rzędu jest powtarzana, a następnie jego długości stopniowo zmniejszają się do 2. Można zastosować inne wzory.

Daje tę samą korzyść, co pudełko z brylantami. W tym przypadku przesyłany tekst, gdy kluczem jest 2-5-4-1-6-3, jest

BEJPU XGMLR ADIOT WCHNS FKQV.

Nieregularne pudełka transpozycji

Istnieje wiele innych możliwości, w tym "niekompletne" prostokąty z kolumnami o różnych długościach, które zwiększają bezpieczeństwo systemu transpozycji. W przypadku przykładu 4.1 pudełko transpozycji 35 komórek nie musi składać się z 5 kolumn składających się z 7 liter lub 7 kolumn z 5 liter, ale może mieć 5 kolumn o różnych długościach, na przykład 10, 4, 11, 7 i 3, aby wprowadzić 35-literowy komunikat z przykładu, jak pokazano w tabeli 4.15,

3	1	5	2	4
M	E	E	T	I
N	G	W	I	L
L	B	E	O	N
F	R	I	D	—
A	—	Y	A	—
T	—	E	L	—
E	—	V	E	—
N	—	T	—	—
H	—	I	—	—
R	—	T	—	—
—	—	Y	—	—

w którym to przypadku wiadomość szyfrowana byłaby

EGBRT IODAL EMNLF ATENH RILNE WEIYE VTITY

Arcydzieła tekstu jawnego są teraz rozdzielane na różne odległości, a ponieważ istnieje 46 376 sposobów wyboru 5 liczb dodatnich, które dają do 35 (patrz rozwiązanie problemu 4.2 poniżej), kryptoanalityk stanąłby przed poważnym problemem. Głębokość nie byłaby zbyt użyteczna, ale gdyby ta sama wiadomość została wysłana do dwóch odbiorców przy użyciu tego samego pola, ale różnych kluczy transpozycji, system może zostać rozwiązany. W każdym razie odbiorca oczywiście musiałby znać zarówno długość kolumny, jak i klucz transpozycji, a gdyby podejrzewać, że są ukryte we wskaźniku, kryptoanalityk z pewnością starałby się go znaleźć. Przy wyborze długości kolumny dla nieregularnego pudełka transpozycji warto upewnić się, że najdłuższa kolumna nie była dłuższa niż, powiedzmy, dwie litery dłuższe niż druga najdłuższa kolumna, ponieważ w przeciwnym razie kilka ostatnich liter wiadomości będzie kolejno tekst szyfrowania. Na przykład dwie ostatnie litery w nieregularnym polu powyżej (TY) pojawiły się razem na końcu tekstu szyfrowania. To, że upadli na końcu, było konsekwencją szczególnej transpozycji, ale zeszliby się gdzieś, ponieważ najdłuższa kolumna (11) pojawiła się po drugiej najdłuższej kolumnie (10) w transpozycji. Gdyby najdłuższa kolumna była o wiele dłuższa niż druga najdłuższa, kryptoanalityk zauważyłby w tekście dobry (wysokiej częstotliwości) poligraf w postaci zwykłego tekstu, który dałby mu ważną wskazówkę.

Ocena bezpieczeństwa szyfrów transpozycji

Podwójny system transpozycji z różnymi transpozycjami lub prosty system transpozycji z pudełkiem o nieregularnym kształcie nie zostałby łatwo złamany, gdyby nie było dostępnych kilku komunikatów szyfrów, podczas gdy prosty system z regularną skrzynką powinien być rozwiązywany, biorąc pod uwagę wystarczająco długi komunikat, przez atak digrafów. W sytuacji, w której dostępne są zarówno zwykłe, jak i szyfrowane teksty, nawet podwójny system powinien być rozwiązywany, jeśli komunikat zawiera kilka liter o niskiej częstotliwości, aby można je było jednoznacznie zidentyfikować w tekstach zwykłych i szyfrów, ale jak wskazuje przykład 4.2, nie byłoby to łatwe zadanie. W trzeciej sytuacji, w której kryptoanalityk może określać zwykłe teksty, zapewniałby, że żaden znak nie pojawiłby się więcej niż jeden raz, jeśli to możliwe, co pozwoliłoby mu zobaczyć, jakie przekształcenia kolumn spowodowałyby obserwowane przesunięcia liter. We wszystkich przypadkach pierwszym zadaniem kryptoanalityka będzie znalezienie długości kluczy transpozycji; dopóki to się nie uda, nie będzie w stanie rozwiązać szyfru. W przypadku nieczęstego stosowania w komunikatach o niskim poziomie bezpieczeństwa podwójny system transpozycji, w którym transpozycja jest regularnie zmieniany, byłby umiarkowanie bezpieczny. W przypadku wiadomości o dużym natężeniu lub o wysokim poziomie bezpieczeństwa takie systemy nie są akceptowane.

Podwójne szyfrowanie w ogóle

Zauważyliśmy, że stosowanie podwójnej transpozycji zwykle zwiększa bezpieczeństwo systemu transpozycji, ale wiąże się z ryzykiem transpozycji w niewłaściwej kolejności. Rodzi to ogólne pytanie, czy szyfrowanie komunikatu dwa razy lub więcej zwiększy jego bezpieczeństwo. Nie ma prostej odpowiedzi na to pytanie, ponieważ zależy to od rodzaju zastosowanych encyklik. W przypadku podwójnego prostego zastąpienia na przykład nie ma żadnej korzyści, ponieważ wynikiem podwójnej substytucji jest po prostu inna prosta substytucja, a zatem nie stanowi większego wyzwania dla kryptoanalityka. Ponadto, jeśli te dwie substytucje są stosowane w niewłaściwej kolejności, tworzony jest inny tekst szyfrowania; to nie pokona kryptoanalityka, który nawet nie będzie świadomy błędu, ale prawdziwy odbiorca nie będzie w stanie odszyfrować wiadomości. Połączenie prostej zamiany i transpozycji z drugiej strony zapewnia większe bezpieczeństwo. Kryptograf, który myśli o użyciu systemu wielu szyfrów, z pewnością zadałby sobie pytanie:

(1) czy zwiększa to bezpieczeństwo?

(2) czy ręczne operacje są wykonywane ręcznie, czy użytkownicy uważają system za nadmiernie żmudny?

(3) czy szyfrowanie jest używane w złej kolejności, czy pomogłoby to kryptoanalitykowi?

Interesujący przykład potrójnego szyfrowania szyfru jest jednym z tych używanych przez garbo podwójnego agenta. Jest to opisane w części 7.

Problem 4.1

30-minutowy komunikat poniżej, zakodowany prostą transpozycją, został wysłany przez młodego człowieka do swojej dziewczyny-przyjaciółki. Uważa się, że kluczowa długość wynosi 6; wszystkie odstępy i znaki interpunkcyjne zostały zignorowane. Znajdź klucz i odszyfruj wiadomość.

LPEUD SCEOE LAEMA AMHSS HOTAR IRTMY

Problem 4.2

Liczba możliwych (regularnych i nieregularnych) skrzynek transpozycji o zadanej szerokości rośnie bardzo szybko wraz ze wzrostem pojemności (liczby liter) ramki. Wyliczenie możliwości pokazuje, że istnieje 28, gdy szerokość wynosi 3, a pojemność wynosi 9.

Problem 4.3

Tekst jawny w systemie transpozycji może być zapisany w kwadracie lub prostokątnym polu wzdłuż wierszy na przemian od lewej do prawej, a następnie od prawej do lewej (jest to tak zwana moda boustropedonowa, ponieważ jest to ścieżka przeorana). Wprowadzanie wiadomości

THISXMETHODXISXNOTXSECURE

w ten sposób podaje Tabela 4.16.

THISX
OHTEM
DXISX
SXTON
ECURE

Jakie poważne słabości wprowadza ten system?

Dwuliterowe szyfry

Może wydawać się naturalne, że szyfr, w przeciwieństwie do kodu, będzie miał właściwość polegającą na tym, że każda pojedyncza litera jest oddzielnie szyfrowana i zastępowana przez pojedynczą literę lub symbol, i tak właśnie jest w przypadku wielu systemów szyfrów. Istnieją jednak systemy szyfrowania, w których każda litera zwykłego tekstu staje się więcej niż jedną literą w szyfrze i są też inne systemy, które szyfrują tekst dwie (lub więcej) litery na raz. Przykładem pierwszego typu jest

Monografia do digrafu

Alfabet jest zapisany w 5 x 5 kwadratów z pominięciem jednej litery Pominiętą literą jest zwykle J, która w razie potrzeby zostaje zastąpiona przez I. Pięć rzędów kwadratu oznaczono literami A, B, C, D i E, podobnie jak kolumny: patrz tabela 5.1.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Każda litera tekstu jawnego jest teraz zamieniana na litery wiersza i kolumny, tak że na przykład M staje się CB. Wynikowy tekst szyfrowania jest zatem dwa razy dłuższy niż oryginalny tekst i zawiera tylko litery A do e

Przykład 5.1

HAPPY BIRTHDAY

szyfrujemy jako

BCAAC ECEED ABBDD BDDBC ADAAE D

W obecnej wersji jest to słaby szyfr, ale jego bezpieczeństwo można poprawić dzięki dwóm modyfikacjom

(i) używając tasiemkowego alfabetu wewnątrz 5x 5 pudełek;

(ii) zastosowanie transpozycji do zaszyfrowanego tekstu.

Pierwszą z nich można czasem częściowo osiągnąć, wybierając słowo kluczowe, wpisując je w polu, a następnie wypełniając pozostałe pola nieużywanymi literami alfabetu, z wyjątkiem J. Jeśli słowo kluczowe ma powtarzające się litery, są one ignorowane.

Przykład 5.2

Powtórz powyższy przykład, używając pola ze słowem kluczowym CZWARTEK i zastosuj transpozycję 5-1-4-2-3 do tekstu zaszyfrowanego. Skrzynia jest pokazana w Tabeli 5.2

	A	B	C	D	E
A	T	H	U	R	S
B	D	A	Y	B	C
C	E	F	G	I	K
D	L	M	N	O	P
E	Q	V	W	X	Z

i HAPPY BIRTHDAY dla szyfrowania jako

ABBBD EDEBC BDCDA DAAAB BABBB C

Ponieważ transpozycja obejmuje 5 liczb, piszemy tekst szyfrowany do pola zawierającego 5 kolumn. Zauważ, że skoro w szyfrze jest 26 liter, jedna kolumna w polu musi zawierać 6 liter. Odbiorca wiadomości musi wiedzieć, które, jeśli w ogóle, są "długimi" kolumnami, więc zostanie to wcześniej ustalone . Podejmiemy arbitralne założenie, że kolumny "długie" powstają w kolejności transpozycji. W przypadku tego przykładu samotna kolumna "długa" to kolumna "1", która jest drugą kolumną od lewej. Wprowadzanie szyfru tekst do pola transpozycji mamy w Tabeli 5.3.

5	1	4	2	3
A	B	B	B	D
E	D	E	B	C
B	D	C	D	A
D	A	A	A	B
B	A	B	B	B
.	C	.	.	.

Tekst jako ostatecznie przekazany jest wtedy

BDDAA CBBDA BDCAB BBECA BAEBD B

a oryginalne pary digrafów zostały rozbite, co czyni szyfr trudniejszym do rozwiązania. Użycie podstawienia digektem monografii 5-5 jest nadal widoczne, ale możemy to ukryć po prostu przez ponowne wykorzystanie kwadratu do konwersji dwuznaków z powrotem na monografie (tabela 5.2), dając nowy tekst monografii zaszyfrowanej

BLUAL BEACE DVM

a metoda szyfrowania jest dobrze ukryta. Oczywiście konieczne jest włączenie transpozycji przed ponownym użyciem kwadratu, ponieważ w przeciwnym razie po prostu odszyfrujemy wiadomość!

Szyfry MDTM

W takim przypadku metoda jest ściśle określona jako system monograficzno-digraf-transpozycja-monografia, MDTM dla zwięzłości. Związek pomiędzy poszczególnymi literami zwykłego tekstu i tekstów zaszyfrowanych jest dość skomplikowany, ponieważ każda oryginalna litera jest zastępowana dwiema literami, z których każda następnie oddzielnie łączy się z literą z innej pary w celu utworzenia dwuznakowego, który jest następnie przekształcany w monografię . W pewnych okolicznościach może to wytworzyć tekst zaszyfrowany, który wygląda dziwne w porównaniu z oryginalnym tekstem jawnym, jak pokazano poniżej.

Przykład 5.3

Użyj metody MDTM do zaszyfrowania 25-literowego alfabetu (J pominięty) przy użyciu normalnie uporządkowanego kwadratu 5 x 5 i transpozycji 3-1-6-4-5-7-2-9-10-8.

Szyfrowanie

"Tekst jawny" to

ABCDEFGHIKLMNOPQRSTUVWXYZ

co przy użyciu kwadratu 5 x5 staje się

AAABA CADAE BABBB CBDBE CACBC CCDCE DADBD CDDDE EAEBE CEDEE

Pisząc to w prostokącie transpozycji, w Tabeli 5.4,

3	1	6	4	5	7	2	9	10	8
A	A	A	B	A	C	A	D	A	E
B	A	B	B	B	C	B	D	B	E
C	A	C	B	C	C	C	D	C	E
D	A	D	B	D	C	D	D	D	E
E	A	E	B	E	C	E	D	E	E

tworzymy tekst "szyfru digraficznego"

AAAAA ABCDE ABCDE BBBBB ABCDE ABCDE CCCCC EEEEE DDDDD ABCDE

a następnie przekonwertuj ponownie, aby uzyskać szyfr monograficzny

AAAHU BOWGG BOVHU NNPZZ TTQHU

który nie odgadłby, że jest to szyfrowanie 25-literowego alfabetu napisanego w normalnej kolejności. To dość dziwne szyfrowanie wynika głównie z faktu, że użyliśmy kwadratu alfabetu 5 x 5 bez słowa kluczowego, a następnie prostokąta transpozycji o szerokości 10. Przy wyborze szerokości transpozycji należy unikać wielokrotności rozmiaru kwadratu alfabetu .

Przykład 5.4 (Szyfr niemieckiego dowództwa z 1918 r.)

Na początku 1918 r. Niemieckie dowództwo zaczęło używać szyfru opartego na kwadracie 5,5. 25 liter alfabetu zostało zaszyfrowanych jako digrafy z użyciem tylko liter A, D, F, G i X. Zmodyfikowana forma, za pomocą kwadratu 6x6, dostarczyła dodatkowe 11 miejsc i umożliwiła użytkownikom uwzględnienie wszystkich 26 liter alfabet i 10 cyfr. Szyfr był znany jako "szyfr ADFGVX". Każda litera pierwotnej wiadomości stała się zatem parą liter, które następnie rozdzielono i transponowano według klucza, który zmieniał się codziennie. Szyfr nie był łatwy do rozwiązania, ale francuski kryptoanalityk, Georges Painvin, opracował metodę wykonywania tego przy wielu wiadomościach z identycznym początkiem lub zakończeniem tekstowym. Chociaż tylko kilka dni zostało rozwiązanych, liczba wiadomości w tych dniach była wysoka, a ich zawartość była szczególnie cenna. Mówi się, że "przy jednej okazji rozwiązanie było tak szybkie, że ważna operacja niemiecka ujawniona przez jedną wiadomość była całkowicie sfrustrowana".

Przykład 5.5 (Japoński szyfr morski)

Podczas II wojny światowej japońska marynarka handlowa używała szyfru, znanego jako JN40, w którym każdy japoński symbol kana został zastąpiony przez dwie cyfry z kwadratu 10? 10. Poszczególne cyfry zostały zapisane w kolumnach prostokąta, przy czym kolejność kolumn została nadana

transpozycji. Cyfry były następnie usuwane wiersz po wierszu, kolejność rzędów podawana przez drugą transpozycję. Transpozycje były zmieniane codziennie. Szyfr został rozwiązany w listopadzie 1942 roku, kiedy operator zostawił pewne szczegóły z wiadomości, a następnie ponownie zaszyfrował pełny tekst za pomocą tych samych kluczy

Problem 5.1

System MDTM ze słowem kluczowym ABSOLUTE i transpozycją 3-1-5-2-4 został zastosowany do wiadomości, a wynikowy tekst szyfrowania jest

CFIGS FLTBC XKEEA EBHTB GLDPI

Odszyfruj wiadomość.

Digraf z digrafem

Tak jak zwykły system zastępowania zastępuje każdą pojedynczą literę alfabetu pojedynczą literą, tak więc można skonstruować system, w którym każdy dwuznak zostanie zastąpiony dwoma literami. "Oczywistym" sposobem na to, jak wskazano wcześniej, jest posiadanie listy wszystkich 676 (= 26x26) możliwych dwuznaków i ich odpowiedniki szyfrowe, np.

AA = TK, AB = LD, AC = ER, ..., ZX = DW, ZY = HB, ZZ = MS,

ale wiąże się to z dwoma listami, jedną dla szyfrowania i jedną dla odszyfrowania, każda o długości 676 i chociaż zapewniłoby to wyższy poziom bezpieczeństwa niż zwykłe zastąpienie, byłoby to żmudne w użyciu. Alternatywną metodą jest użycie kwadratu dwuwymiarowego, który zawiera tylko 25 liter alfabetu, z wyjątkiem J, i utwórz dwuznakowe szyfry z dwuznaków jawnego tekstu według jakiejś reguły. System dziewiętnastowieczny tego typu jest metodą

Szyfrowanie Playfair

Alfabet, ignorując J, jest zapisywany w kwadracie 5x5 w dowolnej kolejności, zaczynając od słowa kluczowego, z pozostałymi literami po kolei lub w kolejności "losowej". Jeśli słowo kluczowe ma powtarzające się litery, drugie i następne wystąpienia są ignorowane. Zatem jeśli JUTRO to słowo kluczowe, trafi ono do kwadratu jako TOMRW.

Szyfrowanie jest następnie przeprowadzana za pomocą dwuznakowego digrafu zgodnie z następującymi zasadami.

(i) Jeśli dwie litery dwuznaku znajdują się w przekątnych przeciwległych narożnikach prostokąta w kwadracie 5x5, szyfrują one do pary w pozostałych dwóch rogach. W poniższym przykładzie przyjęliśmy konwencję, że każdą literę zastępuje się literą narożną w tym samym wierszu, co ona sama. Alternatywna konwencja polega na zastąpieniu każdej litery literą w tej samej kolumnie co ona sama i jest to standardowa praktyka z podwójnymi szyframi Playfair, jak widać poniżej.

(ii) Jeżeli dwie litery znajdują się w tej samej kolumnie kwadratu 5x5, szyfrują one jako litery poniżej, gdzie wiersz 1 uważany jest za poniżej wiersza 5, jeśli jest to konieczne.

(iii) Jeżeli te dwie litery znajdują się w tym samym rzędzie kwadratu 5x5, szyfrują one jako litery po prawej stronie, gdzie kolumna 1 jest uważana za znajdującą się po prawej stronie kolumny 5, jeśli jest to konieczne.

(iv) Jeżeli te dwie litery są identyczne, to między nimi wstawiana jest "smsowa" litera, taka jak Q.

(v) W razie potrzeby na końcu tekstu jawnego wstawia się "manekin".

Przykład 5.6

Zaszyfruj wiadomość

SUPPORT NEEDED URGENTLY

używanie szyfeowania Playfair ze słowem kluczowym WALKING. Kwadrat Playfair pokazano w tabeli 5.5.

W	A	L	K	I
N	G	B	C	D
E	F	H	M	O
P	Q	R	S	T
U	V	X	Y	Z

Szyfruje się jako PY, ponieważ P znajduje się w tym samym wierszu co S i Y w tym samym wierszu co U. Następna para PP będzie musiała wstawić manekina między nimi, a więc stanie się dwiema parami, PQ i PO, które będą kodować jako QR i TE odpowiednio. Kontynuując w ten sposób, stwierdzamy, że tekst szyfrowania jest

PYQRT ESPEP ONONX PNFDP KX

i gdy jedna litera jest wstawiona, długość tekstu była nawet dłuższa niż tekst pierwotny, ponieważ wymagane było jedno pozorne wstawienie. Zauważ, że chociaż tekst zwykły zawierał inną powtarzającą się parę liter, EE w NEEDED, nie było potrzeby wstawiania fałszywej litery, ponieważ w miejscu szyfrowania dwuznaki w tekście rozdzielają EE, jako NE, po którym następuje ED. Gdybyśmy już nie musieli wstawiać jednego fałszywego listu, między PP w SUPPORT, para EE nie zostałaby podzielona i wtedy musiałby zostać wstawiony manekin. Podobnie, nie było potrzeby, aby na końcu pojawił się fałszywy list od czasu, gdy pojedynczy manekin spowodował wyrównanie długości tekstu.

Odszyfrowanie Playfair

W niektórych systemach szyfrowania rozszyfrowanie obejmuje dokładnie takie same kroki, jak szyfrowanie, ale nie jest tak w przypadku innych. W systemie Playfair jest częściowo prawdą, ale istnieje pewna asymetria, ponieważ w przypadku, gdy dwie litery, które mają być zaszyfrowane, znajdują się w tym samym wierszu lub kolumnie, zaszyfrowane litery uzyskuje się, przesuwając odpowiednio w prawo lub w dół. Dlatego przy rozszyfrowaniu, gdy dwie litery szyfrów mieszczą się w tym samym wierszu lub kolumnie, litery w postaci zwykłego tekstu są uzyskiwane odpowiednio poprzez przesunięcie w lewo lub w górę. Tam, gdzie dwie litery szyfrów nie znajdują się w tym samym wierszu lub kolumnie, litery z tekstem otwartym znajdują się w przeciwległych rogach prostokąta jak wcześniej.

Problem 5.2

Wiadomość została zaszyfrowana za pomocą szyfru Playfair ze słowem kluczowym RHAPSODY, tekstem szyfrowania jest

OXBGI HPEOK GHMTT ROIUE VGKGN C.

Odszyfruj wiadomość.

Kryptanalityczne aspekty Playfair

Szyfrowanie Playfair ma pewne właściwości, które może wykorzystać kryptoanalityk, w tym następujące.

(i) Pismo nie może się samoistnie szyfrować.

(ii) Litera może szyfrować tylko jedną z 5 innych liter, które są 4 innymi literami w rzędzie i literą pod nią w kolumnie.

(iii) List jest dwa razy bardziej prawdopodobne, aby zaszyfrować list bezpośrednio po jego prawej stronie niż na jakikolwiek inny list. Tak więc na przykład w kwadracie użytym w Przykładzie 5.6 (Tabela 5.5), jeśli druga litera dwukierunku zaczynającego się na M nie znajduje się w tym samym wierszu lub kolumnie, co M, a następnie M jako E, F, H lub O. Jeśli druga litera dwunastki znajduje się w tym samym rzędzie, co M, a następnie M, jako O, a jeśli druga litera znajduje się w tej samej kolumnie, co M, a następnie M w postaci S. Wynika to z 24 możliwości liter, które mogą podążać za M w tekst jawny (ponieważ J nie jest zawarty, a M spowodowałoby wprowadzenie manekina), E, F, H, O, I, D, T i Z powodują, że O występuje jako litera szyfrująca, podczas gdy pozostałe 16 liter powoduje E , F, H i S występują cztery razy. Tak więc w tym przypadku M będzie encypował do O dwa razy częściej niż do każdej innej litery i ta sama funkcja będzie obowiązywać dla każdej innej litery.

(iv) Istnieje wzajemność między zwykłymi i dwuznakami szyfrów, chyba że litery znajdują się w tym samym wierszu lub kolumnie; to znaczy, jeśli CR, powiedzmy, jest szyfrowany na PJ, to PJ szyfruje do CR, a ponadto, RC szyfruje do JP i na odwrót.

Typową metodą ataku na szyfry Playfair są digrafy. Przy wystarczająco długim tekście liczba digrafów szyfrów powinna ujawnić prawdopodobnych kandydatów na ekwiwalenty szyfrów wysokogatunkowych digrafów jawnego tekstu, takich jak TH, HE, IN i ER, a ponieważ odwrotności dwóch z tych digrafów, HT i EH, są bardzo niskie. identyfikacja częstotliwości jest o wiele łatwiejsza. Po zidentyfikowaniu względnych pozycji niektórych liter może być możliwe ustalenie, które litery znajdują się w słowie kluczowym, a następnie rekonstrukcja kwadratu Playfair.

Podwójny Playfair

Szyfrowanie Playfair było używane przez Brytyjczyków do niektórych swoich wojskowych szyfrów aż do wojny w latach 1914-18, a Niemcy odnieśli znaczny sukces w czytaniu wiadomości. W czasie II wojny światowej armia niemiecka, znając słabość pojedynczego szyfru Playfair, użyła podwójnego systemu Playfair jako swojego średniego stopnia, aż do jesieni 1944 r., Po czym została zastąpiona przez szablonowy szyfr (patrz część 7). W podwójnym systemie Playfair stosuje się dwa kwadraty 5x5, umieszczone obok siebie, przy czym pierwsza litera każdego dwuznacznika tekstu jawnego znajduje się w pierwszej lub lewej stronie, kwadrat i druga litera digrafu znajdującego się w drugiej lub prawej - hand, kwadratowy. Odpowiednie litery szyfrów są uzyskiwane za pomocą zwykłych reguł Playfair, ale prawdopodobnie w celu ułatwienia użycia litery w rogach prostokąta są zastępowane odpowiednimi literami w tych samych kolumnach, co one same, co oznacza, że literę zawsze zastępuje się literą z tego samego kwadratu, co on sam. Ponieważ dwie litery używają różnych kwadratów, nie mogą znajdować się w tej samej kolumnie, ale mogą znajdować się w tym samym rzędzie. Alfabet w każdym kwadracie był w kolejności losowej i był zmieniany codziennie o północy. Aby szyfr był bardziej bezpieczny, wiadomość została zapisana w liniach o stałej długości, a pary liter, które mają być zaszyfrowane, zostały wybrane w pionie, tak aby, jeśli długość linii wynosiła 17, powiedzmy, że litery są szyfrowane, to 17 w oryginalny tekst jawny. Litera X była używana jako separator słów i, jeśli to konieczne, aby tekst był równomierny. Ponieważ litery pary zwykłego tekstu używały dwóch różnych kwadratów, nie było

potrzeby wstawiania fałszywych liter między powtarzającymi się literami. System jest zilustrowany przez

Przykład 5.7

Użyj kwadratów Playfair w Tabeli 5.6

G E U P M	K E O H S
S K R B T	C X U Z F
C Z N X H	M Q B R W
O Y D A W	T G P L Y
L F V I Q	I D N V A

zaszyfrować wiadomość

OURXSITUATIONXISXDESPERATEXSENDXSUPPLIESXATXONCE

na podstawie długości linii 11 znaków.

Szyfrowanie

Ponieważ wiadomość składa się z 48 znaków, będziemy mieli cztery wiersze po 11 i dwie linie po 2, dające 24 pary do zaszyfrowania:

OURXSITUATI
ONXISXDESPE
RATEXSENDXS
UPPLIESXATX
ON
CE

Pierwsza pionowa para to OO; litery te znajdują się w rogach prostokąta i są zastępowane odpowiednimi literami we własnych kolumnach:

GP. Druga pionowa para to ONZ; zastępuje je VO. Trzecia pionowa para to RX; nie znajdują się one w rogach prostokąta, ponieważ oba znajdują się w drugim rzędzie ich pól. Każda z nich jest więc zastępowana literą po prawej, dając BU jako parę szyfrów. Kontynuujemy w ten sposób i tworzymy tekst szyfrowania w 11-znakowym formacie liniowym:

GVBIGBQPPWP

POUMFDXOYUD

BWWYIGURVAK

ZLUHMXKQYMU

SU

TQ

(Weryfikacja jest pozostawiona ćwiczeniu dla czytelnika.) Zostaną one teraz przesłane, wiersz po wierszu w kolejności, jako grupy 5-literowe. Ostatnia grupa może, ale nie musi, być uzupełniona losowymi znakami:

GVBIG BQPPW PPOUM FDXOY UDBWW YIGUR VAKZL UHMXK QYMUS UTQ

Przykład pokazuje, że szyfrowanie jest dość pracochłonne, a niemieccy operatorzy szyfrujący często popełniali błędy, czasami używając niewłaściwych kwadratów, co doprowadziło do żądania powtórzeń, które znacznie pomogły kryptoanalitykom. W wiadomościach było też sporo standardowych zwrotów, a wiadomości były regularnie odczytywane.

Kody

Charakterystyka kodów

Jak wspomniano w części 1, rozróżnienie kodów i szyfrów nie zawsze jest jasne, ale można rzec rozsądnie, że podczas gdy większość kodów ma tendencję do bycia statycznymi, większość szyfrów jest dynamiczna. Znaczy to, że litera lub fraza zakodowana za pomocą kodu generuje ten sam szyfr za każdym razem, gdy kod jest używany, podczas gdy litera lub fraza zakodowana przez system szyfrowania generalnie generuje inny tekst szyfrowania w różnym czasie. Dzieje się tak dlatego, że większość systemów szyfrowania zawiera jeden lub więcej parametrów, takich jak słowa kluczowe lub, jak zobaczymy później, ustawienia kół, które zmieniają się w regularnych lub nieregularnych odstępach czasu, a zatem powodują, że wyjścia szyfrów z tego samego tekstu jawnego są różne. Podstawowy mechanizm lub algorytm generowania szyfru nie zmienia się, ale parametry się zmieniają. Zasadniczo kod nie ma takich parametrów, chociaż sam cały kod może zostać zmieniony, w takim przypadku staje się innym kodem. W praktyce jest to osiągane przez wydawanie nowego kodu książki co jakiś czas. Używając tego kryterium, szyfr Juliusza Cezara został zaklasyfikowany jako kod, ponieważ szyfrowanie stałej litery w wielu wiadomościach jest niezmiennie takie same. Możemy jednak powiedzieć, że istnieje parametr związany z szyframi Juliusza Cezara, a mianowicie przesunięcie, które daje nam 25 różnych szyfrów i jeśli wartość przesunięcia jest w jakiś sposób włączona do komunikatu, tj. W wskaźniku, system Juliusza Cezara. można rozsądnie uznać za szyfr, a nie za kod.

Przykład 6.1

Chociaż istnieje wiele wcześniejszych przykładów kodów opracowanych przez Samuela Morse'a (1791-1872) w 1832 roku w celu przesyłania wiadomości telegraficznie, jest prawdopodobnie najbardziej znanym. W tym kodzie litery alfabetu są reprezentowane przez maksymalnie cztery "kropki" i "kreski", cyfry od 0 do 9 na pięć i niektóre symbole interpunkcyjne przez sześć. Aby przesłać kropkę klucz telegraficzny jest wciśnięty przez około jedną 24 sekundy; dla kreski klucz jest wciśnięty na około jedną ósmą sekundy; odstęp między składnikami litery jest taki sam jak dla kropki i interwału między literami jest równa tej dla myślnika. Kod Morse'a został zaprojektowany w taki sposób, że najczęstsze litery w języku angielskim miały krótszy czas transmisji niż litery rzadsze. W ten sposób E było reprezentowane przez pojedynczą kropkę i T pojedynczym kreskowaniem, podczas gdy J wymagało czterech symboli, kreski kreski kreski. Powodem tego była próba zminimalizowania czasu potrzebnego na przesłanie wiadomości. Międzynarodowa bezprzewodowa wersja liter alfabetu Morse'a jest pokazana w tabeli 6.1.

A ·—	E ·	I ··	M ——	Q ——·—	U ··—	Y —·——
B —···	F ··—·	J ·———	N —·	R ·—·	V ···—	Z ——··
C —·—·	G ——·	K —·—	O ———	S ···	W ·——	
D —··	H ····	L ·—··	P ·——·	T —	X —··—	

Kod Morse'a nie był oczywiście zaprojektowany w celu ochrony tajemnicy wiadomości, lecz jedynie w celu zapewnienia skutecznego jej przekazywania. Dobry operator bezprzewodowy korzystający z tego kodu byłby w stanie przesłać około 30 słów na minutę. Jak wspomniano w rozdziale 1, istnieją inne kody, które mają na celu zapewnienie dokładności komunikatów lub danych, a nie zachowanie tajemnicy ich zawartości. Do takich kodów należą te wykorzystywane do przesyłania danych ze statku kosmicznego lub do przechowywania danych w formie czytelnej komputerowo. Jeśli tajemnica nie jest potrzebna, szczegóły kodu będą zazwyczaj dostępne dla każdego, kto ich potrzebuje. Jeśli wymagana jest poufność i dokładność, dane mogą nie być upublicznione i zastosowana zostanie również pewna forma szyfrowania danych.

Kod jednoczęściowy i dwuczęściowy

Większość kodów wymaga użycia książki kodów, która może zawierać tysiące grup kodu. Kod używany przez wojsko zazwyczaj reprezentuje litery, cyfry lub frazy według grup kodów składających się z czterech lub pięciu liter lub cyfr. Nie jest konieczne, aby wszystkie grupy kodów zawierały tę samą liczbę symboli; słynny telegram Zimmermanna ze stycznia 1917 r., który został odczytany przez brytyjskich kryptoanalityków i który był głównym czynnikiem decyzji Ameryki o przystąpieniu do wojny, miał mieszankę grup kodowych złożonych z czterech i pięciu cyfr [6.1]. Główną zaletą kodu jest to, że może on dostarczać wiele grup kodu; do 10 tysięcy za czterocyfrowy kod i prawie 12 milionów na pięcioliterowy kod. Wadą jest to, że (i) konieczne jest posiadanie przez użytkowników książki kodów wraz z nimi oraz (ii) jeśli wróg zdobędzie kopię książki, poprzez przechwycenie lub złamanie kodu, odczytanie przyszłych wiadomości jest proste. Z tych powodów kody są częściej stosowane przez ambasady lub duże jednostki wojskowe, takie jak statki, niż przez osoby prywatne. Łamanie kodu jest znacznie łatwiejsze, jeśli kod jest jednoczęściowym kodem, co oznacza, że ten sam kodeks jest używany zarówno do szyfrowania, jak i rozszyfrowywania. Jeśli tak jest, grupy kodu dla słów lub fraz, które znajdują się w słowniku, będą blisko siebie nawzajem numerycznie. Zatem część czterocyfrowego, jednoczęściowego słownika może wyglądać tak, jak w Tabeli 6.2.

A	0001
ABLE	0013
AFTER	0023
AM	0051
AN	0075
AND	0078
ANY	0081
AS	0083
ASK	0091
AT	0097

Nie wszystkie z 10 tysięcy możliwych grup kodów byłyby zwykle używane. Prawdopodobnie pozostaną luki, które pozwolą na późniejsze wstawienie innych słów lub fraz. Z kryptograficznego punktu widzenia jednoczęściowy kod oferuje zbyt wielką przewagę kryptoanalitykowi, umożliwiając mu odgadnięcie znaczenia jeszcze niezidentyfikowanych grup kodu, po prostu przez wyszukiwanie prawdopodobnych słów w słowniku, który jest bliski zidentyfikowanym słowom. Ta słabość może być usunięta przez uczynienie uporządkowania liczbowego grup kodowych niezwiązanych z alfabetyczną lub numeryczną kolejnością słów kodowych. Następnie mamy dwuczęściowy kod, a użytkownicy potrzebują dwóch książek kodowych, jednego do szyfrowania i jednego do rozszyfrowania. Powyższe słowa kodowe mogą pojawić się w Tabeli 6.3 w księdze szyfrowania

A	5832
ABLE	2418
AFTER	6941
AM	9075
AN	6948
AND	4729
ANY	8532
AS	4271
ASK	2163
AT	1894

, podczas gdy książka do rozszyfrowania może zacząć się jak w Tabeli 6.4 i tak dalej.

0005	TOMORROW
0009	ATTACK
0014	COME

We wszystkich przypadkach jest prawdopodobne, że bardzo powszechne słowa kodowe byłyby przydzielane więcej niż jednej grupie kodowej, a użytkownicy byliby poinstruowani, aby stosować każdą z alternatyw w sposób "losowy". Chociaż kody, które nie zostały poddane dalszej encyklopedii, nie oferują wysokiego poziomu bezpieczeństwa, z którego korzystano w czasie wojny; włoska marynarka wojenna użyła jednoczęściowego kodu, znanego jako Mengarini, dla niektórych wiadomości o bardzo niskiej jakości, a japońska marynarka wojenna używała dwuczęściowego kodu, znanego im jako OTSU i dla Brytyjczyków jako JN4, podczas II wojny światowej. Nieco inny kod przy użyciu dwóch liter, po których następowały cztery cyfry, był używany przez U-Booty niemieckiej marynarki wojennej do zgłaszania swoich pozycji na Atlantyku i otrzymywania instrukcji atakowania konwojów aliantów. Litery zostały poddane tabelom podstawienia digografu, a cyfry mogły zostać zmodyfikowane.

Kod plus dodatek

Bez względu na to, ile grup kodu zawiera kod, kryptoanalityk, mając wystarczającą liczbę komunikatów, może w końcu znaleźć pewne grupy występujące więcej niż raz, nawet jeśli to samo zwykłe słowo lub wyrażenie ma przypisanych kilka alternatywnych grup kodowych. Ponadto, jeśli kod zostanie przechwycony przez wroga, odszyfrowanie wszystkich wiadomości stanie się banalne. Aby przezwyciężyć te słabości, same grupy kodów są zwykle szyfrowane. Standardowym sposobem wykonania tej czynności jest zastosowanie klucza addytywnego do grup kodów za pomocą nienośnego lub modułowego dodawania. Chociaż to zostało wspomniane wcześniej, aby przypomnieć sobie, jak to się robi, spójrzmy na przykład. Załóżmy, że mamy grupę kodową 6394 i że kluczem do niej jest 2798; następnie grupa kodów jest zapisywana, a klucz umieszczony bezpośrednio pod nią i odpowiadające cyfry są dodawane bez przenoszenia, więc kiedy dodamy ostatnie cyfry kodu i klucza, 4 i 8, suma jest zapisana jako 2, a nie 12 (że to: dodajemy cyfrę po cyfrze (mod 10)). Więc mamy

Grupa kodowa 6394

Klucz 2798

Suma 8082

a tekst zaszyfrowany to 8082. Klucz nie byłby taki sam dla innych grup, ponieważ w praktyce klucz albo nie powtórzyłby się w ogóle, albo, gdyby się powtórzył, zrobiłby to tylko po wielu cyfrach. Ponieważ szyfrowanie polega na dodaniu klucza do grup kodów, osoba odbierająca komunikat musiałaby odjąć cyfrę klucza po cyfrze (mod 10) od szyfru, aby odzyskać grupy kodów i odszyfrować komunikat; a zatem:

Szyfr 8082

Klucz 2798

Grupa kodowa 6394

Oczywiście grupy kodów są teraz zamaskowane, a bezpieczeństwo systemu jest znacznie zwiększone, pod warunkiem, że klucz nie będzie powtarzany przez wystarczająco długi okres. Kwestia tego, jak wytworzyć ciągi cyfr, które nie powtarzają się aż wiele tysięcy zostało wygenerowane, jest jednym z istotnych zainteresowań matematyków i kryptografów, i rozważamy go pełniej w części 8. W

międzyczasie, w celach ilustracyjnych, tutaj jest bardzo prostą metodą, która generuje sekwencję, która powtarza się po 60 cyfrach.

Przykład 6.2

Wygeneruj sekwencję cyfr (mod 10) rozpoczynając od cyfr 3 i 7 i tworząc każdą nową cyfrę, dodając dwie poprzednie cyfry (mod 10).

Rozwiązanie

Rozpocznie się sekwencja

3 7

więc następna cyfra to (3 + 7) = 10, która wynosi 0 (mod 10), a czwarta cyfra to (7 + 0) = 7, a więc piąta cyfra to (0 + 7) = 7. Kontynuując w ten sposób, stwierdzamy, że wygenerowana sekwencja jest

3 7 0 7 7 4 1 5 6 1 7 8 5 3 8 1 9 0 9 9 8 7 5 2 7 9 6 5 1 6 7 3 0 3 3 6 9 5 4

9 3 2 5 7 2 9 1 0 1 1 2 3 5 8 3 1 4 5 9 4, 3, 7, 0 ...

a sekwencja zaczyna się powtarzać po 60 cyfrach, jak wskazuje podkreślenie 3 ostatnich cyfr, które są takie same jak pierwsze 3. Ponieważ każda cyfra jest sumą (mod 10) z poprzednich 2, klawisz zacznie się powtarzać gdy wystąpią 2 cyfry, które już wystąpiły w tej samej kolejności we wcześniejszej kolejności. Wynika z tego, że jakakolwiek wygenerowana sekwencja (mod 10) w ten sposób nie może mieć okresu dłuższego niż 100, ponieważ istnieje tylko 100 par cyfr (mod 10). Sekwencja przykładu, z okresem 60, jest najdłuższą dostępną sekwencją w tym przypadku. Gdybyśmy zaczęli od pierwszych dwóch terminów równych 0, wytworzylibyśmy sekwencję zerową, która, jeśli była używana jako klucz, pozostawiłaby niezmienione grupy kodu. Chociaż jest to najdłuższy dostępny w tej prostej metodzie, kluczowa sekwencja przykładu ma niestety pewne właściwości liczbowe, które czynią go niepożądanym z kryptograficznego punktu widzenia. Szczególnie źle jest, że dwie trzecie cyfr jest nieparzystych, a tylko jedna trzecia jest parzysta, a nie w przybliżeniu jednakowa liczba każdego z nich. Dzieje się tak dlatego, że sekwencja ma bardzo prosty wzór nieparzysty, jak widać od razu, mianowicie:

nieparzyste, nieparzyste, parzyste nieparzyste, nieparzyste parzyste ...

Inną właściwością jest to, że podwójne cyfry (77, 99, 33 i 11) występują regularnie, w odstępie 15 miejsc. Ta szczególna sekwencja jest bardzo dobrze znana i jest szczególnym przypadkiem prawdopodobnie najintensywniej badanej sekwencji w matematyce. Zwykła jego forma zaczyna się od 0 i 1 jako pierwszych 2 wartości i jest kontynuowana jak w przykładzie, ale bez redukcji (mod 10), tj. Terminy są dodawane normalnie. Następnie rozpoczyna się sekwencja

0 1 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597 ...

Terminy rosną w ogromnym tempie (wyrażenie matematyczne polega na tym, że rosną "wykładniczo"); każdy termin po piątym jest więcej niż 1,5 razy większy niż jego poprzednik, a więc na przykład 100. termin w sekwencji zawiera 21 cyfr. Jeśli zredukujemy wszystkie te liczby (mod 10), które są takie same, jak zastąpienie każdej z nich ostatnią cyfrą, otrzymamy

0 1 1 2 3 5 8 3 1 4 5 9 4 3 7 0 7 7 ...

który jest taki sam jak sekwencja w przykładzie, ale zaczyna się od pozycji 48.

Początek sekwencji 0 1 1 ... jest znany jako sekwencja Fibonacciego; został wprowadzony do matematyki przez Leonardo z Pizy, znany również jako Fibonacci, w trzynastym wieku. Aby uzyskać więcej informacji na temat tej słynnej sekwencji zobacz M5.

Problem 6.1

(1) Wygeneruj klucz (mod 10) jak wyżej, ale zaczynając od 0 i 2 jako pierwsze 2 warunki. Jaki jest okres i dlaczego ten klucz zostanie odrzucony przez kryptografa?

(2) Jaki jest okres, w którym zaczynamy od 1 i 3 jako pierwszych 2 terminów?

Sekwencja Fibonacciego jest najprostszą z klas sekwencji, która może być użyta do generowania kluczy do użycia w kryptografii, chociaż czy jakakolwiek konkretna sekwencja dostarcza "dobrych" kluczy, w tym, że wszystkie możliwe kluczowe wartości są równie prawdopodobne, jest pytanie, na które można odpowiedzieć tylko za pomocą zaawansowanej matematyki. Dość oczywiste uogólnienie sekwencji Fibonacciego uzyskuje się przez utworzenie każdego nowego terminu przez dodanie (mod 10) 3 poprzednich terminów, które mogą wytwarzać sekwencje dłuższej długości cyklu, a więc:

Przykład 6.3

Zaczynając od 0, 1, 1 jako pierwsze 3 warunki generują uzyskaną sekwencję (mod 10) przez dodanie razem poprzednich 3 terminów na każdym etapie.

Rozwiązanie

Sekwencja rozpoczyna się od 0 1 1 2 4 7 3 4 4 1 ... i powtarza po 124 terminach. Częstotliwości poszczególnych cyfr są nieco niejednolite; każdy powinien wystąpić 12 lub 13 razy, ale 3 występuje tylko 6 razy, podczas gdy 4 i 9 oba występują 18 razy. Weryfikację tych faktów pozostawia się czytelnikowi. Jeśli wybierzemy trzy różne terminy rozpoczęcia sekwencji, możemy uzyskać krótsze długości cyklu: 0, 1, 2 daje cykl o długości 62, podczas gdy 0, 5, 0 byłoby bardzo złym wyborem, ponieważ generuje sekwencję długości cyklu zaledwie 2 Ta metoda może być używana do generowania kluczy do dowolnego modułu. Na przykład sekwencja rozpoczynająca się od 0, 1, 1 do modułów 2, 3, 5 i 7 powoduje utworzenie cykli długość odpowiednio 4, 13, 31 i 48. Z czysto matematycznego punktu widzenia jest to interesujące, ale ogólnie rzecz biorąc, kryptolodzy prawdopodobnie zastosują 2, 10 lub 100 jako moduł. Jeśli wygenerujemy tę samą sekwencję (mod 100), rozpocznie się

00 01 01 02 04 07 13 24 44 81 49 74 ...

i stwierdzono, że powtórzy się po 1240 terminach. Możliwa jest modyfikacja sekwencji Fibonacciego, aby stosunek liczby nieparzystej był nieco mniejszy, co czyni go nieco lepszym do szyfrowania. Skromny krok w tym kierunku pokazuje:

Przykład 6.4

Wygeneruj 20 terminów sekwencji Fibonacciego (mod 100) zaczynając od 13 i 21 jako pierwszych 2 terminów, a następnie zamień drugą i trzecią cyfrę w każdej grupie czterech, aby uzyskać 20 terminów dwucyfrowego strumienia klucza.

Rozwiązanie

Pierwsze 20 terminów sekwencji Fibonacciego (mod 100) rozpoczynających się od 13 i 21 to

13 21 34 55 89 44 33 77 10 87 97 84 81 65 46 11 57 68 25 93

Wymieniamy drugą i trzecią cyfrę w każdej grupie czterech -

12 31 35 45 84 94 37 37 18 07 98 74 86 15 41 61 56 78 29 53

- i to jest wypadkowy klucz. Obciążenie liczb nieparzystych: parzyste zostało teraz zmniejszone (z 2: 1 do około 7: 5), a klucz, choć nadal niezadowalający, jest na to silniejszy.

Problem 6.2

Dwucyfrowy kod przedstawia litery alfabetu w następujący sposób:

A = 17, B = 20, C = 23, ..., Z = 92,

każda liczba jest o 3 większa niż poprzednia. Następnie wiadomość jest szyfrowana za pomocą tego kodu i klucza dodatku (12 31 35 ...) uzyskanego w powyższym przykładzie, przy czym dodanie jest cyfra po cyfrze bez przenoszenia. Wynikowy tekst szyfrowania jest

86 69 42 19 60 35 08 13 76 48 23 02 50 91. Odszyfrować wiadomość.

Szyfry dla szpiegów

Szpieg działający w kraju X w imieniu kraju ma problem z komunikowaniem się ze swoim kontrolerem w taki sposób, aby chronić zarówno siebie, jak i zawartość swoich wiadomości. Pomysł na wysłanie jego wiadomości będzie musiał być "zmodyfikowany", tak aby ich prawdziwe znaczenie jest ukryte przed kimkolwiek, prócz zamierzonego odbiorcy. Istnieją metody, takie jak użycie mikrodots lub "niewidzialnego" atramentu, które same w sobie nie zawierają szyfrowania, chociaż niektóre "zmiany" tekstu nawet w takich przypadkach prawdopodobnie zostaną wykorzystane w celu zapewnienia dodatkowego bezpieczeństwa. Kiedy mówimy, że tekst został "zmodyfikowany", niekoniecznie oznacza to, że został on zaszyfrowany, ale że "tajny" tekst nie jest po prostu wysyłany w niezmienionej formie: może na przykład być ukryty w pozornie nieszkodliwym komunikacie . Ukrywanie tajnego tekstu wewnątrz niewinnego ma tę zaletę, że będąc najwyraźniej nieuporządkowanym, nie przyciąga automatycznie zainteresowania niezamierzonych odbiorców ani przechwytywaczy, takich jak siły bezpieczeństwa państwa X. Wadą jest to, że nie może być zbyt łatwo skonstruować realistyczny nie-tajny tekst, w którym można go osadzić. Oto prosta ilustracja.

Przykład 7.1 ("Część listu od Agenta 63")

Kiedy wczoraj rano szedłem przez centrum miasta około jedenastej trzydzieści, zobaczyłem Rona Kingstona. Był sam, prowadząc nowatorski samochód ultramaryny, Ford Escort. Wcześniej miał tylko samochody używane, nierzadko nie mniej niż trzy lata. Być może miał dziedzictwo od jakiegoś bogatego krewnego, który niedawno zmarł?

Tajna wiadomość

Jeśli weźmiemy pierwszą literę wiadomości i pierwszą literę co czwartego słowa po tym, przyjmując słowa dzielone jako dwa oddzielne słowa, otrzymamy

ATTACKDUEONTHIRD

Szyfry szablonowe

Powyższy przykład to bardzo prosty i niezabezpieczony przypadek szyfrowania szablonowego. W takim szyfrowaniu niektóre litery na stronie są częścią tajnej wiadomości, a wszystkie pozostałe litery są jedynie "wypełniaczami", które są używane do komponowania przyziemnej komunikacji. "Wzornik" w tym przykładzie jest zbyt regularny, by był zadowalający; bardziej odpowiedni szablon użyłby liter, które są oddzielone od siebie nieregularnymi odstępami i które niekoniecznie są pierwszymi literami słów. Aby zwiększyć bezpieczeństwo, litery tajnego tekstu prawdopodobnie nie pojawiłyby się w poprawnej kolejności w całym tekście. Jeśli cały tekst jest wpisany w zwykłym formacie, nadawca i odbiorca mogą mieć identyczne karty z otworami w nich umieszczonymi na pozycjach liter tajnej wiadomości. Stąd nazwa tego typu szyfru. Każda dziura miałaby pod spodem numer, podając pozycję odpowiadającej jej litery w wiadomości. Szyfr taki byłby trudniejszy do rozwiązania, gdyby ten sam szablon nie był wielokrotnie używany. W takim przypadku, biorąc pod uwagę wystarczającą liczbę komunikatów, może się zdarzyć, że kryptoanalityk odzyska część matrycy, a następnie stopniowo odzyska resztę. Jeśli jednak szablon zmieniał się regularnie, byłoby bardzo trudno, jeśli nie niemożliwe bez dodatkowych informacji, rozwiązać system. Aby zorientować się w trudności, rozważ to.

Tekst wiadomości:

```
Some of Shakespeare's plays such as
     10     6                  8   1
Anthony and Cleopatra are performed
  2      11    9   3         15     7
less frequently than others, Macbeth
            12     4            5   13
King Lear and Hamlet, in particular.
 14          16
```

Liczby pokazują miejsca, w których zostały umieszczone otwory w szablonie i określają kolejność, w jakiej mają być odczytane widoczne litery; tam, gdzie potrzebna jest dwucyfrowa liczba, litera powyżej pierwszej cyfry to ta, w której występuje dziura; litera została podkreślona dla jasności, chociaż oczywiście nie zostałaby podkreślona w przesłanej wiadomości! W ten sposób komunikat czyta, po wstawieniu spacji,

ATTACK DUE ON THIRD

jak wcześniej.

Jeśli szablon zostanie użyty kilka razy, możliwe, że kryptoanalityk odkryje, gdzie są rozmieszczone dziury, w jakiej kolejności są one używane, ale zależy to od tego, czy są dostępne jakieś prawdopodobne frazy lub słowa w tekście otwartym oraz na liczbie i długości wiadomości. Jeśli szablon został zmieniony po każdej stronie, odczytanie wiadomości byłoby niemożliwe, chyba że istniał jakiś związek między składem szablonu wiadomości a jego następcą, ponieważ nie znając szablonu wiele możliwych komunikatów można znaleźć na stronie, jak to ilustruje

Problem 7.1

Sprawdź, czy w tekście powyższego przykładu znajdują się wszystkie oprócz jednego z poniższych komunikatów, a więc są "możliwe rozwiązania" z odpowiednim szablonem:

(1) MERRY CHRISTMAS;

(2) COME AT ONCE;

(3) GO AWAY QUICKLY;

(4) THE AUTHOR OF OTHELLO IS BACON.

W tekście można znaleźć setki innych "możliwych rozwiązań", ponieważ zawiera on ponad sto liter, a dowolny anagram dowolnego podzbioru można wybrać za pomocą odpowiedniego szablonu. Bez dodatkowych informacji, na przykład, że szablon nie będzie miał więcej niż jedną dziurę w żadnym rzędzie lub kolumnie, taki komunikat jest "nie do złamania", ponieważ wiele rozwiązań jest możliwych. Ta sama sytuacja może dotyczyć innego szyfru systemu, w których dostępny jest niewystarczający materiał, aby zapewnić unikalne rozwiązanie. Nawet prosty system zastępowania jest nie do złamania, jeśli jest używany tylko raz dla pojedynczej krótkiej wiadomości. W skrajnym przypadku "jednorazowej podkładki" system jest niezniszczalny, niezależnie od tego, ile wiadomości o dowolnej długości zostanie wysłanych, jak zobaczymy później. Jeżeli ten sam system (proste zastąpienie, przeniesienie, szablon) zostanie użyty więcej niż jeden raz, może przestać być "nierozerwalny"; nawet "jednorazowa podkładka" może stracić swoje bezpieczeństwo, jeśli ta sama podkładka zostanie użyta dwukrotnie.

Szyfrowanie książek

Szpieg musi unikać wzbudzania podejrzeń, a więc każdy sprzęt szyfrujący, który ma w swoim domu, nie może być oczywisty. Nawet pojedynczy szablon może wydawać się podejrzany badaczowi, a stos szablonów może być obciążający. Podobnie szpieg byłby mało prawdopodobny do użycia kodu, jeśli oznaczałoby to posiadanie dużego kodu w domu. Szyfr, który nie wymaga żadnych nietypowych urządzeń, jest zatem bardzo atrakcyjną propozycją, jeśli chodzi o szpiega, a szyfr książki jest właśnie taki; wszystko, co jest wymagane, to książka na dowolny temat, który nie zawiera znaków alfabetu innych niż łacińskie. Książka może na przykład być powieścią angielską lub biografią lub dziełem historycznym, ale prawdopodobnie nie zajmuje się chemią organiczną.

Korzystanie z szyfrowania książek

Aby użyć szyfrowania książki, konieczne jest umożliwienie "dodawania i odejmowania" par liter alfabetu. Odbywa się to, jak wyjaśniono w rozdziale 1, poprzez numerowanie liter alfabetu A = 0, B = 1, C = 2, ..., Z = 25 i dodawanie lub odejmowanie (mod 26) i ponowne przekształcanie odpowiedzi do liter. Ponieważ jest to żmudny proces, lepiej tworzyć tabele raz na zawsze i sprawdzić wynik dodania lub odjęcia w odpowiedniej tabeli, ale aby pokazać, jak to zrobić bez takich tabel, pozwól nam przeprowadzić proces na kilku listy.

Przykład 7.3

Konwertuj alfabet na cyfry zaczynające się od A = 0, B = 1 itd. Następnie "dodaj" razem dwa poniższe teksty (mod 26) i ponownie przekonwertuj wynikowe liczby na litery.

Tekst 1 THEXCURFEWXTOLLSX

Tekst 2 ONCEXUPONXAXTIMEX

Rozwiązanie

Powtarzamy tabelę 1.1 jako tabelę 7.1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Najpierw konwertujemy teksty na liczby za pomocą tabeli:

Text 1	T	H	E	X	C	U	R	F	E	W	X	T	O	L	L	S	X
	19	7	4	23	2	20	17	5	4	22	23	19	14	11	11	18	23
Text 2	O	N	C	E	X	U	P	O	N	X	A	X	T	I	M	E	X
	14	13	2	4	23	20	15	14	13	23	0	23	19	8	12	4	23

Teraz dodajemy je, a następnie redukujemy (mod 26):

	19	7	4	23	2	20	17	5	4	22	23	19	14	11	11	18	23
	14	13	2	4	23	20	15	14	13	23	0	23	19	8	12	4	23
Sum:	33	20	6	27	25	40	32	19	17	45	23	42	33	19	23	22	46
(mod 26):	7	20	6	1	25	14	6	19	17	19	23	16	7	19	23	22	20

Na koniec przeliczamy liczby z powrotem na litery, używając tabeli:

H U G B Z O G T R T X Q H T X W U

i to jest tekst szyfru, który zostanie wysłany. Odbiorca oczywiście musiałby odjąć Text 2 od szyfru (mod 26), aby odzyskać Text 1, a mianowicie:

Szyfr	H	U	G	B	Z	O	G	T	R	T	X	Q	H	T	X	W	U
Teskt 2	O	N	C	E	X	U	P	O	N	X	A	X	T	I	M	E	X
Konwersja	7	20	6	1	25	14	6	19	17	19	23	16	7	19	23	22	20
	14	13	2	4	23	20	15	14	13	23	0	23	19	8	12	4	23

Odejmij (mod 26), tj. Jeśli wynik jest ujemny, dodaj 26:

19 7 4 23 2 20 17 5 4 22 23 19 14 11 11 18 23

Ponownie przekonwertuj na litery:

T H E X C U R F E W X T O L L S X

którym jest Tekst 1, oryginalna "wiadomość".

Oczywiście byłoby to bardzo nużącym i podatnym na błędy procesem przekształcanie tekstów na liczby, dodawanie ich, odejmowanie 26 w razie potrzeby i ponowne przekształcanie na listy za każdym razem, gdy wiadomość miała być szyfrowana, więc warto mieć dwie tabele, jedna do szyfrowania i jedna do rozszyfrowania, z której wynik zastosowania tych procesów można od razu odczytać. Doświadczeni użytkownicy nie potrzebują takich stołów, ponieważ wkrótce nauczą się "dodawać litery", ale dla innych tabele oszczędzają mnóstwo czasu i wysiłku. Są one podane w tabelach 7.2 i 7.3.

	Text 1																								
Text 2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

	Key text																								
Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
O	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
P	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
Q	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
R	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
S	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
T	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
V	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Zauważ, że w tabeli szyfrowania (tabela 7.2) nie ma znaczenia, czy wywołujemy tekst wiadomości "Tekst 1" i tekst kluczowy "Tekst 2", czy odwrotnie, ponieważ dodanie dwóch tekstów daje ten sam wynik w obu kierunkach ("dodanie jest komutatywny "jest to matematyczny zwrot do opisania tego), ale w tablicy deszyfrowania (tabela 7.3) szyfr i klucz muszą być poprawnie zidentyfikowane, ponieważ aby uzyskać tekst zwykły, musimy odjąć klucz od szyfru, a nie odwrotnie. Jest to widoczne, gdy przypomnimy sobie, że

tekst szyfrowany : szyfr = Klucz + Tekst

a więc

tekst odszyfrowany: tekst = klucz - szyfr

tam, gdzie dokonywane są dodatki i odejmowania (mod 26).

Problem 7.2

Wiadomość została zaszyfrowana przy użyciu szyfrowania książki. Używana była Księga Wierszy Ruperta Brooke, a kluczem do przesłania był początek fragmentu

STANDSXTHEXCHURCHXCLOCKXATXTENXTOXTHREE

Tekst szyfrowania to

LAEKV MPILG QZOUJ ZTLXP RZDLX EFOIE MHCIQ

Odszyfruj wiadomość.

Częstotliwości liter w szyfrach książki

Częstotliwości liter alfabetu w szyfrze wytwarzanym przez szyfr książki, gdy klucz jest fragmentem tekstu w języku angielskim, będą inne niż w języku nieuszkodzonego języka angielskiego. Chociaż z pewnością będzie prawdą, że niektóre litery, takie jak litery używane dla "przestrzeni", E i T, nie będą już występować znacznie częściej niż inne, takie jak Z lub J, prawdą jest również, że litery nie będą równie reprezentowane. Możliwe jest oszacowanie częstotliwości liter szyfrujących i stwierdzamy, że chociaż częstotliwości poszczególnych liter nie różnią się tak bardzo jak w próbkach normalnego (niefrasobliwego) angielskiego, to w dalszym ciągu nie są one jednakowe i obserwacja tego typu zmienności ostrzegłoby kryptoanalityka o możliwości użycia szyfrów książki. Odmianę tę można zobaczyć w tabeli 7.4.

	Frequency (per 1000)	
Letter	Normal English	Book cipher
A	64	31
B	14	30
C	27	29
D	35	55
E	100	40
F	20	32
G	14	39
H	42	46
I	63	34
J	3	26
K	6	36
L	35	37
M	20	45
N	56	38
O	56	28
P	17	26
Q	4	37
R	49	46
S	56	52
T	71	38
U	31	26
V	10	39
W	18	34
X	3	32
Y	18	25
Z	2	52
Space etc.	166	47

W lewej kolumnie znajdują się częstotliwości 26 liter alfabetu oraz 27. "litera", która obejmuje wszystkie znaki interpunkcyjne i "spacje", ponieważ występują one w typowej próbie normalnego języka angielskiego, a w prawej kolumna, częstotliwości tych samych liter, które według przewidywań pojawią się w fragmencie zakodowanym za pomocą szyfrów książkowych przy użyciu angielskich tekstów. Wielkość próby w obu przypadkach wynosi 1000, więc "przeciętnie" każda litera powinna wystąpić około 37 razy. Widać, że jest to bardzo dalekie od tego, co jest w nierozwiązanym tekście, a nawet w zaszyfrowanym tekście występuje znaczna zmienność częstotliwości, ale nie o wiele więcej, niż można by oczekiwać przypadkowo (dla dalszych komentarzy patrz M6) . Szyfr książki może być traktowany jako skrajny przypadek szyfru Vigenère, w którym długość klucza jest taka sama jak długość samej wiadomości . Najwyraźniej szyfr książki powinien być bezpieczniejszy niż Vigenère, ponieważ ten

drugi używa klucza o stałej długości. Alternatywą dla używania angielskiego tekstu jest użycie klawisza w innym języku, który używa alfabetu nie większego niż 26 liter. Znaki diakrytyczne, takie jak akcenty lub umlauty, byłyby ignorowane, gdyby użyto francuskiego lub niemieckiego. To by nieco utrudniło życie kryptoanalitykowi, dopóki nie zorientuje się, co się dzieje.

Rozwiązywanie szyfrów książek

Zakładając, że kryptoanalityk zdał sobie sprawę, że tekst szyfrowania jest wynikiem zaszyfrowania angielskiego tekstu z angielską książką używaną jako klucz, w jaki sposób mógłby spróbować rozwiązać ten problem? Chociaż częstotliwości liter w szyfrze mogły mu pomóc dojść do wniosku, że używany jest szyfr książkowy, poszczególne częstotliwości liter nie będą tak różne od przypadkowych, że będą one bardzo pomocne, ani dwuznaków itp. jednak atak, do którego jest podatny szyfr książki, można nazwać "przeciąganiem szopki". Załóżmy, że albo wiadomość, albo tekst klucza zawiera jakieś popularne angielskie słowo, takie jak THE. Zostało to dodane do 3 liter innego wyrazu angielskiego w drugim tekście, aby utworzyć 3 litery szyfru. Jeśli następnie spróbujemy odjąć THE od szyfru w każdej możliwej pozycji i spojrzeć na uzyskane trigrafy, możemy znaleźć prawdopodobne części angielskie, które możemy wtedy uzupełnić, dodając w ten sposób kilka kolejnych liter w drugim tekście, poprzedzającym lub śledząc. Można wypróbować inne popularne trigrafy, a więc oba teksty mogą się "rozwikłać", że tak powiem. Jeśli X jest użyty jako separator, możemy rozszerzyć THE na THEX, a może nawet na XTHEX, chociaż może to spowodować niepowodzenie podnieś słowo takie jak TAM. Nawet krótkie słowo, takie jak A, może być pomocne, jeśli występuje jako XAX. Jeśli w tekście kluczowym znajdą się jakieś nietypowe słowa, możliwe będzie wywnioskowanie rodzaju używanej książki, a nawet identyfikacja książki, co znacznie ułatwi późniejszy proces kryptoanalizy. W praktyce możemy początkowo odzyskać jedynie okazjonalne słowa lub części słów w dwóch tekstach, ale nawet częściowe odzyskiwanie może być przydatne, a kolejne wiadomości mogą dostarczyć dalszych użytecznych "łóżeczek". Jako wskazanie metody, w małej skali (tylko 50 liter):

Przykład 7.4

Następujące 10 grup zostało zaszyfrowanych za pomocą szyfru książek. Użyj techniki przeciągania szopki, aby spróbować odzyskać tekst klucza i wiadomości.

FLIQT NYQFK VACEH UCUAC MOXRG EYYQJ BNOEQ FJXUL ILREJ ATVQB

Wypróbowujemy niektóre popularne słowa, jak to tylko możliwe. Szopka jest najbardziej oczywista. Ściąganie łóżeczka jest niezaprzeczalnie nudne, ponieważ musimy wypróbować łóżeczko we wszystkich możliwych pozycjach tekstu szyfrowania. Ponieważ każda z liter, które wypróbujemy, T, H i E w tym przypadku, może wystąpić w innych łóżeczkach, możemy zaoszczędzić trochę wysiłku, jeśli najpierw zobaczymy, jaka będzie wynikowa zwykła litera, jeśli założymy, że T jest literą, która ma być odjąć od szyfru w każdej pozycji, a następnie, jeśli H jest literą, a na końcu, jeśli E jest literą. Jeśli teraz wypiszemy trzy powstałe strumienie "domniemanego tekstu jawnego" z pierwszą linią (odpowiadającą do T) przesunięcie dwóch miejsc w prawo, a druga linia (linia "H") przesunięcie o jedno miejsce w prawo w stosunku do trzeciej ("E"), wtedy wszelkie możliwe "słowa" pojawią się jako trzy litery w pionie linia; a zatem:

Cipher BHFLIQT NYQFK VACEH UCUAC MOXRG EYYQJ BNOEQ FJXUL ILREJ ATVQB

Tline BHMSPXA UFXMR CHJLO BJBHJ TVEYN LFFXQ IUVLX MQEBS PSYLQ HACXI

Hline HYEBJMG RJYDO TVXAN VNTVF HQKZX RRJCU GHXJY CQNEB EKXCT MOJUH

Eline BHEMPJU MBGRW YADQY QWYIK TNCAU UMFXJ KAMBF TQHEH NAFWP RMXHH

Istnieje kilka prawdopodobnych wyglądających trigrafii, takich jak

MEE na pozycji 1,

ROW w pozycji 10,

ONY na pozycji 15,

BEE na pozycji 39,

PEN na pozycji 41.

Teraz próbujemy rozszerzyć szopkę z THE na THEX, aby sprawdzić, czy tworzy prawdopodobny tetragram w którymkolwiek z tych pięciu przypadków. Wstawiamy X w pozycjach 4, 13, 18, 42 i 44; litery szyfrów w tych pozycjach to odpowiednio Q, C, U, L i L i odszyfrowujemy je przez "odjęcie" X od nich, co oznacza przesunięcie każdej z tych liter o trzy miejsca w przód w alfabecie, dając w ten sposób odszyfrowanie T , F, X, O i H, tak aby wytworzone tetroskopy były:

MEET na pozycji 1,

ROWF na pozycji 10,

ONYX na pozycji 15,

BEEO na pozycji 39,

PENH na pozycji 41.

Pierwsze z nich wygląda szczególnie obiecująco, więc natychmiast zbadamy to dalej, pozostawiając innych do analizy później. Ponieważ pierwsze "trafienie" THE znajdowało się na pozycji 1, badamy tekst zaszyfrowany bezpośrednio po pierwszych 10 pierwszych miejscach. To, co wstępnie mamy, to

Cipher FLIQT NYQFK

Text1 THEX.

Text2 MEET.

Pierwszym słowem w tekście 2 może być MEET, w którym to przypadku powinien następować znak X, jako separator, lub może to być dłuższe słowo, takie jak MEETINGX. W pierwszym przypadku piąta litera tekstu 1 byłaby W; w drugim przypadku litery 5, 6, 7 i 8 TEKSTU 1 to (TI), (NN), (YG) i (Q? X), tj. L, A, S i T, który wygląda wyjątkowo dobrze, ponieważ implikuje to

Rozpoczyna się tekst 1

THE LAST

Spodziewalibyśmy się, że po LAST nastąpi X, w którym to przypadku dziewiąta litera z Tekstu 2 byłaby (F? X), która jest I (moglibyśmy to również uzyskać, przeglądając Tabelę 7.3 (powyższa tabela rozszyfrowania) w punkcie gdzie wiersz F (rząd litery szyfrowej) przecina kolumnę X (kolumna założonej litery tekstu w tekście 1) Pierwsze 15 liter szyfru i częściowe teksty są następnie czytane

Cipher FLIQTNYQFKVACEH

Tekst1 THE LAST...

Tekst2 MEETING I.

Litera po I w tekście 2 najprawdopodobniej będzie N lub S, a w każdym przypadku litera po tym jest prawdopodobnie X. Odpowiadające litery w tekście 1 byłyby wtedy albo (KN) i (VX) albo (KS) i (VX), który jest albo XY albo SY. Ta ostatnia jest znacznie bardziej prawdopodobna, ponieważ pierwsza zakłada podwójną przestrzeń. Wstępnie akceptujemy SX w Text 2 i wynikowy SY w tekście 1, a nasze częściowe odszyfrowanie jest odczytywane

Cipher FLIQTNYQFKVACEH

Text1 THE LAST SY

Text2 MEETING IS ...

Naszym następnym zadaniem jest odkrycie, jaka litera podąża za SY w tekście 1. Nie ma zbyt wielu kandydatów, a B, L, M, N i S są najbardziej rozpowszechnione. Ponieważ literą cyfry w pozycji 12 jest A, odpowiednią literą w tekście 2 w tych pięciu przypadkach jest (AB), (AL), (AM), (AN) lub (AS), czyli Z, P, O, N lub I. Z tych tylko Z wygląda mało prawdopodobne, więc zwracamy naszą uwagę gdzie indziej, aby sprawdzić, czy możemy znaleźć dodatkowe wskazówki. Wracając do pięciu możliwych wystąpień THE widzimy, że potwierdziliśmy pierwszą (na pozycji 1) i wykluczyliśmy drugą (na pozycji 10), więc patrzymy na trzecią (w pozycji 15), która dałaby nam THEX w jednym tekst (nie możemy zdecydować od razu, w którym z dwóch tekstów występuje) i ONYX w drugim. Jeśli THEX występuje w pozycji 15, to X powinno znaleźć się w pozycji 14, a ponieważ literą szyfrowania jest E, litera poprzedzająca ONYX miałaby wtedy postać (EX), która jest H. Trzecim słowem w tekście 1 byłaby wówczas SY..HONY co silnie sugeruje, że jest to SYMPHONY. Jeśli tak jest, to od 12 do 13 liter szyfru A i C odpowiadają odpowiednie litery tekstu

2 to (A-M) i (C-P), tj. O i N, które wygląda obiecująco, a nasze odszyfrowanie jest odczytywane

Cipher FLIQTNYQFKVACEHUCUAC

Tekst1 THE LAST SYMPHONY ..

Text2 MEEtING IS ON THE ...

Zwracamy teraz uwagę na dwa pozostałe miejsca, w których wygląda na to, że THEX może znajdować się w jednym z tekstów, a mianowicie na pozycjach 39 i 41. Są one oczywiście niekompatybilne, ponieważ nakładają się, więc co najwyżej jedno z nich ma rację. Jest trochę więcej dostępnych dowodów, ponieważ jeśli obecne jest THEX, powinno być poprzedzone separatorem X. Odpowiednio odszyfrowujemy X w pozycjach 38 i 40, gdzie litery szyfru X i L, które dają A i O jako odpowiednie litery w postaci zwykłego tekstu i więc dajcie możliwe pentepsuły tekstu jawnego

ABEEO na 38 miejscu

OPENH na pozycji 40

Pierwsze z nich nie wygląda na prawdopodobne; druga wygląda lepiej, a ponieważ wspomina się o spotkaniu, jest całkiem możliwe, że miejsce jest nazwane. Nawet bez informacji dodatkowych, ponieważ COPENHAGEN pasuje do pentagrafu, warto spróbować. Próbujemy zatem C w pozycji 39 i A, G, E, N i X na pozycjach 45, 46, 47, 48 i 49, co daje następujące teksty dla pozycji 39 do 49:

Cipher ULILREJATVQ

Text1 S THE JUPIT

Tekst2 KOPENHAGA

Jest to bardzo przekonujące i daje nam dodatkowe informacje, ponieważ Jowisz jest imieniem ostatniej symfonii Mozarta i dlatego możemy spodziewać się, że jego imię pojawi się w tekście 1, gdzieś pomiędzy pozycjami 19 i 38. Ponadto słowo COPENHAGEN powinno poprzedzony separatorem, a więc wpisując literę szyfrowania X i literę tekstową, która jest również X w tym przypadku, otrzymujemy A w pozycji 38 tekstu 1, który czyta

Text1 .AS THE JUPITE

Ponieważ mamy do czynienia z ostatnią symfonią Mozarta, litera na pozycji 37 może być W, a na 36 to X. Zastąpienie ich w uzyskanym przez nas szyfrku dla pozycji od 36 do 49,

Cipher FJXULILREJATVQ

Text1 BYŁ JUPITEM

Text2 IN COPENHAGEN

Istnieje 50-szy litera szyfru, B, która powinna dać E w TEKST1 i "spacja" w TEKST2, i tak jest w przypadku, dodając dalsze potwierdzenie, jeśli to konieczne, do odszyfrowanych dotychczas. Słowo IN w tekście 2 powinno być poprzedzone spacją, więc odszyfrowujemy X w tym punkcie, w pozycji 35, gdzie literą szyfrowania jest Q, która tworzy T w tekście 1. Pełna sytuacja, w tym momencie jest taka, że mają odszyfrowane pozycje od 1 do 18 i pozycje od 35 do 50, dwie trzecie sumy, a szyfr i teksty są

```
FLIQTNYQFKVACEHUCUACMOXRGEYYQJBNOEQFJXULILREJATVQB
THE LAST SYMPHONY                  T WAS THE JUPITE
MEETING IS ON THE                   IN COPENHAGEN
```

W tekście 1 szukamy słowa MOZART, a T na pozycji 35 może być jego ostatnią literą, więc wypróbowujemy XMOZAR na pozycjach od 29 do 34, które dają TXNOON w tekście 2. T jest prawdopodobnie poprzedzone XA, które daje BY w TEKST1 na pozycjach 27 i 28, a nasze teksty są teraz czytane

```
FLIQTNYQFKVACEHUCUACMOXRGEYYQJBNOEQFJXULILREJATVQB
THE LAST SYMPHONY          BY MOZART WAS THE JUPITE
MEETING IS ON THE           AT NOON IN COPENHAGEN
```

Słowo BY powinno być poprzedzone przez X, które daje (E? X)? H w tekście 2, a ponieważ spodziewalibyśmy się terminu na to spotkanie, możemy rozsądnie wypróbować T jako litera przed H, która daje (G? T)? N w pozycja 25 w tekście 1. Istnieje teraz tylko 6 liter do odcyfrowania, aw TEKST2 są prawie pewne, że reprezentują liczbę, prawdopodobnie datę, która w swojej zwykłej postaci kończy się na TH. ELEVEN, z sześcioma literami, jest dobrym kandydatem i odejmuje te 6 liter od odpowiednich liter szyfru ACMOXR, produkuje WRITTE dla tekstu 1. Odszyfrowywanie jest teraz zakończone i odczytywane

```
FLIQTNYQFKVACEHUCUACMOXRGEYYQJBNOEQFJXULILREJATVQB
THE LAST SYMPHONY WRITTEN BY MOZART WAS THE JUPITE
MEETING IS ON THE ELEVENTH AT NOON IN COPENHAGEN
```

Kryptoanalityk nie tylko odszyfrował wiadomość, ale także odkrył, że książka, która jest używana jako klucz, jest prawdopodobnie książką o muzyce lub o Mozarcie, a to może być przydatne przy odszyfrowywaniu późniejszych wiadomości. Ten przykład, choć krótki i prosty, ilustruje, w jaki sposób

kryptoanalityk potrzebuje połączenia umiejętności analitycznych i językowych, wiedzy ogólnej, wyobraźni i szczęścia, aby osiągnąć sukces. Ponadto, nie zapominaj, że najpierw musiałby sobie uświadomić, że wiadomość została zakodowana za pomocą książki jako klucza, co nie jest od razu widoczne.

Wskaźniki

Zostały one już wspomniane w rozdziale 3, ale są wystarczająco ważne, aby można je było wymienić, ponieważ dostarczenie wskaźnika może okazać się piętą achillesową jakiegokolwiek układu szyfrów. Kiedy używany jest szyfr książkowy, nadawca musi poinformować odbiorcę, w którym wierszu na której stronie księgi klucza rozpoczyna szyfrowanie. Jeśli, na przykład, zaczyna od wiersza 15 na stronie 216, może poprzedzić wiadomość numerem 15216. Jest to jednak zbyt oczywiste, a on byłby bardziej skłonny do ukrycia tego. Istnieje wiele sposobów na zrobienie tego, na przykład:

(1) transponowanie cyfr zgodnie z uzgodnioną regułą, aby 15216 stało się, powiedzmy, 65121;

(2) dodanie uzgodnionego numeru, na przykład 59382, cyfra po cyfrze, co daje 64598;

(3) konwersję cyfr wskaźnika na litery i ukrycie wynikowej grupy pięciu liter w uzgodnionym miejscu w tekście szyfrowania wiadomości; w ten sposób 15216 staje się BFCBG;

(4) połączenie któregokolwiek z nich.

Dostarczenie wskaźnika nie jest oczywiście unikalne dla szyfrów książki; jest istotną częścią wielu systemów szyfrujących, ale podstawowa zasada jest taka sama: nadawca musi jakoś przekazać to do odbiorcy w taki sposób, aby utrudnić kryptoanalitykowi znalezienie go. Z drugiej strony, kryptoanalityk nadaje wysoki priorytet identyfikacji położenia wskaźnika i wykryciu jego metody szyfrowania.

Katastrofalne błędy w korzystaniu z szyfrów książek

Istotnym ryzykiem dla nadawcy komunikatu z szyfrem książki jest to, że jeśli popełni błąd i będzie musiał ponownie wysłać wiadomość, może udostępnić kryptoanalitykowi stosunkowo prostą trasę do odszyfrowania. Taki kluczowy błąd może wystąpić, jeśli nadawca wypisze literę z tekstu klucza książki, na przykład:

Przykład 7.5 (Szpieg popełnia błąd i oddaje grę)

Dwie wiadomości od tej samej osoby i identycznych wskaźników zostały wysłane w ciągu kilku godzin; teksty szyfrów były

ZECBH MOPJO IIUXJ ELFDR WRSJX CQ.

ZECSS HLIEL RVBCM CUAKA OLPBP PPP

Rozpoczynamy odszyfrowywanie przy założeniu, że ponieważ pierwsza wiadomość ma jedną literę mniejszą niż druga, nadawca pominął literę klucza książki w pierwszej wiadomości, a następnie ponownie poprawnie zaszyfrował tekst w drugiej wiadomości.

Początek rozwiązania

Ponieważ pierwsze trzy litery tekstu szyfrowania są takie same w obu przypadkach, zakładamy, że czwarta litera klucza książki nie została użyta w pierwszej wiadomości. Gdybyśmy wypróbowali wszystkie 26 możliwości dla tego listu w drugim komunikacie szyfrowania, uzyskalibyśmy 26 możliwości dla czwartej litery wiadomości i w każdym przypadku dałoby to nam piątą literę klucza księgi z pierwszego szyfru. message.With piątej litery klucza księgi odzyskalibyśmy piątą literę

wiadomości z drugiego komunikatu szyfrowego, co doprowadziłoby nas do szóstej litery klucza książki z pierwszego komunikatu szyfrowania; i tak dalej. Dzięki temu możemy rozwiązać zarówno klucz książki, jak i wiadomość od czwartej litery. Oczywiście początkowo musimy wypróbować wszystkie 26 możliwości czwartej kluczowej litery, ale szybko będziemy w stanie zobaczyć, która z nich była właściwa, gdy pojawił się klucz książki i teksty wiadomości. Aby zaoszczędzić czas i przestrzeń, po prostu przyjrzymy się temu, co się stanie, gdy wybierzemy właściwą literę, która jest F, jako czwartą literę klucza. Będziemy odnosić się do tekstów zaszyfrowanych jako CT1 i CT2; CT2 to poprawny tekst, a CT1 ma błąd. Litery tekstu jawnego można opracować bezpośrednio, jak pokazano poniżej lub przy użyciu tabeli 7.3.

Z CT2: (klucz szyfrowania) w pozycji 4 = litera zwykłego tekstu w pozycji 4; to znaczy

S-F = A= N.

Od CT1: (szyfr-zwykły) w pozycji 4 = litera w pozycji 5;

to znaczy

B-N = O.

Z CT2: (klucz szyfrowania) w pozycji 5 = litera zwykłego tekstu na pozycji

5; to znaczy

S- O= E.

Od CT1: (szyfr-zwykły) w pozycji 5 = kluczowa litera w pozycji 6;

to znaczy

H- E = D.

Z CT2: (klucz szyfrowania) w pozycji 6 = litera zwykłego tekstu na pozycji

6; to znaczy

H- D= E.

Od CT1: (szyfr-zwykły) w pozycji 6 = litera w pozycji 7;

to znaczy

M- E= I.

Z CT2: (klucz szyfrowania) w pozycji 7 = litera zwykłego tekstu na pozycji

7; to znaczy

POKRYWA.

Z CT1: (szyfr-zwykły) w pozycji 7 = litera w pozycji 8;

to znaczy

O- D?= L.

Z CT2: (klucz szyfrowania) w pozycji 8 = litera zwykłego tekstu na pozycji

8; to znaczy

I-L=X.

Patrząc na odzyskany klucz i teksty wiadomości do tej pory mamy

Klucz: ... F O D I L

Wiadomość ... N E E D X

Wygląda to dość obiecująco, więc:

Problem 7.3

Wypełnij rozwiązanie, które zostało uruchomione powyżej.

Szyfry "Garbo"

"Podwójny agent" Jean Pujol (nazwa kodowa garbo), Hiszpan, używał zarówno tajnych atramentów, jak i układów szyfrów podczas swojego pobytu w Anglii (1942-5). Atramenty i szyfry zostały dostarczone przez jego niemiecką "kontrolę" w Madrycie, który oczywiście nie wiedział, że garbo pracuje dla Brytyjczyków. W latach 1942 i 1943 garbo korzystało z prostego systemu substytucji opartego na 5 alfabetach, bardzo słabym systemie, który szybko rozwiązał każdy kompetentny kryptoanalityk. Być może zdając sobie z tego sprawę, w 1944 roku powiedziano mu, aby użył prostej podstawienia 5-literowego i podążał za nią z podwójną transpozycją, czyniąc szyfr bezpieczniejszym, ale nadal wrażliwym, jeśli wystarczająca ilość wiadomości zostały wysłane (tak jak były). Ponieważ Brytyjczycy znali system szyfrów i komponowali wiadomości z garbo, kryptoanalitycy i tak nie mieli nic do roboty.

Pierwszy szyfr Garbo

Wiadomość została napisana jako seria 5-literowych grup, które zostały zaszyfrowane przy użyciu 5 zastępczych alfabetów po kolei. Pierwsza litera każdej grupy została zastąpiona pierwszym alfabetem, druga litera w każdej grupie użyła drugiego alfabetu i tak dalej. Ten słaby system został nawet osłabiony przez fakt, że pierwszy alfabet substytucji był typu Juliusz Caesar, każda litera była przesuwana o 6 pozycji do przodu, a pozostałe alfabety nie były znacznie lepsze. Gdyby garbo naprawdę działało dla Niemców, jego szanse na pozostanie na wolności byłyby bardzo duże .

Drugi szyfr Garbo

Wiązało się to z podstawieniem 5-literowym, a następnie podwójną transpozycją. Alfabety zastępcze opierały się teraz na kwadracie 5,5. To samo w sobie było nawet słabsze niż użycie 5 niezależnych alfabetów, ale podwójna transpozycja znacznie poprawiła bezpieczeństwo. Kwadrat podstawienia 5x5 przedstawiono w Tabeli 7.5.

L	A	C	O	N
F	I	Z	E	G
B	R	T	D	H
J	M	P	Q	S
U	V	W	X	Y

Litera K nie pojawia się w kwadracie; wiadomości garbo były zwykle po hiszpańsku, a K prawie nigdy nie był potrzebny; jeśli to się zdarzyło, tak jak w Yorku czy Kidderminster, pozostało jako K. Wiadomość została ponownie napisana jako seria 5-literowych grup, a część zastępcza dla encyklopedii została przeprowadzona w następujący sposób:

(1) pierwsza litera każdej grupy została zastąpiona literą nad nią w polu;

(2) druga litera każdej grupy została zastąpiona literą po prawej stronie w polu;

(3) trzecia litera w każdej grupie została zastąpiona literą pod nią w polu;

(4) czwarta litera każdej grupy została zastąpiona literą po lewej stronie w polu;

(5) piąta litera każdej grupy pozostała niezmieniona.

Jak zwykle, dolny rząd tego pola był uważany za "powyżej" pierwszego, jeśli to konieczne, skrajnie lewy słup po prawej stronie prawej strony itd. Tak więc litera T szyfruje w 5 kolejnych pozycjach jako ZDPRT, a litera N jako YLGON, podczas gdy początek tekstu

STRON GXIND ICATI ONSXT

po tym pierwszym etapie pojawią się jako

HDMCN NYROD AOIRI XLYWT.

Zastosowano 31-dniową transpozycję. 31 liczb kolumn było w ustalonej, ale "losowej" kolejności. Tekst szyfrowania został zapisany w polu transpozycji w wierszach, przy czym pierwsza litera tekstu została umieszczona pod numerem kolumny odpowiadającym dniu miesiąca. Pierwsze i ostatnie wiersze zwykle zawierają mniej niż 31 liter, ale wiersze pośrednie będą "pełne". Ten tekst został odczytany kolumna po kolumnie zaczynając od kolumny o numerze 1 i kontynuując kolumny w kolejności numerowanej. Ten transponowany tekst szyfrowania został następnie zapisany w tym samym 31-wiecznym polu transpozycji, w którym pierwsza litera została umieszczona pod numerem kolumny odpowiadającym miesiącowi. Tekst ponownie odczytano kolumna po kolumnie zaczynając od kolumny o numerze 1 jak poprzednio. Ten podwójnie transponowany tekst został teraz napisany w 5-literowych grupach i przesłany. Aby zilustrować metodę szyfrowania za pomocą drugiego systemu garbo, modyfikujemy go tak, aby wykorzystał 12-dniową transpozycję i wykorzystał miesiąc transmisji do określenia kolumny początkowej na pierwszym etapie i dnia tygodnia (niedziela? 1) w celu określenia kolumna początkowa w drugim etapie.

Przykład 7.6

Zaszyfruj wiadomość

AGENTXFOURXREPORTSXTHATXCONVOYXLEFTXGLASGOWXTODAYX

używaj drugiego szyfru garbo z podstawieniem, jak wyżej i 12-dniową transpozycją

6 1 10 4 8 11 3 7 12 2 9 5

Data wiadomości to wtorek, 18 maja.

Szyfrowanie

Piszemy wiadomość w 5-literowych grupach:

AGENT XFOUR XREPO RTSXT HATXC ONVOY XLEFT GLASG OWXTO DAYXX

(na końcu dodano dodatkowe X, aby uzupełnić ostatnią grupę). Substytucja pole jest jak w tabeli 7.5. Podstawiony tekst, stosując powyższe zasady, jest zatem VFDOT QIEYR QTDMO IDYWT GCPWC XLACY QADGT NAIQG XXORO ECNWX

Klucz transpozycji to

6 1 10 4 8 11 3 7 12 2 9 5

a ponieważ miesiąc transmisji to maj, musimy rozpocząć wprowadzanie tekstu pod kolumną 5: patrz tabela 7.6.

6	1	10	4	8	11	3	7	12	2	9	5
											V
F	D	O	T	Q	I	E	Y	R	Q	T	D
M	O	I	D	Y	W	T	G	C	P	W	C
X	L	A	C	Y	Q	A	D	G	T	N	A
I	Q	G	X	X	O	R	O	E	C	N	W
X											

Tekst jest teraz usuwany kolumna po kolumnie zaczynając od kolumny o numerze 1:

DOLQQ PTCET ARTDC XVDCA WFMXI XYGDO QYYXT WNNOI AGIWQ ORCGE.

Teraz ponownie używamy pudełka transpozycji. Ponieważ dniem transmisji jest wtorek (data nie ma znaczenia w tej uproszczonej formie szyfru garbo), zaczynamy pisać tekst pod kolumną 3: patrz tabela 7.7.

6	1	10	4	8	11	3	7	12	2	9	5
						D	O	L	Q	Q	P
T	C	E	T	A	R	T	D	C	X	V	D
C	A	W	F	M	X	I	X	Y	G	D	O
Q	Y	Y	X	T	W	N	N	O	I	A	G
I	W	Q	O	R	C	G	E				

Ostatecznie, bierzemy kolumnę tekst po kolumnie, zaczynając od kolumny o numerze 1, i wpisujemy ją w pięcio-listowe grupy gotowe do transmisji:

CAYWQ XGIDT INGTF XOPDO GTCQI ODXNE AMTRQ VDAEW YQRXW CLCYO.

Rozszyfrowanie w tym systemie to żmudny proces, w którym łatwo popełniają błędy. Aby rozpocząć rozszyfrowanie, odbiorca musi ustalić, od dnia tygodnia i długości wiadomości, które kolumny pola transpozycji będą miały dodatkową literę i które są. W powyższym przykładzie, ponieważ wiadomość zawiera 50 znaków, będzie 10 kolumn po 4 litery i 2 kolumny po 5 liter. Ponieważ dzień tygodnia jest wtorek (= 3) kolumny z nagłówkami 3 i 7 będą "długimi" kolumnami, a pozostałe będą "krótkie". Ta sama analiza będzie musiała zostać wykorzystana, gdy transpozycja zostanie ponownie wykorzystana; w tym przypadku miesiącem jest maj (-5), więc długimi kolumnami będą te z nagłówkami 5 i 6 (odkąd kolumna z nagłówkiem 6 ma miejsce

postępować zgodnie z kolumną zatytułowaną "5").

Szyfr z kluczem jednorazowym

Podstawową słabością szyfru książki, stosowaną powyżej, jest to, że zarówno wiadomość, jak i klucz były w języku angielskim i przeciągając szopki na podstawie zwykłych angielskich słów, które mogły wystąpić w obu przypadkach, mogliśmy je odzyskać. Gdyby klucz nie był po angielsku, odszyfrowanie z pewnością byłoby trudniejsze dla kryptoanalityka, ale wiadomości byłyby mimo wszystko czytane, gdy tylko odkryłby, że tak właśnie jest, ponieważ można by również użyć łóżeczek z innego języka. Jeśli z

drugiej strony klucz nie był oparty na języku naturalnym, ale był po prostu "losowym" ciągiem liter, wziętym ze strony "losowych liter", która jest niszczona po użyciu, aby nigdy więcej nie mogła zostać użyta, wtedy mamy coś, co jest znane jako jednorazowy pad, a wynikowy szyfr nie może zostać rozwiązany. Może się to wydawać bardzo śmiałym stwierdzeniem, ale jest to fakt matematyczny. Ponieważ jednorazowe podkładki zapewniają całkowite bezpieczeństwo, dlaczego nie są używane do wszystkich szyfrów? Zasadniczo dlatego, że każda para ludzi, którzy muszą się komunikować, musi mieć zapewnioną inną podkładkę, z których każda ma jedną z dwóch kopii, i choć jest to wykonalne dla kilkuset par, takich jak ambasadorowie komunikujący się ze swoimi rządami, jest to nie do przyjęcia dla dużej liczby jednostek wojskowych w czasie wojny. Należy również zdać sobie sprawę, że sytuacja zmienia się dramatycznie, jeśli pad "jednorazowy" jest używany więcej niż jeden raz. Następnie mamy "głębokość" dwóch lub więcej komunikatów szyfrów zaszyfrowanych tym samym kluczem dodatkowym. Odejmując jeden tekst od drugiego klucz jest eliminowany, a wynikowy tekst różnicowy jest teraz różnicą dwóch nierozdrobnionych tekstów, a "przeciąganie szopki" lub podobna technika może prowadzić do ich odszyfrowania. Jeśli jednorazowy pad jest używany do szyfrowania grup kodu, a nie języka naturalnego, zadanie kryptoanalityka jest o wiele trudniejsze, ponieważ musi on posiadać pewną wiedzę o samym kodzie, aby użyć ataku przeciągania szopki, ale metoda jest zasadniczo podobnie. Z różnych powodów, w tym z dostarczania jednorazowych padów, kryptografowie są bardzo zainteresowani metodami, za pomocą których można generować "losowe" litery (lub liczby).

Tworzenie losowych liczb i liter

Losowe sekwencje

Załóżmy, że mamy długą sekwencję 0s i 1s, to jest długa sekwencja binarna. Co mamy na myśli mówiąc, że sekwencja jest "losowa"? Jako oczywiste pierwsze kryterium wydaje się rozsądnym oczekiwać, że będzie zawierał "około tyle samo 0 jako 1s"; ale co rozumiemy przez "około"? Jeśli sekwencja ma dokładnie 1000 cyfr, niekoniecznie spodziewamy się, że będzie zawierała dokładnie 500 0 i 500 1, ale jeśli zawierała, powiedzmy 700 0 i 300 1, z pewnością myślelibyśmy, że to nie była losowa sekwencja. Gdzieś pomiędzy tymi dwoma skrajnościami oznaczałoby granicę akceptowalności tego, co bylibyśmy gotowi przyjąć jako przypadkową: 530 0s i 470 1s na przykład; ale inna osoba może ustawić inne ograniczenia. Załóżmy jednak, że sekwencja faktycznie składa się z 500 0, a następnie 500 1 s. Ponieważ jest dokładnie 500 z każdej cyfry, czy możemy uważać sekwencję za losową? Oczywiście nie, ponieważ w losowej kolejności spodziewalibyśmy się, że cztery dwucyfrowe liczby, 00, 01, 10 i 11, wystąpią "około 250" razy, ale w tej sekwencji 00 i 11 oba występują 499 razy, 01 występuje tylko raz, a 10 w ogóle nie występuje. Nawet jeśli sekwencja przejdzie ten test, możemy zapytać, czy osiem liczb trzycyfrowych 000, 001, 010, 011, 100, 101, 110 i 111 występuje "około 125" razy i tak dalej. Można zaproponować nieskończoną różnorodność wymagań tego typu i istnieje obszerna literatura matematyczna dotycząca testów, które można zastosować do sekwencji, aby sprawdzić, czy można racjonalnie powiedzieć, że jest "losowa". Odwrotnie, istnieje również obszerna literatura opisująca sposoby wytwarzania sekwencji, które, chociaż nie są ściśle "losowe", spełniają różne testy losowości, a zatem są uważane za wystarczająco nieprzewidywalne, aby były użyteczne w pewnych sytuacjach. Bez wchodzenia w matematyczne kryteria decydujące, czy sekwencja jest losowa, odpowiednia definicja dla naszych celów jest

Definicja 8.1

Binarna sekwencja jest uważana za losową, jeśli, bez względu na to, ile cyfr widzieliśmy, prawdopodobieństwo, że następna cyfra będzie wynosić 0, wynosi 0,5. Jest to sytuacja, która powinna mieć zastosowanie, jeśli ktoś kręci "bezstronny" wiele razy: bez względu na to, co już się stało, prawdopodobieństwo, że spadnie ono "na głowę" następnym razem, powinno wynosić 0,5, lub w kategoriach prawdopodobieństwa, "evens". Nie ma nic szczególnego w sekwencjach binarnych; nasza definicja losowości może być zastosowana jedynie z niewielkimi modyfikacjami sekwencji cyfry lub liter dziesiętnych.

Definicja 8.2

Sekwencja cyfr dziesiętnych jest uważana za losową, jeśli niezależnie od liczby cyfr, które widzieliśmy, prawdopodobieństwo, że następna cyfra będzie miała określoną wartość, wynosi 0,1.

Definicja 8.3

Ciąg liter alfabetu angielskiego jest uważany za losowy, jeśli niezależnie od tego, ile liter widzieliśmy, prawdopodobieństwo, że następna litera będzie jedna, wynosi 1/26.

Tworzenie losowych sekwencji

Prawdziwie losowa sekwencja może być wygenerowana tylko przez proces prawdziwie losowy, a więc w szczególności nie może być generowana przez żadną matematyczną formułę, ponieważ znajomość formuły i wystarczające wartości początkowe (tj. Liczby już wygenerowane przez formułę) umożliwiłoby komuś przewidzieć następną wartość z pewnością. Istnieją jednak formuły, które mogą wytworzyć długą sekwencję liczb, które spełniają wiele kryteriów przypadkowości, zanim zaczną się

powtarzać; takie sekwencje są nazywane "pseudorandom" i opisujemy niektóre z nich poniżej, ale najpierw patrzymy na niektóre sposoby generowania prawdziwie losowych sekwencji.

Kręcenie monetą

Jeśli wielokrotnie kręcimy "uczciwą" monetą i zapisujemy "1" za każdym razem, gdy pojawia się "reszka" i "0" za każdym razem, gdy pojawia się "orzeł", powinniśmy otrzymać losową sekwencję binarną. W praktyce, być może z powodu pewnej regularności w zakresie obrotu, sekwencja może być stronnicza. Jest to ponadto bardzo powolny sposób tworzenia losowej sekwencji, która prawdopodobnie byłaby używana tylko wtedy, gdyby nie było innej metody. Mówi się, że jeniec przeprowadził taką procedurę przez wiele tysięcy obrotów, aby zająć się sobą i przeanalizował powstałą sekwencję różnymi testami.

Rzucanie kostkami

Mniej żmudna procedura może polegać na rzuceniu dwoma kostkami. Kostki muszą być odróżnialne od siebie; załóżmy, że jeden ma kolor czerwony, a drugi kolor niebieski. Rzuć kostką i obliczyć liczbę 6x (liczba na czerwonej kości) + (liczba na niebieskiej matrycy) -7, a następnie

(i) odrzucić numer, jeśli przekracza 29,

(ii) zapisz resztę, gdy liczba zostanie podzielona przez 10.

Wynikowa sekwencja cyfr dziesiętnych powinna być losowa. Niezbędne są raczej dziwne zasady, ponieważ powierzchnie kostek są ponumerowane od 1 do 6, a nie od 0 do 5, i ponieważ istnieje 36 kombinacji, które można wytworzyć. W konsekwencji można uzyskać wartości od 0 do 35 włącznie dla liczby, więc musimy odrzucić dowolną liczbę powyżej 29, aby zapewnić, że wszystkie cyfry od 0 do 9 mają taką samą szansę pojawienia się. Można użyć więcej niż dwóch kości, a przy każdym rzucie można wygenerować więcej niż jedną losową cyfrę. Na przykład z czterema kośćmi 1296 możliwych rezultatów i jeśli kolorujemy kostki czerwone, niebieskie, zielone i białe i obliczamy liczbę 216xred + 36xblue + 6xgreen + white-259 i odrzucamy dowolną liczbę powyżej 999 możemy pobrać trzycyfrową liczbę tak uzyskaną jako kolejne trzy cyfry losowej sekwencji dziesiętnej. Istnieje wiele możliwych wariantów tego rodzaju podejścia; na przykład dwie kości mogą zostać zastąpione kołem ruletki, które ma 37 sektorów ponumerowanych od 0 do 36. Sektory od 30 do 36 byłyby ignorowane, a druga cyfra "zwycięskiego" sektora zapewniałaby następną losową cyfrę dziesiętną. Jest to oczywiście raczej marnotrawstwo i bardziej efektywnym zastosowaniem w tym przypadku byłoby zignorowanie sektorów 32-36 i przekształcenie pozostałych liczb, od 0 do 31 włącznie, w binarne, zapewniając w ten sposób każdorazowo pięć cyfr binarnych. Cyfry binarne są powszechnie znane jako bity i często o których mowa w ten sposób. Klucze binarne są często używane w kryptografii. Nie tylko mają wielką zaletę, że nienajazdowy dodatek (mod 2) jest szczególnie prosty i identyczny z nienoszącym się odejmowaniem (mod 2), co powoduje, że szyfrowanie i rozszyfrowanie są takie same, ale także arytmetyczna (mod 2) jest bardzo łatwa Symuluje elektronicznie, dlatego jest szczególnie przydatna zarówno dla maszyn szyfrujących, jak i dla symulatorów na komputerach.

Losowania typu loterii

System używany do losowania liczb loterii (lub bingo) może być użyty pod warunkiem, że został zmodyfikowany w taki sposób, że liczba, która została wylosowana, natychmiast powraca do puli. W ten sposób 100 kulek o numerach od 00 do 99 jest przędzonych w bębnie i wybieranych jeden po drugim, każda wybrana liczba jest zapisywana i zawiera dwie cyfry dziesiętne dla tabeli liczb losowych. Wybrana piłka musi zostać ponownie umieszczona w beczce, aby nie można było jej ponownie narysować, a każda strona składająca się z 100 dwucyfrowych liczb dziesiętnych zawierałaby każdą

liczbę raz i tylko raz, a więc nie byłaby losowa. Typowa strona składająca się z 100 dwucyfrowych liczb losowych powinna zawierać pewną liczbę trzy, a nawet cztery razy, podczas gdy od 30 do 40 liczb może nie występować wcale. (Aby uzyskać wyjaśnienie, patrz M8.)

Promieniowanie kosmiczne

Promienie kosmiczne powstają, gdy cząsteczki ze Słońca docierają do atmosfery ziemskiej i wytwarzają kaskady innych cząstek w wyniku zderzeń, dzięki czemu zapewniają "naturalne" źródło (przypuszczalnie) zdarzeń losowych. Gdybyśmy zainstalowali dziesięć detektorów, takich jak liczniki Geigera, ponumerowanych od 0 do 9, w pokoju i odnotują kolejność, w której pożar detektorów uzyskalibyśmy prawdziwie nieprzewidywalną sekwencję dziesiętną. Należy zwrócić uwagę, że kiedy detektor "wystrzelił", żadne inne zdarzenie nie jest rejestrowane, dopóki detektor nie zdąży "odzyskać", ponieważ w przeciwnym razie prawdopodobnie wystąpi niedobór "dubletów", takich jak 00, 11 itd. w wynikowej sekwencji.

Szum wzmacniacza

Szum w obwodach elektrycznych jest zwykle uważany za problem, ale można go również wykorzystać w kryptografii. Szum można przekształcić w sygnał, który służy do włączania lub wyłączania bramki, a to z kolei jest interpretowane jako 0 lub 1. Jeśli obwody są starannie wyregulowane, tak wytworzony strumień binarny powinien być efektywnie losowy. Jeżeli występuje pewne odchylenie szczątkowe, to prawdopodobieństwo wystąpienia 0 i 1 jest nieco inne niż 0,5, suma (dwa) dwóch lub więcej takich strumieni znacznie go zmniejszy. Dwa niepowiązane strumienie, z których każdy ma odchylenie od 0,51 do 0,49 na korzyść 0, łączą się, aby wytworzyć strumień o odchyleniu tylko od 0,5002 do 0,4998 (M9).

Pseudo-losowe sekwencje

Napotkaliśmy już sekwencję Fibonacciego w Części 6. Jest to nieskończenie długa sekwencja liczb całkowitych generowana przez prostą regułę, że każda liczba w sekwencji jest sumą dwóch poprzednich liczb. Sekwencja tradycyjnie rozpoczyna się od przyjęcia dwóch pierwszych liczb jako 0 i 1. Sekwencja Fibonacciego ma niestety wiele właściwości arytmetycznych, jak wspomniano wcześniej, a zatem jest zupełnie nieodpowiednia jako źródło liczb pseudolosowych. Załóżmy jednak, że modyfikujemy regułę tak, aby powiedzieć, że każda liczba jest sumą dwukrotności poprzedniej liczby plus poprzedniej liczby, czy otrzymalibyśmy lepszą sekwencję dla naszych celów? Gdyby zacząć od 0 i 1 jako pierwszych dwóch terminów, pierwsze 10 terminów sekwencji

0,1, 2, 5, 12, 29, 70, 169, 408, 985.

Należy zauważyć, że terminy są równe i nieparzyste na przemian, a to samo w sobie wystarcza, aby wykluczyć je jako źródło liczb pseudolosowych. Oczywiście nie musimy zaczynać od 0 i 1 jako pierwszych dwóch terminów, możemy zacząć od dowolnych dwóch liczb, ale wada jest fundamentalna i żadna sekwencja wygenerowana w ten sposób nie byłaby zadowalająca. Sekwencja, jak można się spodziewać po obejrzeniu wielu cech sekwencji Fibonacciego, ma wiele właściwości matematycznych; na przykład, co trzeci termin jest podzielny przez 5, a stosunek kolejnych pojęć szybko zbliża się do wartości stałej

2.41421356 ...

który jest

(1 +√ 2).

Liniowa powtarzalność

Sekwencje przedstawione powyżej są przykładami sekwencji generowanych za pomocą tak zwanych rekonstrukcji liniowych. Ponieważ każdy nowy termin obejmuje sumowanie wielokrotności dwóch poprzednich pojęć, są one bardziej szczegółowo określane jako liniowe nawroty rzędu 2. Bardziej ogólnie, liniowa powtarzalność rzędu k jest taka, że każde nowe wyrażenie jest sumą wielokrotności k poprzedzającej warunki. Tak więc, na przykład, jeśli pozwolimy Un oznaczać n-ty termin sekwencji

$$U_n = U_{(n-1)} + 2U_{(n-2)} - U_{(n-3)}$$

jest liniową powtarzalnością rzędu 3 i

$$U_n = U_{(n-3)} + U_{(n-5)}$$

jest liniową powtarzalnością rzędu 5. Nie ma znaczenia fakt, że w drugim przypadku niektóre z powyższych pojęć nie są zaangażowane; Pięć poprzedzających terminów jest wymaganych do następnej kadencji, ale trzy terminy, $U_{(n-1)}$, $U_{(n-2)}$ i $U_{(n-4)}$, mają mnożniki 0. Mieli termin U(n-5) nie były obecne, ale powtarzanie nie byłoby w porządku 5. Mnożniki, dla naszych celów, są zawsze liczbami całkowitymi, ale mogą być dodatnie, ujemne lub zerowe. Zakłada się, że w liniowym nawrocie porządku k występuje wyrażenie U (n? K) z mnożnikiem dodatnim lub ujemnym, ale nie zerem. Terminy liniowych nawrotów zwykle rosną bardzo szybko i chociaż często mają interesujące własności arytmetyczne, nadają się tylko do celów kryptograficznych, gdy same terminy są zastępowane ich wartościami (mod 2), to znaczy terminy są zamieniane na 0, jeśli są równe. i 1 jeśli są nieparzyste, tworząc w ten sposób binarną sekwencję. Obliczanie warunków liniowego powtarzania (mod 2) jest szczególnie łatwe, nie ma potrzeby obliczania rzeczywistej wartości terminów, a następnie zastępowania ich przez 0 lub 1. Każdy termin jest po prostu zastępowany przez 0 lub 1, gdy tylko jest wyliczone; musimy wtedy dodać tylko liczbę zer i jedynek, co jest dużo łatwiejsze niż dodawanie coraz większej liczby całkowitej. Wynikowa sekwencja binarna jest identyczna z tą, która byłaby uzyskana przez dokładne obliczenie każdego terminu, a następnie zastąpienie go przez 0 lub 1. Tak więc, na przykład, liniowa powtarzalność rzędu 2

$U_n = 3U_{(n-1)} - 2U_{(n-2)}$

z początkowymi wartościami $U_0 = 0$, $U_1 = 1$ trwa

0, 1, 3, 7, 15, 31, 63, 127, 255, 511, ...

Jeśli zastąpimy każdy wyraz przez jego resztę (mod 2), jak tylko zostanie obliczona, odpowiednikiem binarnym jest

0, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...

co jest oczywiście poprawne, ponieważ, oczywiście,

$U_n = 2^n - 1$

a wszystkie terminy po U_0 są nieparzyste.

Ta konkretna sekwencja jest oczywiście bezużyteczna dla kryptologa, ponieważ jest wyjątkowo nieprzypadkowa. Czy jest jednak możliwe, że niektóre binarne sekwencje liniowe mogą być odpowiednie i w jaki sposób można je zastosować? Najpierw przyjrzymy się praktycznemu problemowi, w jaki sposób dwójkowy strumień klucza mógłby zostać użyty do szyfrowania.

Używanie binarnego strumienia klucza do szyfrowania

Kryptograf musiałby najpierw przekonwertować tekst wiadomości z postaci alfabetycznej / numerycznej na binarną. We wczesnych dniach komputerów używano pięciu lub sześciu bitów do przedstawienia najważniejszych postaci. Ponieważ zawierały one odpowiednio tylko 32 lub 64 znaki, co nałożyło ograniczenia na zestaw znaków, które mogły zostać użyte, ostatecznie zostały zastąpione ośmiobitową reprezentacją, która stała się znana jako bajt, pozwalając na 256 znaków, wystarczającą do uwzględnienia nie tylko niżej i wielkie litery, cyfry i znaki interpunkcyjne, ale także wiele innych symboli, takich jak nawiasy różnego rodzaju i akcenty. Dzisiaj ośmiobitowa reprezentacja jest standardem, na przykład

A = 65 = 01000001,

B = 66 = 01000010

itp. i

a = 97 = 01100001,

b = 98 = 01100010,

podczas

$ = 36? = 00100100

i

ê = 136 = 10001000

Po przekonwertowaniu znaków tekstu na ośmiobitowe bajty, zostałyby one zwykle dodane "liniowo" (mod 2), czyli bit po bicie bez "przenoszenia", do klucza binarnego w celu wytworzenia szyfru. Na przykład, jeśli literą wiadomości jest E, a odpowiednia litera klucza to $,

E=01000101,

$= 00100100.

Dodawanie (mod 2)

01100001 = 97 = a,

tj. litera z szyfrem jest. Istnieją alternatywy dla tego "liniowego" lub dodawania bit po bicie; bardzo ważny i bezpieczny system, standard szyfrowania danych (DES) opisany w części 13, traktuje niektóre bity w sposób "nieliniowy".

Binarne sekwencje liniowe jako generatory kluczy

Kiedy generujemy sekwencję binarną za pomocą liniowego powtarzania rzędu k, tworzymy sekwencję 0s i 1s. Czy ta sekwencja może trwać bez końca, bez powtarzania? Odpowiedź brzmi "Nie", ponieważ każdy nowy termin zależy tylko od wartości poprzednich określeń k, a ponieważ każdy z nich to 0 lub 1, istnieje tylko 2^k różnych możliwości dla nich. Wynika z tego, że po 2k terminach, co najwyżej, musi się powtórzyć jakiś zbiór k kolejnych pojęć binarnych. Zatem sekwencja Fibonacciego (mod 2) jest

0, 1, 1, 0, 1, 1, 0, 1, 1, 0, ...

i widzimy, że sekwencja binarna składa się po prostu z tripletu 011 powtarzanego w nieskończoność. Ponieważ sekwencja Fibonacciego powstaje w wyniku liniowego nawrotu rzędu 2, w tym przypadku mamy k = 2, więc wiemy, że w postaci binarnej sekwencja musi się powtarzać najwyżej $2^2 = 4$ terminy.

W rzeczywistości powtarza się po 3 i jest to w rzeczywistości maksimum, jakie może być, ponieważ jedna z 4 możliwych par kolejnych binarnych pojęć wynosi 00 i taka para będzie generować 0 na zawsze. Odwrotnie, żadna inna sekwencja binarna nie może zawierać 00, a więc maksymalna możliwa liczba binarnych terminów, które możemy uzyskać, zanim sekwencja zacznie się powtarzać, wynosi 3, a nie 4. Powodem jest, że maksymalna liczba terminów przed powtórzeniem dwójkowego liniowego powtarzania rzędu k zaczyna się powtarzać to 2^k-1, a nie 2^k. Binarna sekwencja Fibonacciego, choć skromna, ma zatem maksymalny okres. Oczywiście żadna sekwencja binarna z maksymalnym okresem 3 nie jest interesująca dla kryptografów, ale co z sekwencjami binarnymi wyższego rzędu? Aby najpierw podjąć łatwą do zweryfikowania sprawę: sekwencja zamówienia 4 może mieć 15, czyli 2^4- 1. Jeśli zignorujemy banalny przypadek, w którym wszystkie cztery mnożniki to 0, istnieje 15 możliwych binarnych sekwencji liniowych rzędu 4.

Czy któryś z nich tworzy sekwencję binarną o maksymalnym okresie 15? Tylko 2 z nich zrobić; są to

$$U_n = U_{(n-3)} + U_{(n-4)}$$

$$U_n = U_{(n-1)} + U_{(n-4)}$$ i

Przykład 8.1

Zweryfikuj binarną powtarzalność liniową czwartego rzędu

$$U_n = U_{(n-3)} + U_{(n-4)}$$

która generuje sekwencję z maksymalnym okresem 15.

Weryfikacja

Zaczynamy od $U_0 = U_1 = U_2 = U_3 = 1$ i generujemy każdy nowy termin, sumując trzy i cztery miejsca wcześniej w sekwencji i wstawiając 0 lub 1 w zależności od tego, czy suma jest parzysta czy nieparzysta. Stwierdza się, że sekwencja jest

1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1,1,1,1 ...

i widzimy, że sekwencja zaczyna się powtarzać od U15, ale nie wcześniej.

(Zauważ, że jeśli sekwencja binarna generowana przez liniowy cykliczności rzędu k ma maksymalny okres, musi zawierać wszystkie możliwe binarne sekwencje 2^k o długości k oprócz tej składającej się ze wszystkich 0. Możemy zatem przyjąć dowolne wartości początkowe z wyjątkiem 00 ... 00 a okres będzie widoczny jako maksymalny w każdym przypadku, jeśli okres nie jest maksymalny, różne wartości początkowe mogą dawać różne sekwencje.)

Problem 8.1

Sprawdź, czy powtórzenie binarne

$$U_n = U_{(n-1)} + U_{(n-4)}$$

generuje również sekwencję o okresie 15, ale z powtarzalnością

$$U_n = U_{(n-1)} + U_{(n-2)} + U_{(n-3)} + U_{(n-4)}$$

nie.

A co z sekwencjami wyższego rzędu? Sekwencja rzędu 12, na przykład, może mieć okres tak długi jak 2^{12} - 1, który wynosi 4095. Czy jakikolwiek liniowy nawrót rzędu 12 generuje taką maksymalną sekwencję binarną? W wyniku pewnej eleganckiej i zaawansowanej matematyki znana jest formuła, która mówi nam dokładnie, ile binarnych nawrotów liniowych rzędu k wytworzy sekwencję maksymalnego okresu. W przypadku nawrotów rzędu 12 formuła mówi nam, że 144 binarne nawroty liniowe rzędu 12 wytworzą sekwencje binarne z okresu 4095. (Fakt, że 144 = 12 x 12 jest porażeniem!) Pozostałe 3952 nie zrobi tego . Analiza matematyczna nie prowadzi bezpośrednio do tych 144, które należy znaleźć w procesie podobnym do znalezienia liczb pierwszych. Alternatywnie, używając komputera, można przetestować 4095 możliwych powtórzeń i wszystkie, które powtórzy się przed wygenerowaniem 4095 terminów, można odrzucić. Po wykonaniu tej czynności znaleziona zostanie pierwsza udana sekwencja

$$U_n = U_{(n-6)} + U_{(n-8)} + U_{(n-11)} + U_{(n-12)}.$$

Jest to „pierwszy" w tym sensie, że, pisząc 0 i 1 dla mnożników w 12 kategoriach na prawej stronie nawrotu liniowego, sekwencja ta ma reprezentację 12-bitowy

000001010011

który, interpretowany jako liczba całkowita zapisana w postaci binarnej, jest

64+ 16+ 2+ 1 = 83.

Żadna sekwencja z taką liczbą całkowitą poniżej 83 nie daje maksymalnego okresu 4095. Dla części matematyki stojącej za tym wszystkim patrz M11. Wybierając się na tyle dużą porządek i znalezienie liniowy nawrót, który daje maksymalny okres, możemy produkować kluczową strumień, który wydaje się stanowić pseudolosowych binarny strumień, który moglibyśmy użyć jako klucz do szyfrowania. Można na przykład pokazać, że 356960 liniowych powtórzeń porządku 23 wygeneruje maksymalne strumienie klucza, które mają długość ponad 8000000 (M11). Ponieważ początkowe wartości początkowe dają również ponad 8000000 możliwości, można by pomyśleć, że taki klucz stanowiłby ogromny problem dla kryptoanalityka, a na początku byłby. Niestety, klucz kryptograficzny, który został wygenerowany w ten sposób, ma on fatalną wadę: biorąc pod uwagę dość skromną ilość klucza, powtarzalność liniowa, dzięki której została wygenerowana, a wartości początkowe mogą zostać odzyskane. Jest to następstwem następującego.

Kryptoanaliza liniowego powtarania

Biorąc pod uwagę 2k kolejnych bitów klucza generowanych przez dwójkową liniową powtarzalność rzędu k a układ równań liniowych k mnożników warunków nawrotu może być skonfigurowany i rozwiązany. Jeśli kryptoanalityk ma powody, by sądzić, że klucz generowany przez liniową powtarzalność jest zaangażowany, postępuje w następujący sposób:

(i) uzyskać odcinek klucza z wiadomości, dla której znane jest rozwiązanie; mało znaków będzie wymaganych i mogą być dostępne od standardowych początków do wiadomości;

(ii) przyjąć wartość k, kolejność liniowego wznowienia;

(iii) za pomocą 2k kolejnych bitów ustawionych w kluczu równań liniowych w mnożnikach k nieznanych w nawrocie; jeżeli powtórzenie jest porządku k, pojawi się rozwiązanie, w którym wszystkie mnożniki są liczbami całkowitymi (i mają być interpretowane (mod 2), tj. jako nieparzyste lub parzyste); możliwe

jest, że istnieje więcej niż jedno rozwiązanie rzędu k lub, alternatywnie, nie ma takiego rozwiązania; w tym ostatnim przypadku należy wypróbować inną wartość k.

Zatem, w przypadku postaci przedstawionych jako 8-bitowe bajty i strumień klucza generowany przez dwójkową liniową powtarzalność rzędu 23, tylko 46 bitów klucza będzie wymagane w celu rozwiązania systemu. Ponieważ 6 znaków komunikatu spowodowałoby 48 bitów klucza, system mógłby być łatwo rozwiązany, gdyby wiadomości miały tendencję do rozpoczynania TO THE!

Poprawa bezpieczeństwa kluczy binarnych

Oczywiste jest, że klucze binarne generowane przez liniowe nawroty są zbyt łatwe do rozwiązania, aby były użyteczne z punktu widzenia kryptografii, ale czy istnieje sposób na poprawę ich bezpieczeństwa? Ponieważ ich słabość polega na tym, że w nawrocie porządku k każdy bit jest ustaloną liniową kombinacją bitów k, które go poprzedzają, nawet użycie powtarzającego się wysokiego rzędu, takiego jak przyjęcie k = 103, nie zapewni wystarczającego bezpieczeństwa, dla tylko umiarkowany odcinek klucza (26 liter, gdy k = 103) będzie wymagany do odzyskania systemu. Ponadto, użycie powtórzenia wysokiego rzędu do wygenerowania klucza ręcznie (ponieważ może to być robota szpiegowska) byłoby nudnym zadaniem i podatnym na błędy. Szkoda, ponieważ klucz wygenerowany z takiego powtórzenia może mieć bardzo długi okres, ponad 10^{30}, gdy k = 103. Długi okres jest wysoce pożądany, ale czy możemy go uzyskać bez powtarzania się wysokiego rzędu i jednocześnie wzmocnić bezpieczeństwo? W rzeczywistości możemy: kombinując klucze dwóch lub więcej liniowych nawrotów, jak pokazuje poniższy prosty przykład.

Przykład 8.2

Skorzystaj z (mod 2) sumy kluczy wygenerowanych przez dwa liniowe nawroty

$$U_n = U_{(n-1)} + U_{(n-2)}, U_0 = U_1 = 1$$

i

$$U_n = U_{(n-1)} + U_{(n-3)}, U_0 = U_1 = U_2 = 1$$

aby stworzyć nowy klucz. Sprawdź, czy ma to 21 okres.

Weryfikacja

Pierwsza nawrotność, jak widzieliśmy, ma okres długości 3 i wytwarza strumień klucza

110110110110 ...

Drugi cykl ma długość 7 i generuje kluczowy strumień

111010011101001110100 ....

Zapisywanie obu z nich pod jednym i dodawanie bitów (mod 2), które mamy

1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 .....

1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 ....

Dodawanie (mod 2) 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 .....

i widzimy, że klucz powtarza się po 21 miejscach, ale nie wcześniej. Ponieważ pierwszy klucz ma okres 3, a drugi klawisz ma okres 7, łączny klucz nie może przekroczyć 21, ponieważ oba klawisze powtarzają

się po 21 miejscach. Z drugiej strony, ponieważ 3 i 7 nie mają wspólnego współczynnika, połączony klucz nie może się powtórzyć po mniej niż 21 miejscach. Nie ma potrzeby ograniczać się do korzystania z dwóch liniowych nawrotów; możemy użyć trzech lub więcej. Zaletą jest to, że im bardziej używamy trudniej byłoby, aby kryptoanalityk rozwiązał system. Wadą, jeśli pracujemy ręcznie, byłaby nużąca natura generowania klucza i zwiększone prawdopodobieństwo błędów. Oczywiście, jeśli mamy ameanów generujących klucz przez urządzenie amechaniczne lub elektroniczne, wadą znika. Nie jest więc zaskakujące, że zbudowano maszyny, które generują długie okresowe strumienie kluczowe, zarówno binarne (tj. (Mod 2)), jak i alfabetyczne (tj. (Mod 26)), poprzez połączenie wyjścia kilku kluczowych strumieni o krótszych okresach. Onesuchmachine, który wygenerował klucz (mod26), był maszyną szyfrującą Hagelin, która była szeroko wykorzystywana przez kilka krajów PODCZAS II WOJNY ŚWIATOWEJ ,a druga, która wygenerowała klucz (mod 2), to Lorentz SZ42, która była jedną z maszyn szyfrujących używanych przez Niemców.

Pseudolosowe generatory liczb

Czasem konieczne jest użycie liczb losowych w obliczeniach, na przykład typu "Monte Carlo" [8.3], w których metody analityczne są niewykonalne, takich jak problemy z fizyką cząstek elementarnych lub dynamiką gromad gwiazdowych. W takich przypadkach często stosuje się metody matematyczne do generowania strumienia liczb pseudolosowych, a podczas gdy takich liczb nie uważa się za odpowiednie do użycia jako klucze w systemach kryptograficznych, mają one pewne istotne znaczenie i są warte odnotowania.

Metoda średniokwadratowa

Chociaż ta metoda nie może być zalecana do użycia w kryptografii, była używana w niektórych innych aplikacjach. Jeśli weźmiemy liczbę całkowitą losowo i kwadratowo, ostatnia cyfra nie może wynosić 2, 3, 7 lub 8. Wydaje się więc, że rozpoczynanie od losowej liczby i powtarzanie jej w kwadracie w nadziei, że wytworzy sekwencję liczb losowych, jest bezcelowe. Jeśli jednak po wyrównaniu liczby wyrzucamy "część z jej początkowych i końcowych cyfr, pozostałe cyfry mogą być wystarczająco równomiernie rozproszone do użycia jako źródło liczb pseudolosowych. Jest to podstawa metody środkowej, która działa w następujący sposób:

(1) wybierz dużą "losową" liczbę całkowitą, X, o długości n cyfr;

(2) formularz X^2 i zachowaj tylko cyfry środkowe n (w razie potrzeby umieść 0 z przodu); użyj wynikowej liczby całkowitej jako nowej wartości X.

Sekwencja liczb całkowitych n-cyfrowych generowanych w ten sposób musi ostatecznie zacząć się cyklicznie, ponieważ istnieje tylko 10 możliwych wartości. Cykliczne cykle mogą wynikać z powtarzania liczby, niekoniecznie z wartości początkowej, która pojawiła się wcześniej lub z liczby całkowitej składającej się ze wszystkich 0, po których pojawią się tylko 0. Należy zachować ostrożność przy korzystaniu z tej metody w dowolnym celu, jak pokazuje poniższy przykład.

Przykład 8.3

(1) Użyj metody środkowej, aby uzyskać czterocyfrowe liczby zaczynające się od 3317.

(2) Powtórz ćwiczenie, ale zacznij od 2907.

(3) Powtórz ćwiczenie, ale zacznij od 3127.

(Do drugiego i trzeciego przypadku potrzebny jest kalkulator lub komputer).

Rozwiązania

(1) X = 3317, więc X^2 = 11002489. Usunięcie pierwszej i ostatniej pary cyfr daje następną wartość X = 0024, więc X^2 = 00000576 i usunięcie pierwszej i ostatniej pary daje następną wartość X= 0005. Od X^2= 00000025, następna i wszystkie kolejne wartości X to 0000.

(2) Jest to przypadek mniej skrajny. Wartości X zaczynają się od 2907, 4506, 3040 i wydają się kontynuować w sposób zadowalający, ale mimo to 42 wartość X okazuje się być 0.

(3) W tym przypadku występuje cykl, ale sekwencja nie rozpoczyna się ponownie od początku. Zaczynając od X? 3127 stwierdzamy, że sekwencja trwa 7781, 5439, 5827, ... ale od 38 kadencji otrzymujemy 6100, 2100, 4100, 8100, 6100, 4100, ... i te same cztery liczby teraz powtarzaj w nieskończoność.

Chociaż średnie kwadrowanie jest wygodnie prostą metodą, powinno się go używać, jeśli w ogóle, z dużo większą liczbą niż w przykładzie.

Liniowe generatory kongruencji

Najczęściej stosowana metoda generuje sekwencję liczb całkowitych z zakresu od 0 do (M - 1) za pomocą formuły powtarzania tego typu

$U_n = AU(n-1) + B \pmod M$

gdzie A, B i M są liczbami całkowitymi. A nazywa się mnożnikiem, B jest przyrostem i jest modułem. Proces rozpoczyna się od wyboru wartości, znanej jako nasiono, w zakresie od 0 do (M - 1) dla U_0. Takie powtórzenie musi ostatecznie się powtórzyć, a maksymalny okres oczywiście nie może przekroczyć M, więc M powinno być "duże". Odpowiednio dobrane wartości A, B i Ma są osiągalne. W najlepszych przypadkach okres jest maksymalny, a zatem wybór nasion jest nieistotny, ponieważ występują wszystkie oprócz jednej z możliwych wartości (mod M). Większość generatorów liczb losowych wykorzystywanych w komputerach opiera się na tej metodzie z wartościami modułu, inkrementacji i mnożnika wbudowanymi w program oraz z wyborem materiału siewnego pozostawionego użytkownikowi. Aby zapewnić jeszcze lepsze wyniki, więcej niż jeden taki generator może być wykorzystane i ich wyniki połączone w jakiś sposób. Dalsza poprawa może zostać osiągnięta, jeśli liczby nie są używane w kolejności, w której są produkowane, ale stosowana jest funkcja "tasowania" w celu zmniejszenia ryzyka korelacji pomiędzy kolejnymi liczbami. W ten sposób dobry, długi, Mogą być generowane sekwencje "pseudolosowe". Wśród znanych "dobrych" wyborów dla A, B i M są pokazane w Tabeli 8.1.

A	B	M
106	1 283	6 075
171	11 213	53 125
141	28 411	134 456
421	54 773	259 200

Z drugiej strony pojedynczy generator o źle dobranych wartościach A, B i M może wytworzyć klucz o bardzo krótkim czasie. Oto mały przykład ilustrujący te sytuacje.

Przykład 8.4

Użyj powtórzenia

$$U_n = 3U_{(n-1)} + 4 \pmod{17}$$

do generowania sekwencji liczb całkowitych rozpoczynających się od (1)$U_0 = 5$, (2)$U_0 = 15$.

Generacja

(1) Ponieważ $U_0 = 5$, $U_1 = 3 \times 5 \times 4 \times 19 \equiv 2 \pmod{17}$ itp. Sekwencja o długości 16 to

5, 2, 10, 0, 4, 16, 1, 7, 8, 11, 3, 13, 9, 14, 12, 6,5,2,10....

Ten generator, choć skromny, wytwarza maksymalny możliwy cykl, który w tym przypadku wynosi 16.

(2) $U_0 = 15$ daje $U_1 = 3 \times 15 \times 4 \times 49 \equiv 15 \pmod{17}$, więc okres wynosi 1! To wyjaśnia, dlaczego wartość 15 nie występuje w 16-letnim cyklu powyżej.

Problem 8.2

Sprawdź, czy metoda środkowego kwadratu, która wykorzystuje czterocyfrowe liczby zaczynające się od X = 7789, ulega degeneracji w sekwencji czterech liczb.

Problem 8.3

Począwszy od $U_0 = 1$, jakie są długości cyklu nawrotów

(1) $U_n = 3U_{(n-1)} + 7 \pmod{19}$,

(2) $U_n = 4U_{(n-1)} + 7 \pmod{19}$?

Gdy używane są generatory liczb pseudolosowych tego typu, uzyskane wartości są zwykle dzielone przez moduł M, aby uzyskać rzeczywistą liczbę leżącą między 0 a 1,0. Ponieważ wartości całkowite podane przez generator mieszczą się w zakresie od 0 do (M? 1), wartości liczby rzeczywistej mogą zawierać 0,0, ale nie będą zawierać 1,0, ale to małe ograniczenie jest mało prawdopodobne i, z dobrze dobranymi wartościami A, B i M, wygenerowane liczby rzeczywiste powinny być równomiernie rozłożone między 0 a 1.

Maszyna szyfrująca Enigma

Tło historyczne

W części 2 przyjrzeliśmy się prostym szyfrom zastępowania i zobaczyliśmy, jak można je rozwiązać za pomocą liczników częstotliwości, jeśli dostępny jest "wystarczający" tekst szyfrowania. Ile liter jest zawsze "wystarczających", jest kwestią do dyskusji, ale prawdą jest, że 200 liter zwykle wystarcza, a 50 nie. Dla naszych celów załóżmy, że jeśli tylko 25 liter szyfru jest dostępnych, szyfr jest bezpieczny. Ponieważ ograniczenie długości komunikatów do nie więcej niż 25 liter byłoby zbyt restrykcyjne, dochodzimy do wniosku, że użycie prostego szyfru zastępczego jest niepraktyczne. Jeśli jednak nie używamy jednego, ale kilka różnych prostych alfabetów zastępczych, przełączając się pomiędzy alfabetami za każdym razem, gdy zaszyfrujemy literę, możemy zwiększyć bezpieczeństwo systemu. Jako przybliżony przewodnik: jeśli użyjemy N różnych alfabetów, powinno być możliwe uczynienie szyfrów bezpiecznymi dla pojedynczych wiadomości składających się z maksymalnie 25 liter alfabetu; ale ta prosta zasada wymaga kwalifikacji. Jeśli alfabety zastępcze są powiązane w jakiś sposób, odzyskanie któregokolwiek z nich może prowadzić do odzyskania pozostałych. Z drugiej strony, w niektórych systemach dodatkowe funkcje mogą zapewnić bezpieczeństwo wiadomości szyfrujących o długości większej niż 25N. W konkretnym przypadku cylindra Jeffersona na przykład nadawca i odbiorca mogli

albo zgadzają się, że tekst zaszyfrowany zostanie odczytany z wiersza liter w określonej odległości od wiersza liter zwykłego tekstu (odległość może być podana za pomocą jakiejś formy wskaźnika), albo nie mają wskaźnika i używają innej odległości za każdym razem, gdy rząd jest zaszyfrowany.

Podczas gdy druga procedura polega na tym, że odbiorca patrzy na wszystkie 25 rzędów cylindra, aby zobaczyć, który z nich ma sens, bezpieczeństwo systemu zostanie znacznie poprawione. Dzięki systemowi "ustalonej odległości" i cylindrowi, powiedzmy 40 dysków, litery szyfrów w 40 pozycjach różniłyby się od identycznych prostych alfabetów zastępczych. Wynika z tego, że zbiór wiadomości zawierających ponad 2000 literaów byłby podatny na ataki oparte na liczbie wierszy monografii, ponieważ wszystkie wiadomości byłyby "dogłębne", a my mielibyśmy próbkę 50 liter szyfrujących z każdego alfabetu. W systemie o zmiennym dystansie komunikaty nie byłyby "dogłębnie", a do rozwiązania systemu potrzebnych może być więcej znaków szyfrujących; potrzebna liczba będzie oczywiście zależeć od tego, w jaki sposób wybrane zostały odległości zmienne. Najwyraźniej system oparty na alfabetach zastępujących N ma poziom bezpieczeństwa, który rośnie wraz z N, ale z drugiej strony, jeśli szyfrowanie ma być wykonywane ręcznie, żmudne korzystanie z systemu i możliwość błędu, również zwiększyłaby się N. Tak więc, jak to często bywa w życiu, mamy sprzeczne wymagania. W tym przypadku chcielibyśmy, aby N był duży, aby zwiększyć bezpieczeństwo, ale chcielibyśmy również zachować N małe dla łatwości użycia, i nie możemy zrobić obu. W latach 1914-18 wojna zaczęła być wykorzystywana przez jednostki wojskowe do wysyłania wiadomości do siebie nawzajem i do ich centrali. Transmisja radiowa miała tę zaletę, że można było komunikować się z jednostkami znajdującymi się w znacznej odległości od bazy, w tym statków i łodzi podwodnych na morzu. niemal natychmiast, ale wadą, że wiadomości mogą zostać przechwycone przez wroga. Istotne było zatem, aby szyfrować takie wiadomości w bezpiecznym systemie i opracowane zostały systemy szyfrujące o pewnej złożoności; niestety, im bardziej złożony system, tym większe obciążenie dla urzędników szyfrujących i tym większe jest ryzyko błędów o potencjalnie katastrofalnych konsekwencjach. Potrzebne były pewne "przyjazne dla użytkownika", ale bardzo bezpieczne systemy szyfrowania, gdyby sprzeczne wymagania zostały spełnione. Po wojnie wielu ludzi w różnych krajach zdecydowało, że

jedynym sposobem zapewnienia wysokiego poziomu bezpieczeństwa bez zobowiązywania urzędników szyfrujących do przeprowadzania długich, żmudnych i podatnych na błędy procesów było użycie maszyn do wykonania szyfrowania / rozszyfrowania. Jedną z takich osób był Arthur Scherbius, współzałożyciel niemieckiej firmy inżynieryjnej. We wczesnych latach dwudziestych Scherbius zaprojektował wiele maszyn szyfrujących, z których wszystkie miały zapewnić bardzo dużą liczbę alfabetów zastępczych. Inny alfabet byłby automatycznie wykorzystywany za każdym razem, gdy litera byłaby zakodowana, a żaden alfabet zastępczy nie powtórzyłby się, dopóki tysiące liter nie zostało przetworzonych. Decydując się na konkretny projekt, skonstruował maszynę i nazwał ją Enigma.

Oryginalna Enigma

Enigma, którą Scherbius skonstruował i pokazał na Światowym Kongresie Związków Pocztowych w Wiedniu w 1923 roku, opierała się na następujących elementach:

(1) 26-literową klawiaturę do wprowadzania wiadomości tekstowej;

(2) 26 lamp, które zapalają się, aby pokazać litery szyfrów;

(3) zasilacz (bateria 3,5 V lub odpowiednik);

(4) trzy zdejmowane koła przewodowe, które mogą się obracać wokół wspólnej osi;

(5) stacjonarny odbłyśnik światłowodowy;

(6) stałe przewodowe koło wejściowe.

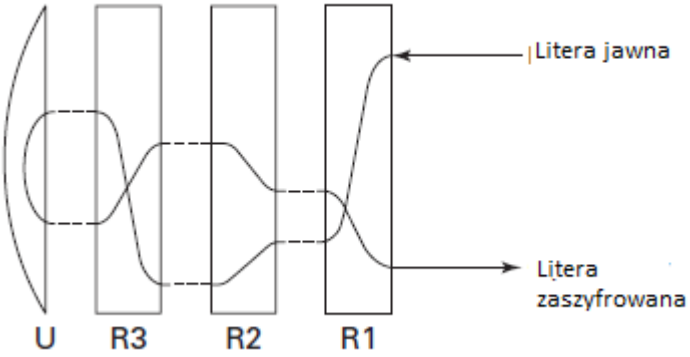
Klawiatura była podobna do klawiatury angielskich maszyn do pisania z niewielkimi wyjątkami, a mianowicie:

(i) litery Y i Z zostały zamienione, tak że Z znajdowało się w górnym rzędzie, a Y w dolnym rzędzie i

(ii) litera P była w dolnym wierszu, a nie na górze. Używano tylko wielkich liter, nie było cyfr, nie było też liter z umlautami, takich jak Ü. To samo ustawienie dotyczy liter na lampach.

Baterie służyły jedynie do przesyłania prądu przez koła i reflektor oraz do zapalania lamp. Nie zapewniało to możliwości poruszania kołami, co zostało zrobione mechanicznie. Wewnątrz każdego zdejmowanego koła znajdowało się 26 drutów, które "przypadkowo" połączyły 26 punktów styku po jednej stronie koła z 26 stykami po drugiej stronie koła. Punkty styku po jednej stronie koła (lewa strona patrząc od przodu maszyny) były w jednej linii z powierzchnią czołową tarczy, ale styki po drugiej stronie ("prawa" strona) wystają z twarzy na małe źródła; miało to zapewnić dobry kontakt między kołem a obok niego. Podobnie zapewniono dobry kontakt między prawym kołem a kołem wlotowym oraz między skrajnym lewym kołem a reflektorem. Opona alfabetyczna "biegła" po obwodzie każdego koła, a po lewej stronie każdego zdejmowanego koła przymocowany został metalowy pierścień "pierścienia wycinającego", który miał jedno wycięcie w kształcie litery V, znajdujące się naprzeciwko jednej z liter na opona. Po prawej stronie tych kół znajdował się zębaty pierścień z 26 zębami, pierścień nastawczy, który umożliwił operatorom szyfrów obrócenie koła w dowolne pożądane położenie. (Słowo "losowo" w odniesieniu do okablowania kół wymaga pewnych kwalifikacji, ale wyjaśnienie wymaga pewnej matematyki) .Reflektory zostały ustalone na miejscu i miały 26 styków tylko z jednej strony. Wewnątrz odbłyśnika 13 drutów połączyło 26 styków parami, a zatem prąd wpływający do jednego z punktów stykowych reflektora opuszczałby się w innym z punktów styku. Wewnętrzne okablowanie odbłyśnika było również "przypadkowe". W przeciwieństwie do trzech przewodowych kół reflektor był na stałe przymocowany do maszyny i był wymieniony tylko raz w latach 1930-45, w 1937 r. Koło wjazdowe zapewniało połączenie między prawym kołem a klawiaturą, a pomiędzy prawym

kołem a Lampy. Nieco zaskakujące jest to, że koło wejściowe było połączone z literami klawiatury w normalnej kolejności alfabetycznej, a nie w kolejności na klawiaturze. Nie zapewniało to przewagi kryptograficznej i musiało wiązać się z niechlujnym okablowaniem wewnętrznym. Uproszczony schemat Enigmy pokazano na rysunku 9.1.



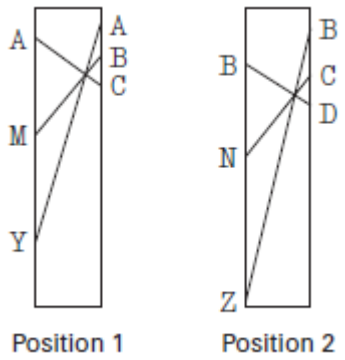
Maszyna została umieszczona w drewnianym pudełku. Kiedy maszyna była zamknięta tylko pierścieniami ustawiającymi na wystających trzech ruchomych kołach, ale litera na oponie alfabetu na każdym zdejmowanym kole była widoczna przez małe "okienko" nad nią. W ten sposób operatorzy mogli korzystać z pierścieni nastawczych, aby obrócić każde koło do pożądanej pozycji początkowej. Gdy pokrywa maszyny była otwarta, operator mógł zobaczyć wszystkie wewnętrzne koła i, za pomocą dźwigni znajdującej się obok reflektora, wyjąć trzy ruchome koła z maszyny, zsunąć je ze wspólnej osi i zmienić ich kolejność. Ponieważ oryginalna Enigma, w przeciwieństwie do późniejszych wersji, miała tylko trzy koła, liczba możliwych rozkazów kół wynosiła tylko sześć. Maszynę można było unieść, ale była dość ciężka: około 12 kg (prawie 30 funtów). Trzy wymienne koła przewodowe to R1, R2 i R3. Stały odbłyśnik to U (jego niemiecka nazwa to Umkehrwalze). Koło wejściowe, bateria, klawiatura i lampy nie są pokazane na tym uproszczonym schemacie. Po naciśnięciu jednej z liter klawiszy następuje kontakt, który powoduje, że prąd z baterii przechodzi przez R1, R2 i R3. Następnie reflektor "odwraca się", po czym przechodzi przez R3, R2 i R1 przed zapaleniem lampy, aby pokazać literę szyfrowania. Ścieżka pobierana przez bieżący nakłada dwie ważne cechy szyfru:

(1) żadna litera nie może sama sobie szyć;

(2) istnieje symetria (lub "wzajemność") zwykłych par szyfrów, np. jeśli A szyfruje do K, to przy tym samym ustawieniu kół K będzie szyfrować na A.

Szyfrowanie za pomocą przewodowych kół

Zanim dowiemy się, w jaki sposób enigma została przeprowadzona w Enigmie, musimy zobaczyć, co dzieje się, gdy prąd z klawiatury przechodzi przez pojedyncze, przewodowe koło. Ponieważ po każdej stronie koła znajduje się 26 punktów styku, a druty łączące pary punktów na przeciwległych powierzchniach są "losowo ułożone", prąd wchodzący w, powiedzmy, A pojawi się w jednym z 26 punktów na przeciwnej stronie. Nie możemy przewidzieć punktu wyjścia, chyba że znamy wewnętrzne okablowanie koła, ale załóżmy, że jest to Y. Jeśli koło się teraz obróci, drut, który przewodził prąd od A do Y, przesunie się o jedną pozycję z każdej strony i będzie teraz przenoszą prąd od B do Z. Podobnie, jeśli B był podłączony do M i C był podłączony do A przed obróceniem koła, to C i D zostaną podłączone odpowiednio do N i B po obróceniu koła. Zilustrowano to na rysunku 9.2.



Gdy koło obróci się 26 razy, przewody powrócą do pierwotnych pozycji, a A, B i C ponownie zostaną podłączone odpowiednio do Y, M i A. Jeśli znamy połączenia przewodów wewnątrz koła, poznajemy szyfrowanie każdej litery, A, B, C, ..., Z w pozycji 1 koła i możemy następnie wyliczyć szyfrowanie dowolnej litery w dowolnym położeniu Koło. Na przykład, jeśli chcemy znać szyfrowanie K w pozycji 6 koła, argumentujemy następująco. Przewód, który ma punkt wejścia K w pozycji 6, jest drutem, który w pozycji 1 miał punkt wejścia na literę, która jest 5 miejsc przed K w alfabecie, to jest F. Jeśli F jest zafałszowane do P, powiedzmy, w pozycji 1, a następnie K będzie szyfrował do litery, która jest 5 miejsc poza P w alfabecie na pozycji 6, czyli U. W skrócie: Jeśli F dojdzie do P w pozycji 1, K przejdzie do U w pozycji 6. Możemy w pełni opisać właściwość encyklopedyczną dowolnego koła, wymieniając szyfrowanie każdej litery na pozycji 1 koła, ponieważ możemy wtedy wyliczyć szyfrowanie dowolnej litery na pozycji 2, a następnie na pozycji 3 i tak dalej. Nie ma nic szczególnego w pozycji 1, a także spis alfabetu szyfrowania (który jest prostym zamiennikiem) w dowolnej pozycji koła. Na przykład, jeśli weźmiemy szyfrowanie pierwszych 6 liter na pozycji 1, możemy zacząć tworzyć tabelę 9.1.

	Position					
Letter	1	2	3	4	5	6 ...
A	Y	.	.	.	.	.
B	M	Z	.	.	.	.
C	A	N	A	.	.	.
D	T	B	O	B	.	.
E	F	U	C	P	C	.
F	R	G	V	D	Q	D

"Kropki" wskazują miejsca, w których nie mamy jeszcze wystarczającej ilości informacji, aby nadać literę szyfrowania. Pełna tablica szyfrowania 26 x 26 może być wypełniona, gdy znamy szyfrowanie wszystkich 26 liter w pozycji 1. Zwróć uwagę na ważną cechę tablicy szyfrów: każda przekątna od północno-zachodniego do południowo-wschodniego stanowi pełny alfabet, w normalnym kolejność, zaczynając od litery w kolumnie 1. Alternatywnie, jeśli znamy szyfrowanie litery A lub jakiejkolwiek innej, we wszystkich 26 pozycjach koła możemy równie dobrze wyliczyć szyfrowanie dowolnej litery w dowolnym położeniu. Załóżmy na przykład, że chcemy poznać szyfrowanie N w pozycji 11. Przewód, który ma N jako punkt wejścia w pozycji 11, to przewód, który miał A jako punkt wejścia 13 pozycji. Ponieważ N ma 13 miejsc po A w alfabecie. Teraz 11 - 13 = -2 , a pozycja - 2 jest taka sama jak pozycja 26 - 2, tj. 24. Wyszukujemy zatem, do jakiej litery A szyfruje do pozycji 24. Jeśli to, powiedzmy, G, a następnie N w pozycji 11 będzie szyfrowanie do litery, która jest 13 miejsc po G w alfabecie na pozycji 11, czyli do T. Czytelnicy, którzy są zaznajomieni z macierzami, rozpoznają, że to, co robimy, w rzeczywistości reprezentuje szyfrowanie dostarczone przez koło jako macierz 26 x 26. Pierwsza kolumna zawiera szyfrowanie całego alfabetu w pozycji 1, a pierwszy wiersz koduje A w każdej z 26

pozycji. Macierz może być wtedy całkowicie wypełniona z pierwszego wiersza lub z pierwszej kolumny przy użyciu "właściwości przekątnej" wyjaśnionej powyżej. Cechą kryptograficzną o pewnym znaczeniu jest to, że każda kolumna zawiera wszystkie 26 liter alfabetu, ponieważ dwie litery nie mogą być szyfrowane tą samą literą w tej samej pozycji koła, wiersze mogą zawierać jedną lub więcej liter dwa lub więcej razy, ponieważ nic nie stoi na przeszkodzie, aby litera szyfrowana była do tej samej litery w dwóch lub więcej miejscach. W rzeczywistości, dzięki kółku o rozmiarze 26 lub dowolnej parzystej liczbie kontaktów, jest pewne, że każdy rząd będzie zawierał co najmniej jedną powtarzaną literę. W powyższym 6-literowym przykładzie to już występuje, C przechodzi do A w pozycjach 1 i 3. Przy nieparzystej liczbie punktów kontaktowych możliwe jest, że wiersze nie będą zawierać żadnych powtarzających się liter. Z kryptograficznego punktu widzenia im mniej powtarzających się liter z rzędu, tym lepiej.

Szyfrowanie przez Enigmę

Właśnie widzieliśmy, jak pojedyncze kółko przewodowe szydzi z literau. W Enigmie prąd z literau klawiaturowego przechodzi przez płytę główną, a następnie przez trzy koła R1, R2 i R3, po czym jest "odwracany" przez odbłyśnik U, a następnie wraca przez trzy koła w kolejności R3, R2 i R1 przed ostatecznym przejściem przez koło wejściowe, aby zapalić lampę, która wskazuje literę szyfrowania. Oryginalny tekst w postaci zwykłego tekstu ulega zatem 9 zmianom, zanim ostatecznie pojawi się jako szyfrowa litera; w rzeczywistości, jak zobaczymy później, w większości wersji militarnych Enigmy nastąpiły 2 dalsze zmiany, w sumie 11. Gdyby wszystkie koła zostały naprawione, Enigma dostarczałaby jedynie złożonego sposobu generowania prostego szyfru zastępczego, ale nie są one ustalone. Po naciśnięciu klawisza z literą prawe koło, R1, natychmiast obraca jedną pozycję, a prąd przechodzi przez maszynę. Po tym, jak 26 liter zostanie zaszyfrowanych, R1 powróci do swojej pierwotnej pozycji. O ile R2 lub R3 nie poruszyły w międzyczasie Enigmy , byłby równoważny 26 prostym szyfrom podstawiania; R2 jednak się poruszy. Pierścień zacinający na R1 porusza się wraz z kołem i tak, w pewnym momencie podczas 26 kodowań, wycięcie w kształcie litery V osiągnie pozycję bezpośrednio przed dźwignią z tyłu maszyny naprzeciwko R1, to pozwoli dźwigni na zaczepić o wycięcie w kształcie litery V, a to z kolei pozwoli dźwigni znajdującej się po przeciwnej stronie R2 spowodować zmianę pozycji R2. Ponieważ R2 teraz przeniósł alfabety encyklopedyczne wszystkie będą się różnić od tego, co było 26 kodowania wcześniej. R2 w ten sposób się porusza co najmniej raz na 26 literowych szyfrów; w rzeczywistości porusza się nieco częściej niż to, ponieważ R2 ma również pierścień nacinający, a gdy jego wycięcie jest przeciwne do dźwigni za R2, trzecie koło R3 zostaje przesunięte o jedno położenie, a R2 również jest obrócony. Konsekwencją tego wszystkiego jest to, że trzy koła nie powróciły do swoich oryginalnych pozycji, dopóki 26 x 25 x 26 = 16900 liter zostało zakodowanych. W ten sposób maszyna Enigma zapewnia automatyczny sposób korzystania z 16900 prostych szyfrów zastępczych. Na przykład, jeśli pierścień karbowania na R1 był tak ustalony, że jego wycięcie spowodowało, że R2 obrócił się, gdy R1 był w ustawieniu Z, jak pokazano w jego oknie, i podobnie z pierścieniem zaciskowym na R2, kolejne pozycje trzech kół, gdy są one uruchamiane w pozycjach A, Y, Y (od lewej do prawej)

być

A Y Y,

A Y Z,

A Z A,

B A B.

Ta mnogość alfabetów zastępczych zapewnia dobre bezpieczeństwo, ale to nie koniec historii, ponieważ zanim 16 900 liter zostało zaszyfrowanych, trzy koła przewodowe można usunąć i przywrócić w innej kolejności na wspólnej osi. W oryginalnej wersji Enigmy w zestawie znajdowały się tylko trzy koła, które zostały dostarczone wraz z maszyną, dzięki czemu można je było zamówić na sześć sposobów. Liczba dostępnych prostych podstawień w związku z tym alfabet

6 x 16900 = 101400.

W rzeczywistości, ponieważ R2 może być uruchomiony w którymkolwiek z jego 26 miejsc, włączając w to Z, nawet jeśli nie może on ruszyć się do pozycji Z podczas normalnej pracy, chyba że R1 również był wcześniej w Z, jest 6 x 26 x 26 x 26 = 105456 możliwy pozycje początkowe i proste alfabety zastępcze. Zakładając, że kryptoanalityk miał taką Enigmę, musiałby zmierzyć się z 105456 możliwymi ustawieniami kół dla początku każdej wiadomości a to, w czasach przed komputerami, wydaje się przedstawiać mu niemożliwe zadanie. Jeśli kryptoanalityk nie miał dostępnej Enigmy i nie znał wewnętrznych obwodów trzech kół i odbłyśnika, liczba możliwości, które musiałby wypróbować, byłaby o wiele większa, ponieważ istnieją

25! (tj. 25 x 24 x 23 x 22 x...x 2 x 1)

możliwe okablowania każdego koła, a ta liczba jest większa niż

10^{25}.

Trzy takie koła mogą być podłączone w więcej niż

10^{75}

sposoby. Co więcej, kryptoanalityk nie znałby wewnętrznego okablowania reflektora i to zwielokrotnia liczbę możliwości o czynnik większy niż

10^{12}

W związku z tym kryptoanalityk w obliczu wiadomości zakodowanych na Enigmie z nieznanymi kablami najwyraźniej będzie musiał spróbować więcej niż

10^{87}

odszyfrowań, zanim uzyska pewność sukcesu. Kryptografowie zakładają jednak, że wróg uzyskał jedną ze swoich maszyn w pierwszym dniu użytkowania, więc ocena bezpieczeństwa pierwotnej Enigmy musi opierać się na liczbie nie 1087, ale 105456 przypadków, które należy rozważyć, w 1923 r., przed wynalezieniem komputera, mogło być uznane za odpowiednie dla maszyny przeznaczonej do czysto komercyjnego wykorzystania. Niemieckie wojsko jednak tak nie uważało i nalegało na pewne zmiany, które znacznie poprawiły bezpieczeństwo, z których najważniejszym było wprowadzenie

Wtyczka Enigma

Wojskowa wersja Enigmy zawierała wtyczkę z przodu, pod klawiaturą maszyny do pisania. Ta wtyczka miała 26 gniazd, które można połączyć parami za pomocą 13 krótkich kabli. Efektem tego była zamiana par liter na etapie wejściowym i wyjściowym. Tak więc, na przykład, jeśli A był podłączony do W kablem, wtedy za każdym razem, gdy operator szyfru wpisał A, wchodziłoby ono w Enigmę jako W i na odwrót. Podobnie litera szyfrowa, która wyłoniła się z ostatniego koła, R1, jako A, rozświetliłaby lampę W, a więc została zapisana jako W. Liczba sposobów sparowania 26 liter wtyczki jest takie samo, jak liczba możliwych kół reflektorowych, tj. więcej niż 10^{12}, a ponieważ parowania na wtyczce były często zmieniane (codziennie na początku i trzy razy dziennie od 1944), to zwiększyło problem dla

kryptoanalityków, którzy mieli teraz do czynienia z koniecznością rozważenia ponad 10^{17} możliwości zamiast 105456.

Pięta achillesowa Enigmy

Wewnętrzne okablowanie trzech kół i reflektora w wojskowej wersji Enigmy było, przy zrozumiałym nacisku wojska, odmienne od tych z oryginalnej wersji cywilnej z 1923 r., Więc posiadanie cywilnej Enigmy w wersji z 1923 r. Nie pomogłoby kryptoanalityki. Dodatkowo wprowadzono wtyczkę. Nawet jeśli kryptoanalityk uzyskał wersję Enigmy w wersji wojskowej, wydaje się, że 10^{17} możliwości uniemożliwiły nawet przesłanie pojedynczego komunikatu. Jeżeli mamy milion odszyfrowań druga próba,potrwa jeszcze kilka tysięcy lat; a w latach trzydziestych nie było komputerów. Jak to się stało, że w 1932 r. doszło do znalezienia metody do odszyfrowania informacyji? Podstawowa wada, która doprowadziła do odszyfrowania wiadomości Enigmy, nie była spowodowana konstrukcją samej maszyny, ale metodą, którą Niemcy wykorzystali do wysyłania wiadomości. Jak zauważono wcześniej, jeśli operator szyfru wysyła wiadomość w dowolnym systemie szyfrowania o zmiennych parametrach, musi w jakiś sposób powiadomić odbiorcę o wartości tych parametrów lub pozostawić go do wykonania. Ta druga sytuacja rzadko ma zastosowanie, choć może mieć zastosowanie w przypadku cylindra Jeffersona. W przypadku Enigmy taki układ jest dość niepraktyczny, a odbiorca musi mieć wszystkie informacje potrzebne do rozszyfrowania wiadomości. Jakie informacje są potrzebne odbiorcy? Zakładając, że zarówno nadawca Enigmy, jak i odbiorca są "w tej samej sieci", to znaczy używają tych samych kół Enigmy, w tej samej kolejności i w tych samych układach wtyczek, nadal istnieje problem polegający na tym, że nadawca musi w jakiś sposób odbiorca zna pozycje trzech kół na początku wiadomości, a ta niezbędna informacja stanowi w tym przypadku "wskaźnik". Wybór tych pozycji wyjściowych lub "ustawień" powinien być "losowo" wybrany przez nadawcę, ponieważ jeśli pewna liczba wiadomości zostanie zaszyfrowana z tym samym początkowym ustawieniem, kryptoanalityk będzie miał "głębokość", a wiadomości mogą wtedy być czytelne, nawet jeśli tożsamość kół i / lub ich początkowe ustawienia mogą nie zostać wykryte. Ponieważ istnieje 17 576 możliwych startów pozycji dla trzech kół prawdopodobieństwo, że każda para wiadomości otrzyma takie same ustawienia początkowe, jest mniejsze niż 0.000 06, jeśli ustawienia są wybierane losowo, ale w praktyce operatorzy szyfrów mogą rozwijać nawyki, na przykład wybierając trzy litery dla ustawienia kół z tego samego rzędu klawiatury, które znacznie zwiększają prawdopodobieństwo głębokości. Nawet z przypadkowo wybranymi ustawieniami, jeśli są duże liczba wiadomości jest wysyłanych z tą samą konfiguracją urządzenia (ta sama kolejność kół i wtyczka), a głębokość może być przypadkowa: na przykład 200 wiadomości spowodowałoby większe prawdopodobieństwo, że przynajmniej jedna para wiadomości będzie głębokość. Aby zmniejszyć prawdopodobieństwo wystąpienia głębokości, konfiguracja musi zostać zmieniona wystarczająco często, aby bardzo duża liczba komunikatów o tym samym ustawieniu była bardzo mało prawdopodobna.

Metoda początkowo przyjęta przez Niemców w celu zaznajomienia odbiorcy z pozycjami wyjściowymi trzech kół opierała się na zastosowaniu wspólnego ustawienia terenu, a procedura dla nadawcy była następująca.

(1) Wybierz "losowy" zestaw trzech liter dla rzeczywistych ustawień koła, które będą używane do szyfrowania wiadomości; załóżmy, że to jest FMZ (powiedzmy).

(2) Sprawdź literaę dostarczoną wszystkim użytkownikom sieci i zanotuj ustawienie naziemne dla danego dnia (lub okresu, jeśli ustawienie podłoża zmienia się częściej niż raz dziennie); załóżmy, że to BLE (powiedzmy).

(3) Obróć koła do ustawienia podłoża, BLE.

(4) Zaszyfruj trzy litery wybranego ustawienia losowego dwa razy; to znaczy, zaszyfruj sześć liter FMZFMZ i zanotuj sześć wynikowych liter szyfrujących; przypuśćmy, że są to LOCWHQ (powiedzmy).

(5) Obróć kółka do wybranego losowego ustawienia, FMZ i zaszyfruj wiadomość.

(6) Poprzedzaj tekst szyfrowany wiadomości sześcioma literami szyfrowania podwójnego wskaźnika LOCWHQ.

(7) Prześlij komunikat szyfrowania z zaszyfrowanym podwójnym wskaźnikiem z przodu.

Po odebraniu komunikatu szyfrowania odbiorca postępował w następujący sposób.

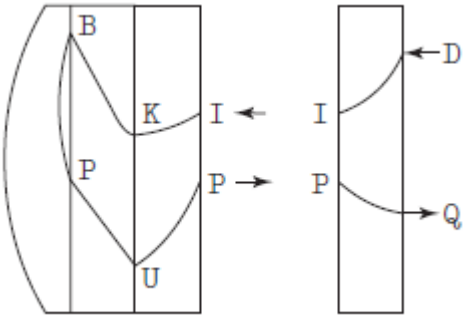
(1) Ustaw trzy koła na ustawienie ziemi na dzień lub na okres, BLE.

(2) Wpisz sześć liter, LOCWHQ, zakodowanego podwójnego wskaźnika. (Pamiętaj, że jest to cechą Enigmy, że szyfrowanie i rozszyfrowanie są równoważne, dlatego, że F w pierwszej encyklopedii stało się L, więc L stałoby się F, co dzieje się, gdy rozszyfrujemy L.)

(3) Powinno to dać dwukrotnie wybrany losowy wskaźnik, a mianowicie: FMZFMZ. Jeśli tak się nie stanie, doszło do pomyłki i konieczne może być ponowne przesłanie wiadomości; niebezpieczna sytuacja, która może spowodować naruszenie bezpieczeństwa.

(4) Jeśli sześć liter odszyfruje do tego samego powtarzanego trigrafu, FMZ w tym przypadku, obróć koła do tych pozycji i rozszyfruj tekst wiadomości.

Zwróć uwagę, że słowo "dwa razy" zaznaczono kursywą. Jak się przekonamy, to właśnie ta procedura operacyjna, wprowadzona w celu zapewnienia poprawnego odbioru ustawień trzyliterowych, okazała się piętą achillesową Enigmy. Zaczynamy od stwierdzenia, że dla koła R2 można poruszać się tylko wtedy, gdy R1 znajduje się w pozycji wycięcia, a na oryginalnej Enigmie było tylko jedno nacięcie na pierścieniu wycinającym z 26 pozycji. Zatem jeśli wycięcie było skuteczne, gdy R1 był na pozycji Z, mogło tylko spowodować, że R2 poruszałoby się podczas sześcioliterowego szyfrowania, gdyby pierwotne ustawienie R1 było U, V, W, X lub Y. (Jeśli pierwotne ustawienie R1 było Koło Z R2 będzie się obracać bezpośrednio przed szyfrowaniem pierwszej litery i pozostanie tam dla następnych pięciu literaowych szyfrów, chyba że R2 sam był w swojej pozycji karbu i spowodował, że zarówno R3, jak i sam, poruszał się przy następnym szyfrowaniu literau; to prawie nie wpływa na prawdopodobieństwo i, dla uproszczenia, zostanie zignorowane. Atak kryptoanalityczny można łatwo zmodyfikować w celu uwzględnienia tej nieprawdopodobnej możliwości). Z tego powodu istnieje zwykle 21 pozycji początkowych R1, które zapewniają, że R2, a zatem R3, pozostają nieruchome w całym łańcuchu znaków sześcioliterowych, a więc prawdopodobieństwo tylko ruchy R1 wynoszą 21/26, czyli więcej niż 0,8. Miałem tam być więcej nacięć na pierścieniu wycięcia, prawdopodobieństwo było oczywiście niższe. W późniejszych etapach wojny niektóre pierścienie wycięcia miały dwa nacięcia, a pierścienie wycięcia Abwehry Enigma miały o wiele więcej, jak widzimy później. Jeśli R2 i R3 nie poruszają się podczas szyfrowania sześcioliterowego wskaźnika, Enigma staje się faktycznie maszyną jednokołową, składającą się z R1 i kompozytowego reflektora, złożonego z U, R3 i R2, z których żaden nie porusza się podczas szyfrowania. Zilustrowano to na rysunku 9.3.



Odbłyśnik kompozytowy, utworzony przez stacjonarne koła R2 i R3 ze stałym odbłyśnikiem U znajduje się po lewej stronie. R1, jedyne koło, które porusza się podczas sześcioliterowej encyklopedii, znajduje się po prawej stronie. Wewnętrzne linie pokazują, jak w typowej encyklopedii tekst jawny D może stać się literą Q. Kluczową sprawą jest to, że jeśli, jak pokazano na schemacie, D jest zakodowane na I, a Q jest zakodowane na P przez R1 , IP to para w kompozytowym odbłyśniku, co oznacza, że podczas sześcioliterowej encyklopedii każda litera wchodząca do kompozytowego odbłyśnika, kiedy ja wynurzę się z niej jako P, i vice versa

Wskaźnik "łańcuchów" w Enigmie

Na rysunku 9.3 zobaczyliśmy, w jaki sposób szyfrowanie litery obejmuje jedną z 13 par w reflektorze kompozytowym; w typowym przykładzie pokazanym na rysunku 9.3 litera D tekstu jawnego została zmieniona na I przez R1, a zatem weszła w kompozytowy reflektor jako I. Po zmianie na K, następnie B, następnie P, odpowiednio przez R2, R3, U i R3, wyłania się z R2, a więc od kompozytowego odbłyśnika jako P, zanim ostatecznie przejdzie z powrotem przez R1 i wytworzy literową literę Q, ponieważ koło wejściowe, połączone w kolejności alfabetycznej, pozostawi niezmienioną literę pochodzącą z R1. Jeśli więc, my znałem tożsamość, wewnętrzne okablowanie i pozycję wyjściową R1 i zaszyfrowałem D, dając I, i zaszyfrowałem Q, dając P, odkrylibyśmy jedną z 13 par kompozytowego reflektora. Gdybyśmy mieli dużą liczbę takich prostych par szyfrów, stwierdzilibyśmy, że gdybyśmy poprawnie zidentyfikowali zarówno koło R1, jak i jego początkowe ustawienie, zawsze otrzymalibyśmy jedną z tych 13 par liter z kompozytowego reflektora. Jeśli z drugiej strony użylibyśmy niewłaściwego koła jako R1, lub właściwego koła, ale w nieprawidłowym ustawieniu, znaleźlibyśmy nie tylko 13 par, ale i więcej, ponieważ istnieje 325 możliwych par 26 liter, a my dostanie sprzeczności, takie jak "IP to para, ale tak samo jest IM". W ten sposób wkrótce dowiedzielibyśmy się, kiedy znaleźliśmy właściwe koło i jego ustawienie. Problem polega na tym, że: nie znamy tożsamości litery wejściowej tekstu jawnego (D w przykładzie), chociaż znamy literę wyjściową szyfrowania (Q); więc jak postępujemy? Odpowiedź jest taka, że istnieje cecha sześcioliterowych wskaźników, pierwotnie odkrytych przez polskich kryptoanalityków w 1932 roku, które pozwalają nam zidentyfikować poprawne R1 i jego ustawienie tą metodą, bez znajomości liter wejściowych. Odkrycie opiera się na dwóch faktach:

(i) pary zwykłego szyfrowania są odwracalne; na przykład jeśli A jest w encyklach M (powiedzmy), to M encyklów do A przy tych samych ustawieniach koła;

(ii) sześcioliterowy wskaźnik zapewnia trzy przypadki, w których ta sama litera została zaszyfrowana na pozycjach w tekście, które są oddalone od siebie o trzy, a więc w powyższym przykładzie, gdzie zaszyfrowany wskaźnik to LOCWHQ, (L, W), (O, H) i (C, Q) są takimi parami, a jeśli R2 nie porusza się podczas szyfrowania wskaźnika, możemy mieć nadzieję na zidentyfikowanie R1 i jego ustawienie.

Ponieważ (i) jest zawsze prawdziwe i (ii) zawiera około 80% czasu, w którym szanse powodzenia, przy użyciu opisywanej metody, są dobre, jeśli dostępna jest wystarczająca ilość informacji. Nawet jeśli R2

się poruszy, atak może się powieść, jeśli R2 poruszy się między drugą a trzecią literą (powiedzmy), wtedy trzecia i szósta litera (C i Q w przykładzie) zostaną wytworzone przez tę samą literę na maszynie, na której tylko R1 się poruszył. W najgorszym przypadku, gdy R2 zmienia się pomiędzy trzecią a czwartą literą, atak jest nieważny, ale fakt, że się nie powie, informuje kryptoanalityka, że R2 prawdopodobnie się poruszył i może to być pomocne w innym ataku. Przed opisaniem metody znajdowania tożsamości i ustawienia R1 warto przyjrzeć się przykładowi małej skali. W tym przykładzie wskaźnik składa się z tylko jednej litery, która jest natychmiast powtarzana, zamiast trzech powtórzeń, jak w samej Enigmie. Atak kryptoanalityczny jest taki sam w obu przypadkach. Łańcuchy powstają z par szyfrów w pozycjach 1 i 2, a nie w pozycjach 1 i 4 (oraz (2, 5) i (3, 6) w przypadku Enigmy).

Przykład 9.1 (Mini-Enigma)

Następujące 12 par liter szyfru jest wynikiem zaszyfrowania 12 liter alfabetu zwykłego AA, BB, ..., KK, LL (w nieznanej kolejności) w kolejnych pozycjach i przy wspólnym ustawieniu ziemi, poprzez 12- litera maszyna szyfrująca typu Enigma:

AK, BL, CI, DD, EB, FG, GE, HH, IA, JC, KJ, LF.

Tworzymy "łańcuchy" z tych par, łącząc pary, w których druga litera jednej pary jest taka sama jak pierwsza litera innej pary, zatrzymując się, gdy litera się powtarza:

AKJCI

BLFGE

DD

HH

Widzimy, że istnieją dwa łańcuchy składające się z 5 różnych liter i dwóch łańcuchów o długości zaledwie jednej litery. Czy to przypadek? Nie; nie jest. Polscy kryptoanalizatorzy odkryli, że szyfrowanie par tej samej litery na pozycjach położonych w jednym lub więcej miejscach, gdy tylko ruchy R1, zawsze spowoduje powstanie łańcuchów, które występują w parach. Dowód na to nie jest bardzo trudny ale jako kolejny dowód jest tu pełnowymiarowy przykład z danymi wygenerowanymi na aktualnej maszynie Enigma.

Przykład 9.2

Z partii dwuliterowych wskaźników, składających się z dubletów zakodowanych na Enigmie przy wspólnym podłożu, wyodrębniono następujący zestaw 26, posortowany według pierwszej litery zaszyfrowanego wskaźnika:

AB BQ CD DK EZ FF GH HC IR JT KS LP ML

NU OO PI QN RA SJ TV UM VY WX XW YG ZE

Tworzymy "łańcuchy".

Począwszy od A mamy łańcuch ABQNUMLPIR o długości 10.

Ponieważ C nie wystąpiło, teraz zacznijmy od tego i znajdź CDKSJTVYGH, także o długości 10.

Ponieważ E nie znajduje się w żadnym z tych łańcuchów, zaczynamy od tego i znajdujemy łańcuch EZ o długości 2.

F wciąż brakuje i widzimy, że idzie do siebie, tworząc łańcuch o długości 1, F.

O, W i X są pozostałymi literami i widzimy z litery, że O idzie do siebie tworząc drugi łańcuch o długości 1, O i W, X idą do siebie, tworząc drugi łańcuch o długości 2, WX.

Podsumowując, mamy:

Dwa łańcuchy o długości 10: ABQNUMLPIR i CDKSJTVYGH.

Dwa łańcuchy o długości 2: EZ i WX.

Dwa łańcuchy o długości 1: F i O.

Gdyby 26 dubletów nie zostało zaszyfrowanych przy tym samym ustawieniu tego samego koła, R1, mielibyśmy sprzeczności w dubletach szyfrów, mając na przykład z jednej strony AB, a także inną parę, taką jak AF. Samo istnienie unikalnego zestawu 26 nie sprzecznych par potwierdza hipotezę, że R1 był taki sam dla wszystkich z nich i nic się nie poruszało. Aby uzyskać łańcuchy, potrzebujemy wystarczającej ilości komunikatów, aby zapewnić wskaźniki zaczynające się od każdej z 26 liter alfabetu. Jeśli wskaźniki zostaną wybrane losowo, wiele początkowych liter pojawi się dwa lub więcej razy, a więc spodziewamy się, że potrzebujemy więcej niż 26 wiadomości, zanim znajdziemy 26 wskaźników zaczynających się od 26 różnych liter alfabetu. Ile wiadomości możemy potrzebować? Można matematycznie wykazać, że prawdopodobnie potrzebowalibyśmy około 100 komunikatów. Jak na ironię, jeśli operatorzy szyfrujący wybiorą swoje wskaźniki w sposób nie losowy, na przykład wybierając wszystkie trzy litery z tego samego rzędu klawiatury, potrzeba jeszcze więcej wiadomości, aby uzyskać pełny zestaw łańcuchów. Z drugiej strony, prawdopodobieństwo znalezienia dwóch lub więcej komunikatów "dogłębnie" byłoby zwiększone, a kryptoanalityki mogłyby wtedy odzyskać jakiś tekst jawny, który doprowadziłby do rozwiązania inną drogą. Jakikolwiek rodzaj nielosowej funkcji w systemie szyfrowania lub w procedurze operacyjnej może pomóc kryptoanalitykom

Wyrównanie łańcuchów

Analiza pokazująca, że łańcuchy o równej długości występują w parach, pokazuje również, jak wykorzystać ten fakt do odkrycia tożsamości i ustawienia R1. Aby to zrobić, musimy wyrównać pary łańcuchów o tej samej długości, ale jeden z łańcuchów takiej pary musi zostać odwrócony. Ponadto musimy wypróbować każde możliwe wyrównanie liter. Tak więc, dla dwóch łańcuchów 10-literowych powyżej, możemy mieć 20 możliwych dopasowań, w zależności od tego, który łańcuch odwracamy i która litera jest pierwsza, a mianowicie:

ABQNUMLPIR

CHGYVTJSKD

to jedno możliwe wyrównanie, ale na przykład jest 19 innych

CDKSJTVYGH

IPLMUNQBAR

Gdy mamy poprawne wyrównanie dwóch powiązanych łańcuchów, pary pionowych liter, które są zaszyfrowane za pomocą właściwego R1 przy pierwszym ustawieniu, ujawnią pary w kompozytowym odbłyśniku, podczas gdy pary przekątnej NW-SE, gdy zostaną zaszyfrowane przy drugim ustawieniu R1, również ujawnią te same pary. Nieprawidłowe koło lub nieprawidłowe ustawienia spowodują sprzeczności. Ten kluczowy fakt, będący następstwem procedury operacyjnej zastosowanej na Enigmie, został odkryty przez polskich kryptoanalityków w 1932 roku. W tym przykładzie mamy kilka krótkich łańcuchów, a ponieważ istnieje mniej możliwości wyrównania, prawdopodobnie zostaną one wypróbowane jako pierwsze.

Identyfikacja R1 i jego ustawienie

Przykład identyfikacji R1 i jej ustawienia na pełnym rozmiarze Enigma ze znanymi kołami, ale nieznanym plug-in wymagałby dużej ilości danych i wielu stron analizy, ale to był problem codziennie spotykany przez kryptoanalityków. Metodę tę można jednak zilustrować za pomocą danych z przykładu 12-punktowego mini-Enigma powyżej. Zakładamy, że jest on znany i musimy sprawdzić, czy którekolwiek ze znanych kół w jednym z 12 możliwych pozycji wyjściowych może być R1. Ponieważ istnieje wiele niepoprawnych możliwości, rozpatrywane będą tylko dwa przypadki: jeden niepoprawny, a drugi poprawny.

Przykład 9.3

Uważa się, że dublety w 12-punktowej mini-Enigmie są zakodowane w kolejnych położeniach koła na wspólnym stole naziemnym z R1 mającym tablicę szyfrowania pokazaną w Tabeli 9.2.

	Setting											
Input letter	1	2	3	4	5	6	7	8	9	10	11	12
A	K	A	G	L	H	F	I	C	F	D	L	E
B	F	L	B	H	A	I	G	J	D	G	E	A
C	B	G	A	C	I	B	J	H	K	E	H	F
D	G	C	H	B	D	J	C	K	I	L	F	I
E	J	H	D	I	C	E	K	D	L	J	A	G
F	H	K	I	E	J	D	F	L	E	A	K	B
G	C	I	L	J	F	K	E	G	A	F	B	L
H	A	D	J	A	K	G	L	F	H	B	G	C
I	D	B	E	K	B	L	H	A	G	I	C	H
J	I	E	C	F	L	C	A	I	B	H	J	D
K	E	J	F	D	G	A	D	B	J	C	I	K
L	L	F	K	G	E	H	B	E	C	K	D	J

Pokaż, że wyrównanie łańcuchów to

D AICJK

H BLFGE

(1) prowadzi do sprzeczności, jeśli założymy, że R1 jest pierwotnie w ustawieniu 1, ale

(2) tworzy rozwiązanie, jeśli weźmiemy R1 początkowo na ustawienie 2.

Rozwiązanie

(1) Zaczynamy od parowania pionowych par z łańcucha na parach ustawień 1 i diagonalnych (NW-SE) w ustawieniu 2. 12 par, które uzyskamy, powinno być spójne i dostarczyć 6 par reflektora kompozytowego: Tabela 9.3.

Setting 1	Setting 2
DH→GA	DH→CD
AB→KF	AL→AF
IL→DL	IF→BK
CF→BH	CG→GI
JG→IC	JE→EH
KE→EJ	KB→JL

Wywołują one szereg sprzeczności: np. Ustawienie 1 oznacza, że (A, G) są sparowane w kompozytowym odbłyśniku, natomiast ustawienie 2 mówi nam, że (A, F) są sparowane. Dlatego R1 nie znajduje się w ustawieniu 1. (2) Powtarzamy ćwiczenie, ale tym razem zaszyfrujemy pary w Ustawieniach 2 i 3: Tabela 9.4.

Setting 2	Setting 3
DH→CD	DH→HJ
AB→AL	AL→GK
IL→BF	IF→EI
CF→GK	CG→AL
JG→EI	JE→CD
KE→JH	KB→FB

Te dwa zestawy są w pełni zgodne i dochodzimy do wniosku, że zidentyfikowaliśmy R1 i że zostało ono ustawione na pozycji 2 na początku szyfrowania. Wiemy również, że pary 12 liter w kompozytowym odbłyśniku są

(A, L), (B, F), (C, D), (E, I), (G, K) i (H, J).

Ponieważ R1 i rzeczywisty reflektor (U) są znane, kryptoanalityk będzie teraz próbował znaleźć, które kombinacje U i dwóch innych kół może wytworzyć te pary. Oryginalna Enigma miała tylko trzy koła w swoim zestawie, a zatem, ponieważ R1 został zidentyfikowany, byłoby "tylko" 2? 26? 26? 1352 możliwości do zbadania. Chociaż może wydawać się, że jest to duża liczba, jest niewielka w porównaniu z przypadkami 105456, z którymi kryptoanalityk musiałby stawić czoło. Inne linie ataku będą teraz również wykorzystane, takie jak wypróbowanie niektórych możliwych początków tekstowych dla niektórych wiadomości. Należy oczywiście zdać sobie sprawę z tego, że przykład daje tylko wskazówkę, w jaki sposób można odszyfrować wiadomości na oryginalnej Enigmie, bez podkładki i tylko trzech kółek w zestawie. Dokonano wielu zmian w samej Enigmie i jej procedurach operacyjnych, szczególnie w latach 1938-45. Na przykład:

(1) powtórzenie trzyliterowego wskaźnika zostało zmodyfikowane przez wstawienie pary atrapowych liter i użycie dwuwymiarowej tablicy zastępczej;

(2) zaniechano korzystania ze wspólnej podstawy naziemnej; operatorzy wybrali własne ustawienie naziemne, które dali, bez poprawek, na początku tekstu zaszyfrowanego;

(3) trzy koła zostały zwiększone do pięciu przez wszystkich użytkowników, a później do ośmiu przez niemiecką marynarkę wojenną, która również użyła czterokołowej Enigmy z 1942 r., Która obejmowała nowy reflektor. Zmiany te zapewniły kryptoanalitykom w Bletchley szereg poważnych wyzwań, które zostały pokonane, w niektórych przypadkach szybko, ale w przypadku maszyny czterokołowej tylko przy dużym wysiłku. Każdy zainteresowany symulowaniem Enigmy na PC i postępowaniem według oryginalnych polskich rozwiązań uznałby za interesujący. Dla tych, którzy chcieliby spróbować ustawić koło (mini-) Enigmy tutaj:

Problem 9.1

Na 10-punktowej mini-Enigmie, która była używana do szyfrowania wiadomości w oparciu o cyfry 0-9, wyniki szyfrowania dubletów 00, 11, ..., 99 przy tym samym ustawieniu gruntu są uzyskiwane ze wskaźników (w nieznanym zamówienie) i są

(0, 2), (1, 6), (2, 3), (3, 9), (4, 8), (5, 5), (6, 4), (7, 7), (8 , 1) i (9, 0).

Pierwsza kolumna tablicy szyfrującej koła, która jest uważana za R1

(0, 8, 6, 4, 3, 7, 1, 5, 9, 2).

Uzupełnij tabelę szyfrowania i, przy odpowiednim wyrównaniu łańcuchów, sprawdź, czy R1 przy ustawieniu 3 jest zgodny z danymi. Jakie są pary w kompozytowym odbłyśniku?

Podwójnie zakodowane wiadomości Enigmy

Kwestia, czy podwójne szyfrowanie jest warte zachodu, została krótko omówiona w rozdziale 4, gdzie w efekcie odpowiedź była "czasami", ponieważ konieczne jest zrównoważenie zwiększonego bezpieczeństwa (jeśli istnieje) z ryzykiem, że operator użyje szyfrów w zła kolejność, tworząc komunikat szyfrowy, który nie może być odczytany przez zamierzonego odbiorcę, ale może pomóc kryptoanalitykowi. Enigma stanowi dobry przykład, który ilustruje oba te punkty. Podczas wojny niektóre szczególnie ważne wiadomości Enigmy zostały podwójnie zaszyfrowane. Oficer szyfrowałby wiadomość za pomocą tych samych kółek, ale inną kasetę, jako urzędnika szyfrującego; ustawienia kół zostaną wybrane ze specjalnej litery 26 możliwości, oznaczonych literami alfabetu. Następnie przekazałby ten komunikat szyfrowania urzędnikowi poprzedzającemu słowo OFFIZIER i inne słowo zaczynające się na literę wskazującą, które z 26 ustawień, których używał. Recepcjonista szyfrowałby tę wiadomość w normalny sposób. To niewątpliwie przyczyniło się do bezpieczeństwa, ale przynajmniej przy jednej okazji oba szyfrowania zostały zastosowane w złej kolejności (oficer i szyfrant byli tą samą osobą w tym dniu). Jack Good domyślił się, co się stało i odszyfrował wiadomość.

Enigma Abwehry

Abwehra (tajna służba wywiadowcza niemieckiego naczelnego dowództwa) użyła zmodyfikowanej wersji Enigmy, która zasługuje na szczególną uwagę. Nie było wkładki, co ułatwiało życie kryptoanalitykom, ale pierścienie wycięcia zawierały 11, 17 lub 19 nacięć zamiast 1 lub 2. Wirniki poruszały się więc znacznie częściej niż w "standardowej" Enigmie i reflektor również się poruszał, co utrudniło życie. Praktyka zaszyfrowania (czteroliterowego) wskaźnika dwukrotnie przy danym ustawieniu gruntu została zachowana, a więc ośmioliterowa grupa poprzedzała tekst szyfrowania. Kryptoanalitycy nadal stosowali metodę "łączenia", ale dodatkowo byli w stanie wykorzystać sytuację, w której wszystkie cztery wirniki poruszają się jednocześnie.

Maszyna szyfrowania Hagelina

Tło historyczne

Można by sądzić, całkiem słusznie, że jakikolwiek kraj będzie starał się zachować w tajemnicy tożsamość swoich maszyn szyfrujących i ogólnie jest to prawda. Jeśli maszyny szyfrujące zostały zaprojektowane i zbudowane w danym kraju, tak jak w przypadku Enigmy w Niemczech, zachowanie tajemnicy i szczegółów byłoby możliwe, ale gdyby maszyna została zakupiona gdzie indziej, byłoby prawie nieuniknione, że inni ostatecznie o tym wiedz. W tych okolicznościach może wydawać się zaskakujące, że przed i podczas II wojny światowej istniała maszyna szyfrująca używana przez kilka krajów po obu stronach, w tym w Niemczech, Włoszech, Wielkiej Brytanii, USA i Francji. Maszyna ta została wyprodukowana w Szwecji, kraju neutralnym, przez firmę Boris Hagelin i została sprzedana każdemu, kto chciał. Był znany pod różnymi nazwami w różnych krajach (Hagelin, M209, C36, C38, C41, ...), ale z pewną odmianą był w zasadzie tą samą maszyną we wszystkich przypadkach. Podstawową funkcją maszyny Hagelin było dostarczenie długiej sekwencji "pseudolosowych" liczb, które były używane jako kluczowy strumień dla szyfrowania zwykłego tekstu za pomocą równania

(litera szyfru) = klucz - (litera jawna)(mod 26). (10.1)

Tak więc, na przykład, jeśli litera z jawnym tekstem byłaby F (odpowiednik liczbowy =5), a klucz miał 18 było liczbą szyfrowania byłaby N ponieważ

18-5=3 (numeryczny odpowiednik N).

Zauważ, że równanie (10.1) można odwrócić, tj.

(Literę tekstu jawnego) = klucz - (Litera szyfrująca) (mod 26), (10.2),

tak aby istniała wzajemność między tekstem jawnym a literami szyfrów, co oznacza, że szyfrowanie i rozszyfrowanie są identyczne, jak w Enigmie. Na Hagelinie jednak litera może się szyfrować sama co nie może się zdarzyć na Enigmie.

Struktura maszyny Hagelin

Hagelin generował kluczowy strumień za pomocą sześciu wiatraków i klatki. Sześciokątne koła zostały zamontowane równolegle na wspólnej osi i mogły być niezależnie poruszane, co było konieczne podczas ustawiania maszyny lub razem, co miało miejsce za każdym razem, gdy list został zaszyfrowany lub rozszyfrowany. Każde koło miało pewną liczbę sworzni na obwodzie, a każdy z nich można było przesunąć tak, aby wystawał na lewą lub prawą stronę koła. Liczba pinów była różna dla każdego koła; spojrzał z przodu maszyny numery pinów na sześciu kołach, od lewej do prawej strony, wynosiły 26, 25, 23, 21, 19 i 17. Za każdym razem, gdy litera była zaszyfrowana, każde koło przesunęło się o jedną pozycję. Ponieważ sześć długości kół nie ma wspólnego współczynnika, wszyscy nie powrócą do swojej początkowej pozycji

26 x 25 x 23 x 21 x 19 x 17 = 101405850

litery zostały zaszyfrowane. Litery alfabetu były wygrawerowane wokół obręczy każdego koła, aby umożliwić operatorom ustawienie kół do ich pozycji wyjściowych. Na 26-kolowym wyryto cały alfabet, ale inne koła oczywiście wymagały mniej liter. Tak więc na 17 kołach wystarczały litery od A do Q. Klatka w kształcie klapy składała się z 27 poziomych prętów ułożonych jako cylinder z końcami każdego pręta przymocowanymi do dwóch okrągłych krążków. Klatka mogłaby się obracać wokół wspólnej osi kołowej, która była równoległa do wspólnej osi kółek kołkowych. Klatka została ustawiona bezpośrednio za kołami wirnikowymi. Na każdym pręcie klatki znajdowały się 2 "łapy", małe kawałki

metalu, które można było wsunąć wzdłuż drążka i zamocować w dowolnej z ośmiu pozycji. Sześć z ośmiu pozycji znajdowało się dokładnie naprzeciw sześciu kół; pozostałe dwie, "neutralne", pozycje nie były przeciwne do żadnych kół, ale leżały między kołami 1 i 2 oraz między kołami 5 i 6. Jeżeli nie więcej niż 1 wypust na dowolnym pręcie znajdował się naprzeciwko koła, maszyna była uważana za "urywaną" tryb'; jeśli jakikolwiek pręt miał 2 wypusty przeciwległe koła, to mówiono, że maszyna jest "w trybie nakładania". Znaczenie tego stanie się jasne później. W obskurnej klatce jeden występ na każdym pręcie prawdopodobnie byłby umieszczony naprzeciwko koła. Nie było konieczne, aby wszystkie 27 końcówek było tak ustawione, ale nie było żadnej korzyści kryptograficznej przy użyciu mniejszej liczby. Na przykład, 27 występów może być rozdzielonych pomiędzy sześć kółek jako

26 25 23 21 19 17

4 1 9 6 5 2

Liczba występów naprzeciwko koła jest czasami określana jako "kopnięcie" tego koła. Tak więc 26-kołowe koło ma "kopnięcie 4" itd. Kolejność jest ważna; klatka powyżej (4, 1, 9, 6, 5, 2) nie wytworzyłaby takiego samego strumienia klucza jak, powiedzmy (9, 1, 4, 2, 6, 5), chociaż byłoby pewne statystyczne podobieństwo. Po lewej stronie maszyny znajdowało się małe kółko z wygrawerowanym alfabetem; to było używane do wprowadzania tekstu w postaci zwykłego tekstu. Było też koło drukujące, które drukowało literę szyfru na cienkim pasku z papierowej taśmy. Ta taśma miała gumę na odwrotnej stronie, której celem było umożliwienie operatorom przyklejenia szyfru lub tekstu jawnego na arkuszach papieru. Rolka tego klejonego papieru mieściła się z tyłu maszyny, a tam był również nacięty śrubokręt, aby umożliwić operatorom ustawienie szpilek i końcówek. Po prawej stronie maszyny znajdował się uchwyt, który po obróceniu obróciłby klatkę i tak zaszyfrował lub rozszyfrował tekst; ten uchwyt również spowodował, że każde z sześciu kółek przesunęło się do przodu o jedną pozycję. Aby zaszyfrować literę operator obrócił kołem wejściowym, aż wybrana litera była przeciwna do strzałki, a następnie przekręciła uchwyt; klatka obróciła się, niektóre paski na klatce przesunęły się i spowodowały, że zarówno koło wejściowe, jak i koło drukujące mogły obracać się w zakresie od 0 do 27 pozycji. Została wydrukowana litera szyfrująca, a sześć kółek przesunęło się o 1 pozycję. Kolejna litera nie mogła zostać zaszyfrowana, chyba że operator podmienił koło wejściowe. Jeśli przypadkiem znajdował się on w miejscu, w którym następna litera znajdowała się naprzeciwko strzałki, trzeba było obrócić kierownicę o kilka miejsc do przodu, a następnie tę samą liczbę miejsc z powrotem. Tak więc, jeśli ostatnią literą szyfrującą było, powiedzmy, T, a następną literą tekstu był również T, operator szyfru musiałby przesunąć koło wejściowe o kilka miejsc, a następnie odwrócić go do T zanim klamka obróci klatkę. W przypadku fotografii Hagelin z zamkniętą i otwartą pokrywą patrz Tablice 10.1 i 10.2.

26-Wheel	4	0	4	4	0	0	0	4	0	4	0	4	4	4	0	4	0	0	0	4
25-Wheel	0	1	1	0	0	0	1	1	0	1	1	1	1	0	0	0	1	0	1	0
23-Wheel	9	9	9	0	0	9	0	0	0	9	0	9	9	0	9	9	0	0	9	9
21-Wheel	6	0	6	6	0	0	0	0	6	6	6	0	6	6	0	0	0	6	6	0
19-Wheel	0	5	5	5	0	5	0	0	5	0	5	5	0	0	0	5	0	5	0	0
17-Wheel	2	0	2	0	2	2	0	2	2	0	0	0	2	2	0	0	2	2	0	2
Key	21	15	27	15	2	16	1	7	13	20	12	19	22	12	9	18	3	13	16	15

	Key value																									
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
C	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
D	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
E	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
F	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
G	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
H	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
I	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
K	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
L	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
P	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Q	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
R	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
S	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
T	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
U	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
V	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
W	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
X	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Y	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Szyfrowanie Hagelina

Każde koło na Hagelinie miało kilka kołków wystających w lewo, a pozostałe po prawej. Operatorzy będą informowani, na początku każdego okresu szyfrowania, do której strony każdy pin ma być popchnięty. Było to żmudne zadanie, ponieważ całkowita liczba pinów była

26 + 25 + 23 + 21 + 19 + 17 = 131.

Pin, który wystawał na lewą stronę koła, nie miałby wpływu na klucz, podobnie jak nieaktywny sworzeń; kołek wystający po prawej stronie (w maszynie przechodzącej przez obrót) powoduje zwiększenie liczby klocków o liczbę występów przeciwnych do tego koła na klatce, tj. za pomocą "kopnięcia" tego koła. Taki pin był nazywany aktywnym. W idealnym przypadku na każdym kole powinna być w przybliżeniu równa liczba aktywnych i nieaktywnych szpilek; gdzieś pomiędzy 40% a 60% aktywności byłoby prawidłowe. Na początku każdego okresu szyfrowania operatorzy musieliby również przesunąć występy na każdym z 27 taktów, aby właściwa liczba znajdowała się naprzeciwko każdego koła, zwracając uwagę, że w obróconej maszynie, co najwyżej jeden występ na każdym pasku był przeciwny. koło, drugie ucho pozostało w jednym z neutralnych położeń. Kiedy litera wejściowa została ustawiona naprzeciwko strzałki, uchwyt został obrócony, a koszyk obrócony. Każde koło miałoby sworzeń w pozycji przeciwnej do niektórych występów; gdyby pinezka znajdowała się po lewej stronie koła, uchwyty mijałyby ją, ale gdyby szpilka znajdowała się po prawej stronie, bolec spowodowałby ruch końcówek, które przesuwałyby pręty, na których zostały umieszczone, i każdy taki ruch spowodowałby koło drukujące, aby przesunąć jedno miejsce. Tak więc, gdyby było 9 występów naprzeciwko 26 koła, koło drukujące byłoby albo poruszane 9 miejsc, jeśli szpilka przeciwna do klatki była aktywna, albo nie poruszała się wcale, gdyby sworzeń był nieaktywny. Gdy klatka zakończy obrót,

wszystkie koła przesuną się o jedną pozycję, a zatem inny zestaw kołków będzie teraz w pozycjach przeciwnych do występów.

Przykład 10.1

W klatce powyżej (4, 1, 9, 6, 5, 2) typowy strumień klucza może być taki, jak pokazano w Tabeli 10.1. Zauważ, że koła 19- i 17-te wykonały pełny cykl podczas generowania tych 20 kluczowych wartości, tak że ich wkład do całkowitego klucza zaczyna się powtarzać, jak wskazują podkreślone wartości. Należy również zauważyć, że ponieważ klucz jest interpretowany przez koło drukujące (mod 26), kluczowa wartość 27 w trzeciej pozycji jest efektywnie wartością kluczową równą 1.

Przykład 10.2

Użyj 20 kluczowych wartości w powyższym przykładzie, aby zaszyfrować poniższy tekst za pomocą metody szyfrowania Hagelin

H A G A M E N T E N I E N I E N I E N I E N I E N IE

Najpierw konwertujemy tekst na liczby

H A G A M E N T E N I E N I E N I E N I E N I E N IE

7 0 6 4 11 8 13 23 4 13 2 8 15 7 4 17 12 4 13 19

następnie odejmujemy te liczby od odpowiednich wartości kluczy (mod 26)

Klucz	21 15 27 15 2 16 1 7 13 20 12 19 22 12 9 18 3 13 16 15
Tekst	7 0 6 4 11 8 13 23 4 13 2 8 15 7 4 17 12 4 13 19
Szyfr	14 15 21 11 17 8 14 10 9 7 10 11 7 5 5 1 17 9 3 22

Konwertując szyfr na litery i dzieląc na grupy pięcioliterowe, tekst szyfrowania będzie przesyłany jako

OPVLR IOKJH KLHFF BRJDW.

Wybór klatki dla Hagelin

Teoretycznie, nienachodzące na siebie klatki Hagelin mogą być dowolną kombinacją sześciu nieujemnych liczb całkowitych, które sumują się do 27 lub mniej. W praktyce wiele z tych klatek byłoby bardzo słabych z punktu widzenia kryptografii. W idealnej sytuacji klatka powinna generować każdą z możliwych wartości klucza, od 0 do 25, równie często. Ten ideał nie jest osiągalny, ponieważ każde z sześciu kół może być aktywne lub nieaktywne w dowolnej pozycji

2^6 = 64 możliwych kombinacji sześciu pinów, a tym samym 64 możliwych wartości klucza. Ponieważ wszystkie kluczowe wartości są interpretowane (mod 26), 26 możliwych wartości nie wszystkie mogą występować równie często, ponieważ 64 nie jest wielokrotnością 26.

Przeciętnie można oczekiwać, że kluczowa wartość wystąpi dwa lub trzy razy w dobrze dobranej klatce. Klatki, takie jak (9, 9, 9, 0, 0, 0) są oczywiście bardzo słabe, ponieważ jedynymi kluczowymi wartościami, jakie można wygenerować, są 0, 1 (które występują jako 27), 9 i 18, a nawet te nie są reprezentowani w sposób jednolity, a mianowicie:

Wartość klucza 0 1 19 18

Liczba zdarzeń na 64 możliwych 8 8 24 24

Rozwiązanie wiadomości wysłanej za pomocą takiej klatki nie byłoby zbyt trudne, ponieważ na każdym etapie istnieją tylko cztery możliwe kluczowe wartości, a dwa z nich są znacznie bardziej prawdopodobne niż dwa pozostałe. W przypadku tak słabej klatki można łatwo zilustrować proces rozwiązania.

Przykład 10.3

Poniżej znajduje się tekst szyfrowania wiadomości, która została zaszyfrowana na Hagelinie z klatką (0, 0, 0, 9, 9, 9). X służy do spacji / interpunkcji.

Odszyfruj wiadomość.

ZCTAL BRDSV IBGDZ SMFVM.

Rozwiązanie

W takiej klatce jedynymi możliwymi wartościami kluczowymi są 0, 1, 9 i 18. Jeśli odejmujemy każdą literę szyfru od tych czterech wartości i zapisujemy wypadkowe teksty w czterech rzędach, odszyfrowanie musi leżeć gdzieś w czterech rzędach. Ponieważ 9 i 18 są trzykrotnie bardziej prawdopodobne niż 0 lub 1, spodziewalibyśmy się, że większość liter w postaci zwykłego tekstu leży w trzecim i czwartym rzędzie. X służy do wstawiania odstępów / interpunkcji i, aby było więcej oczywiste, że zastępujemy je ^ gdziekolwiek występuje. Możemy zaoszczędzić sobie nudy odejmowania liczbowego ekwiwalentu liter szyfrujących od wartości kluczowych, jeśli skonstruujemy stół raz na zawsze. Ma to tę dodatkową zaletę, że w odróżnieniu od tablicowych szyfrogramów z części 7, ta sama tabela może być użyta zarówno do szyfrowania, jak i do szyfrowania/rozszyfrowania, ze względu na wspomnianą wyżej symetrię procesu szyfrowania / rozszyfrowywania Hagelin. Kiedy mamy tabelę, podaną w tabeli 10.2, po prostu sprawdzamy wpisy w wierszu odpowiadającym szyfrowi, lub tekst jawny, literę i kolumnę wartości klucza, aby uzyskać tekst jawny, lub szyfr, literę, dając tabelę 10.3. Znaki spacji są pomocne i łatwo jest wybrać tekst jawny, zaznaczony pogrubioną czcionką w tabeli 10.3:

Text	Z C T A L	B R D S V	I B G D Z	S M F V M
Key = 0	B Y H A O	Z J ^ I F	S Z U ^ B	I O V F O
Key = 1	C Z **I** B P	A K Y J G	T **A** V Y **C**	J P W G P
Key = 9	K **H** Q J ^	**I** **S** G R O	**B** I **D** G K	R ^ **E** O ^
Key = 18	**T** Q Z **S** G	R B P **A** ^	K R M P T	**A** **G** N ^ G

THIS IS A BAD CAGE

Jako nieco trudniejszy przypadek spróbuj tego.

Problem 10.1

Następująca wiadomość została zaszyfrowana na maszynie Hagelin z klatką (0, 5, 5, 5, 5, 5)

CBZPC CJXWY CXSHN IQUSR.

Odszyfruj wiadomość.

Ponieważ niektóre klatki są oczywiście bardzo "złe" (czyli słabe z punktu widzenia kryptografa) rodzi to pytania:

(1) Ile jest możliwych klatek?

(2) Ile z nich to "dobre" klatki?

Możemy znaleźć liczbę odrębnych możliwych klatek dokładnie od tego, ile liczba jest podana przez liczbę możliwych klatek? Liczba reprezentacji 27 jako suma sześciu nieujemnych liczb całkowitych i chociaż nie ma prostej metody obliczania tej liczby, możemy użyć miła tożsamość matematyczna i komputer do odkrycia, że liczba to 811. Jeśli nalegamy, aby każde koło miało co najmniej 1 wypust przeciwległy do niego, ponieważ koło, które nie ma występów przeciwległych, może równie dobrze nie występować, liczba zmniejsza się do 331. Ta sama technika ujawnia, że jeśli używamy tylko 26 lub 25 występów w klatce liczba możliwości, pozwalających na 0 występów przeciwnych do jednego lub więcej kół, zmniejsza się odpowiednio do 709 i 612, lub do 282 i 235, gdy uniemożliwiają występy 0. Musimy jednak pamiętać, że ponieważ sześć liczb klatki może być permutowane, a więc generować różne kluczowe strumienie, chociaż strumienie te będą miały podobne statystyki funkcji, liczba możliwych klatek, które musi rozważyć kryptoanalityk jest znacznie większa. Zatem w przypadku 27 końców istnieje 201376 możliwości, a nie 811. Ile z tych 331 odrębnych możliwych klatek jest "dobrych"? Oczywiście zależy to od tego, co rozumiemy przez "dobre". Jeśli weźmiemy to pod uwagę, że "dobra" klatka to taka, która generuje wszystkie możliwe klucze w zakresie od 0 do 25, wtedy możemy użyć komputera, aby ustalić, ile z 331 to robi. Odpowiedź brzmi: 113. Permuting klatki nie ma wpływu na jej jakość: "dobra" klatka pozostaje "dobra", a "zła" klatka pozostaje "zła". Jeśli zezwalamy na 0 uszek, 881 możliwych klatek daje tylko 120 "dobrych" klatek; innymi słowy, tylko 7 klatek z kołem z końcówkami 0 wytwarza wszystkie 26 możliwych wartości klucza (mod 26). Oczywiście nawet "dobra" klatka może zostać zniszczona przez wysoce asymetryczne ustawienia pinów, takie jak 90% aktywnych, 10% nieaktywnych.

Problem 10.2

Określ, które z poniższych 6 klatek generuje wszystkie kluczowe wartości, od 0 do 25 (mod 26). Dla tych klatek, które tego nie robią, znajdź brak kluczowych wartości.

(a) 0, 2, 3, 4, 8, 10;

(b) 1, 2, 2, 3, 4, 15;

(c) 1, 2, 2, 4, 5, 13;

(d) 2, 3, 3, 3, 4, 12;

(e) 2, 3, 3, 3, 5, 11;

(f) 2, 3, 4, 4, 7, 7.

Teoretyczny "czynnik pracy" dla Hagelin

Kiedy kryptoanalityk ma do czynienia z wiadomościami o zupełnie nieznanej Hagelin, ile jest tam możliwości? Liczba ta jest czasami określana jako czynnik roboczy i reprezentuje liczbę przypadków, które należałoby wypróbować, gdyby kryptoanalityk podjął próbę ataku "brutalnej siły". W odniesieniu do rodzaju Hagelin, o których dyskutowaliśmy do tej pory (istnieją inne opcjonalne cechy, które dodatkowo komplikują, jak zobaczymy) istnieją dwa istotne czynniki:

(1) liczba możliwych klatek;

(2) liczba możliwych ustawień pinów.

Zakładając, że klatka używa 27 występów, a my pozwalamy, aby koła miały 0 występów, istnieje ponad 200000 sposobów dystrybucji między sześcioma kołami, więc weźmiemy pierwszy czynnik jako 2×10^5. Drugi czynnik można zapisać od razu. Jest 131 pinów, a każdy pin może być w jednej z dwóch pozycji, co oznacza, że istnieje 2^{131} możliwych ustawień pinów. Od 2131 roku jest więcej niż 2.5×10^{39} iloczyn

dwóch czynników przekracza 5 x 10^{44}. Ponieważ kryptoanalityk nie może być pewny, że używa się 27 występów, musiałby być przygotowany do wypróbowania innych klatek, takich jak te mające tylko 26 lub 25, które w przybliżeniu potroiłyby współczynnik pracy. Z liczb tych jasno wynika, że atak "brutalnej siły" nie wchodzi w grę. W rzeczywistości kryptoanalitycy nie muszą uciekać się do ataków typu "brute force", aby rozwiązać Hagelin, chociaż samo rozwiązywanie maszyny za pomocą szyfrów jest trudne i wymaga dużo tekstu. Sytuacja jest zupełnie inna, jeśli kryptoanalitykowi udało się zdobyć odcinek klucza, a zobaczymy, że podano około 150 następujących po sobie kluczowych wartości, że rozwiązanie jest stosunkowo łatwe. Ponownie zobaczymy, że oszacowania "brutalnej siły" mogą być bardzo mylące, gdy chodzi o ocenę trudności w rozwiązaniu jakiegokolwiek systemu szyfrów. Jak widzieliśmy w części 2, jest ich 26! możliwe proste szyfry zastępcze i współczynnik pracy z brutalną siłą wynoszą około 1025, ale takie systemy mogą być rozwiązywane ręcznie w mniej niż godzinę, z 200 literami szyfrów. Wiele rodzajów szyfrów, w tym Hagelin, są podatni na ataki z matematycznymi lub statystycznymi słabościami samego szyfru lub jego trybu działania, jak w Enigmie. Szyfr, w którym nie ma znanych słabych punktów lub "pułapek", które umożliwiają kryptoanalitykowi złamanie systemu specjalną trasą, byłby naprawdę potężny. Twierdzi się, że taki system to nowoczesny system DES (Data Encryption Standard). Krótki opis tego znajduje się w części 13.

Rozwiązywanie Hagelin z odcinka klucza

Odzyskiwanie klatek i wzorów pinów nienapętlonej Hagelin jest proste, jeśli mamy więcej niż 131 kolejnych wartości kluczowych, jak pokazano poniżej. "Jak jednak" możesz zapytać ", czy otrzymujemy 131 kolejnych kluczowych wartości?" Odpowiedź brzmi: "Odnajdując tekst jawny o długości 131 znaków lub więcej." Można to osiągnąć na wiele sposobów, w tym:

(1) stwierdzenie, że ta sama wiadomość została wysłana w innym szyfrze, który można odczytać;

(2) stwierdzenie, że dwa lub więcej komunikatów Hagelin jest dogłębnych, które mogą być odczytywane za pomocą metody przeciągania szopka, jak wyjaśniono w Części 7;

(3) przez operatora szyfrującego popełniającego błąd i konieczności ponownego przesłania wiadomości na nieco innym ustawieniu.

(4) tajnymi środkami, np. przez agenta uzyskującego tekst jawny wiadomości.

Aby zilustrować metodę rozwiązania, gdy uzyskano wystarczająco długi odcinek klucza, patrzymy na klucz, który byłby generowany przez "mini-Hagelin" z tylko trzema kołami. Odpowiedni atak na pełną skalę Hagelin niewątpliwie wiąże się z większą ilością pracy, ale metoda jest taka sama i opiera się na fakcie, że kluczem jest suma (mod 26) wkładu sześciu kół, które poruszają się regularnie, a więc, odejmując klucz. Strumień z siebie, odpowiednio przesunięty, możemy usunąć wkład pięciu dowolnych kół, a więc odkryć "kopnięcie" na szóstym kole. Tak więc, jeśli wygenerujemy klucz, dodając razem wkłady dwóch mini-kółek, jednej z długości 7 i kopnięcia 5, a drugiej długości 9 i kopnięcia 3, możemy mieć

7-Kólko 5 0 5 5 0 0 5 5 0 5 5 0 0 5 5 0 5 5 0 5 5 5. . .

9-Kółko 0 3 3 3 0 0 3 0 3 0 3 3 3 0 0 3 0 3 0 3 3 3. . .

Suma 5 3 8 8 0 0 8 5 3 5 8 3 3 5 5 3 5 8 0 3 8 8

Teraz wykonujemy kopię klucza, przesuwamy go o 7 miejsc w prawo (długość jednego z kółek) i odejmujemy od niezmienionego klawisza viz:

5 3 8 8 0 0 8 5 3 5 5 3 3 5 5 3 5 8 0 0 8 8

5 3 8 8 0 0 8 8 5 3 5 8 3 3 5 5

Klawisz powiązany 0 0 -3 0 3 3? 3 0 0 0 0? 3 0 3 3

Zauważamy to

(1) wszystkie klucze różnicowe są wielokrotnościami 3, kopnięciem na 9 kołach,

(2) różnicowy wzór klawiszy powtarza się po 9 pozycjach, długość pozostałego koła.

Powyższy proces jest znany jako "różnicowanie w przedziale7" i jest zwykle symbolizowany w matematyce za pomocą greckiej litery Δ , grecki odpowiednik D, z przyrostkiem oznaczającym odpowiedni przedział, 7 w tym przypadku. Więc proces jest w pełni symbolizowany przez

Δ_7

Proces różnicowania jest często określany jako "delta-ing". Nie było żadnego szczególnego powodu, dla którego najpierw wybrałbym różnicę w przedziale 7, mogliśmy oczywiście odróżnić klucz w przedziale 9, więc zróbmy to:

Suma 5 3 8 8 0 0 8 5 3 5 8 8 3 3 3 3 5 5 3 3 5 8 0 0 3 8 8

Przesunięcie 9 miejsc 5 3 8 800 853 5 833

Odejmij 0 5 -5 -555 -505 -5 -555

Wzór powtarza się w przedziale 7, a kopnięcie na 7 kołowcu to oczywiście 5. Wyraźnie znaleźliśmy wartości kopnięć, ale co z wzorami sworzni na kołach? Można je znaleźć, sprawdzając oryginalne wartości kluczy po poznaniu kopnięć na poszczególnych kołach. Z "prawdziwą" Hagelinem jest komplikacja, którą zignorujemy dla teraźniejszości: kiedy widzimy kluczową wartość 0 lub 1, może to być rzeczywiście klucz 26 lub 27. W międzyczasie metoda odzyskiwania wzorów pinów można zilustrować innym "mini-Hagelin":

Przykład 10.4

Następujący odcinek klucza został odzyskany z mini-Hagelin z trzema kołami o długości 5, 8 i 9. Odzyskać kopnięcia i wzory pinów.

6 4 3 6 8 6 4 5 1 8 4 1 8 6 8 1 6 3 9 0 4 6 8 6 0.

Rozwiązanie

Możemy zastosować operacje różnicowania w dowolnej kolejności. Jeśli zaczniemy od przedziału 5, a następnie wykorzystamy przedział 8, wyeliminujemy wkłady kół 5- i 8-kowych i otrzymamy strumień liczb, z których wszystkie są wielokrotnościami (dodatnie, ujemne lub zerowe) kopnięcia na 9- koło. Więc:

Klucz 64368645 18 4 1868 1 6 6 3 3 9 9 04 0 68 6 6 0 0

Przesunięcie 643 8 68 6 6 45 18 4 4 1 1 8 8 6 6 8 81 8 63 8 9 0 0

Δ_5 002 -50 2 2 3 3350 3 3 5 5 5 5 3 3 8 83 8 05 3 -3 0

Przesunięcie 8 00 2 -5 0 0 2 2 3 -33 2 50 -3 5

Δ_8 Δ_5 50 -5 10 5 5 -50 -55 0 -5

Kopnięcie na 9 kołach wynosi oczywiście 5; zauważ, że wzór zaczyna się powtarzać po 9 miejscach. Zauważ również, że klucz podwójnie różnicowany ma jedną wartość równą dwukrotności rzutu; jest to szczególny przypadek: "Kiedy kluczowy strumień jest różny N razy wartość może wynosić do $\pm 2^{(N-1)}$ razy kopnięcie może wystąpić". Teraz znajdujemy kopnięcie na 8 kołach. Wymaga to różnicowania w przedziale 5 i przedziale 9, w dowolnej kolejności. Ponieważ mamy już klucz różnicowy w przedziale 5 (tj.powyżej Δ_5) potrzebujemy tylko różnicy, która w przedziale 9:

Δ_5	0	0	2	−5	0	−2	−3	3	5	0	−3	5	−5	3	−8	3	0	5	−3	0
Shift 9									0	0	2	−5	0	−2	−3	3	5	0	−3	
$\Delta_9\Delta_5$									0	−3	3	0	3	−6	6	−3	0	−3	3	

Wzór zaczyna się powtarzać po 8 miejscach, tak jak powinien, a kopnięcie na 8 kółku jest oczywiście 3. Podobnie, różnicując oryginalny strumień klucza w przedziale 8, a następnie w przedziale 9, otrzymujemy

$\Delta_9\Delta_8$	0	1	−2	1	0	0	1	−2

Wzór zaczyna się powtarzać po 5 miejscach, a kopnięcie na 5 kołach jest oczywiście 1. Teraz musimy znaleźć wzory na trzech kołach. Robimy to, patrząc na kluczowe wartości i widząc, jak mogą powstać z kombinacji kopnięć (1, 3 i 5) na kołach. Łatwo to zrobić. Pełne rozmiary Hagelin z sześcioma kołami nie byłyby tak łatwe, ale bardzo pomocne jest to, że wkład każdego koła do ogólnego klucza powtarza się w odstępach długości koła. W przypadku tej mini-Hagelin możemy wymienić osiem możliwości. Oznaczając aktywny pin przez X i nieaktywny pin przez O jedyne możliwości pokazano w tabeli 10.4

5-Wheel Kick = 1	8-Wheel Kick = 3	9-Wheel Kick = 5	Key
O	O	O	0
O	O	X	5
O	X	O	3
O	X	X	8
X	O	O	1
X	O	X	6
X	X	O	4
X	X	X	9

Teraz zapisujemy strumień kluczy i domniemany stan pinów dla każdego koła:

Key	6	4	3	6	8	6	4	5	1	8	4	1	8	6	8	1	6	3	9	0	4	6	8	6	0
5-Wheel	X	X	O	X	O	X	X	O	X	O	X	X	O	X	O	X	X	O	X	O	X	X	O	X	O
8-Wheel	O	X	X	O	X	O	X	O	O	X	X	O	X	O	X	O	O	X	X	O	X	O	X	O	O
9-Wheel	X	O	O	X	X	X	O	X	O	X	O	O	X	X	X	O	X	O	X	O	O	X	X	X	O

Wzory powtarzają się we właściwych odstępach czasu, więc możemy powiedzieć:

Wzór na 5 kołach to X X O X O

Wzór na 8-kołowym to O X X O X O X O

Wzór na 9 kołach to X O O X X X O O O

Przy pełnej wielkości Hagelina potrzebujemy oczywiście dłuższego odcinka klucza. Za każdym razem, gdy tracimy klucz, tracimy kilka wartości, których liczba jest równa długości koła, przy którym się różnimy. Tak więc w powyższym przykładzie, który został wymuszony w przedziale 5, pierwotne 25 kluczowych wartości zostało zredukowanych do 20, a gdy następnie zmieniliśmy w przedziale 8, pozostało nam tylko 12 wartości. W przypadku pełnowymiarowej Hagelin potrzebujemy minimum 131 kluczowych wartości, ponieważ 131 jest sumą długości sześciu kół. Raczej więcej niż 131 jest pożądane, ponieważ chcielibyśmy mieć dodatkowe wartości klucza, aby potwierdzić, że ostateczne (pięciokrotnie różnicowane) wartości powtarzają się w odpowiednim przedziale; wystarczy 150 kluczowych wartości. Ponadto, pełnowymiarowa Hagelin ma cechy, które sprawiają, że zadanie jej rozwiązania jest znacznie trudniejsze, jak już wskazano, i jak teraz widzimy.

Dodatkowe funkcje maszyny Hagelina

Maszyna Hagelin, opisana i przeanalizowana do tej pory, jest najbardziej podstawowym typem i zignorowaliśmy fakt, że dwie z możliwych wartości klucza, 0 i 1, są niejednoznaczne i mogą wynosić odpowiednio 26 i 27. Oznacza to, że jeśli odcinek odzyskanego klucza zawiera wartości 0 lub 1, kryptoanalityk będzie musiał rozważyć 26 i 27 jako alternatywę przy różnicowaniu. Może to obejmować zbadanie wielu alternatywnych wersji kluczowego strumienia; niepowodzenie ataku różnicowego wskazywałoby, że jedna lub więcej niejednoznacznych wartości zostało błędnie zidentyfikowanych. W wyniku kompensacji kryptoanalityk staje się getomereward za prawidłową identyfikację klucza 0 lub klucza 27, ponieważ ten pierwszy oznacza, że wszystkie sześć kół jest nieaktywnych w tym punkt i to ostatnie oznacza, że wszystkie są aktywne; ponadto, a oryginalna wartość klucza 1 oznacza, że jest koło z kopnięciem 1, podobnie jak klucz z 26 (zakładamy, że wszystkie 27 słupków są używane, bez "nakładania się"). Jednak w równowadze zadanie jest utrudnione przez te niejednoznaczności. Oprócz tego powikłania, które dotyczy wszystkich modeli Hagelin, w przypadku większości modeli, które znacznie zwiększają jego bezpieczeństwo, istnieją dwie dodatkowe funkcje:

(1) "presuwanie";

(2) "nakładanie się".

<u>Przesuwanie</u>

Na maszynach Hagelin wyposażonych w tę funkcję znajduje się małe kółko na zewnątrz, które ma alfabet wokół obręczy. Można go obrócić w dowolne z 26 pozycji i pozostać w tej pozycji, gdy wiadomość jest szyfrowana lub odszyfrowywana. Efektem przesunięcia jest zwiększenie klucza o stałą, więc jeśli presunięcie jest równy E, wszystkie wartości klucza są zwiększone o 4. Ogólnie, zasada kodowania zmienia się od

cipher letter = key- (zwykła litera) (mod 26)

do cipher letter = (klawisz + suwak) - (zwykła litera) (mod 26),

wartość liczbowa przesunięcia jest zwykle równa

viz: A= 0, B= 1,. . . . , Z =25.

W maszynach, które nie mają tej cechy, przeusnięcie ma trwale stałą wartość: na przykład w M209 jest to Z, które jest liczbowo równoważne 25, lub -1, ponieważ cała arytmetyczna jest (mod 26). Tak więc, na M209 kluczowa wartość, która wyglądała na 25, byłaby w rzeczywistości wygenerowana przez sześć kół jako 0 lub 26, a kluczowa wartość, która wyglądała na 0, byłaby generowana przez koła jako 1 lub 27. Identyfikacja slajdu byłaby pierwszym krokiem w kluczowej analizie. Identyfikowanie slajdu w wiadomości szyfrowania Kryptoanalityk może być w stanie zidentyfikować slajd w komunikacie

szyfrowym, jeśli zna klatkę, która jest używana. Aby to zrobić, musi obliczyć "teoretyczną dystrybucję szyfru" i porównać ją statystycznie z faktycznymi częstotliwościami literowymi liter w komunikacie. Istnienie tego slajdu nie unieważnia ataku różnicowego, ale utrudnia wstępne rozpoznanie wartości klucza 0 i 1. Przesunięcie zostanie prawdopodobnie zmienione dla każdej wiadomości i szyfru operator musiałby mieć jakiś sposób komunikowania swojej tożsamości.

Nakładanie się

Ta funkcja była dostępna we wszystkich modelach Hagelin. Przypomnij sobie, że na klatce za kółkami znajduje się 27 pasków i 54 występy. Na każdym pręcie 2 występy mogą być ustawione naprzeciw dowolnego z sześciu kół lub w jednym z dwóch pozycji "neutralnych". W obróconej Hagelinem jeden z 2 występów na każdym pasku znajdowałby się w jednej z neutralnych pozycji. W zachodzącym na siebie Hagelinie 1 lub więcej słupków będzie miało 2 występy naprzeciw dwóch kółek. Powoduje to, że gdy dwa kółka mają występ na tym samym pręcie, ich wkład w ogólny klucz, gdy oba są aktywne, wynosi 1, nie 2. Dzieje się tak dlatego, że pręty przesuwają tylko położenie koła drukującego 1 niezależnie od tego, czy 1 lub 2 występy włączyć aktywne szpilki. Na przykład, jeśli 26-kołowy ma kopnięcie równe 5, a 25-kołowe ma kopnięcie równe 6 i dzielą one dwa pręty, w których oba mają aktywny sworzeń, ich łączny aktywny udział w całkowitym kluczu nie wynosi 11, ale 11 – 2 = 9. Więc

26- i 25-kółek obojętne - wkład do klucza wynosi 0;

26-kołowe aktywne, 25 nieaktywne - "" "" wynosi 5;

26-kołowe nieaktywne, 25 aktywne - "" "" wynosi 6;

26- i 25-kołowe, oba aktywne - "" "" wynosi 9.

Nakładanie się będzie miało oczywiście wpływ na rozkład kluczowych wartości. Przypuśćmy, że znów spojrzymy na bardzo słabą klatkę (9, 9, 9, 0, 0, 0), ale tym razem nakładamy kopnięcia w następujący sposób:

(26, 25) - koła zachodzą na siebie = 2;

(26, 23) - koła zachodzą na siebie = 3;

(25, 23) - koła zachodzą na siebie = 1.

Następnie możliwe wartości kluczy są podane w Tabeli 10.5, gdzie X oznacza aktywny pin i O nieaktywny pin, jak poprzednio:

26-Wheel	25-Wheel	23-Wheel	Key
O	O	O	0
O	O	X	9
O	X	O	9
O	X	X	17
X	O	O	9
X	O	X	15
X	X	O	16
X	X	X	21

Chociaż jest to nadal bardzo słaba klatka, produkuje ona co najmniej sześć różnych kluczowych wartości zamiast czterech, a to wszystko, co mogłaby wytworzyć uformowana klatka; kluczowa wartość 9 jest jednak nadal najbardziej rozpowszechniona, ponieważ wystąpiłaby 24 razy na 64, przy pozostałych pięciu kluczowych wartościach, z których każda wystąpiła zaledwie 8 razy. Co ważniejsze

jednak, atak różnicowy zakończyłby się niepowodzeniem, ponieważ nie byłoby już prawdą, że udział koła w całkowitym kluczu powtórzyłby się w odstępach długości koła. Jest to główna zaleta nakładania się z punktu widzenia kryptografa. Kolejną zaletą nakładania się jest to, że liczba możliwych klatek jest ogromnie zwiększona, ponieważ zamiast 27 pojedynczych występów ma być rozłożonych 27 par występów. Czy nakładanie ma jakieś wady? Z czysto kryptograficznego punktu widzenia prawdopodobnie nie, pod warunkiem, że nakładanie zostało przypisane rozważnie. Nakładanie się powoduje zmianę dystrybucji klucza i obrócona w klatkę klatka, która generuje wszystkie możliwe 26 wartości kluczy, może przestać to robić, jeśli się nakłada. Ponadto operatorzy szyfrów, którzy muszą skonfigurować maszynę, muszą zachować szczególną ostrożność. Zapewnienie, że poszczególne koła są wzajemnie zachodzące na siebie w odpowiednim stopniu, ma zasadnicze znaczenie; jakiekolwiek błędy mogą wymagać ponownego przesłania wiadomości, a kryptoanalityk uzyska przydatne informacje, porównując te dwa teksty. Najlepszym sposobem, aby operatorzy dowiedzieli się o kopnięciu i zachodzących na siebie wzorach kół, jest dostarczenie im "mapy" pokazującej położenie 2 występów na każdym z 27 prętów klatki. "Mapa" może albo wskazywać położenie każdego występu na każdym pasku, co wymagałoby ośmiu kolumn - sześciu dla kół i dwóch dla pozycji neutralnych; lub może wyświetlać tylko sześć kolumn koła, a gdy słupek ma tylko 1 występ, operator musi ustawić drugie ucho w jednym z neutralnych położeń. Druga metoda jest używana poniżej

Przykład 10.5

"Dobra" klatka przechylona (9, 7, 5, 3, 2, 1) jest zmodyfikowana do klatki zachodzącej na siebie (11, 9, 7, 5, 3, 1), gdzie pierwsze cztery koła mają zakładkę 2 koło po prawej i piąte koło ma zakładkę 1 z szóstym kołem. Narysuj odpowiednią mapę klatki bębna dla operatorów szyfrów. Czy zachodząca klatka generuje wszystkie 26 możliwych wartości kluczy (mod 26)?

Rozwiązanie

Patrz tabela 10.6.

Bar	26-Wheel	25-Wheel	23-Wheel	21-Wheel	19-Wheel	17-Wheel
1	X					
2	X					
3	X					
4	X					
5	X					
6	X					
7	X					
8	X					
9	X					
10	X	X				
11	X	X				
12		X				
13		X				
14		X				
15		X				
16		X				
17		X	X			
18		X	X			
19			X			
20			X			
21			X			
22			X	X		
23			X	X		
24				X		
25				X	X	
26				X	X	
27					X	X

Badanie zestawu 64 kluczowych wartości generowanych przez tę klatkę pokazuje, że 5 kluczowych wartości 2, 4, 13, 20 i 25 nie może wystąpić, natomiast wartość klucza 17 występuje sześć razy. Nie jest to zatem szczególnie satysfakcjonująca klatka, mimo że stwarza trudności dla kryptoanalityka z powodu nakładania się.

Problem 10.3

Znajdź, które kombinacje pinów w powyższej klatce zachodzą na wartość 17.

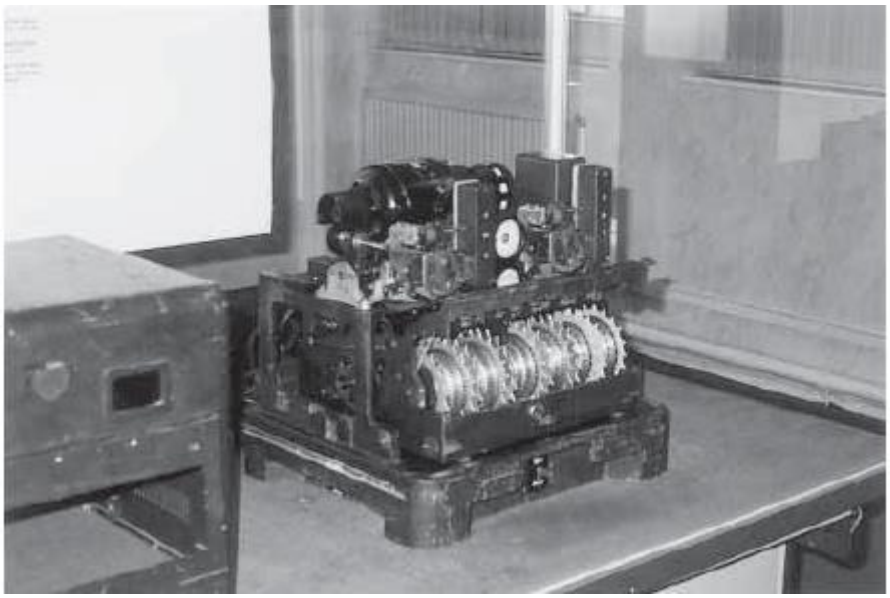
Rozwiązywanie

Hagelin tylko z tekstów szyfrów Rozwiązywanie problemu z szyfrowaniem Hagelin "od zera" wymaga mnóstwa żmudnej pracy i tylko wskażę, w jaki sposób kryptoanalityk prawdopodobnie by się do tego zabrał. Szczegółowe przykłady rozwiązania z komunikatów szyfrów zostały opublikowane, a zainteresowany czytelnik powinien się skonsultować Kiedy wiadomości Hagelin zostaną po raz pierwszy przechwycone, kryptoanalityk nie będzie miał wiedzy o ustawieniach klatki lub pinezki. Początkowo może nawet nie wiedzieć, że jest to Hagelin, który jest używany. Jeśli operatorzy szyfrów nie popełniają błędów, kryptoanalityk czeka cię ciężka praca. Aby mieć jakąkolwiek szansę na sukces, będzie potrzebował albo jedna bardzo długa wiadomość szyfrowana o kilku tysiącach liter, lub kilka wiadomości o jeszcze większej całkowitej długości. Musiałby wtedy obliczyć różne statystyki, począwszy od ogólnej liczby liter szyfrujących, co pomogłoby ustalić, że prawdopodobnie używana jest maszyna Hagelin, ponieważ nierównomierny rozkład 26 możliwych kluczowych wartości byłby wykrywalny w dostatecznym stopniu. długi tekst. Gdyby trzeba było użyć kilku tekstów, możliwe byłoby określenie ich "slajdów" względem siebie poprzez obliczenie ich współczynników korelacji częstotliwościowej w parach (gdyby maszyna była M209, z ustalonym suwakiem, nie powstałoby to). Najdłuższy tekst szyfru zostałby teraz zapisany na szerokości 17 kolumn i zliczeń wykonanych z liter szyfrujących w każdej kolumnie. Celem tutaj jest próba umieszczenia każdej kolumny w jednej z dwóch klas: odpowiadającej aktywnemu pinowi i odpowiadającym nieaktywnemu pinowi. Jeśli zachodzi nakładanie się, nieaktywne kolumny z pinami nie zostaną zmienione, ale aktywne są kolumny. Porównując liczby częstotliwości liter alfabetu w "nieaktywnych" kolumnach z odpowiednimi licznikami w "aktywnych" kolumnach, kryptoanalityk miałby nadzieję, że uda się ustalić kopnięcie na 17 kole. Może mu się to nie udać, ale czy zrobi to, czy nie, przeprowadzi taką samą analizę szerokości pozostałych pięciu kółek. Gdyby był w stanie wydedukować jeden lub więcej kopnięć z pewną dozą pewności, wówczas zobaczyłby, jaki rozkład szyfrów na pozostałych kołach byłby po uwzględnieniu znanych kopnięć. W ten sposób przeprowadziłby iteracyjny proces, miejmy nadzieję stale zwiększając ilość informacji o klatkach i wzorach sworzni. Jeśli zachodzi nakładanie się, analiza jest jeszcze trudniejsza, szczególnie, gdy wszystkie koła mają pewne nakładanie. Z drugiej strony, jak pokazał powyższy przykład, zbyt duże nakładanie się może zamienić "dobrą" klatkę w kiepską!

Poza Enigmą

SZ42: maszyna pre-elektroniczna

Maszyny Enigma i Hagelin zapewniały o wiele większy stopień bezpieczeństwa niż jakikolwiek wcześniejszy system szyfrowania inny niż niezniszczalny jednorazowy pad. Zasady kryptograficzne, na których oparte były te dwa urządzenia, były dość proste. Enigma dostarczyła dużą liczbę alfabetów zastępczych, podczas gdy Hagelin generowała bardzo długi strumień pseudolosowego klucza. Teoretycznie można zmodyfikować maszynę, aby była jeszcze bezpieczniejsza. Liczba kół może zostać zwiększona, a w Hagelinie koła mogą być dłuższe. W praktyce modyfikacja istniejącej maszyny szyfrującej może stwarzać poważne trudności w produkcji, dystrybucji i kompatybilności z oryginalną maszyną, co może mieć kluczowe znaczenie. Czterokołowa Enigma została wprowadzona w 1942 r., A kompatybilność z oryginalną wersją trójkołową uzyskaną dzięki temu, że z nowymi komponentami w określonych pozycjach stare i nowe wersje były identyczne kryptograficznie. Kilka nowych modeli Hagelin zostało wyprodukowanych przez tę firmę w latach 50-tych z kołami o różnych rozmiarach i innymi cechami, ale były to naprawdę różne maszyny i nie próbowano zapewnić zgodności z oryginałem. Może wydawać się oczywiste, że zwiększenie liczby komponentów lub zwiększenie złożoności maszyny szyfrującej zwiększy jej bezpieczeństwo, ale niekoniecznie tak jest. Im więcej elementów, tym bardziej prawdopodobne staje się, że operatorzy będą popełniać błędy. Im większa złożoność, tym większa szansa na awarię urządzenia. Może się zdarzyć, że próbując zwiększyć bezpieczeństwo maszyny, kryptograf może ją skutecznie zmniejszyć. Przykład, w którym zwiększona złożoność spowodowała problemy, jest podana później. Ponadto, gdy maszyny szyfrujące były urządzeniami mechanicznymi, zwiększenie liczby komponentów spowodowałoby, że maszyna byłaby cięższa i mniej przenośna. Trójkołowy Enigma ważył około 12 kilogramów, co należało wziąć pod uwagę, ponieważ maszyny te były przeznaczone do powszechnego użytku przez jednostki operacyjne wszystkich sił zbrojnych. Czterokołowa Enigma była używana tylko przez niemiecką marynarkę wojenną, a ponieważ była przewożona tylko na statkach i łodziach podwodnych, ciężar nie był istotny. Gdyby tylko niewielka liczba maszyn szyfrujących była potrzebna do jakiegoś celu, być może dlatego, że miałyby być oparte na stałych lokalizacjach, można by rozważyć znacznie większe maszyny. Tak było w 1941 roku, gdy niemiecka armia wprowadziła maszynę, znaną później jako SZ42, do komunikacji między Wiedniem a Atenami, a niedługo potem nieco podobną maszynę, zwaną T52, wykorzystały niemieckie lotnictwo. Stosowano stosunkowo niewielką liczbę maszyn SZ42, być może 52 na 26 ogniwach. Wiadomości, które niosły, miały największe znaczenie, a maszyna została zaprojektowana w celu zapewnienia wyjątkowo wysokiego poziomu bezpieczeństwa. Nie miało to być przenośne urządzenie; mierzyła 20''x 18''x18 '' i była znacznie większa i cięższa niż Enigma. Zobacz 11.1, aby zobaczyć zdjęcie SZ42.



Opis maszyny SZ42

SZ42 zawierał 12 kół o różnych rozmiarach. Wokół obwodu każdego koła znajdowały się szpilki, z których każda mogła być umieszczona w jednej z dwóch pozycji, które możemy uznać za "aktywne" i "nieaktywne". Na pozór może to wydawać się większą wersją maszyny Hagelin, ale, jak zobaczymy, było zupełnie inaczej, zarówno w ruchu jego kółek, jak iw sposobie szyfrowania. 12 kół zostało rozmieszczonych w trzech zestawach, które będą określane jako A, B i C. Każdy zestaw A i C składa się z 5 kół, które oznaczamy jako (A_1, A_2, A_3, A_4, A_5) i (C_1, C_2, C_3, C_4, C_5). Zestaw B miał pozostałe 2 koła, które można określić jako (B_1, B_2). Długości kół zostały przedstawione w Tabeli 11.1.

Wheel	Length	Wheel	Length	Wheel	Length
A_1	41	B_1	61	C_1	43
A_2	31	B_2	37	C_2	47
A_3	29			C_3	51
A_4	26			C_4	53
A_5	23			C_5	59

Całkowita liczba pinów jest sumą długości kół, 501. Piny były zmieniane codziennie; To musiało być uciążliwe zadanie dla operatorów szyfrów. Koła w zestawie A i kółku B1 przesuwały się o jedno miejsce za każdym razem, gdy litera była szyfrowana. Koło B2 przesunęło się o jedno miejsce wtedy i tylko wtedy, gdy aktywny był bolec na B_1. Koła w zestawie C przesuwały się o jedno miejsce wtedy i tylko wtedy, gdy aktywny kołek B_2 był aktywny. Więc chociaż koła zestawu A poruszały się regularnie, koła zestawu C poruszały się nieregularnie

Szyfrowanie na SZ42

Proces szyfrowania w SZ42 był zupełnie inny niż w przypadku Hagelin. Przede wszystkim alfabet zawierał 32 znaki, a nie 26. 32 znaki były alfabetem International Teleprinter Alphabet (ITA), który idealnie nadaje się do użycia na taśmie z pięcioma otworami, gdzie może być użyty do reprezentowania 26 liter i 6 znaków. funkcje, takie jak "spacja" i "powrót karetki". Od $32= 2^5$, 32 znaki mogą być zapisane jako kombinacje pięciu "0 lub 1", tj. Jako pięć bitów. Pełny alfabet ITA można znaleźć w wielu książkach, , ale jako próbka, wystarczająca dla naszych potrzeb, zauważamy, że

A wynosi 11000

B to 10011

...

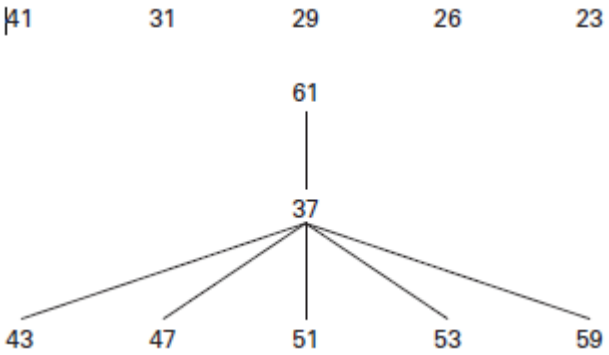
P oznacza 01101

Q to 11101

...

Z to 10001

nie ma oczywistego związku między reprezentacjami kolejnych liter alfabetu). Chociaż koła 61- i 37-kołowe określały ruch kół w zestawie C, nie odegrały bezpośredniej roli w rzeczywistym procesie szyfrowania, który obejmował tylko pięć binarnych elementów listu tekstu jawnego i obecnych pięciu szpilek zestawu A i prądu pięć kołków zestawu C. Schematyczny schemat sterowania ruchem w SZ42 pokazano na rysunku 11.1.



Szyfrowanie listu na SZ42 zostało przeprowadzone w następujący sposób:

(1) litera zwykłego tekstu, P, została przekształcona na pięciobitowy odpowiednik binarny w kodzie ITA;

(2) każde z pięciu bitów P było szyfrowanych oddzielnie;

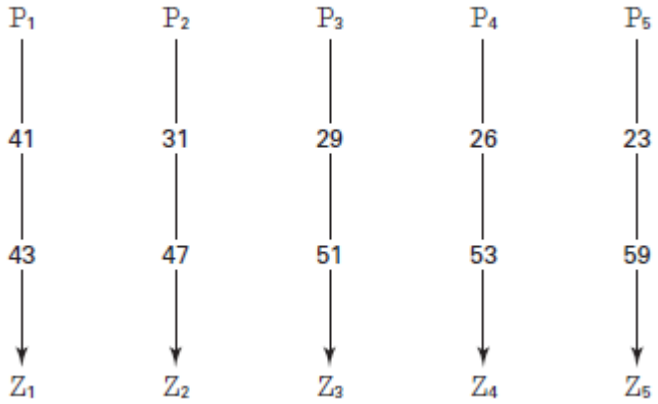
(3) każdy bit Pwas dodany (mod 2) do wartości bieżącego kołka na jednym z kół zestawu A, wartość wynosi 0 dla nieaktywnego pinu i 1 dla aktywnego pin

(4) pięć bitów ze stopnia (3) zostało dodanych osobno (mod 2) do wartości bieżącej szpilki na jednym z kół zestawu C, przy czym wartość ta wynosi 0 lub 1 na etapie (3);

(5) wynikowy pięciobitowy znak, Z, został przekonwertowany z powrotem, za pomocą kodu ITA, w celu nadania litery szyfrowania w mechanizmie drukowania;

(6) każde koło poruszało się zgodnie z mechanizmem kontroli ruchu.

Szyfrowanie każdego strumienia zależało tylko na 2 z 10 kół: 1 od zestawu A i 1 od zestawu C. Na przykład pierwszy strumień został zaszyfrowany 41-kołem w zestawie A i 43-kołem w zestawie C, podczas gdy piąty strumień został zaszyfrowany 23 kołem w zestawie A i 59 kołem w zestawie C. Schemat procesu szyfrowania SZ42 pokazano na rysunku 11.2.



Ponieważ włączono tylko (mod 2) tekst jawny i klucze, procesy dekodowania i szyfrowania były identyczne, ponieważ dodawanie i odejmowanie są takie same (mod 2). Jako ilustrację procesu szyfrowania:

Przykład 11.1

Jeśli wartości pinów na kołach zestawów A i C są

SetA 0 1 0 1 1

SetC 1 0 0 1 0

a litera jawnego tekstu to S (= 10100 w ITA), jaka będzie litera szyfrowa? Sprawdź, czy odszyfrowanie daje oryginalny tekst w postaci zwykłego tekstu.

Rozwiązanie

Litera zwykłego tekstu (S)	1 0 1 0 0
Ustaw wartości styków	0 1 0 1 1
(mod 2) suma	1 1 1 1 1
Ustaw wartości styków C	1 0 0 1 0
(mod 2) suma	0 1 1 0 1 = P.

Zatem literą szyfrowania będzie P. Jeśli zaczniemy teraz od litery szyfrowania P, to przy tych samych wartościach pinów proces odszyfrowania daje

Litera szyfrowania (P)	0 1 1 0 1
Ustaw wartości styków	0 1 0 1 1
(mod 2) suma	0 0 1 1 0
Ustaw wartości styków C	1 0 0 1 0
(mod 2) suma	1 0 1 0 0 = S,

potwierdzenie oryginalnego listu z tekstem otwartym.

Łamanie i ustawianie SZ42

Zakładając, że kryptoanalityk znał szczegóły projektu SZ42, jak podano na Rysunku 11.1, i że był on używany, ile możliwości musiałby rozważyć, zanim byłby pewien, że będzie w stanie odszyfrować wiadomość? Odpowiedź jest łatwo dostępna. Ruch kół i encyklopedii są całkowicie określone przez kołki na 12 kołach. Ponieważ we wszystkich znajduje się 501 szpilek, a każdy z nich może być umieszczony w jednym z dwóch stanów: "aktywny" lub "nieaktywny", liczba możliwości jest

$2^{501} \approx 10^{151}$.

Jest to "czynnik przełamujący pracę" i jest tak duży, że gdyby każda cząstka we Wszechświecie była komputerem i została przydzielona w pełnym wymiarze czasu od czasu "Wielkiego Wybuchu" do wypróbowania wszystkich możliwości, rozwiązanie nie zostałoby znalezione. Najwyraźniej podejście "brutalnej siły ataku" do zerwania SZ42 jest beznadziejne. Jeśli kryptoanalityk znał wszystkie wzory pinów i pojawiła się nowa wiadomość, miałby "łatwiejsze" zadanie znalezienia ustawień 12 kółek na początku wiadomości. Liczba możliwości, które musiałby wypróbować, to iloczyn długości kół, a mianowicie:

23x26 x 29 x 31 x 37 x 41 x 43 x 47 x 51 x 53 x 59 x 61

która wynosi około 1,6 x 10^{19}. Jest to "czynnik roboczy" i choć wygląda na nieistotny w stosunku do czynnika roboczego do zerwania, nadal wyklucza brutalny atak sił nawet na dzisiejsze najpotężniejsze komputery, a w 1942 r. Nie było żadnego. Historia odszyfrowania komunikatów SZ42 została szczegółowo opisana w [11.3]. Podstawowym atakiem było znalezienie ustawień kół zestawu A, przy użyciu analizy statystycznej, aby znaleźć "prawdopodobnych kandydatów". Ponieważ nawet to dotyczyło ponad 22000000 możliwości (iloczyn długości kół zestawu A), maszyna (znana jako Colossus) została zaprojektowana i zbudowana do tego celu. Chociaż był przeznaczony do jednego specjalnego celu, Colossus był pod pewnym względem wczesnym elektronicznym komputerem.

Problem 11.1

Operator szyfru popełnił jeden błąd podczas ustawiania jednego z kołków na jednym z kół w każdym z poniższych przypadków, a komunikaty szyfrów zostały ponownie wysłane przy użyciu poprawionych ustawień kołków. Co zauważy kryptoanalityk przy porównywaniu obu komunikatów szyfrów w każdym przypadku?

(1) Komunikaty zostały zaszyfrowane na maszynie Hagelin, a niepoprawny pin był na 23 koła;

(2) komunikaty zostały zaszyfrowane na SZ42, a niepoprawny pin na 31-kolowym;

(3) komunikaty zostały zaszyfrowane na SZ42, a niewłaściwa szpilka na 61-kolowym.

Z 131 pinami na Hagelin i 501 na SZ42 takie błędy mogą łatwo wystąpić.

Modyfikacje SZ42

Aby zwiększyć złożoność SZ42, a tym samym utrudnić życie dla kryptoanalityków, wprowadzono trzy modyfikacje w różnych momentach. Wszystkie z nich były przeznaczone do tego, aby stopniowanie kół zestawu B było bardziej nieprzewidywalne. Zamiast ruchu kół zestawu B sterowanego wyłącznie przez bieżącą wartość sworznia na 37-kołowym:

(1) aktualna wartość sworznia na kole 31 została dodana (mod 2) do bieżącej wartości sworznia na 37-kole; lub

(2) aktualna wartość sworznia 43 koła została dodana (mod 2) do bieżącej wartości sworznia na 37-kole; lub

(3) wartość P5 dwie pozycje backwas dodano (mod 2) do bieżącej wartości pin na 37-kole.

Trzecia z nich została wkrótce porzucona, ponieważ wymagała dokładnej transmisji wiadomości, która nie zawsze była gwarantowana. Jeśli wystąpi "garbles", operator odbierający może uznać, że odszyfrowanie stało się bez znaczenia, a więc poprosić o ponowną transmisję, która może pomóc kryptoanalitykom.

Kryptografia klucza publicznego

Tło historyczne

Pierwsze komputery ogólnego zastosowania zostały zbudowane w latach 40. XX wieku. Były duże, wypełniając duże pokoje. Użyli setek zaworów i zużyli wiele kilowatów energii elektrycznej. Wykonali około tysiąca instrukcji na sekundę, co w owym czasie uważano za zadziwiające i popularnie określano ich mianem "gigantycznych mózgów". Kilka osób, w tym Alan Turing, dyskutowało o tym, "czy maszyny mogą myśleć" i postawiło zakłady, czy maszyna pokona mistrza świata w szachach w ciągu najbliższych 25 lat. To pierwsze pytanie pozostaje przedmiotem debaty; ten ostatni został rozstrzygnięty około 45 lat później, kiedy mistrz świata w szachach przegrał mecz z komputerem. Te wczesne maszyny miały bardzo małe pamięci o bezpośrednim dostępie, a jedynie około tysiąca "słów", opartych na lampach katodowych lub liniach opóźniających rtęć. Rzadko funkcjonowały dłużej niż kilka minut, zanim się zepsuły. Ich wejście i wyjście były prymitywne: taśma papierowa lub karty dziurkowane i maszyna do pisania. Kosztują też dużo pieniędzy; 100 000 funtów w 1948 roku, co było równowartością kilku milionów 30 lat później. Bardzo niewiele osób wiedziało, jak pisać programy dla nich. Nie było praktycznie żadnego oprogramowania (jak później stało się znane) i wszystkie programy musiały być napisane w "absolutnym kodzie maszynowym". Nawet kody instrukcji tych maszyn były bardzo ograniczone. Pierwsza maszyna na Uniwersytecie w Manchesterze w 1948 roku, na przykład, nie miała instrukcji dzielenia , więc dzielenie musiało być zaprogramowane przez wielokrotne odejmowanie. Programiści, którzy zazwyczaj byli matematykami, naukowcami lub inżynierami, byli bardzo zręczni i rywalizowali ze sobą o znalezienie eleganckich i skutecznych sposobów wykonywania różnych procesów, takich jak ustalenie, czy binarna reprezentacja liczby zawiera tylko jeden niezerowy bit. To była, oczywiście, bardzo ekscytująca era dla tych, którzy byli zaangażowani. Wydawało się, że nie trzeba dużej liczby komputerów; według jednego szacunku sześć maszyn o mocy komputera Manchesteru wystarczyłoby dla całego świata. Wydawało się również, że programowanie komputerów pozostanie ezoteryczną sztuką dostępną tylko dla elity. Jest wątpliwe, czy ktokolwiek mógłby sobie wyobrazić ogromne postępy, które w ciągu kilku lat zmieniłyby sytuację obliczeniową. Zmiany nastąpiły szybko. W ciągu kilku lat programiści, męczący się pisaniem tych samych fragmentów absolutnego kodu maszynowego, opracowywali kompilatory dla języków znanych jako języki wyższego poziomu. Niektóre z nich dotyczyły konkretnych typów maszyn, ale wkrótce inne, takie jak fortran, który stał się "tłumaczeniem formuły", stały się powszechnie dostępne. Umożliwiło to pisanie programów przez wiele osób iw znacznie krótszym czasie niż dotychczas, ponieważ duże fragmenty kodu maszynowego mogły być teraz wytwarzane przez napisanie kilku linijek w języku wyższego poziomu. W tym samym czasie technologia się zmieniała W szybkim tempie lampy katodowe i linie opóźniające zostały zastąpione przez pamięci rdzeniowe, które były szybsze i bardziej niezawodne, a także zapewniały znacznie większą pojemność w znacznie mniejszej przestrzeni. Zawory zostały zastąpione przez tranzystory, co wkrótce doprowadziło do powstania układów scalonych z setkami, a następnie tysiącami, a następnie milionami tranzystorów na kilku centymetrach kwadratowych krzemu, który zastąpił nieporęczne obwody drukowane. W ciągu 20 lat liczba komputerów wzrosła tysiąckrotnie, a pojemność pamięci wzrosła stukrotnie. Tam była niezliczona liczbaprogramistów na całym świecie i niezliczona liczba innych, którzy używali "paczek" do przetwarzania tekstów, arkuszy kalkulacyjnych lub po prostu "gier" na komputerach, nie mając pojęcia o setkach tysięcy linii kodu maszynowego, oni się wołali. Kolejna ważna zmiana rozpoczęła się w latach 60. XX wieku, kiedy opracowano "wielodostępowe" komputery, w których wiele osób używało połączeń z komputerem typu mainframe, a w ciągu kilku lat sieci komputerów. Zostały ustanowione, pozwalając ludziom na dostęp do więcej niż jednej maszyny i komunikowanie się z innymi w odległych miejscach. Korzyści były oczywiste, a ludzie na różnych kontynentach nie tylko wysyłali do siebie pocztę elektroniczną, ale także współpracowali w badaniach, nigdy się nie spotykając. Koszt komputerów również spadł, nie tylko w

ujęciu realnym, ale w wartościach bezwzględnych, o współczynnik 100 lub więcej. Wszystko to szybko stało się historią i mogło zaginąć w mgle czasu, ale w niektórych relacjach z historii komputerów do około 1980 roku zostały opublikowane i tak zachowane co najmniej część historii tego, co było jednym z najbardziej niezwykłych osiągnięć technologicznych wszechczasów

Problemy z bezpieczeństwem

Bezpieczeństwo stało się problemem od samego początku. Początkowo była to głównie kwestia bezpieczeństwa fizycznego: ochrona sprzętu przed fizycznymi uszkodzeniami, takimi jak pożar czy zalanie. Jednak w ciągu kilku lat pojawiły się doniesienia o niezadowolonych pracownikach, którzy spowodowali spustoszenie, modyfikując lub niszcząc kluczowe programy. Często cytowany przypadek, być może apokryficzny, ale na pewno wiarygodny, był programistą, który napisał program płac i zauważył, że jego pracodawcy mieli zwyczaj zwalniać pracowników w bardzo krótkim czasie. Dlatego wstawił sekcję kodu do programu, aby sprawdzić że jego nazwisko wciąż znajduje się na liście płac, a jeśli nie, to usunąć cały program. W odpowiednim czasie został zwolniony, a program płacowy sam się usunął. Historia mówi dalej, że programista musiał zostać ponownie zatrudniony przy zwiększonej pensji, aby wszystko naprawić. Może to być prawdą lub nie, ale zwraca uwagę na poważną możliwość, zwaną później "atakiem konia trojańskiego", a także na potrzebę sprawdzenia, czy programy te nie zostały "zmodyfikowane", co z kolei doprowadziło do rozwój "oprogramowania antywirusowego". Problemy te nadal występują, a wirusy komputerowe są regularnie zgłaszane; wiele z nich jest po prostu uciążliwością, ale niektóre są potencjalnie katastrofalne.

Ochrona programów i danych

Integralność programów i danych może być chroniona za pomocą lub bez szyfrowania. Programy składają się z bloków kodu. Dane są zwykle przechowywane lub przesyłane w blokach lub pakietach. Jeśli każdy blok zostanie przekształcony w zbiór liczb, które następnie poddane są jakiejś matematycznej funkcji, wynik końcowy może być pozostawiony jako taki lub zaszyfrowany. W obu przypadkach końcową wartość funkcji można zapisać jako sumę kontrolną na końcu bloku. Jeśli ktoś chce coś zmienić w bloku, musi być w stanie obliczyć zarówno funkcję matematyczną, jak i, w stosownych przypadkach, jej szyfrowanie dla nowego bloku. Jeśli nie będzie mógł tego zrobić, suma kontrolna się nie powiedzie i oczywiste będzie, że blok został zmodyfikowany. Wczesną i bardzo prostą wersją tego podejścia było wykorzystanie kontroli parzystości programów i danych przechowywanych na taśmach magnetycznych na komputerach w 1950 roku. W tym przypadku nie było żadnej ingerencji. Suma kontrolna, określana jako boczna kontrola parzystości, została automatycznie wygenerowana dla każdego sześciobitowego (później ośmiobitowego) znaku w bloku i innej sumy kontrolnej, podłużnej kontroli parzystości, w oparciu o liczbę 1 w każdym z sześć (lub osiem) oddzielnych strumieni zostało wygenerowanych na końcu bloku. Te sumy kontrolne zostały skonstruowane w taki sposób, że każdy strumień 0s i 1s miał nieparzystą liczbę 1s. Było to wystarczające do wykrycia i skorygowania pojedynczego błędu w bloku. Jeśli wystąpiły dwa lub więcej błędów, nie można było ich skorygować, a nawet nie wykryć. Napędy taśm przeprowadzają automatyczne sprawdzanie i ponownie odczytują każdy blok, który nie przeszedł testu parzystości. Pył na taśmie może spowodować błędne odczytanie, a taśmy często będą się przesuwać do tyłu i do przodu kilka razy, zanim zaczną się poruszać. Ponieważ sam komputer generował bity kontroli parzystości, nie było żadnych trudności w zmianie danych, jeśli wykryto prawdziwy pojedynczy błąd. Kontrole parzystości nie zostały zaprojektowane, aby pokonać oszustów, którzy mogliby zmienić zarówno dane, jak i sumy kontrolne; były tam tylko po to, aby chronić dane przed kurzem, w tym przed popiołem z papierosów i uszkodzeniami maszyny. Palenie w maszynowni, rozpowszechnione na początku, często było przyczyną błędów taśmowych, a następnie było zakazane. Czasami nie było nic złego w danych na taśmie magnetycznej

i to właśnie obwody sprawdzające w napędach taśmowych były wadliwe. Operatorzy komputerów szybko to odkryli i odkryli, że w Stanach Zjednoczonych jedna czwarta dolara umieszczona w odpowiednim gnieździe na napędzie taśm spowodowała przesłonięcie obwodów kontrolnych. Kiedy stało się możliwe łączenie komputerów razem, aby "wiadomości", które mogą być programami lub danymi, mogły zostać przekazane między nimi, pytanie, w jaki sposób zapewnić, że wiadomości nie zostały "zniekształcone", przypadkowo lub celowo, po drodze do rozważenia. Podczas gdy kontrola parzystości, szczególnie w przypadku bardziej wyrafinowanych kodów korygujących błędy, mogłaby zapewnić ochronę przed przypadkowym uszkodzeniem, oszust byłby w stanie wygenerować odpowiednie sumy kontrolne dla każdego bloku, który zmienił i tym samym uniknął wykrycia. W ten sposób uświadomiono sobie, że konieczne jest szyfrowanie przy użyciu systemu, którego oszust nie mógł powtórzyć.

Szyfrowanie programów, danych i wiadomości

Na początku lat siedemdziesiątych XX wieku większość dużych firm, urzędów państwowych i instytucji akademickich korzystało z komputerów, a sieci komputerowe rozwijały się. Typowa instalacja miałaby jedną lub więcej dużych maszyn, w tym komputery mainframe, z nielicznymi gatunkami, lub później terminale graficzne komunikujące się z nimi za pomocą linii telefonicznych. Wiele z tych organizacji korzystało również z komputerów znajdujących się w odległych lokalizacjach, a także w domach. Aby różnorodni użytkownicy mogli się ze sobą bezpiecznie komunikować, potrzebna była pewna powszechna forma szyfrowania. Ponieważ wszyscy użytkownicy musieliby wiedzieć, w jaki sposób szyfrowanie zostanie przeprowadzone, było jasne, że algorytm szyfrowania musiałby zostać upubliczniony, a poszczególni użytkownicy musieliby mieć swoje własne, tajne klucze, bez których byłoby to niemożliwe rozszyfrować ich wiadomości. To z kolei oznaczało, że metoda szyfrowania musi być wyjątkowo bezpieczna. Oprócz problemów już wspomnianych przy wprowadzaniu sieci komputerowych pojawiły się nowe aspekty bezpieczeństwa. Oto dwa przykłady:

(1) "Problem z uwierzytelnieniem". Użytkownik, X mówi, otrzymuje wiadomość e-mail, która najwyraźniej pochodzi od Y. Skąd X wie, że wiadomość naprawdę została wysłana przez Y i, nawet jeśli ma, że nie została w jakiś sposób zmieniona? Fakt, że wiadomość zawiera adres e-mail Y nie jest gwarancją, ponieważ ktoś mógł używać komputera Y pod jego nieobecność. Nawet jeśli Y ma hasło, możliwe jest, że po zalogowaniu się, wyszedł z pokoju na kilka minut, pozostawiając komputer bezczynny, zły nawyk, który zachęca do niewłaściwego użycia. Umożliwiłoby to użycie strony trzeciej, Z. Komputer Y pod jego nieobecność wysyła wiadomość do X. Jeśli X jest bankiem Y, a wiadomość zezwala na przekazanie dużej sumy pieniędzy z konta Y na rachunek zagraniczny, bank musi mieć jakiś sposób sprawdzenia, czy wiadomość jest autentyczne, w przeciwnym razie można z powodzeniem popełnić oszustwo. Alternatywnie, czy jest możliwe, że Y rzeczywiście wysłał wiadomość do X i że Z w jakiś sposób ją przechwycił i zmienił jej część tak, aby była dla niego korzystna?

(2) "Problem z weryfikacją podpisu". Użytkownik X wysyła wiadomość do Y zezwalającą na jakąś akcję lub inną. Następnie X zaprzecza, że wysłał wiadomość do Y. Spór trafia do strony trzeciej, być może sędziego, który musi zdecydować, czy X naprawdę wysłał wiadomość, czy nie. Czy istnieje sposób, w jaki X, po podpisaniu wiadomości, nie może później zaprzeczyć, że ją wysłał, i odwrotnie, że Y nie może twierdzić, że otrzymał inną wiadomość? Są to problemy praktyczne, które były przedmiotem wielu badań i dyskusji odkąd powstały sieci komputerowe i powrócimy do nich w następnym rozdziale. Zaproponowano różne rozwiązania, ale zasadniczą cechą większości z nich jest to, że istnieje metoda, dzięki której dwie osoby, które chcą się komunikować, mogą to zrobić za pomocą wspólnego systemu szyfrowania, który wymaga użycia jednego lub więcej kluczy, które tylko one wiedzieć. Problem polega na tym, "jak mogą sobie nawzajem poznać sekretne klucze bez odkrywania ich przez inne osoby?".

Kluczowy problem z dystrybucją

Sytuacja jest taka, że X i Y chcą komunikować się ze sobą za pomocą uzgodnionego systemu szyfrowania. Osoba trzecia, Z, zna uzgodniony system szyfrowania, jest w stanie przechwycić wiadomości i chce je odczytać. X i Y mogą, ale nie muszą wiedzieć o istnieniu Z, ale chcą mieć pewność, że ich wiadomości będą niezrozumiałe dla kogokolwiek innego niż oni sami. System, który muszą przyjąć, jest znany Z lub komukolwiek innemu, wymaga użycia jednego lub więcej kluczy, które oni zamierzają zachować w tajemnicy, ale które mogą być zmieniane od czasu do czasu, ewentualnie z każdą wiadomością lub ewentualnie rzadziej. Każdy, kto zdobędzie klucze i zna metodę szyfrowania, może odszyfrować ich wiadomości. Dlatego kluczowe jest, aby klucze pozostały tajne, ale w jaki sposób X i Y mogą sobie nawzajem powiedzieć klucze, nie ryzykując, że Z przechwyci i będzie w stanie je wykorzystać?

System wymiany kluczy Diffiego-Hellmana

Eleganckie rozwiązanie problemu wymiany kluczy zaproponowali Diffie i Hellman w 1976 r. Ich metoda została zaimplementowana przez X i Y w następujący sposób.

(1) X i Y zgadzają się na użycie dwóch liczb całkowitych p i m (powiedzmy), gdzie p to duża liczba pierwsza i leży między 1 i (p? 1). Wartości p i m nie muszą być utrzymywane w tajemnicy.

(2) X wybiera tajną liczbę , x, a Y wybiera tajną liczbę, y. Zarówno x, jak i y leżą między 1 a (p- 1) i żaden z nich nie powinien mieć żadnego wspólnego czynnika z (p- 1). W szczególności, ponieważ (p-1) jest parzyste, ani x, ani y nie powinny być parzyste. X i Y nie ujawniają sobie swoich tajnych numerów ani nikomu innemu.

(3) X oblicza liczbę

$k_x = m^x \pmod p$

i wysyła ją do Y, która podnosi ją do potęgi y, podając liczbę $(k_x)^y$.

Y oblicza liczbę

$k_y = m_y \pmod p$

i wysyła ją do X, który podnosi ją do potęgi x, podając liczbę $(k_y)^x$.

(4) Teraz $(k_x)^y = (k_x)^y = m^{xy} \pmod p = K$ (powiedzmy) i K jest wspólnym kluczem, z którego mogą korzystać zarówno X, jak i Y, nawet jeśli żaden z nich nie zna tajnego klucza drugiego.

Zanim będzie można użyć systemu Diffiego-Hellmana, trzeba będzie znaleźć bardzo dużą liczbę pierwszą, a to nie jest trywialne zadanie. Znów napotykamy ten problem w systemie szyfrowania RSA (gdzie potrzebne są dwie duże liczby pierwsze) , gdzie można znaleźć odniesienia do interesującego podejścia. W realistycznym przykładzie prime p byłoby bardzo duże, ale istotę tej metody można zilustrować za pomocą wielkości umiarkowanej.

Przykład 12.1

W systemie Diffiego-Hellmana, jeśli p = 59, m = 3, x =7 i y =11, jakie będą wartości k_x, k_y i K?

Rozwiązanie

(1) Po pierwsze zauważmy, że (p-1)= 58= 2 x 29 i tak nie ma czynnika wspólnego z x lub y.

(2) X oblicza 37 (mod 59), a Y oblicza 3^{11} (mod 59). Obliczenia te można wykonać na różne sposoby, niektóre bardziej wydajne niż inne. W tym przypadku liczby są na tyle małe, że uprawnienia mogą być obsługiwane za pomocą kalkulatora kieszonkowego. A zatem

3^7= 2187 = 37 x 59 + 4,

3^{11}= 177147 = 59 x 3002 + 29

więc k_x = 4 i k_y = 29.

(3) Wartość wspólnego klucza, K, jest następnie podawana albo przez 4^{11} (mod 59) albo przez 29^7 (mod 59). Powinny dać tę samą wartość; jeśli nie, popełniliśmy błąd. Dlatego sprawdzamy je oba. Liczby tym razem są nieco większe, więc obliczamy je, tworząc potęgi i redukując (mod 59) na każdym etapie:

(i) 4^5 = 1024 = 17 x 59 + 21 = 21 (mod 59)

więc

4^{10} = 441 = 7 x 59+ 28 = 28 (mod 59)

i dlatego

4^{11} = 4 x 28 = 112 = 1 x 59 + 53 = 53 (mod 59).

Wnioskujemy, że wspólny klucz K ma wartość 53.

(ii) Sprawdzamy to, obliczając 29^7 (mod 59).

29^2 = 841 = 14 x 59 + 15 = 15 (mod 59)

więc

29^3=29x15 = 435 = 7 x59+22=22 (mod 59).

Kwadratura,

29^6= 484= 8 x 59 + 12 = 12 (mod 59).

Wreszcie,

29^7 = 29x12= 348 = 5 x 59 + 53 = 53 (mod 59)

a my potwierdziliśmy, że k= 53 w tym przypadku.

Powodem ograniczenia, że ani x, ani y nie mają wspólnego z (p - 1), jest to, że jeśli x, powiedzmy, ma taki współczynnik, wartość k_x, a więc i wspólny klucz K, może okazać się 1, niezależnie od wartości y, która jest niepożądana pod względem kryptograficznym. Na przykład, jeśli p = 31 i m = 2, x i y nie powinny mieć wspólnego współczynnika z 30. Jeśli X miałby wybrać x = 5, powiedzmy, to

k_x= 2^5 = 32 ≡ 1 (mod 31),

stąd k_x = 1 a więc K = 1 bez względu na to, jaką wartość Y wybiera dla y.

Wytrzymałość systemu Diffiego-Hellmana

Jak bezpieczny jest system Diffiego-Hellmana? Należy założyć, że zainteresowana strona trzecia, Z, może uzyskać wartości m, p, k_x i k_y, ale nie z x lub y. Zabezpieczenie zależy więc od tego, jak trudno będzie mu uzyskać wartość x, powiedzmy, biorąc pod uwagę wartość k_x(=m^x (mod p)). Jest to niezwykle trudny problem (dyskretny problem logarytmiczny), chyba że prime, p, ma specjalną postać. Ogólnie

można uznać, że jest niemożliwe, jeśli p jest większe niż około 10^{200}. Powiązany problem wynika z metody szyfrowania RSA, jak zobaczymy. Istnieje jednak alternatywny atak, który Z mógłby zastosować, jeśli może przechwytywać wiadomości na trasie między X a Y i nieco je opóźniać. Ponieważ zna wartości m i p, może być w stanie zachować wartości k_x i k_y i zastąpić wartość własną, powiedzmy $k_z = m^z$, i wysłać ją zarówno do X, jak i Y. X i Y wtedy nieświadomie użyliby k_z w ich szyfrach, a Z odczytałoby ich wiadomości. Następnie ponownie zaszyfrowałby wiadomości, używając oryginalnego klucza k_x lub k_y, a X i Y nie byliby świadomi, że ich wiadomości były czytane. Istnieje duże zainteresowanie sposobami zapobiegania atakom takim jak ten. Pomimo tej potencjalnej słabości system Diffiego-Hellmana zapewnia metodę wymiany kluczy, która pokonałaby wszystkich, oprócz najbardziej zdeterminowanego i dobrze wyposażonego przeciwnika. W szczególności może być używany jako punkt wyjścia do korzystania z systemów szyfrujących takich jak DES, z którymi mamy do czynienia później.

Szyfrowanie i Internet

Uogólnienie prostej substytucji

W prostym szyfrze podstawienia litery alfabetu zostają zastąpione permutacją samych siebie. Widzieliśmy, że taki szyfr jest łatwy do rozwiązania, biorąc pod uwagę zaledwie 200 liter, licząc ich częstotliwości i wykorzystując znajomość języka. Aby użyć takiego szyfru, po prostu wymaga 26 długiego stołu z permutowanym alfabetem. Jeśli, powiedzmy, A zostanie zastąpione przez R, N przez C i T przez H, to AN stanie się RC w szyfrze, a AT stanie się RH. Zatem R, podstawienie dla A pojawi się za każdym razem. Ponieważ prosty szyfr zastępczy zastępuje pojedyncze litery tym samym za każdym razem, niezależnie od tego, jaka litera poprzedza lub podąża za nimi, atak liczenia częstotliwości ostatecznie się powiedzie. Aby temu przeciwdziałać, gdybyśmy mieli system, w którym szyfrowanie litery zależało od niektórych liter po obu jego stronach, wówczas AN może szyfrować RC, podczas gdy AT może szyfrować na przykład KW, a metoda liczenia częstotliwości nie powiedzie się. Taki system mógłby opierać się na tabeli substytucji, która zawierała wszystkie digrafy 676 (= 26x26) i ich odpowiedniki w postaci szyfrów. W efekcie będziemy mieli dwuczęściowy kodeks; pierwsza część wymieniłaby wszystkie 676 dwuwymiarowych digrafów w porządku alfabetycznym po lewej stronie stron z ich odpowiednikami w postaci cyfr po prawej stronie. Druga część zawiera listę digrafów 676 w kolejności alfabetycznej po lewej stronie z odpowiednikami tekstów prostopadłych po prawej stronie. System ten, który można nazwać substytucją digraficzną, byłby bezpieczniejszy niż zwykłe zastąpienie, ale byłby bardziej żmudny w użyciu, a użytkownik musiałby mieć dwie tabele łatwo dostępne, chyba że miałby wyjątkową pamięć. Jeśli kryptograf był przygotowany na dwie tabele pod ręką, wymieniające 17576 (= 26x26x26) zwykły tekst i trigrafy szyfrujące, można by użyć jeszcze bezpieczniejszego systemu, substytucji trigrafów. Oczywiście można opracować w ten sposób coraz bezpieczniejsze systemy, ale w praktyce tabele byłyby nieporęczne, a nawet system oparty na ciągi 4 liter (tj. tetragramów) są praktycznie niewykonalne. Załóżmy jednak, że można opracować system, który pobierałby ciągi liter o stałej długości i jakoś automatycznie konwertował je na inny łańcuch, który gwarantował, że zmiana dowolnej litery w pierwszym łańcuchu spowoduje utworzenie zupełnie innego drugiego ciągu znaków. Taki system nie wymagałby wydrukowanych tabel i mógł być bardzo bezpieczny, w zależności od metody konwersji ciągu i liczby liter w łańcuchach. Na niższym końcu skali takich systemów mamy metodę Juliusza Cezara: konwersja odbywa się poprzez przesunięcie każdej litery o trzy miejsca w przód w alfabecie, a stała długość ciągu wynosi 1. Na górnym końcu skali mamy metoda znana jako RSA, po Rivest, Shamir i Adelman, którzy opracowali metodę w 1978 roku, która może być używana do szyfrowania bardzo długich łańcuchów, na przykład 100 liter, co zapewnia wyjątkowo wysoki poziom bezpieczeństwa. Może się to wydawać wystarczająco godne uwagi, ale jeszcze bardziej niezwykłe jest to, że RSA jest systemem klucza publicznego, co oznacza, jak wyjaśniono w części 12, że szczegóły szyfrowania wiadomości są publicznie dostępne, ale tylko "właściciel" "klucza publicznego wie, jak odszyfrować wiadomości, które są mu wysyłane. Właściciel może jednak odpowiedzieć swoim korespondentom, szyfrując swoje wiadomości w taki sposób, że mogą je odszyfrować. Chociaż teoretycznie szyfrowanie RSA można przeprowadzić ręcznie, obliczenia, które obejmują arytmetykę modułową z bardzo dużą liczbą całkowitą, można było realistycznie przeprowadzić na komputerze z urządzeniami do arytmetycznej wielościowej.

Faktoryzacja dużych liczb całkowitych

Relatywnie łatwo jest pomnożyć dwie liczby, szczególnie jeśli dysponujemy kalkulatorem, o ile nie są one zbyt duże. Jeśli liczby są mniejsze niż 10, dziecko powinno być w stanie zrobić to samodzielnie. Jeśli obaj mają mniej niż 100 osób, mam nadzieję, że dostaną odpowiedź za pomocą papieru i ołówka. Jeśli obie liczby są większe niż 10000, prawdopodobnie użyjemy kalkulatora. Przeciwny problem, znalezienie dwóch lub więcej liczb, które po pomnożeniu razem dają określoną liczbę, nazywa się

faktoryzacją. Jest to o wiele trudniejsze zadanie niż pomnażanie liczb, o czym wie każdy, kto próbował. Na przykład: jeśli zostaniemy poproszeni o pomnożenie 89 przez 103, powinniśmy być w stanie uzyskać odpowiedź, 9167, w mniej niż minutę. Gdybyśmy jednak zostali poproszeni o znalezienie dwóch liczb, których produkt jest 9167, prawdopodobnie zajęłoby nam to znacznie dłużej. Jak byśmy to zrobili?

Standardowa metoda faktoryzacji

Jeśli zostaniemy poproszeni o faktoryzowanie dużej liczby, N, powinniśmy użyć faktu, że jeśli N jest liczbą pierwszą, musi on mieć co najmniej dwa czynniki, a mniejszy z nich nie może przekraczać pierwiastka kwadratowego N. Oznacza to, że w przypadku gdzie N =9167 potrzebujemy tylko testu na podzielność przez liczby początkowe mniejsze niż √9167, czyli prawie 96. Największa liczba podstawowa poniżej 96 wynosi 89, więc w tym przypadku powiedzie nam się na ostatnim teście, w którym to czasie mielibyśmy przeprowadził ponad 20 dzieleń. Gdybyśmy przeprowadzili testy na N = 9161 nie znaleźlibyśmy dzielnika, ponieważ 9161 jest liczbą pierwszą. Wraz ze wzrostem N rośnie liczba testów, które musimy wykonać. Tak więc, jeśli N = 988027 N albo jest liczbą pierwszą, albo jest podzielna przez liczbę mniejszą niż √988027, która jest nieco mniejsza niż 994. Następnie spróbowalibyśmy podzielić 988027 przez każdą liczbę pierwszą mniej niż 994. Jeśli znajdziemy liczbę podstawową, która dzieli 988027 dokładnie, tj. bez pozostawiania reszty, rozwiązaliśmy problem. Jeśli taka liczba nie zostanie znaleziona, będziemy wiedzieć, że 988027 jest liczbą pierwszą. W rzeczywistości

988027 = 991 x 997

a ponieważ zarówno 991 jak i 997 są liczbami pierwszymi, faktoryzacja jest zakończona. Zrobilibyśmy dość dużo wysiłku, aby to zrobić, ponieważ istnieje ponad 160 liczb pierwszych mniejszych niż 991, i musielibyśmy spróbować wszystkie przed sukcesem. Nawet z kalkulatorem byłoby to czasochłonną i żmudną pracą. Ktoś, kto ma komputer i może programować, może oczywiście zabrać komputer do pracy. Niezależnie od tego, jak to zrobiono, zwiększając N z 9167 do 988027, współczynnik około 108, my lub komputer, stanęliśmy w obliczu wzrostu liczby dzieleń z około 20 do ponad 160. Należy zauważyć, że chociaż N wzrosła o współczynnik ponad 100, tak że √N wzrosła o współczynnik większy niż 10, liczba testów wzrosła o współczynnik wynoszący tylko około 8. Ta metoda znajdowania czynników pierwszych liczb przez podzielenie liczby przez każdą liczbę pierwszą mniejszą niż pierwiastek kwadratowy jest zasadniczo spowodowana przez Eratostenesa i jest standardową metodą zarówno dla faktoryzowania (jeśli działa), jak i dla wykazania, że liczba jest liczbą pierwszą (jeśli się nie powiedzie). Nie jest to jedyna metoda, którą można zastosować, czasami można znaleźć skrót; na przykład ktoś może to zauważyć

$9167=9216-49 =(96)^2 - (7)^2 = (96 - 7)(96 + 7) = 89 \times 103$

a nawet lepiej

$$988\,027 = 988\,036 - 9 = (994)^2 - (3)^2 = (994 - 3)(994 + 3)$$
$$= 991 \times 997$$

ale generalnie nie mamy tyle szczęścia. Czasami, na przykład gdy liczba, którą próbujemy zliczyć, ma szczególną postać, taką jak

2p-1,

gdzie p jest liczbą pierwszą, istnieją specjalne techniki, które zmniejszają liczbę możliwości, ale w rodzaju liczby, która jest istotna dla w systemie RSA te specjalne techniki nie mają zastosowania. Opisany poniżej system szyfrowania RSA polega na szyfrowaniu jego bezpieczeństwa na tym fakcie: że

bardzo czasochłonne jest zliczanie dużej liczby, nawet jeśli powiedziano nam, że jest to produkt dwóch dużych liczb pierwszych. Jeśli chodzi o proces szyfrowania w systemie RSA, podstawą tego jest eleganckie i mocne twierdzenie, bez dowodu potwierdzone przez francuskiego matematyka Pierre'a Fermata na początku XVII wieku. Jest to często nazywane "Małym twierdzeniem Fermata" i nie należy go mylić z osławionym "Ostatnim twierdzeniem Fermata", które również stwierdził bez dowodu, a które nie zostało udowodnione do 1993 r. Fermat mógł mieć na to dowód. "Małe twierdzenie"; jest bardzo mało prawdopodobne, aby miał dowód na swoje "Wielkie twierdzenie". Szwajcarski matematyk Leonhard Euler dał dowód Małego Twierdzenia Fermata w 1760 r., A także uogólnił go, dając nam tak zwane Twierdzenie Fermata-Eulera i właśnie to jest używane w procesie szyfrowania / deszyfrowania RSA. Na wstępie warto zapoznać się z kilkoma przykładami

"Małe twierdzenie" Fermata

Oto kilka podstawowych ćwiczeń.

Co to jest, gdy

(1) 2^4 dzieli się przez 5?

(2) 3^4 dzieli się przez 5?

(3) 3^6 dzieli się przez 7?

(4) 5^6 dzieli się przez 7?

(5) 3^{10} dzieli się na 11?

(6) 8^{10} dzieli się przez 11?

(7) 59^{96} dzieli się przez 97?

Rozwiązania

(1) $2^4 = 16 = 3 \times 5 + 1$. Reszta 1.

(2) $3^4 = 81 = 16 \times 5 + 1$ Reszta 1.

(3) $3^6 = 729 = 104 \times 7 + 1$. Reszta 1.

(4) $5^6 = 15625 = 2232 \times 7 + 1$. Reszta 1

(5) $3^{10} = 59049 = 5368 = 11 + 1$. Reszta 1

(6) W tym przypadku unikamy konieczności radzenia sobie z dużymi liczbami za pomocą arytmetyki modułowej, jak opisano w części1:

$8 = 2^3$

więc

$8^{10} = 2^{30} (2^5)^6 = (32)^6$

i

$32 \equiv -1 \pmod{11}$

więc

$(32)^6 \equiv (-1)^6 = (1 \pmod{11}$

więc reszta to 1.

(7) Reszta to znowu 1. Ponieważ $(59)^{96}$ jest bardzo dużą liczbą, zawierającą 171 cyfr, jeszcze bardziej istotne jest stosowanie arytmetyki modularnej. Czy reszta zawsze wynosi 1, gdy wykładnik po lewej stronie jest o 1 mniejszy niż moduł po prawej? Nie, nie jest. Rozważać

$2^{14} = 16384 = 1092 \times 15 + 4$.

W takim przypadku pozostała część to 4, a nie 1. Dlaczego tak jest? Odpowiedź brzmi, że 15=3x3 nie jest liczbą pierwszą, a małe twierdzenie Fermata ma zastosowanie tylko wtedy, gdy moduł jest liczbą pierwszą , taką jak 5, 7, 11 lub 97, jak w przykładach powyżej. Euler pokazał, jak należy zmodyfikować twierdzenie, gdy moduł nie jest pierwiastkiem. Pierwotnym twierdzeniem jest jednak

Twierdzenie Małego Fermata

Jeśli p jest liczbą pierwszą, a m jest dowolną liczbą, która nie jest podzielna przez p, wtedy

$m^{(p-1)} \equiv 1 \pmod{p}$,

tj. $m^{(p-1)}$ pozostawia resztę 1, gdy jest podzielona przez p.

Dowód nie jest trudny i uogólniony dość łatwo dając dowód twierdzenia Fermata-Eulera. Uogólnienie odkryte i udowodnione przez Eulera odnosi się do dowolnego modułu, ale wersja wymagana przez system RSA wymaga tylko przypadku, w którym moduł jest iloczynem zaledwie dwóch różnych liczb pierwszych i tak jest warte samodzielnego stwierdzenia:

Twierdzenie Fermata-Eulera (w razie potrzeby w systemie RSA)

Jeśli p i q są różnymi liczbami pierwszymi, a m jest dowolną liczbą, która nie jest podzielna przez

p lub q wtedy

$m^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

W powyższym przykładzie mieliśmy p=3, q=5 i m = 2 i twierdzenie to mówi nam

$2^{(2)(4)} \equiv 1 \pmod{15}$

i rzeczywiście $2^8 = 256 = 17 \times 15 + 1$.

Klucze szyfrowania i rozszyfrowania w systemie RSA

Aby zaszyfrować tekst za pomocą metody RSA, potrzebujemy:

(1) dużej liczby n(= Pq), która jest iloczynem tylko dwóch różnych liczb pierwszych, p i q (Pytanie o to, w jaki sposób można stwierdzić, że bardzo duże liczby pierwsze są bardzo istotne, już wcześniej napotkaliśmy ten problem w związku z system wymiany kluczy Diffiego-Hellmana. Ogólnie wymagana jest znaczna ilość obliczeń. Ponieważ liczby pierwsze, które mają być użyte, nie powinny w tym przypadku mieć żadnej specjalnej formy, takiej jak $2^p - 1$, nie ma naprawdę szybkich metod; istnieje jednak metoda wyszukiwania liczb, które są prawdopodobnie liczbami pierwszymi, gdzie prawdopodobieństwo może być arbitralnie zbliżony do 1, tj. do prawie pewności;

(2) liczbę całkowitą, e, zwaną kluczem szyfrującym, która nie ma czynnika wspólnego z (p-1) (q- 1) lub samą n; Aby odszyfrować tekst, który został zakodowany przy użyciu metody RSA, wymagamy dodatkowo

(3) liczby całkowitej, d, znana jako klucz deszyfrujący, która spełnia warunek, że

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

W tym miejscu warto zauważyć, że relacja między e i d jest symetryczna, co mówi nam, że jeśli d jest kluczem do rozszyfrowania dla e, to e jest kluczem do rozszyfrowania dla d. Znaczenie tego stanie się jasne, kiedy zobaczymy, w jaki sposób "właściciel" klucza do odszyfrowania, d, może odpowiedzieć swoim korespondentom. Gdy n i e są wybrane, d musi zostać znaleziony. Istnieje metoda na to, jeśli p i q są znane; ale jeśli p i q nie są znane, d nie można znaleźć, a ten fakt jest podstawą bezpieczeństwa systemu RSA. Jeśli p i q są wyjątkowo duże, np. Większe niż 10^{200}, znalezienie ich wartości w rozsądnym czasie, co oznacza rozłożenie n, byłoby poza mocą nawet najszybszych komputerów. Przed przystąpieniem do samego procesu szyfrowania są tu dwa przykłady pokazujące, w jaki sposób można znaleźć d, jeśli wartości p, q i e są znany. Pierwszy przykład obejmuje tylko małe liczby; w drugim przypadku liczby są nieco większe, chociaż nadal są dużo mniejsze, niż byłoby prawdopodobne, że będą stosowane w szyfrowaniu RSA.

Przykład 13.1

Znajdź klucz odszyfrowujący, d, gdy n = 91 a klucz szyfrujący, e, to 29.

Rozwiązanie

Zaczynamy od zauważenia, że 91 = 7 x 13 i tak, biorąc p= 7 i q=13 mamy

(p -1) (q - 1)= 6x12 = 72

a ponieważ 29 nie ma czynnika wspólnego z 91 lub 72, jest to ważny klucz kodowania dla metody RSA. Aby znaleźć odpowiedni klucz odszyfrowujący, d, używamy algorytmu Euklidesa, ale metoda jest zilustrowana przez:

$$72 = 2 \times 29 + 14,$$
$$29 = 2 \times 14 + 1,$$

więc

1 =29 – 2 x 14

ale widzieliśmy, w pierwszym wierszu powyżej, że 14 = 72 – 2 x 29 a więc

$$1 = 29 - 2 \times (72 - 2 \times 29) = 5 \times 29 - 2 \times 72,$$
$$5 \times 29 = 2 \times 72 + 1,$$

lub

5 x 29 ≡ 1 mod (72)

)tj.. 145 = 144 +1) co oznacza ,że d, klucz deszyfrujący to 5

To może wydawać się mylące, ale metoda polega na użyciu algorytmu Euklidesa w celu znalezienia najwyższego wspólnego współczynnika klucza szyfrowania, e, i liczby (p-1) (q-1). Ponieważ e i (p-1) (q-1) nie mają wspólnego czynnika, najwyższy wspólny współczynnik wynosi 1. Jeśli teraz "pracujemy wstecz" przez algorytm Euklidesowy od ostatniej linii do pierwszej, zastępując ostatnią liczbę po prawej stronie każdej tożsamości przez inne liczby zaangażowany, ostatecznie uzyskamy klucz do odszyfrowania, d, jak podano na podstawie zgodności w punkcie (3) powyżej. Formalny opis i alternatywne podejście,

Przykład 13.2 (Nieco bardziej realistyczny przypadek, który wykorzystamy poniżej) Znajdź klucz rozszyfrowujący, d, gdy n = 3127 i klucz szyfrujący, e, to 17.

Rozwiązanie

Zauważmy, że n = 3127 = 53 x 59 i 53 i 59 są obie liczbami pierwszymi. Wynika z tego, że n jest prawidłowym modułem dla RSA i że (p-1) (q-1)= (52)(58)= 3016. Ponadto, ponieważ 17 nie ma czynnika wspólnego z 3127 lub z 3016, jest to poprawny klucz szyfrowania. Postępowanie jak poprzednio, czyli

$$3016 = 177 \times 17 + 7,$$
$$17 = 2 \times 7 + 3,$$
$$7 = 2 \times 3 + 1,$$

więc

1 = 7 – 2 x 3

ale z drugiej linii powyżej, 3 = 17 – 2 x 7 i tak

$$1 = 7 - 2 \times (17 - 2 \times 7) = 5 \times 7 - 2 \times 17$$

ale od pierwszej linii powyżej 7 = 3016 - 177 x17 i tak

$$1 = 5 \times (3016 - 177 \times 17) - 2 \times 17 = 5 \times 3016 - 887 \times 17$$

lub

887x 17 ≡ 1 (mod 3016).

Potrzebujemy wartości d, która pomnożona przez 17, pozostawia resztę +1, gdy jest podzielona przez 3016, a zatem jest to -887, a nie +887. Teraz – 887 ≡ 2129 (mod 3016), więc klucz do odszyfrowania, d, to 2129. (Sprawdź: 2129 x 17 = 36 193 = 12x 3016 + 1).

Procesy szyfrowania i rozszyfrowywania w systemie RSA

Aby szyfrować komunikat za pomocą metody RSA, potencjalny użytkownik musi znać wartości modułu, n(=pq) i klucz szyfrowania, e; są one publicznie dostępne. Tylko "właściciel" systemu, który jest używany, zna wartości p i q oraz klucz do rozszyfrowania, d. Aby zaszyfrować wiadomość, która ma zostać wysłana do "właściciela" i którą sam może rozszyfrować, użytkownik musi:

(1) zamienić litery swojej wiadomości na liczby, takie jak te podane w tabeli 1.1, tak, że na przykład A= 00, B= 01, ..., Z= 25;

(2) jeżeli moduł n zawiera nie więcej niż cyfry D, przerwij numer wersji wiadomości na bloki składające się z maksymalnie D cyfr; oznaczają te bloki przez B_1, B_2, ...;

(3) szyfrować bloki w porządku i niezależnie przez obliczanie

(4) $(B_I)^e$ (mod n), I = 1, 2, ..., podając bloki szyfrów C_1, C_2, ...

Komunikat szyfrowy to C_1C_2 ... (ciąg cyfr, nie liter). Aby odszyfrować komunikat, procedura jest dokładnie taka sama, jak w przypadku szyfrowania, z tą różnicą, że bloki, które mają być obsługiwane, to bloki szyfrów C_I, a klucz dezszyfrującego , d, jest używany zamiast klucza szyfrującego, e, na etapie (4). Jest to konsekwencją sposobu, w którym d zostało określone, że $(C_I)^d = B^I$, lub innymi słowy, że oryginalna wiadomość jest odzyskiwana.

Przykład 13.3

Zaszyfruj wiadomość

COMEXATXNOON

przy użyciu systemu RSA z n = 3127 i kluczem szyfrującym, e = 17.

Szyfrowanie

Konwertujemy tekst na liczby używając Tabeli 1.1 w zwykły sposób. Ponieważ moduł 3127 zawiera cztery cyfry, dzielimy tekst na pary liter, a mianowicie:

CO ME XA TX NO ON

0214 1204 2300 1923 1314 1413

Musimy teraz obliczyć wartość każdej z sześciu czterocyfrowych liczb podniesionych do potęgi 17 w odniesieniu do modułu 3127. Obliczenia są pracochłonne i dlatego są podane szczegółowo tylko dla pierwszej liczby, 0214. Pozostałe wartości można łatwo uzyskać za pomocą prostego programu komputerowego. Naszym zadaniem jest następnie obliczyć $(0214)^{17}$ (mod 3127). Gdy tylko jest to możliwe w obliczeniach modułowych tego rodzaju, używamy powtarzających się skracania, aby uzyskać moc liczb, a następnie pomnożymy razem odpowiednie uprawnienie. Ponieważ $16 = 2^4$ możemy zbliżyć się do wymaganej mocy, więc postępujemy w następujący sposób:

$$(214)^2 = 45\,796 = 14 \times 3127 + 2018 \equiv 2018 \pmod{3127}$$

więc

$$(214)^4 \equiv (2018)^2 = 4\,072\,324 = 1302 \times 3127 + 970 \equiv 970 \pmod{3127}$$

i

$$(214)^8 \equiv (970)^2 = 940\,900 = 300 \times 3127 + 2800 \equiv 2800 \pmod{3127},$$

stąd

$$\begin{aligned}(214)^{16} &\equiv (2800)^2 = 7,840,000 = 2507 \times 3127 + 611 \\ &\equiv 611 \pmod{3127}.\end{aligned}$$

Wreszcie

$$\begin{aligned}(214)^{17} &\equiv (214)(611) = 130\,754 = 41 \times 3127 + 2547 \\ &\equiv 2547 \pmod{3127}.\end{aligned}$$

Szyfrowanie 0214 to zatem 2547. Pozostałe bloki tekstu wiadomości są szyfrowane w ten sam sposób, to znaczy podnosząc każdą czterocyfrową liczbę do potęgi 17 (mod 3127). Wynikowy tekst szyfrowania to 2547 3064 2831 0063 2027 1928.

Nie można tego przekształcić z powrotem w litery, ponieważ niektóre, w rzeczywistości najbardziej, cyfry są większe niż 25. Aby odszyfrować ten komunikat szyfrowania, odbiorca ("właściciel") podniósł każdą czterocyfrową liczbę do potęgi klucza rozszyfrowującego, 2129, (mod 3127).

$$2129 = 2048 + 64 + 16 + 1 = 2^{11} + 2^6 + 2^4 + 1$$

obliczenie wymagałoby podniesienia każdej czterocyfrowej liczby do potęgi 2^4, 2^6 i 2^{11} poprzez wielokrotne kwadrowanie, a następnie tworzenie odpowiednich produktów. Zastosowanie tej metody "wielokrotnego kwadrowania", podnoszącego bloki szyfru do potęgi 2129, wymaga "tylko" czternastu multiplikacji lub podziałów zamiast ponad 4000, co wymagałoby obliczenie bezpośredniej "brutalnej siły". Aby pokazać, jak to zrobić i potwierdzić, że 2129 jest kluczem do rozszyfrowania w tym przypadku, oto obliczenia dotyczące rozszyfrowania czwartego czterocyfrowego bloku w powyższym komunikacie szyfrowym (tj. 0063). Obliczamy $(63)^{2129}$ i znajdujemy pozostałą część, gdy dzielimy się przez 3127. Z powyższego,

$(63)^{2129} = (63)^{2048} \times (63)^{64} \times (63)^{16} \times (63)^{1}$

i przystępujemy do tworzenia tabeli 2 razy moc od 63 do n = 11 przez wielokrotne kwadrowanie. Tak więc $(63)^2 = 3969 = 3127 + 842$, więc umieszczamy 842 w tabeli naprzeciwko n = 2. Kontynuujemy w ten sposób, a pełną tabelę pokazano w tabeli 13.1.

n	$N = 2^n$	$(63)^N \pmod{3127}$
0	1	63
1	2	842
2	4	2262
3	8	872
4	16	523
5	32	1480
6	64	1500
7	128	1687
8	256	399
9	512	2851
10	1024	1128
11	2048	2822

Aby uzyskać $(63)^{2129} \pmod{3127}$, mnożymy teraz cztery liczby po prawej stronie, przeciwne n 0, 4, 6 i 11:

$(63)^{2129}$ (63)(523)(1500)(2822)

Teraz

$$63 \times 523 = 32\,949 = 10 \times 3127 + 1679 \equiv 1679 \pmod{3127},$$

i

$$1500 \times 2822 = 4\,233\,000 = 1353 \times 3127 + 2169 \equiv 2169 \pmod{3127}$$

a ponieważ

$$1679 \times 2169 = 3\,641\,751 = 1164 \times 3127 + 1923 \equiv 1923 \pmod{3127},$$

rozszyfrowane 0063 jest zatem 1923. To zamienia z powrotem na litery jako TX, który jest czwartym digrafem pierwotnej wiadomości. Obliczenia te, choć żmudne, można wykonać na kalkulatorze kieszonkowym, ale w prawdziwym zastosowaniu systemu RSA liczby całkowite byłyby znacznie większe i niezbędny byłby komputer z oprogramowaniem zdolnym do obsługi takich liczb całkowitych. Nawet

jeśli używany jest komputer, zmniejszenie liczby multiplikacji i podziałów przy użyciu techniki "ponownej kwadratury" ma ogromne znaczenie. W typowym zastosowaniu systemu RSA, w którym moduł może wynosić co najmniej rzędu 10^{100}, klucz szyfrowania lub rozszyfrowania może z łatwością wynosić około 10^{50}, a ponieważ bloki liczb muszą zostać podniesione do tej mocy, " obliczenia z użyciem siły ciężkiej nie wchodzą w rachubę. Z drugiej strony liczba powtórzeń i podziałów jest zredukowana do kilkuset, co zajmuje co najwyżej milisekundy.

W jaki sposób właściciel klucza odpowiada na korespondentów?

Po otrzymaniu wiadomości zakodowanej w systemie RSA przy użyciu jego klucza publicznego, w jaki sposób może odpowiedzieć właściciel klucza odszyfrowania? Odpowiedź jest bardzo prosta: poprzez zaszyfrowanie wiadomości za pomocą (tajnego) klucza do rozszyfrowania, d; odbiorca odszyfrowuje wiadomość szyfrowaną, którą odebrał, używając (publicznego) klucza szyfrowania. Spowoduje to wygenerowanie oryginalnego komunikatu w postaci zwykłego tekstu, ponieważ, jak zauważono wcześniej, istnieje symetria między kluczami szyfrowania i rozszyfrowania w systemie RSA: każde odblokowuje drugie. Algorytm RSA jest szczególnym przypadkiem systemu szyfrowania kluczy publicznych, ponieważ każdy, kto chce otrzymywać zaszyfrowane wiadomości, zapewnia klucz w niektórych publikacjach, które są publicznie dostępne, na przykład w książce telefonicznej. To jest klucz do szyfrowania. Tylko właściciel klucza szyfrowania ma odpowiedni klucz do rozszyfrowania, tak więc chociaż każdy może wysłać mu zaszyfrowaną wiadomość, sam może ją rozszyfrować. Aby tak było metoda szyfrowania musi być taka, aby w rozsądnym czasie niemożliwe było znalezienie klucza do odszyfrowania, nawet gdy znana jest metoda szyfrowania i klucz szyfrowania. W przypadku RSA bezpieczeństwo zależy od faktu, że łatwo jest pomnożyć dwie duże liczby razem, ale bardzo trudno jest znaleźć dwie duże liczby, jeśli otrzymamy tylko ich produkt. Funkcja, która jest łatwa do obliczenia, ale bardzo trudna do odwrócenia, taka jak RSA, nazywana jest funkcją jednokierunkową. Innym przykładem jest dyskretny problem logarytmiczny, który spotkaliśmy wcześniej w systemie Diffiego-Hellmana.

Problem 13.1

Jest możliwe, że w systemie RSA ciąg będzie sam się szyfrował. Najbardziej oczywistymi przypadkami w powyższym dwucyfrowym przykładzie są ciągi AA i AB, które są reprezentowane numerycznie odpowiednio przez 0000 i 0001, a ponieważ oba z nich podniesione do dowolnej mocy pozostają niezmienione, będą szyfrować się same, bez względu na klucz szyfrowania lub moduł . Istnieją jednak inne przypadki; sprawdzić, czy z modułem 3127 i kluczem kodowania 17 liczby 0530 i 0531 zarówno szyfrują same w sobie w systemie RSA. (Aby nie twierdzić, że 0530 i 0531 nie odpowiadają parom liter, należy zauważyć, że 0825 i 2302, formy liczbowe IZ i XC, również są dla siebie szyfrowane.) Należy jednak stwierdzić, że prawdopodobieństwo, że blok tekstu w "prawdziwym" zastosowaniu RSA sam z siebie szyfr jest nieistotny.

Standard szyfrowania danych (DES)

W 1973 r. Rząd Stanów Zjednoczonych, w odpowiedzi na ponawiane prośby ze strony przemysłu i różnych organizacji, przekazał Departamentowi Handlu zadanie ustanowienia jednolitych federalnych standardów automatycznego przetwarzania danych, a w ramach tego działu odpowiedzialność została przekazana Krajowemu Biuru Norm (NBS).). Jednym z aspektów rozważanych przez NBS było opracowanie standardu szyfrowania danych. Zamiast samodzielnie proponować sam algorytm, NBS opublikował zaproszenie dla zainteresowanych stron do przedłożenia propozycji "Standardu szyfrowania danych" w maju 1973 r. Specyfikacja standardu szyfrowania danych opublikowana przez NBS określa warunki, które każdy proponowany algorytm musi spełniać: że musi zapewniać wysoki poziom bezpieczeństwa, że bezpieczeństwo nie może opierać się na tajemnicy algorytmu, że musi być

ekonomicznie wdrażane elektronicznie, wydajne w użyciu i dostępne dla wszystkich użytkowników i dostawców. Początkowa odpowiedź okazała się rozczarowująca, drugie zaproszenie zostało opublikowane w sierpniu 1974 r., W wyniku czego wniosek przedłożony przez IBM został wybrany do oceny w marcu 1975 r. Po około 18 miesiącach dyskusji i komentarzy oferta IBM została zaakceptowana i stała się "The Data Encryption Standard", DES w skrócie, w listopadzie 1976 r. DES był przedmiotem wielu analiz i poświęcono mu znaczną literaturę. Pełne szczegóły, głównie z zainteresowania specjalistów, można znaleźć w wielu książkach. Podstawowe informacje można podsumować w następujący sposób.

Tło

(1) Algorytm służy do szyfrowania bloków 64-bitowych danych pod kontrolą 64-bitowego klucza (K). DES jest zatem przykładem tego, co jest znane jako szyfr blokowy.

(2) Dwie osoby, które chcą się komunikować za pomocą DES, muszą uzgodnić klucz (tajny), K. Wszystko inne na temat DES jest wiedzą publiczną.

(3) W przypadku tajnego klucza, K, użytkownicy wybierają siedem 8-bitowych znaków (tj. 56 bitów we wszystkich), a DES następnie łączy się z kolejnymi 8 bitami kontroli parzystości, aby nadać wymagany 64-bitowy klucz tajny.

Procedura szyfrowania

(4) 64-bitowy blok danych jest poddawany początkowej permutacji (IP).

(5) 64 bity danych są podzielone na dwa segmenty 32-bitowe, lewy (L) i prawy (R).

(6) Czterdzieści osiem bitów klucza, K, jest połączonych z "rozwiniętą" 48-bitową wersją R w sposób nieliniowy ("rozwinięcie" składa się z powtarzania 16 z 32 bitów R), a te 48 bitów jest następnie "zredukowanych" do 32-bitowego łańcucha, X (powiedzmy).

(7) L jest zastąpione przez R i R jest zastąpione przez (mod 2) sumą X i L, dając nowy 32-bitowy R.

(8) Kroki (6) i (7) są powtarzane 16 razy przy użyciu różnych 48-bitowych segmentów K w kroku (6) za każdym razem.

(9) 64 bity ostatniego (16) etapu są poddawane odwrotności początkowej permutacji, tj. (IP)? 1.

(10) Otrzymane 64 bity są szyframi.

Procedura odszyfrowywania

(11) Rozszyfrowanie odbywa się za pomocą procedury kodowania w odwrotnej kolejności z tym samym kluczem, K.

Bezpieczeństwo DES

Warto zauważyć, że dwie osoby, które chcą się komunikować za pomocą DES, muszą uzgodnić wspólny klucz, co można uzgodnić między nimi za pomocą systemu wymiany kluczy Diffiego-Hellmana. Chyba że strona trzecia może przechwycić i zmienić swoją komunikację, to powinno być bezpieczne. Co do samego DES: przeprowadzono wiele statystycznych i innych testów na danych zaszyfrowanych za pomocą różnych kluczy przy użyciu DES i uznano je za zadowalające. Szczególnie ważna jest tak zwana próba lawinowa: jeśli zmieni się jeden z 64 bitów wejścia, ile z 64 bitów wyjścia zostanie zmienionych? W słabym systemie szyfrowania odpowiedź brzmi "1"; w idealnym systemie szyfrowania będzie to "około 32" i tak dzieje się w DES. Niemniej jednak, zanim DES został wprowadzony do użytku, pojawiły

się argumenty dotyczące jego poziomu bezpieczeństwa. Ponieważ użytkownicy określają klucz o 56 bitach, istnieje "tylko" 256 możliwych kluczy do wypróbowania przez przeciwnika. Teraz 2^{56} jest w przybliżeniu równe $10^{16,86}$, a jeśli komputer mógłby przetestować jeden klucz w mikrosekundzie, mógł wypróbować je wszystkie za około 2300 lat. Jest to oczywiście niepraktyczne, ale krytycy DES sugerują, że milion takich komputerów pracujących równolegle może znaleźć klucz pod jednym dniem. Ponieważ kosztowałoby to ogromną ilość pieniędzy i wymagałoby wielu organizacji, trudno sobie wyobrazić, by ktokolwiek uznał to za warte, chyba że wiadomo, że dotyczy ono istotnej kwestii bezpieczeństwa narodowego. Sugerowano również, że być może istnieje tajemna "zapadnia", czyli pięta achillesowa, znana projektantom DES, która umożliwiłaby tym, którzy ją znają, odnalezienie klucza w realistycznym czasie. To może być prawda, ale nikt nie znalazł dowodów na istnienie takiej rzeczy. Sugerowano również, że DES powinien być oparty na dłuższym kluczu, a 128 bitów jest najpopularniejszym wyborem. To niewątpliwie podważyłoby jego bezpieczeństwo i od tego czasu 128-bitowe szyfrowanie zostało wprowadzone w innych systemach, ale w 1977 r. Nie uznano tego za konieczne. Alternatywą dla kluczy 128-bitowych wydaje się być użycie dwóch 64-bitowych kluczy po kolei, ale można to wykazać tylko dwa razy bezpieczniej niż przy użyciu pojedynczego klucza 64-bitowego pod warunkiem, że dostępna jest ogromna ilość pamięci komputerowej . Atak zakłada, że dostępny jest zwykły tekst i jego odpowiednik z szyfrowaniem. Znany tekst jawny jest szyfrowany pod wszystkimi możliwymi kluczami 64-bitowymi, a znany tekst szyfrowania jest niezależnie rozszyfrowywany pod wszystkimi możliwymi 64-bitowymi kluczami. Te dwa zestawy danych są sortowane i porównywane. Oznacza to, że wymagane jest 2^{57} testów, a nie 2^{112}. Po znalezieniu dwóch identycznych tekstów mamy kandydatów na dwa nieznane klucze. Wiele par fałszywych kluczy (w rzeczywistości około 2^{48}) zostanie znalezionych i będzie musiało zostać przetestowanych na kolejnych znanych parach tekstowych szyfrogramu. Ten atak "spotkać się w środku" nie jest obecnie praktyczny i jest mało prawdopodobne, aby był w przewidywalnej przyszłości. Bezpieczeństwo DES jest ogromnie zwiększone, jeśli użyjemy potrójnej szyfrowania. Wymagane są tylko dwa klucze, ale są one stosowane w następujący sposób:

(1) szyfrowanie z kluczem 1;

(2) deszyfrujemy kluczem 2;

(3) szyfrujemy z kluczem 1.

Przeciwnik musi teraz wypróbować 2^{112} możliwych par kluczy i jest to uważane za niemożliwe w realnym czasie. Ta potrójna encyklopedia DES jest uważana za bezpieczną i jest obecnie w użyciu. Ta forma potrójnej szyfrowania ma dodatkową zaletę, że staje się identyczna z pojedynczą enkoderem DES, jeśli oba klucze są takie same, ponieważ pozwoliłoby to użytkownikowi z potrójną szyfracją na komunikację z pojedynczym użytkownikiem szyfrowania i na odwrót. Inna forma potrójnej szyfrowania używa trzech różnych kluczy w trzech etapach powyżej. Po raz kolejny zgodność z inne formy uzyskuje się, wykonując dwa lub więcej klawiszy tego samego

Łańcuch

Ponieważ kodowanie DES w krótkich blokach zawiera tylko 64 bity, oczywistym pytaniem jest: w jaki sposób szyfrujemy komunikaty, które są dłuższe niż to? Prostym sposobem jest rozbicie wiadomości na bloki składające się z 8 znaków (= 64 bity) i szyfrowanie ich sekwencyjnie za pomocą tego samego 64-bitowego klucza. Oznaczałoby to, że wszystkie 64-bitowe komunikaty szyfru były "głębokie", ale nieliniowa natura encyklopedii DES czyni tę cechę, co byłoby katastrofalne, gdyby szyfrowanie było liniowe, o małej lub żadnej wartości dla kryptoanalityka. Jednak bezpieczniejszą metodą jest zmiana klucza dla każdego 8-znakowego łamania bloków, przy czym każdy klucz zależy od oryginalnego klucza i niektórych lub wszystkich tekstów jawnych poprzedzających bloków. Uprawniony odbiorca odzyska tekst jawny pierwszego bloku, ponieważ zna oryginalny klucz; będzie on w stanie skonstruować klucz

do drugiego bloku i tak go rozszyfrować. Będzie teraz miał tekst jawny drugiego bloku, a więc będzie w stanie zbudować klucz do odszyfrowania trzeciego bloku; i tak dalej. Nieautoryzowany odbiorca, któremu uda się włamać do części wiadomości, prawdopodobnie z powodu powtarzalnego tekstu standardowego, nie będzie mógł dalej się rozwijać, ponieważ nie znając wszystkich wcześniejszych bloków tekstu jawnego, nie będzie mógł zrekonstruować pozostałych kluczy. Gdyby ten sam klucz został użyty dla każdego bloku, który byłby w stanie odszyfrować całą wiadomość. Użytkownicy systemów szyfrowania opartych na kluczach zastosowanych do krótkich bloków tekstu, takich jak DES, zdecydowanie zaleca się stosowanie łańcuchów.

Implementacja DES

Chociaż nie jest trudno napisać program do szyfrowania / deszyfrowania przy użyciu algorytmu DES, żadna implementacja oprogramowania nie może być zatwierdzona, częściowo dlatego, że można modyfikować programy. Ponadto wersje oprogramowania byłyby znacznie wolniejsze niż wersje sprzętu na specjalnie zaprojektowanych układach scalonych, a wkrótce po zatwierdzeniu DES różni producenci zaprojektowali i wyprodukowali urządzenia zawierające chipy do wykonywania algorytmu DES. Urządzenia te mogą szyfrować lub rozszyfrowywać z szybkością sto tysięcy znaków i więcej, na sekundę.

Używanie zarówno RSA, jak i DES

W systemach klucza publicznego, takich jak RSA, ogólnie algorytm szyfrowania / rozszyfrowywania wymaga dużej ilości obliczeń i dlatego może działać "wolno", podczas gdy w systemach szyfrowych blokowych, takich jak DES, procesy szyfrowania / deszyfrowania mogą być wykonywane znacznie szybciej, być może tysiąc razy szybciej. Jeśli jednakże

(1) nadawca szyfruje klucz DES za pomocą metody RSA i wysyła go do odbiorcy, a następnie

(2) nadawca szyfruje wiadomość za pomocą klucza DES, zachowując znaczną ilość obliczeń bez zmniejszania bezpieczeństwa jako całości. Jeśli stosuje się "łańcuchowanie", algorytm RSA musiałby być użyty tylko raz, aby zaszyfrować początkowy klucz DES

on będzie utrzymywał znaczną ilość obliczeń bez zmniejszania bezpieczeństwa jako całości. Jeśli stosuje się "łańcuchowanie", algorytm RSA musiałby być użyty tylko raz, aby zaszyfrować początkowy klucz DES.

Zbawienna notatka

Z punktu widzenia "brutalnej siły" proste szyfry zastępcze, w przypadku których istnieje ponad 1026 możliwości do rozważenia, powinny być trudniejsze do rozwiązania niż komunikaty zaszyfrowane DES, gdzie liczba możliwości jest mniejsza niż 1017. To jeszcze raz ilustruje, jak wprowadzające w błąd ". argumenty brutalnej siły mogą być.

Poza DES

Pierwotny DES otrzymał oficjalne zezwolenie rządu Stanów Zjednoczonych na około 10 lat. Po tym czasie potrójny DES, jak opisano powyżej, nadal był zatwierdzany, ale dodatkowo poszukiwano nowych algorytmów szyfrowania. W 1993 r. Algorytm o nazwie Skipjack został autoryzowany i zaimplementowany na chipie znanym jako Clipper. Szczegóły algorytmu Skipjack były początkowo utrzymywane w tajemnicy, ale zostały odtajnione 24 czerwca 1998 r. "Nieoficjalny" system szyfrowania (tj. Taki, który został opracowany przez osoby prywatne), który przyciągnął wielu użytkowników, to PGP, co jest skrótem od "Pretty Good Privacy". ". PGP został opracowany przez Philipa Zimmermanna i jest swobodnie dostępny dla każdego, kto chce. Obejmuje następujące kroki:

(1) "losowy" klucz jest generowany w oparciu o ruchy użytkownika myszy i naciśnięcia klawiszy; jest to nazywane kluczem sesji;

(2) tekst jawny wiadomości jest skompresowany; stopień kompresji zależy od charakteru i długości tekstu; typowy tekst w języku angielskim może być skompresowany o 50% bez wprowadzania niejasności, ale w przypadku krótkich tekstów oszczędność w czasie transmisji może nie być opłacalna;

(3) klucz wygenerowany w (1) służy do zaszyfrowania skompresowanego tekstu wytworzonego w (2) za pomocą algorytmu o nazwie IDEA ("Międzynarodowy algorytm szyfrowania danych") wynalezionego przez Lai i Massey w ETH w Zurychu;

(4) klucz sesji jest teraz zaszyfrowany przy użyciu klucza publicznego odbiorcy;

(5) zaszyfrowany klucz sesji znajduje się z przodu zaszyfrowanego tekstu, a całość jest wysyłana do odbiorcy;

(6) po otrzymaniu zaszyfrowanego tekstu odbiorca najpierw używa swojego klucza prywatnego do odszyfrowania klucza sesji na początku tekstu;

(7) tym odszyfrowanym kluczem może odszyfrować tekst wiadomości i rozpakować jeśli to konieczne.

Podobnie jak w przypadku RSA, a następnie wspomnianego wcześniej DES, użycie dwóch systemów szyfrowania w PGP nie tylko zwiększa bezpieczeństwo, ale także znacznie zwiększa szybkość, ponieważ czas potrzebny do zaszyfrowania lub odszyfrowania za pomocą systemu, w którym klucze szyfrowania / odszyfrowywania są w zasadzie to znacznie mniej niż czas wymagany do zaszyfrowania / odszyfrowania w systemie klucza publicznego, takiego jak RSA, gdzie klucze są całkowicie różne. W PGP tylko względnie krótki klucz sesji jest szyfrowany przez system klucza publicznego; sam tekst jest szyfrowany przez system kluczy niepublicznych (IDEA). PGP i powiązane tematy doprowadziły do tysięcy artykułów, które można znaleźć w Internecie. Każdy, kto chce więcej szczegółów, powinien się skonsultować. Algorytmy szyfrowania do użytku publicznego były przedmiotem wielu badań i należy się spodziewać, że będzie to trwało.

Uwierzytelnianie i weryfikacja podpisu

Jak wspomniano wcześniej, problemy te można rozwiązać za pomocą systemów klucza publicznego. DES nie jest takim systemem, ale metoda RSA jest. Przypomnijmy, że w systemie klucza publicznego każdy użytkownik ma publiczny klucz (szyfrowania), E i klucz tajny (odszyfrowanie) D. Załóżmy, że X chce wysłać wiadomość, M, do Y i tego

E_X, D_X, E_Y i D_Y

są kluczami do szyfrowania i odszyfrowywania odpowiednio X i Y.

Jak można:

(1) Y upewnij się, że wiadomość została wysłana przez X?

(2) X upewnić się, że Y nie może twierdzić, że otrzymał inny komunikat, M', powiedzmy?

(3) Y upewnić się, że X nie może twierdzić, że wysłał inną wiadomość, M'' , powiedzmy?

Istnieje kilka sposobów rozwiązania tych problemów, wszystkie z nich wymagają użycia niektórych lub wszystkich kluczy szyfrowania i rozszyfrowania. Typowe rozwiązanie to:

(1) X poprzedza informację Mwith, która zawiera datę i godzinę, a także jego tożsamość, a zatem Mis przedłużony do dłuższego komunikatu M1, na przykład, który jest podobny do

M1: "Jestem X, data 13-06-2001, a godzina 1827. M 'gdzie Mis oryginalna wiadomość.

(2) X odszyfrowuje M1, używając swojego klucza prywatnego, DX, tworząc komunikat szyfrowy DX (M1), który wysyła do Y.

(3) Y stosuje publiczny klucz szyfrowania X, EX, do tego komunikatu szyfrowego, a więc odzyskuje rozszerzoną wiadomość, M1, ponieważ

$E_X(D_X(M1)) = M1$.

Teraz:

(1) Y może być pewien, że X wysłał M1, ponieważ tylko X może wytworzyć DX (M1).

(2) Jeśli Y twierdzi, że otrzymał inną wiadomość, M ?, X rzuca wyzwanie Y, aby wytworzyć tekst szyfrowania DX (M?). Y nie będzie w stanie tego zrobić, ponieważ nie zna tajnego klucza X, DX.

(3) Jeśli X twierdzi, że wysłał inną wiadomość, M'', do Y, ta ostatnia może pokazać wiadomość szyfrowania, D_X (M1), sędziemu, który poprosi X o swój tajny klucz, aby mógł sprawdzić, czy wiadomość M1 został wysłany. Ponieważ Y nie zna sekretnego klucza X, nie mógł skonstruować D_X (M1). Jeśli X odmówi podania tajnego klucza sędziemu, straci swoją sprawę.

Ważne jest, aby rozszerzona wiadomość M1 zawierała datę i godzinę, w przeciwnym razie stary M może być zastąpiony przez M1, co unieważnia punkt podany w punkcie (2) powyżej.

Kryptografia krzywych eliptycznych

W ostatnich latach interesująca metoda weryfikacji podpisów spotkała się z dużym zainteresowaniem zarówno na uniwersytetach, jak iw przemyśle. Metoda, znana jako kryptografia krzywej eliptycznej (w skrócie ECC) po głębszych matematycznych pomysłach niż algorytm RSA i jest uważany za bardziej bezpieczny. Matematyka stojąca za tą metodą jest zbyt zaawansowana, aby ją tu opisać