Odpowiedzi na CZĘSTO ZADAWANE PYTANIA O kryptografii

1 Ogólne

1.1 Co to jest szyfrowanie?

Szyfrowanie polega na przekształceniu danych w postać niemożliwą do odczytania przez nikogo bez tajnego klucza odszyfrowywania. Jego celem jest zapewnienie prywatności poprzez ukrywanie informacji przed kimkolwiek, dla kogo nie jest przeznaczona, nawet tymi, którzy mogą zobaczyć zaszyfrowane dane. Na przykład można chcieć zaszyfrować pliki na dysku twardym, aby uniemożliwić intruzowi ich odczytanie. W ustawieniu dla wielu użytkowników szyfrowanie umożliwia bezpieczną komunikację przez niezabezpieczony kanał. Ogólny scenariusz jest następujący: Alicja chce wysłać wiadomość do Boba, aby nikt poza Bobem nie mógł jej przeczytać. Alicja szyfruje wiadomość, która nazywa się tekstem jawnym, za pomocą klucza szyfrowania; zaszyfrowana wiadomość, nazywana szyfrogramem, zostaje wysłana do Boba. Bob odszyfrowuje szyfrogram z kluczem odszyfrowującym i odczytuje komunikat. Atakujący, Charlie, może spróbować uzyskać tajny klucz lub odzyskać tekst jawny bez użycia tajnego klucza. W bezpiecznym kryptosystemie tekst jawny nie może zostać odzyskany z zaszyfrowanego tekstu za wyjątkiem użycia klucza deszyfrującego. W symetrycznym kryptosystemie pojedynczy klucz służy zarówno jako klucze szyfrowania i odszyfrowywania.

1.2 Co to jest uwierzytelnianie? Co to jest podpis cyfrowy?

Uwierzytelnianie w ustawieniu cyfrowym jest procesem, w którym odbiorca wiadomości cyfrowej może mieć pewność co do tożsamości nadawcy i / lub integralności wiadomości. Protokoły uwierzytelniania mogą opierać się na konwencjonalnych kryptosystemach tajnego klucza, takich jak DES lub na systemach klucza publicznego, takich jak RSA; uwierzytelnianie w systemach klucza publicznego wykorzystuje podpis cyfrowy. W tym dokumencie uwierzytelnienie będzie ogólnie dotyczyć używania podpisów cyfrowych, które pełnią funkcję dla dokumentów cyfrowych podobnych do tych, które odtwarzane są odręcznymi podpisami do wydrukowanych dokumentów: podpis jest niewiarygodnym zbiorem danych potwierdzającym, że wskazana osoba napisała lub w inny sposób uzgodniła do dokumentu, do którego dołączony jest podpis. Odbiorca, jak również osoba trzecia, może zweryfikować, czy dokument rzeczywiście pochodzi od osoby, której podpis jest dołączony, i że dokument nie został zmieniony od czasu podpisania. Bezpieczny system cyfrowego podpisu składa się zatem z dwóch części: sposobu podpisania dokumentu, który uniemożliwia fałszowanie, oraz metody sprawdzania, czy podpis został rzeczywiście wygenerowany przez tego, kogo reprezentuje. Ponadto nie można odmówić bezpiecznego podpisu cyfrowego; tj. osoba podpisująca dokument nie może później go odrzucić, twierdząc, że została sfałszowana. W przeciwieństwie do szyfrowania podpisy cyfrowe są najnowszym rozwiązaniem, którego potrzeby pojawiły się wraz z rozprzestrzenianiem się komunikacji cyfrowej.

1.3 Czym jest kryptografia klucza publicznego?

Tradycyjna kryptografia opiera się na nadawcy i odbiorcy wiadomości znającej i używającej tego samego tajnego klucza: nadawca używa tajnego klucza do zaszyfrowania wiadomości, a odbiorca używa tego samego tajnego klucza do odszyfrowania wiadomości. Ta metoda znana jest jako kryptografia z kluczem tajnym. Główny problem polega na tym, aby nadawca i odbiorca uzgodnili tajny klucz, aby nikt nie dowiedział się o tym. Jeśli znajdują się w oddzielnych fizycznych lokalizacjach, muszą zaufać kurierowi, systemowi telefonicznemu lub innemu systemowi transmisji, aby nie ujawnić tajnego klucza, który jest przekazywany. Każdy, kto podsłucha lub przechwyci klucz tranzytowy, może później odczytać wszystkie wiadomości zaszyfrowane za pomocą tego klucza. Generowanie, przesyłanie i przechowywanie kluczy nazywa się zarządzaniem kluczowym; wszystkie kryptosystemy muszą radzić

sobie z kluczowymi problemami z zarządzaniem. Kryptografia tajnego klucza często ma trudności z zapewnieniem bezpiecznego zarządzania kluczami. Kryptografia klucza publicznego została wymyślona w 1976 roku przez Whitfielda Diffiego i Martina Hellmana w celu rozwiązania kluczowego problemu zarządzania. W nowym systemie każda osoba otrzymuje parę kluczy, zwanych kluczem publicznym i kluczem prywatnym. Klucz publiczny każdej osoby jest publikowany, a klucz prywatny jest trzymany w tajemnicy. Zapotrzebowanie nadawców i odbiorców na dzielenie się tajnymi informacjami jest wyeliminowane: cała komunikacja obejmuje tylko klucze publiczne, a żaden klucz prywatny nie jest nigdy przesyłany ani udostępniany. Nie trzeba już ufać, że jakiś kanał komunikacyjny jest zabezpieczony przed podsłuchem lub zdradą. Każdy może wysyłać poufne wiadomości tylko za pomocą informacji publicznej, ale może być odszyfrowany tylko za pomocą klucza prywatnego, który jest w wyłącznym posiadaniu zamierzonego odbiorcy. Ponadto kryptografia z kluczem publicznym może być używana do uwierzytelniania (podpisów cyfrowych), a także do prywatności (szyfrowania). Oto jak działa szyfrowanie: kiedy Alicja chce wysłać wiadomość do Boba, wyszukuje klucz publiczny Boba w katalogu, używa go do szyfrowania wiadomości i jej wysyłania. Następnie Bob używa swojego klucza prywatnego do odszyfrowania wiadomości i przeczytania jej. Nikt nie może odszyfrować wiadomości. Każdy może wysłać zaszyfrowaną wiadomość do Boba, ale tylko Bob może ją przeczytać. Najwyraźniej jednym z wymagań jest to, że nikt nie może znaleźć klucza prywatnego z odpowiedniego klucza publicznego. Oto jak działa uwierzytelnianie: Alice, aby podpisać wiadomość, wykonuje obliczenia dotyczące zarówno jej klucza prywatnego, jak i samej wiadomości; wynik jest nazywany podpisem cyfrowym i jest dołączany do wiadomości, która jest następnie wysyłana. Bob, aby zweryfikować podpis, wykonuje pewne obliczenia dotyczące wiadomości, rzekomego podpisu i klucza publicznego Alicji. Jeśli wyniki prawidłowo utrzymują się w prostej relacji matematycznej, podpis jest weryfikowany jako prawdziwy; w przeciwnym razie podpis może być fałszywy lub wiadomość zostanie zmieniona i zostaną one odrzucone.

1.4 Jakie są zalety i wady kryptografii z kluczem publicznym w stosunku do kryptografii z kluczem tajnym?

Podstawową zaletą kryptografii z kluczem publicznym jest zwiększone bezpieczeństwo: klucze prywatne nie muszą być nigdy przekazywane ani ujawniane nikomu. Natomiast w systemie tajnego klucza zawsze istnieje szansa, że wróg może odkryć tajny klucz podczas jego przesyłania. Inną ważną zaletą systemów klucza publicznego jest to, że mogą zapewnić metodę podpisów cyfrowych. Uwierzytelnianie za pomocą tajnego klucza wymaga dzielenia się tajemnicą, a czasem wymaga zaufania również strony trzeciej. Nadawca może następnie odrzucić poprzednio podpisaną wiadomość, twierdząc, że wspólna tajemnica została w jakiś sposób naruszona przez jedną ze stron udostępniających sekret. Na przykład system uwierzytelniania klucza tajnego Kerberos [79] obejmuje centralną bazę danych, która przechowuje kopie tajnych kluczy wszystkich użytkowników; wiadomość uwierzytelniona za pomocą protokołu Kerberos najprawdopodobniej nie byłaby prawnie wiążąca, ponieważ atak na bazę danych pozwoliłby na powszechne fałszowanie. Uwierzytelnianie za pomocą klucza publicznego zapobiega temu rodzajowi odrzucania; każdy użytkownik ponosi wyłączną odpowiedzialność za ochronę swojego klucza prywatnego. Ta właściwość uwierzytelniania za pomocą klucza publicznego jest często nazywana niezaprzeczalnością. Ponadto podpisane cyfrowo wiadomości mogą być udowodnione autentycznie osobom trzecim, takim jak sędzia, dzięki czemu takie wiadomości są prawnie wiążące. Systemy uwierzytelniania za pomocą klucza tajnego, takie jak Kerberos, zostały zaprojektowane do uwierzytelniania dostępu do zasobów sieciowych, a nie do uwierzytelniania dokumentów, co lepiej jest osiągnąć za pomocą podpisów cyfrowych. Wadą stosowania szyfrowania z kluczem publicznym do szyfrowania jest szybkość: istnieją popularne metody szyfrowania tajnymi kluczami, które są znacznie szybsze niż jakakolwiek dostępna obecnie metoda szyfrowania kluczem publicznym. Ale kryptografia klucza publicznego może dzielić ciężar kryptografii z kluczem tajnym, aby

uzyskać najlepsze z obu światów. W przypadku szyfrowania najlepszym rozwiązaniem jest połączenie systemów klucza publicznego i klucza tajnego, aby uzyskać zarówno zalety związane z bezpieczeństwem systemów klucza publicznego, jak i zalety szybkości systemów sekretnych kluczy. System klucza publicznego może być używany do szyfrowania tajnego klucza, który jest następnie używany do szyfrowania większości pliku lub wiadomości. Zostało to wyjaśnione bardziej szczegółowo w pytaniu 2.12 w przypadku RSA. Kryptografia klucza publicznego nie ma zastąpić kryptografii z kluczem tajnym, ale raczej ją uzupełnić, aby była bezpieczniejsza. Pierwsze zastosowanie technik klucza publicznego dotyczyło bezpiecznej wymiany kluczy w systemie z innym kluczem tajnym [29]; to nadal jest jedna z jego podstawowych funkcji. Kryptografia tajnego klucza pozostaje niezwykle ważna i jest przedmiotem wielu trwających badań i badań.

1.5 Czy kryptografia jest patentowa w USA?

Systemy kryptograficzne są patentowalne. Wiele tajnych kluczy kryptosystemów zostało opatentowanych, w tym DES. Podstawowe idee kryptografii o kluczu publicznym zawarte są w patencie US 4,200,770 przez M. Hellmana, W. Diffiego i R. Merkle'a wydanym 4/29/80 oraz w patencie USA 4,218,582 przez M. Hellmana i R. Merkle'a, wydany 8/19/80; podobne patenty zostały wydane na całym świecie. Wyłączne prawa licencyjne do obu patentów należą do Public Key Partners (PKP) z Sunnyvale w Kalifornii, który posiada również prawa do patentu RSA. Zwykle wszystkie patenty w kluczu publicznym są licencjonowane razem. Wszelkie prawne wyzwania związane z patentami pod kluczem publicznym zostały rozstrzygnięte przed wydaniem wyroku. W niedawnym przypadku, na przykład, PKP wniosła pozew przeciwko korporacji TRW, która używała kryptografii z kluczem publicznym (system ElGamal) bez licencji; TRW twierdziło, że nie potrzebuje licencji. W czerwcu 1992 r. Osiągnięto porozumienie, w którym TRW zgodziło się na licencję na patenty. Niektóre zgłoszenia patentowe dotyczące kryptosystemów zostały zablokowane przez interwencję NSA lub innych agencji wywiadowczych lub obronnych, pod nadzorem Ustawy o tajemnicy wynalazczości z 1940 r. I Ustawy o bezpieczeństwie narodowym z 1947 r .; patrz Landau dla niektórych ostatnich przypadków związanych z kryptografią.

1.6 Czy kryptografia może być eksportowana z USA?

Wszystkie produkty kryptograficzne wymagają licencji na wywóz od Departamentu Stanu, działającego pod nadzorem Międzynarodowego Regulaminu Zarządzania Bronią (ITAR), który definiuje urządzenia kryptograficzne, w tym oprogramowanie, jako amunicję. Rząd USA od dawna niechętnie udzielał licencji na wywóz produktów szyfrowania silniejszych niż niektóre podstawowe poziomy (nie podawano publicznie). Zgodnie z obowiązującymi przepisami sprzedawca, który chce wyeksportować produkt za pomocą kryptografii, najpierw składa wniosek do biura Departamentu Obrony Departamentu Stanu w Departamencie Stanu. Jurysdykcja eksportowa może następnie zostać przekazana do Departamentu Handlu, którego procedury wywozu są generalnie proste i skuteczne. Jeśli jurysdykcja pozostaje w Departamencie Stanu, konieczna jest dalsza ocena, być może długotrwała, zanim eksport zostanie zatwierdzony lub odrzucony; Agencja Bezpieczeństwa Narodowego (NSA, zob. pytanie 7.3) może zostać bezpośrednio zaangażowana w tym momencie. Szczegóły procesu zatwierdzania eksportu zmieniają się często. NSA ma de facto kontrolę nad eksportem produktów kryptograficznych. Departament Stanu nie udzieli licencji bez zgody NSA i rutynowo udziela licencji, gdy NSA go zatwierdzi. Dlatego decyzje strategiczne dotyczące eksportu kryptografii ostatecznie spoczywają na NSA. Zgodnie z przyjętą polityką NSA nie ogranicza eksportu kryptografii do uwierzytelniania; dotyczy tylko użycia kryptografii dla prywatności. Sprzedawca, który chce wyeksportować produkt wyłącznie w celu uwierzytelnienia, otrzyma pozwolenie na wywóz, o ile może wykazać, że produktu nie można łatwo zmodyfikować w celu zaszyfrowania; Dotyczy to nawet bardzo mocnych systemów, takich jak RSA o dużych rozmiarach kluczy. Ponadto procedury biurokratyczne są

prostsze w przypadku produktów uwierzytelniających niż w przypadku produktów związanych z prywatnością. Produkt uwierzytelniający wymaga zatwierdzenia NSA i Departamentu Stanu tylko raz, podczas gdy produkt szyfrujący może wymagać zatwierdzenia dla każdej sprzedaży lub każdej wersji produktu. Polityka eksportowa jest obecnie przedmiotem wielu kontrowersji, ponieważ wielu dostawców oprogramowania i sprzętu uważa obowiązujące przepisy eksportowe za zbyt restrykcyjne i uciążliwe. Stowarzyszenie Software Publishers (SPA), grupa branży oprogramowania, negocjowała ostatnio z rządem w celu złagodzenia ograniczeń w zakresie eksportu; osiągnięto porozumienie, które pozwala na uproszczenie procedur eksportu dwóch szyfrów szyfrujących, RC2 i RC4 (patrz pytanie 8.6), gdy wielkość klucza jest ograniczona. Ponadto polityka eksportowa jest mniej restrykcyjna dla zagranicznych spółek zależnych i zagranicznych biur spółek amerykańskich. W marcu 1992 r. Rada Doradcza ds. Bezpieczeństwa Komputerów i Ochrony Prywatności głosowała jednogłośnie, zalecając krajowy przegląd polityki kryptograficznej, w tym polityki eksportowej. Rada jest oficjalną radą doradczą NIST (patrz pytanie 7.1), której członkowie pochodzą zarówno z sektora publicznego, jak i prywatnego. Rada stwierdziła, że debata publiczna jest jedyną drogą do osiągnięcia polityki konsensusu w celu jak najlepszego zaspokojenia konkurencyjnych interesów: bezpieczeństwa narodowego i organów ścigania, takich jak ograniczenia dotyczące kryptografii, szczególnie w odniesieniu do eksportu, podczas gdy inne agencje rządowe i przemysł prywatny chcą większej swobody korzystania i eksportowanie kryptografii. Polityka eksportowa tradycyjnie była podejmowana wyłącznie przez agencje zajmujące się bezpieczeństwem narodowym, bez dużego wkładu ze strony tych, którzy chcą wspierać handel w kryptografii. Polityka eksportowa USA może ulec znaczącym zmianom w ciągu najbliższych kilku lat.

RSA

2.1 Czym jest RSA?

RSA to kryptosystem klucza publicznego do szyfrowania i uwierzytelniania; został wynaleziony w 1977 roku przez Rona Rivesta, Adi Shamira i Leonarda Adlemana. Działa on w następujący sposób: weź dwie duże liczby pierwsze, p i q, i znajdź ich produkt n = pq; n nazywa się modułem. Wybierz liczbę, e, mniej niż n i względnie pierwszą (p-1) (q-1), i znajdź jej odwrotność, d, mod (p-1) (q-1), co oznacza, że ed = 1 mod (p-1) (q-1); eid są nazywane odpowiednio wykładnikami publicznymi i prywatnymi. Klucz publiczny to para (n, e); klucz prywatny to d. Czynniki p i q muszą być utrzymywane w tajemnicy lub zniszczone. Trudno (prawdopodobnie) uzyskać klucz prywatny d z klucza publicznego (n, e). Jeśli jednak można było wpisać n na p i q, to można uzyskać klucz prywatny d. Tak więc całe bezpieczeństwo RSA opiera się na założeniu, że faktoring jest trudny; Łatwa metoda faktorowania spowodowałaby "złamanie" RSA. Oto, w jaki sposób RSA może być używany do prywatności i uwierzytelniania (w praktyce rzeczywiste użycie jest nieco inne, zobacz Pytania 2.12 i 2.13): prywatność RSA (szyfrowanie): załóżmy, że Alicja chce wysłać prywatną wiadomość, m, do Boba. Alice tworzy zaszyfrowany tekst c, potęgując: c = m ^ e mod n, gdzie e i n są kluczem publicznym Boba. Aby odszyfrować, Bob również potęguje: m = c ^ d mod n, i odzyskuje oryginalną wiadomość m; relacja między e a d zapewnia, że Bob poprawnie odzyskuje m. Ponieważ tylko Bob zna d, tylko Bob może odszyfrować. Uwierzytelnianie RSA: załóżmy, że Alicja chce wysłać podpisany dokument m do Boba. Alice tworzy cyfrową sygnaturę s, potęgując: s = m ^ d mod n, gdzie d i n należą do pary kluczy Alice. Wysyła s i m do Boba. Aby zweryfikować podpis, Bob potęguje i sprawdza, czy wiadomość m została odzyskana: m = s ^ e mod n, gdzie e i n należą do klucza publicznego Alicji. Szyfrowanie i uwierzytelnianie odbywa się zatem bez udostępniania kluczy prywatnych: każda osoba używa tylko kluczy publicznych innych osób i swojego prywatnego klucza. Każdy może wysłać zaszyfrowaną wiadomość lub zweryfikować podpisaną wiadomość, używając tylko kluczy publicznych, ale tylko osoba posiadająca poprawny klucz prywatny może odszyfrować lub podpisać wiadomość.

2.2 Dlaczego warto używać RSA zamiast DES?

RSA nie jest alternatywą ani zamiennikiem DES; jest raczej uzupełnieniem DES (lub dowolnego innego szybkiego szyfrowania szyfrującego) i jest używany razem z DES w bezpiecznym środowisku komunikacyjnym. RSA umożliwia dwie ważne funkcje, których nie zapewnia DES: bezpieczną wymianę kluczy bez wcześniejszej wymiany tajnych kluczy i podpisów cyfrowych. W przypadku szyfrowania wiadomości, RSA i DES są zwykle łączone w następujący sposób: najpierw wiadomość jest szyfrowana losowym kluczem DES, a następnie, przed wysłaniem przez niezabezpieczony kanał komunikacji, klucz DES jest szyfrowany za pomocą RSA. Razem wysyłana jest wiadomość zaszyfrowana DES i szyfrowany klucz RSA RSA. Ten protokół jest znany jako koperta cyfrowa RSA. Można się zastanawiać, dlaczego po prostu nie użyć RSA do zaszyfrowania całej wiadomości i nie używać DES w ogóle? Chociaż może to być dobre dla małych wiadomości, DES (lub inny szyfr) jest preferowany dla większych wiadomości, ponieważ jest znacznie szybszy niż RSA. W niektórych sytuacjach RSA nie jest konieczne, a sam DES wystarcza. Obejmuje to środowiska wielu użytkowników, w których może odbywać się bezpieczna umowa DES, na przykład przez obie strony, które spotykają się prywatnie. Ponadto, RSA zwykle nie jest konieczne w środowisku pojedynczego użytkownika; na przykład, jeśli chcesz zachować zaszyfrowane pliki osobiste, zrób to, używając DES, powiedzmy, osobistego hasła jako klucza DES. RSA i ogólnie kryptografia z kluczem publicznym najlepiej nadaje się do środowiska wielu użytkowników. Również każdy system, w którym pożądane są podpisy cyfrowe, wymaga RSA lub innego systemu klucza publicznego.

2.3 Jak szybki jest RSA?

Operacja RSA, niezależnie od tego, czy jest to szyfrowanie, czy odszyfrowywanie, podpisywanie lub weryfikacja, jest w istocie modularną potęgowaniem, którą można przeprowadzić za pomocą serii modularnych multiplikacji. W zastosowaniach praktycznych często wybiera się mały publiczny wykładnik klucza publicznego; w rzeczywistości całe grupy użytkowników mogą korzystać z tego samego publicznego wykładnika. Dzięki temu szyfrowanie jest szybsze niż odszyfrowywanie i weryfikacja szybciej niż podpisywanie. Algorytmicznie, operacje z kluczem publicznym przyjmują kroki O (k ^ 2), operacje na kluczach prywatnych przyjmują kroki O (k ^ 3), a generowanie kluczy zajmuje kroki O (k ^ 4), gdzie k jest liczbą bitów w module; Zapis "O" odnosi się do górnej granicy asymptotycznego czasu działania algorytmu. Istnieje wiele dostępnych na rynku implementacji sprzętu RSA i często pojawiają się ogłoszenia o nowszych i szybszych układach. Najszybszy obecnie układ RSA [76] ma przepustowość większą niż 600 kilobitów na sekundę przy 512-bitowym module, co oznacza, że wykonuje ponad 1000 operacji klucza prywatnego RSA na sekundę. Oczekuje się, że prędkości RSA osiągną 1 Mbit / sekundę w ciągu roku. Dla porównania DES jest znacznie szybszy niż RSA. W oprogramowaniu DES jest na ogół co najmniej 100 razy szybszy niż RSA. W sprzęcie DES jest od 1000 do 10 000 razy szybszy, w zależności od implementacji. RSA prawdopodobnie nieco zmniejszy lukę w nadchodzących latach, ponieważ znajdzie rosnące rynki komercyjne, ale nigdy nie będzie pasować do wydajności DES.

2.4 Ile dodatkowej długości wiadomości wynika z używania RSA?

W przypadku korzystania z RSA wykorzystywana jest tylko bardzo mała ilość danych. W przypadku szyfrowania wiadomość może zostać dopełniona do długości, która jest wielokrotnością długości bloku, zwykle 64-bitową, ponieważ RSA jest zwykle łączony z szyfrem bloków tajnego klucza, takim jak DES. Szyfrowanie klucza DES zajmuje tyle dodatkowych bitów, co rozmiar modułu RSA. W celu uwierzytelnienia podpis cyfrowy RSA jest dołączany do dokumentu. Sygnatura RSA, w tym informacje takie jak nazwa osoby podpisującej, ma zazwyczaj kilkaset bajtów długości. Można również dołączyć

jeden lub więcej certyfikatów; certyfikaty mogą być używane w połączeniu z dowolną metodą podpisu cyfrowego. Typowy certyfikat RSA ma kilkaset bajtów długości.

2.5 Co by było, aby złamać RSA?

Istnieje kilka możliwych interpretacji "łamania RSA". Najbardziej szkodliwe byłoby dla atakującego odkrycie klucza prywatnego odpowiadającego danemu kluczowi publicznemu; to umożliwi atakującemu zarówno odczytanie wszystkich wiadomości zaszyfrowanych za pomocą klucza publicznego, jak i fałszowanie podpisów. Oczywistym sposobem na wykonanie tego ataku jest uwzględnienie modułu społecznego, n, w jego dwóch głównych czynnikach, p i q. Z p, q i e, publicznego wykładnika, atakujący może łatwo uzyskać d, prywatny klucz. Najtrudniejszą częścią jest faktoring n; bezpieczeństwo RSA zależy od faktu, że faktoring jest trudny. W rzeczywistości zadanie odzyskania klucza prywatnego jest równoważne z zadaniem faktorowania modułu: można użyć d do współczynnika n, a także użyć faktoryzacji n, aby znaleźć d. Zobacz pytania 4.5 i 4.6 dotyczące aktualnego stanu faktoringu. Należy zauważyć, że same udoskonalenia sprzętowe nie osłabi RSA, o ile stosowane będą odpowiednie długości kluczy; w rzeczywistości ulepszenia sprzętowe powinny zwiększyć bezpieczeństwo RSA. Innym sposobem na złamanie RSA jest znalezienie techniki obliczania e-tego modelu korzenia. Ponieważ c = m ^ e, e-ty katalog główny c jest komunikatem m. Ten atak pozwoliłby komuś odzyskać zaszyfrowane wiadomości i fałszować podpisy nawet bez znajomości klucza prywatnego. Ten atak nie jest uznawany za równoważny faktoringowi. Obecnie nie są znane żadne metody, które próbowałyby złamać RSA w ten sposób. Wymienione ataki są jedynymi sposobami na złamanie RSA w taki sposób, aby móc odzyskać wszystkie wiadomości zaszyfrowane pod danym kluczem. Istnieją jednak inne metody, które mają na celu odzyskiwanie pojedynczych wiadomości; sukces nie umożliwi atakującemu odzyskania innych wiadomości zaszyfrowanych za pomocą tego samego klucza. Najprostszym pojedynczym atakiem jest odgadnięty atak tekstowy. Osoba atakująca widzi szyfrogram, domyśla się, że wiadomość może być "Atak o świcie" i zakodowuje to przypuszczenie za pomocą klucza publicznego odbiorcy; w porównaniu z faktycznym zaszyfrowanym tekstem, atakujący wie, czy domysły były poprawne. Ten atak można powstrzymać, dołączając do niego losowe bity. Kolejny atak pojedynczej wiadomości może wystąpić, jeśli ktoś wyśle tę samą wiadomość m do trzech innych, z których każdy ma publiczny wykładnik e = 3. Osoba atakująca, która to wie i widzi te trzy wiadomości, będzie mogła odzyskać wiadomość m; ten atak i sposoby zapobiegania temu są dyskutowane przez Hastada. Istnieje również kilka "wybranych ataków zaszyfrowanych", w których atakujący tworzy jakiś zaszyfrowany tekst i dostrzega odpowiedni tekst jawny, być może podszywając legalnego użytkownika do odszyfrowania fałszywej wiadomości ; David podaje kilka przykładów. Oczywiście są też ataki, których celem nie jest sama RSA, ale pewna niepewna implementacja RSA; nie są one uważane za "łamiące RSA", ponieważ nie jest wykorzystywana żadna słabość algorytmu RSA, ale raczej słabość w konkretnej implementacji. Na przykład, jeśli ktoś przechowuje niepoprawnie swój klucz prywatny, osoba atakująca może je wykryć. Nie można podkreślić wystarczająco mocno, że aby być naprawdę bezpiecznym, RSA wymaga bezpiecznej implementacji; matematyczne zabezpieczenia, takie jak wybór długiego klucza, nie wystarczą. W praktyce, najbardziej skuteczne ataki będą prawdopodobnie kierowane na niezabezpieczone wdrożenia i na kluczowych etapach zarządzania systemem RSA.

2.6 Czy RSA wymaga silnych liczb pierwszych?

W literaturze dotyczącej RSA często sugerowano, że przy wyborze pary kluczy należy używać "silnych" liczb pierwszych p i q, aby wygenerować moduł n. Silne liczby pierwsze to te o określonych właściwościach, które sprawiają, że produkt jest trudny do uwzględnienia w konkretnych metodach faktoringowych; takie właściwości obejmują, na przykład, istnienie dużego czynnika pierwotnego p-1 i dużego czynnika pierwotnego p + 1. Powodem tych obaw jest to, że niektóre metody faktoringowe są

szczególnie odpowiednie dla liczb pierwszych tak, że p-1 lub p + 1 ma tylko małe czynniki; silne liczby pierwsze są odporne na te ataki. Jednak ostatnie postępy w faktoringu (patrz pytanie 4.6) wydają się eliminować przewagę silnych liczb pierwszych; Algorytm faktorowania krzywych eliptycznych jest jednym z takich postępów. Nowe metody faktoringowe mają równie dużą szansę na sukces na silnych liczbach pierwszych, jak i na "słabych" liczbach pierwszych; dlatego wybór silnych liczb pierwszych nie zwiększa znacząco odporności na ataki. Tak więc na razie odpowiedź jest negatywna: silne liczby pierwsze nie są konieczne przy używaniu RSA, chociaż nie ma niebezpieczeństwa w ich używaniu, z wyjątkiem tego, że generowanie pary kluczy zajmuje więcej czasu. Jednak w przyszłości mogą zostać opracowane nowe algorytmy faktoringu, które po raz kolejny będą ukierunkowane na liczby pierwsze o pewnych właściwościach; jeśli tak, wybór silniejszych liczb pierwszych może ponownie przyczynić się do zwiększenia bezpieczeństwa.

2.7 Jak duży moduł (klucz) powinien zostać użyty w RSA?

Najlepszy rozmiar dla modułu RSA zależy od potrzeb bezpieczeństwa. Im większy moduł, tym większe bezpieczeństwo, ale także wolniejsze operacje RSA. Należy wybrać długość modułu po rozważeniu, po pierwsze, czyich potrzeb bezpieczeństwa, takich jak wartość chronionych danych i jak długo musi być chroniona, a po drugie, jak potężny jest potencjalny wróg. Możliwe jest również, że większy rozmiar klucza pozwoli dokumentowi podpisanemu cyfrowo być ważny przez dłuższy czas; Dobra analiza bezpieczeństwa uzyskanego przez daną długość modułu jest podana przez Rivest, w kontekście dyskretnych logarytmów modulo a prime, ale dotyczy również RSA. Według szacunków Rivesta 512-bitowy moduł może być warty 8,2 miliona dolarów, mniej w przyszłości. Dlatego może być wskazane użycie dłuższego modułu, może o długości 768 bitów. Osoby posiadające niezwykle cenne dane (lub duże potencjalne uszkodzenia spowodowane fałszowaniem cyfrowym) mogą chcieć użyć jeszcze dłuższego modułu. Instytucja certyfikująca może użyć modułu o długości 1000 bitów lub więcej, ponieważ ważność tak wielu innych par kluczy zależy od bezpieczeństwa jednego klucza centralnego. Klucz indywidualnego użytkownika wygaśnie po upływie pewnego czasu, powiedzmy, dwa lata. Po wygaśnięciu użytkownik wygeneruje nowy klucz, który powinien być o co najmniej kilka cyfr dłuższy niż stary klucz, aby odzwierciedlić wzrosty prędkości komputerów w ciągu dwa lata. Zalecane harmonogramy kluczy kluczowych prawdopodobnie zostaną opublikowane przez niektóre organy lub organy publiczne. Użytkownicy powinni pamiętać, że szacowane czasy na złamanie RSA są jedynie wartościami średnimi. Duży wysiłek faktoringowy, atakujący wiele tysięcy modułów RSA, może skutecznie rozliczyć co najmniej jeden w rozsądnym czasie. Mimo że bezpieczeństwo każdego klucza jest wciąż silne, niektóre metody faktoringowe zawsze mają niewielką szansę, że atakujący może mieć szczęście i szybko je zliczyć. Jeśli chodzi o spowolnienie spowodowane zwiększeniem rozmiaru klucza, podwojenie długości modułu podniosłoby średnio czas wymagany do operacji klucza publicznego (szyfrowanie i weryfikacja podpisu) o współczynnik 4 i zwiększyłoby czas potrzebny na operacje na kluczach prywatnych (odszyfrowywanie i podpisywanie) przez współczynnik 8. Powodem, że operacje klucza publicznego są dotknięte mniej niż operacje klucza prywatnego, jest to, że wykładnik publiczny może pozostać niezmienny, gdy moduł jest zwiększany, podczas gdy wykładnik prywatny rośnie proporcjonalnie. Czas generowania klucza zwiększyłby się 16 razy po podwojeniu modułu, ale jest to stosunkowo nieczęsta operacja dla większości użytkowników.

2.8 Jak duże powinny być liczby pierwsze?

Dwie liczby pierwsze, p i q, które składają się na moduł, powinny być mniej więcej jednakowej długości; to sprawi, że moduł będzie trudniejszy do zobrazowania, niż gdyby jeden z liczb pierwszych był bardzo mały. Zatem jeśli ktoś zdecyduje się na użycie modułu 512-bitowego, wartości początkowe powinny mieć długość około 256 bitów.

2.9 Jak znaleźć przypadkowe liczby dla kluczy?

Potrzebne jest źródło liczb losowych, aby znaleźć dwie losowe liczby pierwsze do skomponowania modułu. Jeśli użyje się przewidywalnej metody generowania liczb pierwszych, przeciwnik może przeprowadzić atak, próbując odtworzyć proces generowania klucza. Liczby losowe uzyskane z procesu fizycznego są z zasady najlepsze. Można użyć urządzenia sprzętowego, takiego jak dioda; niektóre są sprzedawane komercyjnie na komputerowych płytach rozszerzeń do tego celu. Innym pomysłem jest użycie fizycznych ruchów użytkownika komputera, takich jak czasy naciśnięcia klawisza mierzone w mikrosekundach. Niezależnie od metody, liczby losowe mogą nadal zawierać pewne korelacje zapobiegające wystarczającej statystycznej losowości. Dlatego najlepiej jest uruchomić je za pomocą dobrej funkcji mieszania, zanim faktycznie ich użyjesz. Innym podejściem jest użycie generatora liczb pseudolosowych zasilanych przez losowe nasiono. Ponieważ są to algorytmy deterministyczne, ważne jest znalezienie takiego, który jest bardzo nieprzewidywalny, a także użycie prawdziwie losowego materiału siewnego. Istnieje szeroka literatura na temat generatorów liczb pseudolosowych. Zauważ, że nie trzeba liczb losowych, aby określić publicznych i prywatnych wykładników w RSA, po wybraniu modułu. Można po prostu wybrać dowolną wartość dla publicznego wykładnika, który następnie określa prywatny wykładnik lub odwrotnie.

2.10 Co jeśli użytkownicy RSA zabraknie różnych liczb pierwszych?

Istnieje wystarczająco dużo liczb pierwszych, których użytkownicy RSA nigdy nie zabraknie. Na przykład liczba liczb pierwszych o długości 512 bitów lub mniejszych przekracza 10 ^ {150}, zgodnie z twierdzeniem liczby pierwszej; to więcej niż liczba atomów w znanym wszechświecie.

2.12 W jaki sposób RSA jest wykorzystywany do szyfrowania w praktyce?

RSA jest łączony z kryptosystemem tajnego klucza, takim jak DES, w celu zaszyfrowania wiadomości za pomocą cyfrowej koperty RSA. Załóżmy, że Alicja chce wysłać zaszyfrowaną wiadomość do Boba. Najpierw szyfruje komunikat za pomocą DES, używając losowo wybranego klucza DES. Następnie wyszukuje klucz publiczny Boba i używa go do szyfrowania klucza DES. Wiadomość zaszyfrowana DES i szyfrowany klucz RSA razem tworzą cyfrową kopertę RSA i są wysyłane do Boba. Po otrzymaniu koperty cyfrowej

2.13 W jaki sposób RSA służy do uwierzytelniania w praktyce?

Załóżmy, że Alicja chce wysłać podpisaną wiadomość. 2.11 Skąd wiadomo, że liczba jest pierwsza? Generalnie zaleca się stosowanie probabilistycznego testowania pierwszości, które jest o wiele szybsze niż udowodnienie liczby pierwszej. Można użyć testu probabilistycznego, który decyduje, czy liczba jest liczbą pierwszą z prawdopodobieństwem błędu mniejszym niż 2 ^ {- 100}. . Dla niektórych wyników empirycznych dotyczących rzetelności prostych testów pierwszościowych, można wykonać bardzo szybkie testy pierwotności i być bardzo pewnym wyników. Prosty algorytm wybierania prawdopodobnych liczb pierwszych został niedawno przeanalizowany przez Brandta i Damgarda.

2.14 Czy RSA pomaga wykrywać zmienione dokumenty i błędy transmisji?

Podpis cyfrowy RSA jest lepszy od podpisu odręcznego, ponieważ świadczy o treści wiadomości, a także tożsamości osoby podpisującej. Dopóki używana jest bezpieczna funkcja skrótu (patrz pytanie 8.2), nie ma sposobu na pobranie czyjegoś podpisu z jednego dokumentu i dołączenie go do innego lub modyfikację podpisanej wiadomości w jakikolwiek sposób. Najmniejsza zmiana w podpisanym dokumencie spowoduje niepowodzenie procesu weryfikacji podpisu cyfrowego. W ten sposób uwierzytelnianie RSA umożliwia ludziom sprawdzenie integralności podpisanych dokumentów.

Oczywiście, jeśli weryfikacja podpisu nie powiedzie się, może być niejasne, czy doszło do próby fałszerstwa, czy po prostu błędu transmisji.

2.15 Jakie są alternatywy dla RSA?

Zaproponowano wiele innych kryptosystemów z kluczem publicznym, co szybko ujawnia przebieg corocznych konferencji Crypto i Eurocrypt. Problem matematyczny, zwany problemem plecakowym, był podstawą wielu systemów, ale te straciły przychylność, ponieważ kilka wersji zostało zerwanych. Inny system, zaprojektowany przez ElGamal, oparty jest na dyskretnym logarytmie problemu. System ElGamal był po części podstawą wielu późniejszych metod podpisu, w tym jednej przez Schnorr, która z kolei była podstawą DSS, standardu podpisu cyfrowego zaproponowanego przez NIST. Ze względu na propozycję NIST wiele uwagi poświęcono względnym zaletom tych sygnatur w porównaniu z sygnaturami RSA; System ElGamal był z powodzeniem stosowany w aplikacjach; jest wolniejszy dla szyfrowania i weryfikacji niż RSA, a jego sygnatury są większe niż podpisy RSA. W 1976 r. Przed RSA Diffie i Hellman [29] zaproponowali system wymiany kluczy; pozwala na bezpieczną wymianę kluczy w konwencjonalnym tajnym systemie. Ten system jest dziś w użyciu. Zaproponowano również kryptosystemy oparte na operacjach matematycznych na krzywych eliptycznych, a także kryptosystemy oparte na dyskretnej potęgowaniu w polu skończonym GF (2 ^ n). Te ostatnie są bardzo szybkie w sprzęcie; jednakże pojawiły się wątpliwości co do ich bezpieczeństwa, ponieważ podstawowy problem może być łatwiejszy do rozwiązania niż faktoring. Istnieją również pewne probabilistyczne metody szyfrowania, które są atrakcyjne, ponieważ są odporne na odgadnięcie zaszyfrowanego tekstu, ale kosztem rozszerzenia danych. W szyfrowaniu probabilistycznym ten sam tekst zaszyfrowany dwukrotnie pod tym samym kluczem da z dużym prawdopodobieństwem dwa różne szyfrogramy. W przypadku podpisów cyfrowych, Rabin zaproponował system, który jest równoważny z faktoringiem; jest to zaleta w porównaniu z RSA, gdzie można wciąż martwić się o atak niezwiązany z faktoringiem. Metoda Rabina jest jednak podatna na wybrany atak wiadomości, w którym atakujący nakłania użytkownika do podpisania wiadomości o specjalnym formularzu. Kolejny system podpisów, autorstwa Fiata i Shamira, oparty jest na interaktywnych protokołach zerowej wiedzy, ale może być dostosowany do podpisów. Jest szybszy niż RSA i jest prawdopodobnie równoznaczny z faktoringiem, ale podpisy są znacznie większe niż podpisy RSA. Inne warianty zmniejszają jednak niezbędną długość podpisu; System jest "równoważny z faktoringiem", jeśli odzyskanie klucza prywatnego jest tak samo trudne, jak faktoring; fałszowanie może być łatwiejsze niż faktoring w niektórych systemach. Zalety RSA w porównaniu do innych kryptosystemów z kluczem publicznym obejmują fakt, że może on być używany zarówno do szyfrowania, jak i uwierzytelniania, i że istnieje od wielu lat i z powodzeniem przetrwał wiele kontroli. RSA otrzymał znacznie więcej uwagi, badań i faktycznego wykorzystania niż jakikolwiek inny kryptosystem klucza publicznego, a zatem RSA ma więcej dowodów empirycznych na jego bezpieczeństwo niż nowsze i mniej zbadane systemy. W rzeczywistości wiele kryptosystemów z kluczem publicznym, które początkowo wyglądały na bezpieczne, zostało później złamanych;

2.16 Czy RSA jest obecnie w użyciu?

Stosowanie RSA przechodzi okres szybkiej ekspansji i może stać się wszechobecne w ciągu kilku lat. Jest on obecnie używany w wielu różnych produktach, platformach i branżach na całym świecie. Znajduje się w wielu komercyjnych programach i jest planowany na wiele innych. RSA jest wbudowany w bieżące lub planowane systemy operacyjne firm Microsoft, Apple, Sun i Novell. W sprzęcie RSA można znaleźć w bezpiecznych telefonach, na kartach sieci Ethernet i na kartach inteligentnych. RSA jest również stosowana wewnętrznie w wielu instytucjach, w tym w oddziałach rządu USA, dużych korporacjach, laboratoriach krajowych i uniwersytetach. Wydaje się, że przyjęcie RSA postępuje szybciej w celu uwierzytelnienia (podpisów cyfrowych) niż w przypadku prywatności (szyfrowania), być

może po części dlatego, że produkty do uwierzytelniania są łatwiejsze do wyeksportowania niż produkty do prywatności.

2.17 Czy RSA jest obecnie oficjalnym standardem?

RSA jest częścią wielu oficjalnych standardów na całym świecie. Norma ISO (Międzynarodowa Norma Organizacji) 9796 wymienia RSA jako zgodny algorytm kryptograficzny, podobnie jak Komitet Doradczy ds. Bezpieczeństwa Międzynarodowego Telegrafii i Telefonii (CCITT) X.509. RSA jest częścią standardu Society for Worldwide Interbank Financial Telecommunications (SWIFT), standardu ETEBAC 5 francuskiej branży finansowej oraz projektu standardu ANSI X9.31 dla sektora bankowego w USA. Australijski standard zarządzania kluczami, AS2805.6.5.3, również określa RSA. RSA znajduje się w proponowanym przez Internet standardzie PEM (Privacy Enhanced Mail) i standardzie PKCS dla branży oprogramowania Warsztat wdrożeniowy OSI (OIW) wydał umowy implementacyjne odnoszące się do PKCS i PEM, z których każdy zawiera RSA. Obecnie opracowywanych jest wiele innych standardów, które zostaną ogłoszone w ciągu najbliższych kilku lat; wiele z nich ma zawierać RSA jako zatwierdzony lub zalecany system ochrony prywatności i / lub uwierzytelniania.

2.18 Czy RSA to de facto standard?

Dlaczego standard de facto jest ważny? RSA jest obecnie najczęściej stosowanym kryptosystemem klucza publicznego i często nazywany jest de facto standardem. Niezależnie od oficjalnych standardów istnienie standardu de facto ma ogromne znaczenie dla rozwoju gospodarki cyfrowej. Jeśli jeden system klucza publicznego jest wszędzie wykorzystywany do uwierzytelniania, podpisane dokumenty cyfrowe mogą być wymieniane między użytkownikami w różnych krajach przy użyciu różnych programów na różnych platformach; interoperacyjność jest niezbędna do rozwoju prawdziwej gospodarki cyfrowej. Brak bezpiecznego uwierzytelniania był główną przeszkodą w osiągnięciu obietnicy, że komputery zastąpią papier; papier jest nadal potrzebny prawie wszędzie w przypadku umów, czeków, listów urzędowych, dokumentów prawnych i identyfikacji. Dzięki temu trzem niezbędnym transakcjom papierowym nie było możliwe całkowite przekształcenie się w społeczeństwo oparte na transakcjach elektronicznych. Podpisy cyfrowe są dokładnym narzędziem niezbędnym do konwersji najbardziej podstawowych dokumentów papierowych na cyfrowe nośniki elektroniczne. Podpisy cyfrowe umożliwiają na przykład dzierżawę, testament, paszport, transkrypcje, czeki i formularze rejestracyjne wyborców, które istnieją tylko w formie elektronicznej; każda wersja papierowa byłaby po prostu "kopią" oryginału elektronicznego. Wszystko to jest możliwe dzięki zaakceptowanemu standardowi podpisów cyfrowych.

2.19 Czy opatentowany jest RSA?

RSA jest opatentowany pod patencie USA 4,405,829, wydanym 9/20/83 i przechowywany przez Public Key Partners (PKP), z Sunnyvale w Kalifornii; patent wygasa 17 lat po wydaniu, w 2000 r. RSA jest zwykle licencjonowany razem z innymi patentami kryptografii o kluczu publicznym (patrz Pytanie 1.5). PKP ma standardową, opartą na tantiem politykę licencyjną, którą można modyfikować w szczególnych okolicznościach. Jeśli sprzedawca oprogramowania, posiadając licencję na patenty z kluczem publicznym, włącza RSA do produktu komercyjnego, to każdy, kto kupi produkt końcowy, ma prawo do używania RSA w kontekście tego oprogramowania. Rząd USA może używać RSA bez licencji, ponieważ został wynaleziony w MIT przy częściowym finansowaniu przez rząd. RSA nie jest opatentowany poza Ameryką Północną. W Ameryce Północnej licencja jest potrzebna do "robienia, używania lub sprzedawania" RSA. Jednakże, PKP zazwyczaj zezwala na bezpłatne, niekomercyjne wykorzystanie RSA, z pisemną zgodą, z powodów osobistych, naukowych lub intelektualnych. Ponadto RSA Laboratories udostępniło (w USA i Kanadzie) bezpłatną kolekcję procedur kryptograficznych w

kodzie źródłowym, w tym algorytm RSA; może być używany, ulepszany i rozpowszechniany niekomercyjnie

2.20 Czy można wyeksportować RSA z USA?

Eksport RSA podlega tym samym prawom amerykańskim, co wszystkie inne produkty kryptograficzne. Numer RSA używany do uwierzytelniania jest łatwiej eksportowany niż w przypadku prywatności. W pierwszym przypadku eksport jest dozwolony niezależnie od wielkości klucza (modułu), chociaż eksporter musi wykazać, że produkt nie może być łatwo przekonwertowany do użycia w celu zaszyfrowania. W przypadku RSA używanego do ochrony prywatności (szyfrowania), rząd Stanów Zjednoczonych generalnie nie zezwala na eksport, jeśli rozmiar klucza przekracza 512 bitów. Polityka eksportowa jest obecnie przedmiotem debaty, a status eksportu RSA może się zmienić w następnym roku lub dwóch. Bez względu na politykę eksportową USA, RSA jest dostępny za granicą w produktach innych niż amerykańskie.

3 Zarządzanie kluczami

3.1 Jakie kluczowe kwestie zarządzania są zaangażowane w kryptografię klucza publicznego? Bezpieczne metody zarządzania kluczami są niezwykle ważne. W praktyce większość ataków na systemy klucza publicznego będzie prawdopodobnie kierowana na kluczowe poziomy zarządzania, a nie na sam algorytm kryptograficzny. Wymienione tutaj kluczowe kwestie zarządzania omówiono szczegółowo w późniejszych pytaniach. Użytkownicy muszą być w stanie bezpiecznie uzyskać parę kluczy odpowiednią do ich wydajności i bezpieczeństwa. Musi być sposób na sprawdzenie kluczy publicznych innych osób i nagłośnienie własnego klucza. Użytkownicy muszą mieć zaufanie do legalności kluczy publicznych innych osób; w przeciwnym razie intruz może albo zmienić klucze publiczne wymienione w katalogu, albo podszyć się pod innego użytkownika. W tym celu wykorzystywane są certyfikaty. Certyfikaty muszą być niezniszczalne, dostępne w bezpieczny sposób i przetwarzane w taki sposób, aby intruz nie mógł ich nadużywać. Wydawanie certyfikatów musi przebiegać w sposób bezpieczny, odporny na atak. Jeśli klucz prywatny użytkownika zostanie zgubiony lub naruszony, inne osoby muszą zostać o tym poinformowane, aby nie szyfowały wiadomości pod nieprawidłowym kluczem publicznym ani nie akceptowały wiadomości podpisanych przy użyciu niepoprawnego klucza prywatnego. Użytkownicy muszą mieć możliwość bezpiecznego przechowywania swoich kluczy prywatnych, aby żaden intruz nie mógł ich znaleźć, ale klucze muszą być łatwo dostępne do legalnego użytku. Klucze muszą być ważne tylko do określonej daty wygaśnięcia. Data wygaśnięcia musi być odpowiednio wybrana i opublikowana w bezpieczny sposób. Niektóre dokumenty muszą mieć możliwe do zweryfikowania podpisy po upływie czasu, w którym klucz do ich podpisania wygasł. Chociaż większość tych kluczowych problemów związanych z zarządzaniem pojawia się w jakimkolwiek kryptosystemie klucza publicznego, dla wygody są one omawiane tutaj w kontekście RSA.

3.2 Kto potrzebuje klucza?

Każdy, kto chce podpisywać wiadomości lub odbierać zaszyfrowane wiadomości, musi mieć parę kluczy. Ludzie mogą mieć więcej niż jeden klucz. Na przykład ktoś może mieć klucz związany z jego pracą i oddzielny klucz do osobistego użytku. Inne podmioty będą miały również klucze, w tym podmioty elektroniczne, takie jak modemy, stacje robocze i drukarki, a także jednostki organizacyjne, takie jak dział korporacyjny, punkt rejestracji hotelu lub biuro rejestracji uniwersyteckiej.

3.3 Jak uzyskać kluczową parę?

Każdy użytkownik powinien wygenerować swoją własną parę kluczy. Może być kuszące wewnątrz organizacji, aby mieć jedną stronę, która generuje klucze dla wszystkich członków, którzy jej zażądają, ale jest to ryzyko bezpieczeństwa, ponieważ wiąże się z przesyłaniem kluczy prywatnych przez sieć, jak również katastrofalnymi konsekwencjami, jeśli atakujący wniknie w klucz strona generująca. Każdy węzeł w sieci powinien mieć możliwość generowania kluczy lokalnych, aby klucze prywatne nie były nigdy przesyłane, a żadne źródło klucza zewnętrznego nie było zaufane. Oczywiście oprogramowanie generujące lokalne oprogramowanie samo w sobie musi być godne zaufania. Systemy uwierzytelniania z tajnym kluczem, takie jak Kerberos, często nie zezwalają na generowanie klucza lokalnego, ale zamiast tego używają serwera centralnego do generowania kluczy. Po wygenerowaniu użytkownik musi zarejestrować swój klucz publiczny w centralnej administracji, zwanej certyfikującym. Instytucja certyfikująca zwraca użytkownikowi certyfikat potwierdzający wiarygodność klucza publicznego użytkownika wraz z innymi informacjami. Większość użytkowników nie powinna uzyskiwać więcej niż jednego certyfikatu dla tego samego klucza, aby uprościć różne zadania związane z księgowaniem związane z kluczem.

3.4 Czy klucz publiczny lub prywatny muszą być udostępniane użytkownikom?

W RSA każda osoba powinna mieć unikalny moduł i prywatny wykładnik, tj. Unikalny klucz prywatny. Z drugiej strony, publiczny wykładnik może być wspólny dla grupy użytkowników bez naruszenia bezpieczeństwa. Niektóre publiczne wykładniki powszechnie używane dzisiaj to 3 i 2 ^ {16} +1; ponieważ liczby te są małe, operacje klucza publicznego (szyfrowanie i weryfikacja podpisu) są szybkie w stosunku do operacji na kluczach prywatnych (odszyfrowywanie i podpisywanie). Jeśli jeden publiczny wykładnik staje się standardem, oprogramowanie i sprzęt mogą być zoptymalizowane pod kątem tej wartości. W systemach klucza publicznego opartych na logarytmach dyskretnych, takich jak ElGamal, Diffie-Hellman lub DSS, często sugerowano, że grupa ludzi powinna dzielić moduł. To spowodowałoby, że złamanie klucza było bardziej atrakcyjne dla atakującego, ponieważ można złamać każdy klucz przy odrobinie więcej wysiłku, niż by złamać pojedynczy klucz. Dla atakującego średni koszt złamania klucza jest znacznie niższy przy wspólnym module, niż gdy każdy klucz ma odrębny moduł. Dlatego należy być bardzo ostrożnym przy używaniu wspólnego modułu; jeśli wybrany zostanie wspólny moduł, powinien on być bardzo duży.

3.5 Czym są certyfikaty?

Certyfikaty są cyfrowymi dokumentami potwierdzającymi powiązanie klucza publicznego z osobą lub innym podmiotem. Pozwalają one zweryfikować twierdzenie, że dany klucz publiczny faktycznie należy do danej osoby. Certyfikaty pomagają zapobiec użyciu fałszywego klucza do podszywania się pod inną osobę. W najprostszej formie certyfikaty zawierają klucz publiczny i nazwę. Powszechnie używane, zawierają również datę wygaśnięcia klucza, nazwę instytucji certyfikującej, która wydała certyfikat, numer seryjny certyfikatu i być może inne informacje. Co najważniejsze, zawiera cyfrowy podpis wydawcy certyfikatu. Najpowszechniej akceptowany format certyfikatów określa międzynarodowy standard CCITT X.509; w ten sposób certyfikaty mogą być odczytywane lub zapisywane przez dowolną aplikację zgodną z X.509. Dalsze udoskonalenia można znaleźć w zestawie standardów PKCS oraz w standardzie PEM. Szczegółowe omówienie formatu certyfikatu można również znaleźć w Kent. Certyfikat jest wydawany przez instytucję certyfikującą i podpisywany za pomocą klucza prywatnego instytucji certyfikującej.

3.6 W jaki sposób używane są certyfikaty?

Certyfikat jest wyświetlany w celu wygenerowania zaufania do legalności klucza publicznego. Osoba sprawdzająca podpis może również zweryfikować certyfikat osoby podpisującej, aby upewnić się, że nie wystąpiło fałszerstwo lub nieprawdziwe przedstawienie. Te kroki mogą być wykonywane z większą

lub mniejszą dokładnością w zależności od kontekstu. Najbezpieczniejsze korzystanie z uwierzytelniania polega na załączaniu jednego lub więcej certyfikatów z każdą podpisaną wiadomością. Odbiorca wiadomości sprawdzi certyfikat za pomocą publicznego klucza instytucji certyfikującej i, mając pewność, że jest publiczny klucz nadawcy, weryfikuje podpis wiadomości. Mogą być dwa lub więcej certyfikatów dołączonych do wiadomości, tworząc łańcuch hierarchiczny, w którym jeden certyfikat świadczy o autentyczności poprzedniego certyfikatu. Na końcu hierarchii certyfikatów znajduje się urząd certyfikacji najwyższego poziomu, który jest zaufany bez certyfikatu z żadnej innej instytucji certyfikującej. Klucz publiczny organu certyfikującego najwyższego poziomu musi być niezależnie znany, na przykład poprzez jego szerokie publikowanie. Im lepiej znany jest nadawca odbiorcy wiadomości, tym mniej potrzeba do załączenia i weryfikacji certyfikatów. Jeśli Alicja codziennie wysyła wiadomości do Boba, Alicja może zamknąć łańcuch certyfikatów pierwszego dnia, który sprawdza Bob. Następnie Bob przechowuje klucz publiczny Alicji i nie są potrzebne żadne certyfikaty ani weryfikacje certyfikatów. Nadawca, którego firma jest znana odbiorcy, może potrzebować dołączyć tylko jeden certyfikat (wydany przez firmę), podczas gdy nadawca, którego firma nie jest znana odbiorcy, może potrzebować dołączyć dwa certyfikaty. Dobrą zasadą jest zamknięcie tylko tyle łańcucha certyfikatów, aby wydawca certyfikatu najwyższego poziomu w łańcuchu był dobrze znany odbiorcy. Zgodnie ze standardami PKCS dotyczącymi kryptografii z kluczem publicznym (patrz Pytanie 8.9) każda sygnatura wskazuje certyfikat, który potwierdza klucz publiczny podpisującego. W szczególności każdy podpis zawiera nazwę wydawcy certyfikatu i numer seryjny certyfikatu. Dlatego nawet jeśli do wiadomości nie dołączono żadnych certyfikatów, weryfikator może nadal używać łańcucha certyfikatów do sprawdzania statusu klucza publicznego.

3.7 Kto wydaje certyfikaty i jak?

Certyfikaty są wydawane przez instytucję certyfikującą (CA), która może być dowolną zaufaną administracją centralną, która chce ręczyć za tożsamość osób, którym wystawia certyfikaty. Firma może wydawać swoim pracownikom certyfikaty, uniwersytet swoim studentom, miasto swoim obywatelom. Aby zapobiec fałszowaniu certyfikatów, klucz publiczny urzędu certyfikacji musi być godny zaufania: urząd certyfikacji musi upublicznić swój klucz publiczny lub dostarczyć certyfikat z urzędu wyższego poziomu potwierdzający ważność jego klucza publicznego. To drugie rozwiązanie powoduje powstanie hierarchii urzędów certyfikacji. Wydanie certyfikatu przebiega w następujący sposób. Alice generuje swoją własną parę kluczy i wysyła klucz publiczny do odpowiedniego CA z pewnym dowodem jej identyfikacji. CA sprawdza identyfikację i podejmuje wszelkie inne kroki niezbędne do upewnienia się, że żądanie rzeczywiście pochodzi od Alicji, a następnie przesyła jej certyfikat potwierdzający powiązanie Alice z jej kluczem publicznym, wraz z hierarchią certyfikatów weryfikujących urzędowy urząd certyfikacji. klawisz. Alice może zaprezentować ten łańcuch certyfikatów, ilekroć jest to pożądane, aby wykazać legitymację swojego klucza publicznego. Ponieważ CA musi sprawdzić poprawność identyfikacji, organizacje uznają, że wygodnie jest działać jako ośrodek dla swoich członków i pracowników. Będą również urzędy certyfikacji wydające certyfikaty osobom nieoficjalnym. Różne urzędy certyfikacji mogą wydawać certyfikaty o różnych poziomach wymagań dotyczących identyfikacji. Jeden urząd certyfikacji może nalegać na uzyskanie prawa jazdy, inny może chcieć, aby formularz wniosku o certyfikat został poświadczony notarialnie, a jeszcze inny może wymagać odcisków palców każdego, kto zażąda certyfikatu. Każdy urząd certyfikacji powinien publikować własne wymagania i standardy identyfikacyjne, aby weryfikatorzy mogli przywiązywać odpowiedni poziom zaufania do certyfikowanych powiązań z kluczami nazw. Przykładem protokołu wystawiającego certyfikat jest otwarte środowisko współpracy Apple Computer (OCE). Użytkownicy OCE firmy Apple mogą wygenerować parę kluczy, a następnie zażądać i otrzymać certyfikat dla klucza publicznego; żądanie certyfikatu musi być poświadczone notarialnie

3.8 Co to jest CSU, lub w jaki sposób instytucje certyfikujące przechowują swoje klucze prywatne?

Niezmiernie ważne jest, aby prywatne klucze instytucji certyfikujących były bezpiecznie przechowywane, ponieważ kompromis umożliwiłby niewykrywalne fałszerstwa. Jednym ze sposobów osiągnięcia pożądanego bezpieczeństwa jest przechowywanie klucza w pudełku zabezpieczonym przed manipulacją; takie pudełko nazywa się jednostką podpisu certyfikatów lub CSU. CSU najlepiej zniszczyłaby jego zawartość, jeśli kiedykolwiek byłaby otwarta, i była chroniona przed atakami wykorzystującymi promieniowanie elektromagnetyczne. Nawet pracownicy instytucji certyfikującej nie powinni mieć dostępu do samego klucza prywatnego, a jedynie możliwość korzystania z klucza prywatnego w procesie wydawania certyfikatów. Istnieje wiele możliwych projektów dla CSU; tutaj jest opis jednego wzoru znalezionego w niektórych obecnych implementacjach. CSU jest aktywowany przez zestaw kluczy danych, które są fizycznymi kluczami zdolnymi do przechowywania informacji cyfrowych. Klucze danych wykorzystują technologię udostępniania sekretów, tak, że kilka osób musi wszystkie używać swoich kluczy danych do aktywacji CSU. Zapobiega to wytwarzaniu fałszywych certyfikatów przez jednego niezadowolonego pracownika CA. Zauważ, że jeśli CSU zostanie zniszczona, powiedz w ogniu, żadne zabezpieczenie nie zostanie naruszone. Certyfikaty podpisane przez CSU są nadal ważne, o ile weryfikator używa poprawnego klucza publicznego. Niektóre jednostki CSU zostaną wyprodukowane w taki sposób, aby zagubiony klucz prywatny mógł zostać przywrócony do nowej jednostki CSU. Zobacz pytanie 3.10 w celu omówienia kluczy prywatnych zaginionych CA. Bolt, Beranek i Newman (BBN) sprzedają obecnie CSU, a RSA Data Security sprzedaje pełnoprawny system wydawania certyfikatów zbudowany wokół BBN CSU.

3.9 Czy instytucje certyfikujące są podatne na atak?

Można pomyśleć o wielu atakach skierowanych do instytucji certyfikującej, które muszą być przygotowane przeciwko nim. Rozważ następujący atak. Załóżmy, że Bob chce podszyć się pod Alice. Jeśli Bob może przekonująco podpisać wiadomości jako Alicja, może wysłać wiadomość do banku Alicji, mówiąc: "Chcę wypłacić 10 000 $ z mojego konta. Wyślij mi pieniądze. "Aby przeprowadzić ten atak, Bob generuje parę kluczy i wysyła klucz publiczny do instytucji certyfikującej, mówiąc:" Jestem Alice. Oto mój klucz publiczny. Prześlij mi zaświadczenie. "" Jeśli CA zostanie oszukany i wyśle mu taki certyfikat, może wtedy oszukać bank, a jego atak się powiedzie. Aby zapobiec takiemu atakowi, urząd certyfikacji musi sprawdzić, czy wniosek o wydanie certyfikatu rzeczywiście pochodzi od jego rzekomego autora, tj. Musi on wymagać wystarczającego dowodu, że to właśnie Alicja żąda certyfikatu. CA może na przykład wymagać od Alicji osobistego stawienia się i okazania aktu urodzenia. Niektóre urzędy certyfikacji mogą wymagać bardzo małej identyfikacji, ale bank nie powinien honorować wiadomości uwierzytelnianych za pomocą takich certyfikatów o niskiej wiarygodności. Każdy urząd certyfikacji musi publicznie podać swoje wymogi i zasady identyfikacji; inni mogą następnie przywiązać odpowiedni poziom zaufania do certyfikatów. Osoba atakująca, która odkryje klucz prywatny instytucji certyfikującej, może następnie sfałszować certyfikaty. Z tego powodu instytucja certyfikująca musi podjąć nadzwyczajne środki ostrożności, aby zapobiec nieuprawnionemu dostępowi do jej klucza prywatnego. Klucz prywatny powinien być przechowywany w skrzynce o wysokim poziomie bezpieczeństwa, znanej jako jednostka podpisu certyfikatu lub CSU (patrz pytanie 3.8). Klucz publiczny instytucji certyfikującej może być celem rozległego ataku faktoringowego. Z tego powodu urzędy certyfikacji powinny używać bardzo długich kluczy, najlepiej o długości 1000 bitów lub więcej, a także regularnie zmieniać klucze. Najwyższe organy certyfikujące są wyjątkami: zmiana kluczy często może nie być dla nich praktyczna, ponieważ klucz może zostać zapisany w oprogramowaniu używanym przez dużą liczbę weryfikatorów. W kolejnym ataku Alice przekupuje Boba, który pracuje dla instytucji certyfikującej, aby wydał jej certyfikat na nazwisko Fred. Teraz Alicja może wysyłać wiadomości podpisane pod imieniem Freda, a każdy, kto otrzyma taką wiadomość, uzna ją za autentyczną,

ponieważ towarzyszy jej pełny i weryfikowalny łańcuch certyfikatów. Atak ten może zostać utrudniony przez wymaganie współpracy dwóch (lub więcej) pracowników w celu wygenerowania certyfikatu; atakujący musi teraz przekupić dwóch pracowników zamiast jednego. Na przykład w niektórych dzisiejszych CSU trzech pracowników musi wstawić klucz danych zawierający tajne informacje, aby upoważnić CSU do generowania certyfikatów. Niestety, mogą istnieć inne sposoby na wygenerowanie fałszywego certyfikatu, przekupując tylko jednego pracownika. Jeśli każde żądanie certyfikatu jest sprawdzane tylko przez jednego pracownika, można go przekupić i przesłać fałszywe żądanie do stosu prawdziwych żądań certyfikatu. Pamiętaj, że skorumpowany pracownik nie może ujawnić klucza prywatnego instytucji certyfikującej, o ile jest prawidłowo przechowywany. Kolejny atak polega na wykuwaniu starych dokumentów. Alice próbuje uwzględnić współczynnik certyfikujący instytucji certyfikującej. Potrzeba jej 15 lat, ale w końcu się to udaje, a teraz ma stary klucz prywatny instytucji certyfikującej. Klucz już dawno minął, ale ona może wykuć certyfikat datowany 15 lat temu świadczący o fałszywym kluczu publicznym innej osoby, powiedzmy Bob; może teraz sfałszować dokument z podpisem Boba z 15 lat temu, być może wolą pozostawienia wszystkiego Alice. Podstawową kwestią poruszoną podczas tego ataku jest uwierzytelnianie podpisanego dokumentu sprzed wielu lat; kwestia ta została omówiona w pytaniu 3.17. Należy zauważyć, że ataki na instytucje certyfikujące nie zagrażają prywatności wiadomości między użytkownikami, ponieważ mogą być wynikiem ataku na centrum dystrybucji kluczy tajnych.

3.10 Co się stanie, jeśli klucz instytucji certyfikującej zaginie lub zostanie naruszony?

Jeśli klucz instytucji certyfikującej zostanie zgubiony lub zniszczony, ale nie zostanie naruszony, certyfikaty podpisane starym kluczem są nadal ważne, o ile weryfikator wie, że używa starego klucza publicznego do weryfikacji certyfikatu. W niektórych projektach CSU przechowywane są zaszyfrowane kopie zapasowe klucza prywatnego urzędu certyfikacji. Urząd certyfikacji, który traci klucz, może następnie przywrócić go, ładując zaszyfrowaną kopię zapasową do CSU, która może odszyfrować ją za pomocą unikalnych informacji przechowywanych w CSU; zaszyfrowaną kopię zapasową można odszyfrować tylko za pomocą CSU. Jeżeli sama CSU ulegnie zniszczeniu, producent może dostarczyć drugiej takiej samej informacji wewnętrznej, co umożliwi odzyskanie klucza. Zagrożony klucz CA jest znacznie bardziej niebezpieczną sytuacją. Osoba atakująca, która odkryje klucz prywatny instytucji certyfikującej, może wydawać fałszywe certyfikaty w imieniu instytucji certyfikującej, które umożliwiłyby niewykrywalne fałszerstwa; z tego powodu należy przedsięwziąć wszelkie środki ostrożności, aby zapobiec kompromisowi, w tym te wymienione w pytaniach 3.8 i 3.9. Jeśli dojdzie do kompromisu, urząd certyfikacji musi natychmiast zaprzestać wydawania certyfikatów pod starym kluczem i zmienić na nowy klucz. Jeśli podejrzewa się, że wydano fałszywe certyfikaty, wszystkie certyfikaty powinny zostać przywołane, a następnie ponownie wysłane za pomocą nowego klucza urzędu certyfikacji. Środki te mogłyby zostać nieco złagodzone, gdyby certyfikaty zostały zarejestrowane w cyfrowej usłudze znakowania czasem (patrz pytanie 3.18). Należy zauważyć, że naruszenie klucza dostępu do urzędu certyfikacji nie powoduje unieważnienia kluczy użytkowników, ale tylko certyfikaty, które je uwierzytelniają. Kompromis dotyczący klucza urzędu najwyższego poziomu powinien być uznany za katastrofalny, ponieważ klucz może być wbudowany w aplikacje, które weryfikują certyfikaty.

3.11 Czym są listy odwołań certyfikatów (CRL)?

Lista odwołań certyfikatów (CRL) to lista kluczy publicznych, które zostały odwołane przed datą ich wygaśnięcia. Istnieje kilka powodów, dla których klucz może zostać odwołany i umieszczony na liście CRL. Klucz mógł zostać naruszony. Klucz może być wykorzystywany zawodowo przez jednostkę dla firmy; na przykład oficjalną nazwą związaną z kluczem może być "Alice Avery, wiceprezes Argo Corp." "Jeśli Alice zostałaby zwolniona, jej firma nie chciałaby, aby mogła podpisywać wiadomości za pomocą

tego klucza i dlatego firma umieść klucz na CRL. Podczas sprawdzania podpisu można sprawdzić odpowiednią listę CRL, aby upewnić się, że klucz osoby podpisującej nie został odwołany. To, czy warto poświęcić czas na sprawdzenie, zależy od znaczenia podpisanego dokumentu. Listy CRL są utrzymywane przez instytucje certyfikujące (CA) i zawierają informacje o unieważnionych kluczach oryginalnie certyfikowanych przez urząd certyfikacji. Listy CRL podają tylko aktualne klucze, ponieważ wygasłe klucze nie powinny być w żadnym wypadku akceptowane; gdy unieważniony klucz minął pierwotną datę wygaśnięcia, zostaje usunięty z listy CRL. Chociaż listy CRL są utrzymywane w sposób rozproszony, mogą istnieć centralne repozytoria list CRL, to jest witryny w sieciach zawierających najnowsze listy CRL wielu organizacji. Instytucja taka jak bank może chcieć wewnętrznego repozytorium CRL, aby umożliwić wykonywanie wyszukiwań CRL przy każdej transakcji.

3.12 Co stanie się, gdy klucz wygasa?

Aby zabezpieczyć się przed długoterminowym atakiem factoringowym, każdy klucz musi mieć datę ważności, po której traci ważność. Czas do wygaśnięcia musi być zatem znacznie krótszy niż przewidywany czas faktoringu, lub równoważnie, długość klucza musi być wystarczająco długa, aby szanse faktorowania przed wygaśnięciem były bardzo małe. Okres ważności dla pary kluczy może również zależeć od okoliczności, w których klucz zostanie użyty, chociaż będzie również standardowy okres. Okres ważności, wraz z wartością klucza i szacowaną siłą oczekiwanego napastnika, określa odpowiedni rozmiar klucza. Data wygaśnięcia klucza towarzyszy kluczowi publicznemu w certyfikacie lub wykazie katalogu. Program weryfikacji podpisu powinien sprawdzić datę wygaśnięcia i nie powinien akceptować wiadomości podpisanej przy wygasłym kluczu. Oznacza to, że po wygaśnięciu własnego klucza, wszystko podpisane z nim nie będzie już uważane za ważne. Oczywiście zdarzają się przypadki, w których ważne jest, aby podpisany dokument był ważny przez znacznie dłuższy czas; Po wygaśnięciu użytkownik wybiera nowy klucz, który powinien być dłuższy niż stary klucz, prawdopodobnie o kilka cyfr, aby odzwierciedlić zarówno wzrost wydajności sprzętu komputerowego, jak i wszelkie ostatnie ulepszenia w algorytmach faktoringu. Zalecane harmonogramy kluczy kluczowych prawdopodobnie zostaną opublikowane. Użytkownik może odnowić klucz, który wygasł, jeśli jest wystarczająco długi i nie został naruszony. Instytucja certyfikująca wyda nowy certyfikat dla tego samego klucza, a wszystkie nowe podpisy wskażą nowy certyfikat zamiast starego. Jednak fakt, że sprzęt komputerowy ciągle się poprawia, przemawia za zastąpieniem wygasłych kluczy nowymi, dłuższymi kluczami co kilka lat. Wymiana klucza umożliwia skorzystanie z ulepszeń sprzętowych w celu zwiększenia bezpieczeństwa kryptosystemu. Szybszy sprzęt ma wpływ na zwiększenie bezpieczeństwa, być może ogromnie, ale tylko wtedy, gdy regularnie zwiększa się długość klucza

3.13 Co się stanie, jeśli zgubię swój klucz prywatny?

Jeśli Twój klucz prywatny zostanie zgubiony lub zniszczony, ale nie zostanie naruszony, nie będzie można już podpisywać ani odszyfrowywać wiadomości, ale wszystko, co wcześniej podpisano zgubionym kluczem, jest nadal ważne. Może się to zdarzyć, na przykład, jeśli zapomnisz hasła używanego do uzyskania dostępu do klucza lub jeśli dysk, na którym przechowywany jest klucz, jest uszkodzony. Musisz od razu wybrać nowy klucz, aby zminimalizować liczbę wiadomości wysyłanych przez Ciebie zaszyfrowanych pod starym kluczem, wiadomości, których już nie możesz przeczytać.

3.14 Co się stanie, jeśli mój klucz prywatny zostanie naruszony?

Jeśli twój klucz prywatny zostanie naruszony, to znaczy, jeśli podejrzewasz, że atakujący mógł uzyskać twój prywatny klucz, musisz założyć, że jakiś wróg może odczytać zaszyfrowane wiadomości wysłane do ciebie i sfałszować twoje imię na dokumentach. Powaga tych konsekwencji podkreśla znaczenie ochrony klucza prywatnego za pomocą bardzo silnych mechanizmów. Musisz natychmiast powiadomić swoją instytucję certyfikującą i umieścić swój stary klucz na liście cofnięcia certyfikatu (patrz pytanie

3.11); to poinformuje ludzi, że klucz został odwołany. Następnie wybierz nowy klucz i zdobądź dla niego odpowiednie certyfikaty. Możesz użyć nowego klucza do ponownego podpisania dokumentów, które podpisałeś z zaatakowanym kluczem; dokumenty, które zostały opatrzone datą i podpisane, mogą nadal być ważne. Powinieneś również zmienić sposób przechowywania klucza prywatnego, aby nie narażać na szwank nowego klucza.

3.15 Jak mam przechowywać mój klucz prywatny?

Klucze prywatne muszą być bezpiecznie przechowywane, ponieważ fałszerstwa i utrata prywatności mogą być wynikiem naruszenia. Klucz prywatny nigdy nie powinien być przechowywany w dowolnym miejscu w postaci zwykłego tekstu. Najprostszym mechanizmem przechowywania jest zaszyfrowanie klucza prywatnego pod hasłem i zapisanie wyniku na dysku. Oczywiście samo hasło musi być utrzymywane z wysokim poziomem bezpieczeństwa, a nie zapisywane i niełatwo odgadnąć. Przechowywanie zaszyfrowanego klucza na dysku, który nie jest dostępny za pośrednictwem sieci komputerowej, takiej jak dyskietka lub lokalny dysk twardy, utrudni niektóre ataki. Ostatecznie klucze prywatne mogą być przechowywane na przenośnym sprzęcie, takim jak karta inteligentna. Ponadto protokół typu challenge-response będzie bezpieczniejszy niż prosty dostęp do hasła. Użytkownicy o bardzo wysokim poziomie bezpieczeństwa, np. Instytucje certyfikujące, powinni używać specjalnych urządzeń sprzętowych do ochrony swoich kluczy

3.16 Jak znaleźć klucz publiczny innej osoby?

Załóżmy, że chcesz znaleźć klucz publiczny Boba. Istnieje kilka możliwych sposobów. Możesz zadzwonić do niego i poprosić go o przesłanie swojego klucza publicznego za pośrednictwem poczty e-mail; możesz również poprosić o to za pośrednictwem poczty e-mail. Instytucje certyfikujące mogą świadczyć usługi katalogowe; jeśli Bob pracuje dla firmy Z, zajrzyj do katalogu prowadzonego przez instytucję certyfikującą Z. Katalogi muszą być zabezpieczone przed nieuprawnioną ingerencją, aby użytkownicy mogli mieć pewność, że klucz publiczny wymieniony w katalogu rzeczywiście należy do wymienionej osoby. W przeciwnym razie możesz wysłać prywatne zaszyfrowane informacje do niewłaściwej osoby. W końcu pojawią się pełnowartościowe katalogi służące jako białe lub żółte strony online. Jeśli są one zgodne ze standardami CCITT X.509 [19], katalogi będą zawierać certyfikaty, a także klucze publiczne; obecność certyfikatów obniży potrzeby bezpieczeństwa katalogów.

3.17 W jaki sposób podpisy mogą pozostać ważne po wygaśnięciu ich kluczy lub, w jaki sposób weryfikuje się podpis 20-letni?

Zwykle klucz traci ważność po, powiedzmy, dwóch latach, a dokument podpisany kluczem, który wygasł, nie powinien być akceptowany. Istnieje jednak wiele przypadków, w których podpisane dokumenty należy uznać za ważne przez okres znacznie dłuższy niż dwa lata; długoterminowe umowy najmu i umowy są przykładami. W jaki sposób należy załatwić te sprawy? Zaproponowano wiele rozwiązań, ale nie jest jasne, które z nich będą najlepsze. Oto kilka możliwości. Można mieć specjalne klucze długoterminowe, a także normalne klucze dwuletnie. Długoterminowe klucze powinny mieć o wiele dłuższe moduły i być przechowywane bezpieczniej niż klucze dwuletnie. Jeśli klucz długoterminowy wygasa za 50 lat, każdy podpisany z nim dokument zachowa ważność w tym czasie. Problem z tą metodą polega na tym, że każdy zagrożony klucz musi pozostać na odpowiedniej liście CRL do czasu wygaśnięcia; jeśli klucze 50-letnie są rutynowo umieszczane na listach CRL, listy CRL mogą rosnąć w rozmiarze niemożliwym do zarządzania. Ten pomysł można zmodyfikować w następujący sposób. Zarejestruj klucz długoterminowy według zwykłej procedury, tj. Na dwa lata. W momencie wygaśnięcia, jeśli nie zostało naruszone, klucz może zostać ponownie wydany, tj. Wydany nowy certyfikat przez instytucję certyfikującą, tak że klucz będzie ważny przez kolejne dwa lata. Teraz skompromitowany klucz musi być przechowywany na CRL przez maksymalnie dwa lata, a nie

pięćdziesiąt. Jednym z problemów z poprzednią metodą jest to, że ktoś może próbować unieważnić długoterminową umowę, odmawiając odnowienia klucza. Ten problem można obejść, rejestrując umowę za pomocą cyfrowej usługi znakowania czasem w chwili jej podpisania. Jeżeli wszystkie strony umowy zachowują kopię znacznika czasu, wówczas każdy może udowodnić, że umowa została podpisana ważnymi kluczami. W rzeczywistości znacznik czasu może udowodnić ważność umowy, nawet jeśli klucz osoby podpisującej zostanie naruszony w pewnym momencie po podpisaniu umowy. To rozwiązanie do znakowania czasem może współpracować ze wszystkimi podpisanymi dokumentami cyfrowymi, a nie tylko z wielostronnymi umowami.

3.18 Co to jest cyfrowa usługa znakowania czasem?

Usługa cyfrowego znakowania czasem (DTS) emituje znaczniki czasu, które wiążą datę i godzinę z dokumentem cyfrowym w sposób silny pod względem kryptograficznym. Cyfrowy znacznik czasu może zostać użyty w późniejszym terminie, aby udowodnić, że dokument elektroniczny istniał w czasie określonym na jego znaczniku czasu. Na przykład fizyk, który ma genialny pomysł, może napisać o nim za pomocą edytora tekstu i opatrzyć go stemplem czasu. Datownik i dokument razem mogą później udowodnić, że naukowiec zasługuje na Nagrodę Nobla, mimo że jeden z rywali mógł być pierwszym, który opublikował. Oto jeden ze sposobów, w jaki taki system mógłby działać. Załóżmy, że Alicja podpisuje dokument i chce go oznaczyć na czas. Oblicza skrót wiadomości dokumentu za pomocą bezpiecznej funkcji skrótu (patrz Pytanie 8.2), a następnie przesyła skrót wiadomości (ale nie sam dokument) do DTS, który wysyła jej w zamian cyfrowy znacznik czasu składający się z skrótu wiadomości , datę i godzinę, w jakiej została otrzymana w DTS, oraz podpis DTS. Ponieważ treść wiadomości nie zawiera żadnych informacji o zawartości dokumentu, system DTS nie może podsłuchiwać dokumentów w postaci znaczników czasu. Później Alice może przedstawić dokument i znacznik czasu, aby udowodnić, kiedy dokument został napisany. Weryfikator oblicza skrót komunikatu dokumentu, upewnia się, że pasuje do skrótu w znaczniku czasu, a następnie weryfikuje podpis DTS na znaczniku czasu. Aby być wiarygodnym, znaczniki czasu nie mogą być przeszukiwalne. Rozważ wymagania dotyczące DTS właśnie opisanego typu. Po pierwsze, sam DTS musi mieć długi klucz, jeśli chcemy, aby znaczniki czasu były niezawodne przez, powiedzmy, kilka dziesięcioleci. Po drugie, prywatny klucz DTS musi być przechowywany z najwyższym zabezpieczeniem, tak jak w pudełku zabezpieczonym przed manipulacją. Po trzecie, data i godzina muszą pochodzić z zegara, również wewnątrz skrzynki, której nie można wyzerować, a która zachowa dokładny czas przez lata lub nawet przez dziesięciolecia.

4 Rozkład na czynniki i Logarytm dyskretny

4.1 Co to jest funkcja jednokierunkowa?

Funkcja jednokierunkowa jest funkcją matematyczną, która jest znacznie łatwiejsza do wykonania w jednym kierunku (w kierunku do przodu) niż w przeciwnym kierunku (kierunek odwrotny). Można na przykład obliczyć funkcję w minutach, ale tylko w stanie obliczyć odwrotność w miesiącach lub latach. Funkcja jednokierunkowa w postaci pułapki na drzwi jest funkcją jednokierunkową, w której odwrotny kierunek jest łatwy, jeśli znasz pewną informację (drzwi pułapki), ale trudniej inaczej.

4.2 Jakie znaczenie mają funkcje jednokierunkowe dla kryptografii?

Kryptosystemy klucza publicznego są oparte na (domniemanych) jednostronnych funkcjach pułapkowych. Klucz publiczny podaje informacje o konkretnym wystąpieniu funkcji; klucz prywatny podaje informacje o drzwiach pułapki. Ktokolwiek zna drzwi pułapki, może łatwo wykonać tę funkcję w obu kierunkach, ale każdy, kto nie ma drzwi pułapki, może wykonać tę funkcję tylko w kierunku do przodu. Kierunek do przodu służy do szyfrowania i weryfikacji podpisu; odwrotny kierunek służy do

odszyfrowywania i generowania sygnatur. W prawie wszystkich systemach klucza publicznego rozmiar klucza odpowiada wielkości wejść do funkcji jednokierunkowej; im większy klucz, tym większa różnica między wysiłkiem niezbędnym do obliczenia funkcji w kierunku do przodu i odwrotnie (dla kogoś, kto nie ma drzwi pułapki). Aby na przykład podpis cyfrowy był bezpieczny przez lata, konieczne jest użycie funkcji jednokierunkowej pułapki drzwiowej z wejściami wystarczająco dużymi, aby osoba bez drzwi pułapki potrzebowała wielu lat na obliczenie funkcji odwrotnej. Wszystkie praktyczne kryptosystemy z kluczem publicznym oparte są na funkcjach, które są uważane za jednokierunkowe, ale nie udowodniono, że tak jest. Oznacza to, że teoretycznie jest możliwe, że zostanie znaleziony algorytm, który może łatwo obliczyć odwrotność funkcji bez drzwi pułapki; rozwój ten spowodowałby, że każdy kryptosystem oparty na tej funkcji jednokierunkowej byłby niepewny i bezużyteczny.

4.3 Jaki jest problem faktoringu?

Faktoring jest aktem dzielenia liczby całkowitej na zbiór mniejszych liczb całkowitych (współczynników), które po pomnożeniu razem tworzą oryginalną liczbę całkowitą. Na przykład współczynniki 15 wynoszą 3 i 5; problem faktoringowy polega na znalezieniu 3 i 5, gdy są podane. 15. Podstawowa faktoryzacja wymaga podziału liczby całkowitej na czynniki, które są liczbami pierwszymi; każda liczba całkowita ma wyjątkową faktoryzację pierwotną. Pomnożenie dwóch liczb całkowitych razem jest łatwe, ale o ile wiemy, faktoring produktu jest znacznie trudniejszy.

4.4 Jakie znaczenie ma faktoring w kryptografii?

Faktoring to podstawowy, przypuszczalnie trudny problem, na którym opiera się kilka kryptosystemów klucza publicznego, w tym RSA. Faktoring modułu RSA (patrz pytanie 2.1) pozwoliłby intruzowi na ustalenie klucza prywatnego; w ten sposób każdy, kto może czynnik moduł, może odszyfrować wiadomości i fałszować podpisy. Bezpieczeństwo RSA zależy więc od trudnego problemu faktoringu. Niestety, nie udowodniono, że faktoring musi być trudny, i istnieje możliwość, że można łatwo znaleźć szybką i łatwą metodę faktoringową, chociaż badacze zajmujący się faktoringiem uważają tę możliwość za zdalną. Faktoring dużych liczb zajmuje więcej czasu niż faktoring mniejsze liczby. Właśnie dlatego wielkość modułu w RSA określa, jak bezpieczne jest rzeczywiste użycie RSA; im większy moduł, tym dłużej będzie on atakował, tym samym bardziej odporny na atak będzie implementacja RSA.

4.5 Czy faktoring stał się łatwiejszy?

Fakturowanie stało się łatwiejsze w ciągu ostatnich piętnastu lat z dwóch powodów: sprzęt komputerowy stał się potężniejszy i opracowano lepsze algorytmy faktoringowe. Ulepszenia sprzętu będą nadal nieubłagane, ale ważne jest, aby zdać sobie sprawę, że ulepszenia sprzętowe czynią RSA bezpieczniejszym, a nie mniejszym. Dzieje się tak dlatego, że udoskonalenie sprzętu, które pozwala intruzowi na zliczanie dwóch cyfr dłużej niż wcześniej, pozwoli jednocześnie legalnym użytkownikom RSA użyć klucza o dziesiątkach cyfr dłuższego niż poprzednio; użytkownik może wybrać nowy klucz kilkanaście razy dłużej niż stary bez spowolnienia wydajności, jednak atak faktoringowy stanie się znacznie trudniejszy. Tak więc chociaż ulepszenie sprzętu pomaga atakującemu, znacznie pomaga legalnym użytkownikom. Ta ogólna zasada może zawieść w tym sensie, że faktoring może odbywać się za pomocą szybkich maszyn przyszłości, atakując klucze RSA z przeszłości; w tym scenariuszu tylko atakujący ma przewagę w ulepszaniu sprzętu. To rozważanie przemawia za użyciem większego rozmiaru klucza dzisiaj, niż można by uznać za uzasadnione. Opowiada się również za zastąpieniem klucza RSA dłuższym kluczem co kilka lat, aby skorzystać z dodatkowego bezpieczeństwa oferowanego przez ulepszenia sprzętu. Ten punkt dotyczy również innych systemów klucza publicznego. Lepsze algorytmy faktoringu były bardziej pomocne dla atakującego RSA niż ulepszenia sprzętu. Ponieważ system RSA i ogólnie kryptografia przyciągnęły wiele uwagi, tak samo jest z problemem faktoringu, a wielu badaczy znalazło nowe metody faktoringowe lub ulepszyło je na innych. To ułatwiło faktoring,

dla liczb o dowolnej wielkości i niezależnie od szybkości sprzętu. Faktoring jest jednak nadal bardzo trudnym problemem. Ogólnie rzecz biorąc, każdy ostatni spadek bezpieczeństwa spowodowany poprawą algorytmu można zrekompensować zwiększeniem rozmiaru klucza. W rzeczywistości, pomiędzy ogólnymi ulepszeniami sprzętu komputerowego i usprawnieniami sprzętowymi RSA specjalnego przeznaczenia, zwiększenie klucza wielkości (utrzymywanie stałej prędkości operacji RSA) zachowało tempo lub przekroczyło wzrost wydajności algorytmu, nie powodując utraty bezpieczeństwa sieci. Tak długo, jak sprzęt będzie się poprawiał w szybszym tempie niż to, w którym zmniejsza się złożoność algorytmów faktoringowych, bezpieczeństwo RSA wzrośnie, zakładając, że użytkownicy RSA regularnie zwiększą swój rozmiar klucza o odpowiednie kwoty. Otwarte pytanie brzmi: ile można uzyskać szybszych algorytmów faktoringowych; musi istnieć pewne wewnętrzne ograniczenie prędkości faktoringu, ale ten limit pozostaje nieznany.

4.6 Jakie są najlepsze obecnie stosowane metody faktoringowe?

Faktoring jest bardzo aktywną dziedziną badań wśród matematyków i informatyków; najlepsze algorytmy faktoringowe są wymienione poniżej z pewnymi referencjami i ich dużą asymptotyczną wydajnością. Notacja O mierzy jak szybki jest algorytm; daje górną granicę liczby operacji (rzędu wielkości) w kategoriach n, liczby do uwzględnienia i p, współczynnika głównego n. Algorytmy faktoryzacji występują w dwóch smakach, specjalnym celu i ogólnym celu; wydajność tych pierwszych zależy od nieznanych czynników, podczas gdy wydajność tych ostatnich zależy od liczby, która ma być uwzględniona. Algorytmy specjalnego przeznaczenia są najlepsze do obliczania liczb z małymi czynnikami, ale liczby stosowane dla modułu w systemie RSA nie mają żadnych małych czynników. Dlatego algorytmy do faktoringu ogólnego są ważniejsze w kontekście systemów kryptograficznych i ich bezpieczeństwa. Algorytmy faktoringu specjalnego obejmują metodę Pollard rho, z przewidywanym czasem przebiegu O (sqrt (p)) oraz metodą Pollard p-1, z czasem biegu O (p '), gdzie p' jest największym czynnikiem 1. Oba wymagają czasu wykładniczego o wielkości p, pierwszorzędnego czynnika, który znajdują; dlatego te algorytmy są zbyt wolne dla większości zadań faktoringowych. Metoda krzywych eliptycznych (ECM) [50] jest lepsza od tych; jego asymptotyczny czas działania to O (exp (sqrt (2 ln pnnnnp))). ECM jest często wykorzystywana w praktyce do znajdowania czynników losowo generowanych liczb; nie jest wystarczająco silny, aby zważyć duży moduł RSA. Obecnie najlepszym algorytmem do faktoringu ogólnego jest sito pola liczbowego, które działa w czasie w przybliżeniu O (exp (1.9 (nn) ^ {1/3} (in n) ^ {2/3})). Niedawno został on wdrożony [15] i nie jest jeszcze wystarczająco praktyczny, aby wykonać najbardziej pożądane czynniki. Zamiast tego, najczęściej stosowanym algorytmem ogólnego przeznaczenia jest wielomianowy kwadratowy sito (mpqs), który ma czas działania O (exp (sqrt (ln n ln n ln n n))). Mpqs (i niektóre jego odmiany) jest jedynym algorytmem ogólnego zastosowania, który z powodzeniem uwzględnił liczby większe niż 110 cyfr; odmiana znana jako ppmpqs była szczególnie popularna. Oczekuje się, że w ciągu kilku lat sito pola liczbowego prześciga mpqs jako najszerzej stosowany algorytm faktoringu, ponieważ wielkość liczb uwzględnianych zwiększa się z około 120 cyfr, co jest bieżącym progiem liczb ogólnych, które można obliczyć , do 130 lub 140 cyfr. "Ogólny numer" to taki, w którym nie ma specjalnej formy, która mogłaby ułatwić czynność; moduł RSA jest liczbą ogólną. Zauważ, że 512-bitowy numer ma około 155 cyfr. Liczby, które mają specjalną formę, mogą już uwzględniać do 155 cyfr lub więcej. Projekt Cunningham śledzi rozkład liczb za pomocą tych specjalnych formularzy i utrzymuje listę pożądanych współczynników o nazwie "10 najbardziej poszukiwanych". Dobrym sposobem na sprawdzenie aktualnej zdolności faktoringu jest spojrzenie na ostatnie wyniki RSA Factoring Challenge.

4.7 Jakie są perspektywy teoretycznego przełomu w faktoringu?

Chociaż faktoring jest uważany za trudny problem matematyczny, nie zostało to udowodnione. Dlatego istnieje możliwość, że zostanie odkryty łatwy algorytm faktoringu. Ten rozwój, który mógłby poważnie

osłabić RSA, byłby bardzo zaskakujący i możliwość ta jest uważana za wyjątkowo odległą przez naukowców najbardziej aktywnie zaangażowanych w badania faktoringowe. Inną możliwością jest to, że ktoś udowodni, że faktoring jest trudny. Ten negatywny przełom jest prawdopodobnie bardziej prawdopodobny niż pozytywny przełom omawiany powyżej, ale byłby również nieoczekiwany w obecnym stanie teoretycznych badań faktoringowych. Ten rozwój zagwarantowałby bezpieczeństwo RSA poza pewną kluczową wielkością.

4.8 Co to jest RSA Factoring Challenge?

RSA Data Security Inc. (RSADSI) zarządza konkursem faktoringowym z kwartalnymi nagrodami pieniężnymi. Ci, którzy uwzględniają liczby wymienione przez RSADSI, zdobywają punkty w nagrodach; faktoring mniejsze liczby zarabia więcej punktów niż faktoring większe liczby. Wyniki konkursu mogą być przydatne dla osób, które chciałyby poznać stan faktyczny w faktoringu; wyniki pokazują rozmiar liczb uwzględnionych, które algorytmy są używane, i ile czasu było wymagane do zliczenia każdej liczby. Wyślij wiadomość e-mail na adres challenge-info@rsa.com, aby uzyskać informacje.

4.9 Co to jest problem dyskretnego logarytmu?

Dyskretny problem z logarytmami, w jego najbardziej rozpowszechnionym sformułowaniu, polega na znalezieniu wykładnika x we wzorze y = g ^ x mod p; innymi słowy, stara się odpowiedzieć na pytanie: Do jakiej potęgi należy dążyć, aby uzyskać y, modulo, pierwszą liczbę p? Istnieją również inne, bardziej ogólne sformułowania. Podobnie jak w przypadku problemu faktoringowego, dyskretny problem z logiem jest uważany za trudny, a także trudny w kierunku funkcji jednokierunkowej. Z tego powodu był on podstawą kilku kryptosystemów z kluczem publicznym, w tym systemu ElGamal i DSS. Dyskretny problem z logami ma taki sam związek z tymi systemami, jak faktoring dla RSA: bezpieczeństwo tych systemów opiera się na założeniu, że dyskretne logi są trudne do obliczenia. Dyskretny problem z logami wzbudził wiele uwagi w ostatnich latach; Najlepsze problemy z logowaniem dyskretnym przewidywały czasy działania podobne do najlepszych algorytmów faktoringowych. Rivest przeanalizował przewidywany czas na rozwiązanie dyskretnego dziennika zarówno pod względem mocy obliczeniowej, jak i pieniędzy.

4.10 Co jest łatwiejsze, faktoring lub dyskretny logarytm?

Asymptotyczny czas działania najlepszego algorytmu logicznego dyskretnego jest w przybliżeniu taki sam jak w przypadku najlepszego algorytmu do faktoringu ogólnego. Dlatego wymaga on tyle samo wysiłku, aby rozwiązać problem modulo dyskretnego logu z 512-bitową liczbą pierwszą, aby współczynnik 512-bitowego modułu RSA. W jednym z artykułów przytaczamy dowody eksperymentalne, że dyskretny problem z logami jest nieco trudniejszy niż faktoring: autorzy sugerują, że wysiłek potrzebny do zliczenia 110-cyfrowej liczby całkowitej jest taki sam jak wysiłek w celu rozwiązania logarytmów dyskretnych modulo 100-cio cyfrowy. Różnica ta jest tak niewielka, że nie powinna stanowić istotnego elementu przy wyborze kryptosystemu. Historycznie, było tak, że algorytmiczny postęp w logach problemowych, faktoringowych lub dyskretnych został zastosowany do drugiego. Sugeruje to, że stopnie trudności obu problemów są ze sobą ściśle powiązane i że każdy przełom, zarówno pozytywny, jak i negatywny, wpłynie w równym stopniu na oba problemy.

5 DES

5.1 Czym jest DES?

DES jest standardem szyfrowania danych, szyfrem bloków kodowania zdefiniowanym i zatwierdzonym przez rząd USA w 1977 r. Jako oficjalny standard; szczegóły można znaleźć w oficjalnej publikacji FIPS [59]. Pierwotnie został opracowany w IBM. DES był szeroko badany przez ostatnie 15 lat i jest

najbardziej znanym i powszechnie stosowanym kryptosystemem na świecie. DES to tajny klucz, symetryczny kryptosystem: gdy jest używany do komunikacji, zarówno nadawca, jak i odbiorca muszą znać ten sam tajny klucz, który jest używany zarówno do szyfrowania i odszyfrowywania wiadomości. DES może być również używany do szyfrowania pojedynczego użytkownika, na przykład do przechowywania plików na dysku twardym w postaci zaszyfrowanej. W środowisku wielu użytkowników bezpieczna dystrybucja kluczy może być trudna; Kryptografia klucza publicznego została wymyślona, aby rozwiązać ten problem. DES działa na 64-bitowych blokach z kluczem 56-bitowym. Został zaprojektowany do wdrożenia w sprzęcie, a jego działanie jest stosunkowo szybkie. Działa dobrze w przypadku szyfrowania zbiorczego, czyli do szyfrowania dużego zestawu danych. NIST ponownie certyfikował DES jako oficjalny standard szyfrowania w USA co pięć lat; DES był ostatnio recertyfikowany w 1993 r., Domyślnie. NIST wskazał jednak, że może ponownie nie recertyfikować DES.

5.2 Czy DES zostało złamane?

DES nigdy nie został "złamany", pomimo wysiłków wielu badaczy na przestrzeni wielu lat. Oczywistą metodą ataku jest wyczerpujące przeszukanie kluczowej przestrzeni; wymaga to średnio 2 ^ {55} kroków. Na początku zasugerowano, że bogaty i potężny wróg może zbudować komputer specjalnego przeznaczenia zdolny do złamania DES przez wyczerpujące poszukiwania w rozsądnym czasie. Później Hellman wykazał kompromis w zakresie pamięci czasu, który umożliwia ulepszenie w przypadku wyczerpujących poszukiwań, jeśli pamięć jest obfita, po wyczerpującym porównaniu. Pomysły te podsycały wątpliwości dotyczące bezpieczeństwa DES. Pojawiły się również zarzuty, że NSA celowo osłabiła DES. Pomimo tych podejrzeń, nie ma żadnego możliwego sposobu na złamanie DES szybciej niż odkryto wyczerpujące poszukiwania. Koszt wyspecjalizowanego komputera do wykonywania wyczerpujących poszukiwań został oszacowany przez Wienera na milion dolarów. Niedawno jednak pierwszy atak na DES, który jest lepszy niż wyczerpujące wyszukiwanie, został ogłoszony przez Eli Bihama i Adi Shamira przy użyciu nowej techniki znanej jako kryptoanaliza różnicowa. Ten atak wymaga szyfrowania 2 ^ {47} wybranych jawnych tekstów, tj. Tekstów jawnych wybranych przez atakującego. Chociaż teoretyczny przełom, atak ten nie jest praktyczny w normalnych okolicznościach, ponieważ wymaga od atakującego łatwego dostępu do urządzenia DES w celu zaszyfrowania wybranych jawnych tekstów. Kolejny atak, znany jako liniowa kryptoanaliza [51], nie wymaga wybranych tekstów jawnych. Konsensus jest taki, że DES, gdy jest właściwie używany, jest bezpieczny przed wszystkimi, oprócz najpotężniejszych wrogów. W rzeczywistości potrójne szyfrowanie DES może być bezpieczne w stosunku do kogokolwiek. Biham i Shamir oświadczyli, że uważają DES za bezpieczny. Jest szeroko stosowany w wielu systemach kryptograficznych, a większość implementacji kryptografii z kluczem publicznym zawiera DES na pewnym poziomie.

5.3 Jak bezpiecznie używać DES?

Podczas korzystania z DES istnieje kilka praktycznych uwag, które mogą mieć wpływ na bezpieczeństwo zaszyfrowanych danych. Należy często zmieniać klawisze DES, aby zapobiec atakom wymagającym ciągłej analizy danych. W kontekście komunikacji należy również znaleźć bezpieczny sposób komunikowania klucza DES zarówno z nadawcą, jak i odbiorcą. Wykorzystanie RSA lub innej techniki klucza publicznego do zarządzania kluczami rozwiązuje oba te problemy: dla każdej sesji generowany jest inny klucz DES, a bezpieczne zarządzanie kluczami zapewnia szyfrowanie klucza DES kluczem publicznym RSA odbiorcy. RSA, w takich okolicznościach, może być uważane za narzędzie do poprawy bezpieczeństwa DES (lub jakiegokolwiek innego tajnego klucza szyfrowego). Jeśli chce się używać DES do szyfrowania plików przechowywanych na dysku twardym, nie jest możliwe częste zmienianie kluczy DES, ponieważ wymagałoby to odszyfrowania, a następnie ponownego zaszyfrowania wszystkich plików po każdej zmianie klucza. Zamiast tego należy mieć główny klucz DES, za pomocą którego szyfruje się listę kluczy DES używanych do szyfrowania plików; można wtedy często zmieniać klucz

główny bez większego wysiłku. Potężną techniką zwiększania bezpieczeństwa DES jest potrójne szyfrowanie, czyli szyfrowanie każdego bloku komunikatów pod trzema różnymi klawiszami DES po kolei. Potwierdza się, że potrójne szyfrowanie jest równoważne dwukrotnemu podwojeniu klucza DES, do 112 bitów, i powinno zapobiegać odszyfrowywaniu przez wroga zdolnego do wyczerpującego wyszukiwania z jednym kluczem. Oczywiście użycie potrójnego szyfrowania zajmuje trzy razy więcej czasu niż pojedyncze szyfrowanie DES. Oprócz kwestii wymienionych powyżej, DES może być używany do szyfrowania w kilku oficjalnie zdefiniowanych trybach. Niektóre są bardziej bezpieczne niż inne. Tryb EBC (elektroniczny spis kodów) po prostu szyfruje każdy 64-bitowy blok tekstu zwykłego jeden po drugim w tym samym 56-bitowym kluczu DES. W trybie CBC (łańcuch bloków szyfru) każdy 64-bitowy blok tekstu jawnego jest XORed z poprzednim blokiem tekstu zaszyfrowanego przed jego zaszyfrowaniem przy pomocy klucza DES. Szyfrowanie każdego bloku zależy więc od poprzednich bloków, a ten sam 64-bitowy blok z jawnym tekstem może szyfrować do różnych szyfrogramów w zależności od kontekstu w całej wiadomości. Tryb CBC pomaga chronić się przed pewnymi atakami, chociaż nie w przypadku wyczerpujących poszukiwań lub kryptoanalizy różnicowej. Tryb CFB (feedback cipher) pozwala używać DES z blokami o długości mniejszej niż 64 bity. W praktyce CBC jest najczęściej stosowanym trybem DES i jest określona w kilku standardach. Dla dodatkowego bezpieczeństwa można użyć potrójnego szyfrowania z CBC, ale ponieważ pojedynczy DES w trybie CBC jest zwykle uważany za wystarczająco bezpieczny, potrójne szyfrowanie nie jest często używane

5.4 Czy DES może być eksportowany z USA?

Eksport DES, w sprzęcie lub oprogramowaniu, jest ściśle regulowany przez Departament Stanu USA i NSA (patrz Pytanie 1.6). Rząd rzadko akceptuje eksport DES, mimo że DES jest szeroko dostępny za granicą; instytucje finansowe i zagraniczne spółki zależne od firm amerykańskich są wyjątkami.

5.5 Jakie są alternatywy dla DES?

Z biegiem lat różne algorytmy szyfrowania zostały zaprojektowane jako alternatywy dla DES. Jednym z nich jest FEAL (Fast Encryption ALgorithm), szyfr, dla którego wykryto ataki, chociaż zaproponowano nowe wersje. Kolejny niedawno zaproponowany szyfr zaprojektowany przez Lai i Masseya i znany jako IDEA wydaje się obiecujący, chociaż nie otrzymał jeszcze wystarczającej analizy, aby wzbudzić pełne zaufanie do jego bezpieczeństwa. Niedawno rząd USA ogłosił nowy algorytm o nazwie Skipjack w ramach swojego projektu Capstone. Skipjack działa na 64-bitowych blokach danych, podobnie jak DES, ale wykorzystuje klucze 80-bitowe, w przeciwieństwie do 56-bitowych kluczy w DES. Szczegóły Skipjack są jednak sklasyfikowane, więc Skipjack jest dostępny tylko w sprzęcie od autoryzowanych przez rząd producentów. Rivest opracował szyfry RC2 i RC4, które mogą być tak bezpieczne, jak to konieczne, ponieważ używają zmiennych rozmiarów kluczy. Szybsze niż DES, przynajmniej w oprogramowaniu, mają dodatkową zaletę specjalnego statusu rządu USA, dzięki czemu uproszczenie eksportu jest przyspieszone, jeśli kluczowy rozmiar jest ograniczony do 40 bitów.

5.6 Czy DES to grupa?

Często pytano, czy szyfrowanie DES jest zamknięte pod skład; tj. szyfruje zwykły tekst pod jednym kluczem DES, a następnie szyfruje wynik pod innym kluczem zawsze równoważnym pojedynczemu szyfrowaniu pod jednym kluczem. Algebraicznie, czy DES to grupa? Jeśli tak, to DES może być słabszy niż w innym przypadku. Jednak odpowiedź brzmi: nie, DES nie jest grupą; kwestia ta została rozstrzygnięta dopiero niedawno, po wielu latach spekulacji i poszlak. Wynik ten zdaje się sugerować, że techniki takie jak potrójne szyfrowanie w rzeczywistości zwiększają bezpieczeństwo DES.

6 Capstone, Clipper i DSS

6.1 Co to jest Capstone?

Capstone to długofalowy projekt rządu USA, którego celem jest opracowanie zestawu norm dla publicznie dostępnej kryptografii, zgodnie z ustawą Computer Security Act z 1987 roku. Głównymi agencjami odpowiedzialnymi za Capstone są NIST i NSA (patrz sekcja 7). Plan zakłada, że elementy Capstone staną się oficjalnymi standardami rządu USA, w którym to przypadku zarówno rząd, jak i wszystkie prywatne firmy prowadzące interesy z rządem będą musiały stosować Capstone. Istnieją cztery główne składniki Capstone: ogólny algorytm szyfrowania danych, algorytm podpisu cyfrowego, protokół wymiany kluczy i funkcja skrótu. Algorytm szyfrowania danych nazywa się Skipjack (patrz pytanie 6.5), ale często nazywa się go Clipper, który jest chipem szyfrującym, który zawiera Skipjack (patrz pytanie 6.2). Algorytm podpisu cyfrowego to DSS (patrz pytanie 6.8), a funkcją skrótu jest SHS (patrz pytanie 8.4 dotyczące SHS i pytania 8.2 na temat funkcji skrótu). Protokół wymiany kluczy nie został jeszcze ogłoszony. Wszystkie części Capstone mają 80-bitową ochronę: wszystkie klucze mają długość 80 bitów, a inne aspekty są tak zaprojektowane, aby wytrzymać cokolwiek mniej niż "80-bitowy" atak, to znaczy wysiłek 2 ^ {80 } operacje. Ostatecznie rząd planuje umieścić cały system kryptograficzny Capstone na jednym chipie.

6.2 Czym jest Clipper?

Clipper to chip szyfrujący opracowany i sponsorowany przez rząd Stanów Zjednoczonych w ramach projektu Capstone (patrz pytanie 6.1). Ogłoszony przez Biały Dom w kwietniu 1993 r. [65] Clipper został zaprojektowany w celu zrównoważenia konkurujących ze sobą problemów federalnych organów ścigania z prywatnymi obywatelami i przemysłem. Organy ścigania chcą mieć dostęp do komunikacji podejrzanych przestępców, na przykład przez podsłuch; potrzeby te są zagrożone przez bezpieczną kryptografię. Jednak przemysł i obywatele chcą bezpiecznej komunikacji i szukają kryptografii. Technologia Clippera próbuje zrównoważyć te potrzeby za pomocą ukrytych kluczy. Chodzi o to, że komunikacja będzie szyfrowana bezpiecznym algorytmem, ale klucze będą przechowywane przez jedną lub więcej stron trzecich ("agencje depozytowe") i udostępniane organom ścigania, gdy uzyskają zezwolenie wydane przez sąd. nakaz. Tak więc, na przykład, komunikacja osobista byłaby niewrażliwa na rozrywkowe podsłuchy, a komunikacja handlowa nie byłaby odporna na szpiegostwo przemysłowe, a jednak FBI mogło podsłuchiwać podejrzanych terrorystów lub gangsterów. Clipper został zaproponowany jako standard rządu USA [62]; byłby wtedy używany przez każdego, kto prowadzi interesy z rządem federalnym, a także za komunikację wewnątrz rządu. Dla kogokolwiek innego użycie Clippera jest całkowicie dobrowolne.

6.3 Jak działa układ Clipper?

Chip Clippera zawiera algorytm szyfrowania o nazwie Skipjack, którego szczegóły nie zostały upublicznione. Każdy chip zawiera również unikalny 80-bitowy klucz U, który jest przechowywany w dwóch częściach w dwóch agencjach depozytowych; obie części muszą być znane, aby odzyskać klucz. Obecny jest również numer seryjny i 80-bitowy klucz rodzinny F; ten ostatni jest wspólny dla wszystkich układów Clippera. Chip jest produkowany w taki sposób, że nie można go poddać inżynierii wstecznej; oznacza to, że algorytmu Skipjack i kluczy nie można odczytać z układu. Gdy dwa urządzenia chcą się komunikować, najpierw zgadzają się na 80-bitowy klucz sesyjny K. Metoda, według której wybierają ten klucz, pozostaje w gestii podmiotu wdrażającego; metoda klucza publicznego, taka jak RSA lub Diffie-Hellman, wydaje się być prawdopodobnym wyborem. Wiadomość jest szyfrowana za pomocą klawisza K i wysyłana; zauważ, że klucz K nie jest zabezpieczony. Oprócz zaszyfrowanej wiadomości tworzony jest także inny element danych, nazywany polem dostępu do prawa (LEAF). Zawiera klucz sesji K zaszyfrowany za pomocą klucza jednostki U, a następnie połączony z numerem seryjnym nadawcy i ciągiem uwierzytelniającym, a następnie, w końcu, wszystkie zaszyfrowane kluczem

rodzinnym. Dokładne dane dotyczące dziedziny egzekwowania prawa są klasyfikowane. Odbiornik odszyfrowuje pole ścigania, sprawdza ciąg uwierzytelniania i odszyfrowuje wiadomość za pomocą klucza K. Przypuśćmy teraz, że organ ścigania chce dotknąć linii. Używa klucza rodziny do odszyfrowania pola egzekwowania prawa; agencja zna teraz numer seryjny i ma zaszyfrowaną wersję klucza sesji. Przedstawia upoważnienie dla dwóch agencji depozytowych wraz z numerem seryjnym. Agencje depozytowe przekazują dwie części klucza jednostki do organu ścigania, który następnie odszyfrowuje, aby uzyskać klucz sesji K. Teraz agencja może użyć K do odszyfrowania aktualnej wiadomości. Dalsze szczegóły operacji chipper Clipper, takie jak generowanie klucza jednostki, są naszkicowane przez Denninga

6.4 Kim są agencje depozytowe?

Nie ustalono jeszcze, które organizacje będą pełnić funkcję agencji depozytowych, czyli utrzymywać klucze chipowe Clippera. Żadna agencja egzekwująca prawo nie będzie agencją depozytową i możliwe jest, że co najmniej jedna z agencji depozytowych będzie organizacją poza rządem. Ważne jest, aby agencje depozytowe zachowywały kluczowe bazy danych w wyjątkowo bezpieczny sposób, ponieważ nieautoryzowany dostęp do obu baz danych może umożliwić nieautoryzowane podsłuchiwanie prywatnych komunikatów. W rzeczywistości agencje depozytowe są prawdopodobnie jednym z głównych celów dla każdego, kto próbuje skompromitować system Clipper; fabryka Clipperów to kolejny prawdopodobny cel.

6.5 Czym jest Skipjack?

Skipjack to algorytm szyfrowania zawarty w układzie Clipper; został zaprojektowany przez NSA. Używa klucza 80-bitowego do szyfrowania 64-bitowych bloków danych; ten sam klucz jest używany do deszyfrowania. Skipjack może być używany w tych samych trybach, co DES, i może być bezpieczniejszy niż DES, ponieważ używa 80-bitowych kluczy i szyfruje dane dla 32 kroków lub "rund"; przeciwnie, DES używa 56-bitowych kluczy i szyfruje dane tylko przez 16 rund. Szczegóły Skipjack są klasyfikowane. Decyzja o niepublicznym udostępnianiu szczegółów algorytmu była szeroko krytykowana. Wiele osób podejrzewa, że Skipjack nie jest bezpieczny, albo ze względu na nadzór projektantów, albo przez celowe wprowadzenie tajnego zapadni. W przeciwieństwie do tego, wiele lat próbowało znaleźć słabości DES przez lata, ponieważ jego szczegóły są publiczne. Te liczne próby (i fakt, że zawiodły) sprawiły, że ludzie są pewni bezpieczeństwa DES. Ponieważ Skipjack nie jest publiczny, ta sama analiza nie może być zastosowana do niego, a zatem nie może powstać odpowiedni poziom zaufania. Zdając sobie sprawę z takiej krytyki, rząd zaprosił niewielką grupę niezależnych kryptologów do zbadania algorytmu Skipjack. Wydali raport, w którym stwierdzono, że chociaż ich badania są zbyt ograniczone, aby osiągnąć ostateczny wniosek, to jednak uważają, że Skipjack jest bezpieczny. Inną konsekwencją tajnego statusu Skipjack jest to, że nie można go zaimplementować w oprogramowaniu, a jedynie w sprzęcie przez autoryzowanych przez rząd producentów układów.

6.6 Dlaczego Clipper jest kontrowersyjny?

Propozycja chipa Clippera wzbudziła wiele kontrowersji i była przedmiotem wielu krytyki. Niestety, dwa różne problemy zostały zdezorientowane w dużej liczbie publicznych komentarzy i dyskusji. Najpierw kontrowersje na temat całej idei kluczy depozytowych. Osoby popierające klucze depozytowe postrzegają je jako sposób na zapewnienie bezpiecznej komunikacji dla ogółu społeczeństwa, a jednocześnie umożliwiają organom ścigania monitorowanie komunikacji podejrzanych o przestępstwa. Przeciwnicy ukrytych kluczy postrzegają to jako niepotrzebne i nieskuteczne wtargnięcie rządu w prywatne życie obywateli. Twierdzą, że deponowane klucze naruszają ich prawa do prywatności i wolności słowa. To zajmie dużo czasu i wiele publicznych dyskusji dla społeczeństwa, aby dojść do konsensusu co do tego, jaką rolę powinny mieć klucze powiernicze.

Drugi obszar kontrowersji dotyczy różnych zastrzeżeń do konkretnej propozycji Clippera, to jest zastrzeżeń do tej konkretnej implementacji kluczy depozytowych, w przeciwieństwie do idei kluczy depozytowych w ogóle. Typowe zastrzeżenia: algorytm Skipjack nie jest publiczny i może nie być bezpieczny; kluczowe agencje depozytowe będą podatne na atak; nie ma wystarczającej liczby kluczowych agencji depozytowych; klawisze na chipach Clippera nie są generowane w wystarczająco bezpieczny sposób; nie będzie wystarczającej konkurencji wśród podmiotów wdrażających, co spowoduje kosztowne i powolne układy; implementacje oprogramowania nie są możliwe; a rozmiar klucza jest stały i nie można go zwiększyć w razie potrzeby. Niedawno Micali zaproponowała alternatywny system, który również próbuje zrównoważyć obawy dotyczące prywatności przestrzegających prawo obywateli, z kwestiami dochodzeniowymi organów ścigania. Nazwana kryptografia z kluczem publicznym jest podobna pod względem funkcji i celu do propozycji chipa Clippera, ale użytkownicy mogą wybrać własne klucze, które rejestrują w agencjach depozytowych. Ponadto system nie wymaga bezpiecznego sprzętu i może być całkowicie zaimplementowany w oprogramowaniu.

6.7 Jaki jest obecny status Clippera?

Clipper jest w trakcie przeglądu. Zarówno branża wykonawcza, jak i Kongres zastanawiają się nad tym, a panel doradczy zalecił niedawno całoroczną publiczną dyskusję na temat zasad kryptografii. NIST zaprosił społeczeństwo do wysyłania komentarzy w ramach własnej recenzji.

6.8 Czym jest DSS?

DSS to proponowany standard podpisu cyfrowego, który określa algorytm podpisu cyfrowego (DSA) i jest częścią projektu Capstone rządu USA. Został wybrany przez NIST, we współpracy z NSA, jako cyfrowy standard uwierzytelniania rządu USA; czy rząd powinien go przyjąć, ponieważ oficjalna norma jest nadal przedmiotem debaty. DSS opiera się na dyskretnym logowaniu i pochodzi z kryptosystemów zaproponowanych przez Schnorr i ElGamal. Dotyczy tylko uwierzytelniania. DSS w przeważającej części było postrzegane niekorzystnie przez przemysł komputerowy, z czego wiele miało nadzieję, że rząd wybierze algorytm RSA jako oficjalny standard; RSA jest najczęściej stosowanym algorytmem uwierzytelniania. Kilka artykułów w prasie, takich jak, omawia niezadowolenie branży z DSS. Krytyka DSS skupiła się na kilku głównych kwestiach: brak kluczowej zdolności wymiany; podstawowy kryptosystem jest zbyt aktualny i został poddany zbyt małej analizie, aby użytkownicy byli pewni jego siły; weryfikacja podpisów z DSS przebiega zbyt wolno; istnienie drugiego standardu uwierzytelniania spowoduje trudności dla dostawców sprzętu komputerowego i oprogramowania, którzy już ujednolicili na RSA; oraz że proces, w którym NIST wybrał DSS, był zbyt tajemniczy i arbitralny, a NSA miał zbyt duży wpływ. Inne krytyczne uwagi zostały skierowane przez NIST, modyfikując pierwotną propozycję. W systemie DSS generowanie sygnatur jest szybsze niż weryfikacja podpisu, podczas gdy w systemie RSA weryfikacja podpisu jest szybsza niż generowanie sygnatur (jeśli do tej właściwości wybrano publicznych i prywatnych wykładników, co ma zwykle miejsce). NIST twierdzi, że zaletą DSS jest to, że podpisywanie jest szybsze, ale wiele osób w kryptografii uważa, że lepiej jest, aby weryfikacja była szybszą operacją.

6.9 Czy DSS jest bezpieczny?

Najpoważniejsza krytyka DSS dotyczy jego bezpieczeństwa. Program DSS został pierwotnie zaproponowany ze stałym 512-bitowym rozmiarem klucza. Po wielu krytycjach, że nie jest to wystarczająco bezpieczne, NIST zrewidował DSS, aby umożliwić kluczom wielkości do 1024 bitów. Bardziej krytyczny jest jednak fakt, że DSS nie był wystarczająco długi, aby wytrzymać wielokrotne próby jego złamania; chociaż dyskretny problem z logami jest stary, to po raz pierwszy zaproponowano zastosowanie kryptograficznego zastosowania problemu w DSS w 1989 r. przez Schnorr i nie otrzymał

on zbyt wielu publicznych badań. Ogólnie rzecz biorąc, każdy nowy kryptosystem może mieć poważne wady, które zostały odkryte dopiero po latach analizowania przez kryptografów. Rzeczywiście zdarzyło się to wiele razy w przeszłości. RSA od ponad 15 lat intensywnie badała słabości. Wobec braku matematycznych dowodów bezpieczeństwa nic nie buduje zaufania do kryptosystemu, jak ciągłe próby jego złamania. Chociaż DSS może okazać się silnym kryptosystemem, jego stosunkowo krótka historia pozostawi wątpliwości na długie lata. Niektórzy badacze ostrzegali przed istnieniem "pułapek" w PRS, które mogłyby umożliwić łatwe złamanie klucza. Te wstępne zapadki są jednak stosunkowo rzadkie i można je łatwo uniknąć, jeśli zostaną zastosowane odpowiednie procedury generowania kluczy.

6.10 Czy korzystanie z DSS jest objęte jakimikolwiek patentami?

NIST złożył wniosek patentowy dla DSS i pojawiły się zarzuty, że DSS jest objęty innymi patentami o kluczowym znaczeniu. NIST ogłosił niedawno zamiar przyznania wyłącznych praw do sublicencjonowania patentu DSS na rzecz Public Key Partners (PKP), który posiada również prawa do udzielania sublicencji na inne patenty, które mogą obejmować DSS. W umowie między NIST a PKP, PKP publicznie stwierdziło jednolite który wyda licencje na wykonywanie DSS. PKP stwierdził, że DSS może być używany bez opłat licencyjnych w przypadku osobistego, niekomercyjnego lub wykorzystania przez rząd USA.

6.11 Jaki jest obecny status DSS?

Po tym, jak NIST wydał wniosek DSS w sierpniu 1991 r., Był okres, w którym zwrócono się do opinii publicznej; NIST dokonał następnie zmiany swojej propozycji w świetle komentarzy. DSS może być wydany jako FIPS i stać się oficjalnym standardem rządu USA, ale nie jest jasne, kiedy to się zdarzy. Obecnie DSS staje się standardem, wraz z RSA, dla branży usług finansowych; najnowszy projekt standardu zawiera poprawioną wersję DSS.

7 NIST i NSA

7.1 Co to jest NIST?

NIST jest akronimem dla National Institute of Standards and Technology, oddziału Departamentu Handlu USA; był wcześniej znany jako National Bureau of Standards (NBS). Poprzez swoje Laboratorium Systemów Komputerowych ma na celu promowanie otwartych systemów i interoperacyjności, które pobudzą rozwój komputerowej działalności gospodarczej. NIST wydaje standardy i wytyczne, które mają być przyjęte przez wszystkie systemy komputerowe w USA, a także sponsoruje warsztaty i seminaria. Oficjalne standardy publikowane są jako FIPS (Federal Information Processing Standards). W 1987 roku Kongres przyjął ustawę Computer Security Act, która upoważniła NIST do opracowania standardów zapewniających bezpieczeństwo wrażliwych, ale niesklasyfikowanych informacji w rządowych systemach komputerowych. Zachęcił NIST do współpracy z innymi agencjami rządowymi i prywatnym przemysłem w zakresie oceny proponowanych standardów bezpieczeństwa komputerowego.

7.2 Jaką rolę odgrywa NIST w kryptografii?

NIST wydaje standardy dla procedur kryptograficznych; Amerykańskie agencje rządowe muszą z nich korzystać, a sektor prywatny często również je przyjmuje. W styczniu 1977 r. NIST uznał DES za oficjalny standard szyfrowania w USA i opublikował go jako publikację FIPS 46; DES wkrótce stał się standardem de facto w USA. Kilka lat temu NIST został poproszony o wybranie zestawu standardów kryptograficznych dla USA; stało się to znane jako projekt Capstone (patrz rozdział 6). Po kilku latach raczej skrytych rozważań i we współpracy z NSA, NIST przedstawił propozycje różnych standardów kryptografii, w tym cyfrowych podpisów (DSS) i szyfrowania danych (chip Clipper); są to fragmenty

całego projektu Capstone. NIST został skrytykowany za umożliwienie NSA zbyt wiele uprawnień w ustalaniu standardów kryptograficznych, ponieważ interesy NSA są sprzeczne z interesami Departamentu Handlu i NIST. Jednak NSA ma znacznie więcej doświadczenia z kryptografią i wieloma innymi wykwalifikowanymi kryptografami i kryptoanalitykami, niż NIST; nierealistyczne byłoby oczekiwać, że NIST zrezygnuje z takiej dostępnej pomocy.

7.3 Czym jest NSA?

NSA jest Narodową Agencją Bezpieczeństwa, wysoce tajną agencją rządu USA, którą stworzył Harry Truman w 1952 r .; jego istnienie było utrzymywane w tajemnicy przez wiele lat. NSA ma mandat do wysłuchania i odkodowania wszystkich zagranicznych komunikatów będących przedmiotem zainteresowania dla bezpieczeństwa Stanów Zjednoczonych. Wykorzystywał on także swoją władzę na różne sposoby, aby spowolnić rozpowszechnianie publicznie dostępnej kryptografii, aby uniemożliwić wrogim krajom stosowanie metod szyfrowania zbyt silnych, aby NSA mogło się zepsuć. Jako najważniejsza agencja rządowa zajmująca się kryptografią, NSA ma ogromne zasoby finansowe i komputerowe oraz zatrudnia wielu kryptografów. Zmiany w kryptografii osiągnięte w NSA nie są upubliczniane; Ta tajemnica doprowadziła do wielu plotek na temat zdolności NSA do przełamywania popularnych kryptosystemów takich jak DES, a także do plotek, że NSA potajemnie umieszczała słabości, zwane drzwiami pułapki, w wspieranych przez rząd kryptosystemach, takich jak DES. Plotki te nigdy nie zostały udowodnione ani obalone, a kryteria stosowane przez NSA przy wyborze standardów kryptografii nigdy nie zostały upublicznione. Ostatnie postępy w branży komputerowej i telekomunikacyjnej sprawiły, że działania NSA zostały poddane bezprecedensowej analizie, a agencja stała się obiektem ostrej krytyki za utrudnianie przemysłu w USA, który chce używać lub sprzedawać silne narzędzia kryptograficzne. Dwoma głównymi przyczynami tej zwiększonej krytyki są upadek Związku Radzieckiego oraz rozwój i rozpowszechnianie dostępnych komercyjnie narzędzi kryptograficznych o kluczu publicznym. Pod presją NSA może zostać zmuszony do zmiany swojej polityki.

7.4 Jaką rolę odgrywa NSA w komercyjnej kryptografii?

Karta NSA ogranicza działalność do wywiadu zagranicznego. Jednak NSA zajmuje się rozwojem komercyjnej kryptografii, ponieważ dostępność silnych narzędzi szyfrujących za pośrednictwem kanałów komercyjnych może przeszkodzić misji NSA w zakresie dekodowania komunikacji międzynarodowej; innymi słowy, NSA martwi się, że silna komercyjna kryptografia nie wpadnie w niepowołane ręce. NSA oświadczyła, że nie ma zastrzeżeń do stosowania bezpiecznej kryptografii przez przemysł amerykański. Nie ma również zastrzeżeń do narzędzi kryptograficznych używanych do uwierzytelniania, w przeciwieństwie do prywatności. Jednak NSA jest szeroko postrzegana jako następujące polityki, które mają praktyczny wpływ na ograniczenie i / lub osłabienie narzędzi kryptograficznych stosowanych przez przestrzegających prawo obywateli i korporacje USA; NSA wywiera wpływ na komercyjną kryptografię na kilka sposobów. Po pierwsze, kontroluje eksport kryptografii z USA; NSA generalnie nie zatwierdza wywozu produktów używanych do szyfrowania, chyba że kluczowy rozmiar jest ściśle ograniczony. Jednakże zezwala na eksport wszelkich produktów używanych tylko do uwierzytelniania, bez względu na wielkość klucza, o ile nie można przekonwertować produktu na szyfrowanie. NSA zablokowała również publikowanie lub opatentowanie metod szyfrowania, powołując się na zagrożenie bezpieczeństwa narodowego; Ponadto NSA pełni rolę doradcy wobec NIST przy ocenie i selekcji oficjalnych standardów bezpieczeństwa komputerowego w USA; w tym charakterze odegrał znaczącą i kontrowersyjną rolę w wyborze DES oraz w rozwoju grupy standardów znanych jako projekt Capstone, który obejmuje DSS i chip Clipper. NSA może również wywierać presję rynkową na firmy amerykańskie, aby produkowały (lub powstrzymywały się od produkcji) towary kryptograficzne, ponieważ sama NSA często jest dużym

klientem tych firm. Kryptografia jest w oczach opinii publicznej jak nigdy dotąd i stała się przedmiotem publicznej debaty publicznej. Status kryptografii i rola NSA w niej prawdopodobnie ulegną zmianie w ciągu najbliższych kilku lat.

8 Różne

8.1 Jaki jest status prawny dokumentów podpisanych cyfrowymi podpisami?

Jeżeli podpis cyfrowy ma zastąpić podpis odręczny, musi mieć taki sam status prawny jak podpisy odręczne, tzn. Dokumenty podpisane podpisem cyfrowym muszą być prawnie wiążące. NIST stwierdził, że proponowana przez niego norma dotycząca podpisu elektronicznego powinna umożliwiać "udowodnienie stronie trzeciej, że dane zostały faktycznie podpisane przez generator podpisu." "Ponadto, zamówienia rządowe federalnego rządu USA będą podpisywane przez każdy taki standard; oznacza to, że rząd będzie wspierać legalne upoważnienie podpisów cyfrowych w sądach. Niektóre wstępne badania prawne zaowocowały również opinią, że podpis cyfrowy spełnia wymagania prawnie wiążących podpisów do większości celów, w tym do użytku komercyjnego, jak określono w jednolitym kodeksie handlowym (UCC). Decyzja GAO (Government Accounting Office), o którą wnioskuje NIST, również wyraża opinię, że podpis cyfrowy spełnia standardy prawne odręcznych podpisów. Ponieważ jednak ważność dokumentów z podpisami cyfrowymi nigdy nie została zakwestionowana w sądzie, ich status prawny nie jest jeszcze dobrze zdefiniowany. Poprzez takie wyzwania sądy wydadzą orzeczenia, które wspólnie określają, które metody podpisu cyfrowego, kluczowe rozmiary i środki bezpieczeństwa są dopuszczalne, aby podpis cyfrowy był prawnie wiążący. Podpisy cyfrowe mogą posiadać większą władzę prawną niż podpisy odręczne. Jeśli dziesięciostronicowa umowa jest podpisana ręcznie na dziesiątej stronie, nie można mieć pewności, że pierwszych dziewięć stron nie zostało zmienionych. Jeśli jednak umowa została podpisana cyfrowymi podpisami, strona trzecia może sprawdzić, czy nie zmienił się jeden bajt umowy. Obecnie, jeśli dwie osoby chcą cyfrowo podpisać serię umów, mogą najpierw podpisać umowę papierową, w której wyrażą zgodę na związanie się w przyszłości umowami cyfrowymi podpisanymi przez nich przy pomocy określonej metody podpisu i minimalnej wielkości klucza.

8.2 Co to jest funkcja skrótu? Co to jest skrót wiadomości?

Funkcja skrótu to obliczenie, które pobiera dane wejściowe o zmiennych rozmiarach i zwraca ciąg o stałym rozmiarze, który jest nazywany wartością mieszania. Jeśli funkcja hash jest jednokierunkowa, tzn. Trudna do odwrócenia, jest również nazywana funkcją skrótu komunikatu, a wynik nazywany jest skrótem wiadomości. Chodzi o to, że skrót jest zwięzłą dłuższą wiadomością lub dokumentem, z którego został obliczony; można pomyśleć o skrócie wiadomości jako "cyfrowym odcisku palca" większego dokumentu. Przykładami dobrze znanych funkcji skrótu są MD4, MD5 i SHS. Chociaż funkcje skrótu mają na ogół wiele zastosowań w programach komputerowych, w kryptografii są one używane do generowania małego ciągu znaków (skrótu wiadomości), który może bezpiecznie reprezentować znacznie większy ciąg, taki jak plik lub wiadomość. Ponieważ funkcje mieszające są szybsze niż funkcje podpisywania, znacznie wydajniejsze jest obliczanie podpisu cyfrowego za pomocą skrótu wiadomości dokumentu, który jest mały, niż za pomocą samowolnie dużego dokumentu. Ponadto podsumowanie może zostać upublicznione bez ujawniania zawartości dokumentu, z którego pochodzi. Jest to ważne w cyfrowym znakowaniu czasem, w którym za pomocą funkcji skrótu można uzyskać znacznik czasu dokumentu bez ujawniania jego zawartości serwisowi znakowania czasem. Funkcja skrótu używana do cyfrowego uwierzytelniania musi mieć określone właściwości, które sprawiają, że jest ona wystarczająco bezpieczna do użytku kryptograficznego. W szczególności musi być niemożliwe znalezienie komunikatu, który ma wartości mieszane i nie można znaleźć dwóch różnych komunikatów, które będą mieszały z tą samą wartością. Możliwość znalezienia skrótu wiadomości o danej wartości

umożliwi atakującemu zastąpienie fałszywej wiadomości prawdziwą wiadomością, która została podpisana. Umożliwiłoby to również fałszywemu odrzuceniu wiadomości, twierdząc, że faktycznie podpisał ona inną wiadomość o tej samej wartości, naruszając w ten sposób własność podpisów cyfrowych niezaprzeczalności. Możliwość znalezienia dwóch różnych komunikatów mieszających się do tej samej wartości może umożliwić atak, w wyniku którego ktoś zostanie oszukiwany w podpisaniu wiadomości, która ma wartości o tej samej wartości co inna wiadomość o zupełnie innym znaczeniu. W związku z tym skrót musi być wystarczająco długi, aby uniemożliwić napastnikowi wykonanie wyczerpujących poszukiwań kolizji. Na przykład, jeśli funkcja skrótu generuje ciągi 100-bitowe, wyszukiwanie kompletne wymagałoby przeciętnie 2 ^ {100} prób dopasowania do podanej wartości, a około 2 ^ {50} próbuje średnio znaleźć dwa dane wejściowe wytwarzające to samo podsumowanie. System podpisu elektronicznego może zostać złamany przez zaatakowanie albo trudnego problemu matematycznego, na którym opiera się metoda sygnatury, albo funkcji skrótu używanej do tworzenia podsumowań wiadomości. Wybierając system uwierzytelniania, ogólnie dobrym pomysłem jest wybranie metody podpisu i funkcji mieszania, która wymaga porównywalnych wysiłków w celu zerwania; jakiekolwiek dodatkowe zabezpieczenie jednego z dwóch komponentów jest marnowane, ponieważ ataki będą kierowane na słabszy komponent. W rzeczywistości atakowanie funkcji haszującej jest trudniejsze w praktyce, ponieważ wymaga dużej ilości pamięci i umiejętności oszukiwania ofiary do podpisania specjalnej wiadomości. W przypadku operacji 2 ^ {64} atakujący może znaleźć dwie wiadomości, które są mieszane z tym samym skrótem w dowolnej funkcji skrótu MD; wysiłek ten jest porównywalny z wysiłkiem niezbędnym do złamania 512-bitowego RSA; dlatego MD5 jest dobrym wyborem przy użyciu RSA z 512-bitowym modułem. Jednak ci, którzy mają większe potrzeby w zakresie bezpieczeństwa, na przykład instytucje certyfikujące, powinni użyć dłuższego modułu i funkcji mieszania, która zapewnia dłuższe streszczenie wiadomości; albo SHS (160-bitowy skrót), albo zmodyfikowana wersja MD4, która generuje 256-bitowy skrót, będzie wystarczająca.

8.3 Co to są MD2, MD4 i MD5?

MD2, MD4 i MD5 (MD oznacza Message Digest) są szeroko stosowanymi funkcjami hash zaprojektowanymi przez Rona Rivesta specjalnie do zastosowań kryptograficznych. Produkują 128-bitowe produkty trawiące i nie ma znanego ataku szybciej niż wyczerpujące wyszukiwanie. MD2 jest najwolniejszym z trzech; MD4 jest najszybszy. MD5 został nazwany "MD4 z paskami bezpieczeństwa" przez Rivest, ponieważ ma bardziej konserwatywny wzór niż MD4; konstrukcja zapewnia zwiększone bezpieczeństwo przed atakiem, ale kosztem około 33% wolniej niż MD4. MD5 jest najczęściej używanym z trzech algorytmów. MD4 i MD5 są publicznie dostępne do nieograniczonego użytku; MD2 jest dostępny do użytku z PEM. Szczegóły MD2, MD4 i MD5 z przykładowym kodem C są dostępne w Internetowych RFC (Requests For Comments) 1319, 1320 i 1321, odpowiednio. Nie znaleziono możliwych do wykonania ataków na żaden z algorytmów MD, chociaż niektóre ostatnie prace teoretyczne wykazały pewne interesujące właściwości strukturalne

8.4 Co to jest SHS?

Standard Secure Hash (SHS) to funkcja hashowana zaproponowana przez NIST i przyjęta jako standard rządowy USA. Jest i jest częścią rządowego projektu CapstoneSHS generuje 160-bitową wartość mieszającą z danych wejściowych o zmiennych rozmiarach. SHS jest strukturalnie podobny do MD4 i MD5. Jest on mniej więcej o 25% wolniejszy od MD5, ale może być bezpieczniejszy, ponieważ generuje skrócenie wiadomości o 25% dłuższe niż w przypadku funkcji MD. SHS jest obecnie jedyną częścią Capstone, która została oficjalnie przyjęta jako standard rządowy.

8.5 Czym jest Kerberos?

Kerberos to tajny system uwierzytelniania sieci opracowany w MIT; używa DES do szyfrowania i uwierzytelniania. W przeciwieństwie do systemu uwierzytelniania z kluczem publicznym nie generuje podpisów cyfrowych: protokół Kerberos został zaprojektowany do uwierzytelniania żądań zasobów sieciowych zamiast do uwierzytelniania autorstwa dokumentów. Kerberos zapewnia uwierzytelnianie w czasie rzeczywistym w środowisku rozproszonym, ale nie zapewnia przyszłej weryfikacji dokumentów przez zewnętrzną stronę. W systemie Kerberos istnieje określona strona w sieci, zwana serwerem Kerberos, która wykonuje scentralizowane zarządzanie kluczami i funkcje administracyjne. Serwer utrzymuje bazę danych zawierającą tajne klucze wszystkich użytkowników, generuje klucze sesji, gdy dwóch użytkowników chce się bezpiecznie komunikować i uwierzytelnia tożsamość użytkownika żądającego pewnych usług sieciowych. Kerberos, podobnie jak inne systemy z kluczem tajnym, wymaga zaufania do strony trzeciej, w tym przypadku serwera Kerberos. Jeśli serwer został naruszony, integralność całego systemu spadłaby. Kryptografia klucza publicznego została zaprojektowana właśnie w celu uniknięcia konieczności zaufania stronom trzecim lub linii komunikacyjnych. Kerberos może być odpowiedni dla tych, którzy nie potrzebują bardziej niezawodnych funkcji i właściwości systemów klucza publicznego.

8.6 Czym są RC2 i RC4?

RC2 i RC4 to funkcje szyfrowania o zmiennych kluczach zaprojektowane przez Rona Rivesta do szybkiego szyfrowania zbiorczego. Są alternatywą dla DES i są tak szybkie lub szybsze niż DES. Mogą być bardziej bezpieczne niż DES ze względu na ich zdolność do używania długich rozmiarów kluczy; mogą być również mniej bezpieczne niż DES, jeśli używane są krótkie rozmiary kluczy. RC2 jest symetrycznym blokowym szyfrowaniem o zmiennych kluczach i może służyć jako zamienny zamiennik dla DES, na przykład w eksportowych wersjach produktów, które inaczej używają DES. RC2 może być używany w tych samych trybach co DES, w tym potrójnego szyfrowania. RC2 jest około dwa razy szybszy od DES, przynajmniej w oprogramowaniu. RC4 jest szyfrem symetrycznym o zmiennym kluczu i jest 10 lub więcej razy szybszy niż DES w oprogramowaniu. Zarówno RC2, jak i RC4 są bardzo kompaktowe pod względem wielkości kodu. Umowa między Software Publishers Association (SPA) a rządem USA nadaje specjalny status RC2 i RC4, dzięki czemu proces zatwierdzania eksportu jest prostszy i szybszy niż zwykły proces eksportu kryptograficznego. Jednakże, aby zakwalifikować się do szybkiego zatwierdzenia eksportu, produkt musi ograniczyć rozmiary kluczy RC2 i RC4 do 40 bitów; 56 bitów jest dozwolone dla zagranicznych spółek zależnych i zagranicznych biur spółek amerykańskich. Dodatkowy 40-bitowy łańcuch, zwany solą, może zostać wykorzystany do udaremnienia napastnikom, którzy próbują wstępnie obliczyć dużą tabelę przeglądową możliwych zaszyfrowań. Sól jest dołączana do klucza szyfrującego, a ten przedłużony klucz służy do szyfrowania wiadomości; sól jest następnie wysyłana, niezaszyfrowana, z wiadomością. RC2 i RC4 były szeroko stosowane przez programistów, którzy chcą eksportować swoje produkty; DES prawie nigdy nie jest zatwierdzony do eksportu. RC2 i RC4 są zastrzeżonymi algorytmami RSA Data Security, Inc .;

8.7 Co to jest PEM?

PEM jest standardem Internet-Enhanced Mail, zaprojektowanym, proponowanym, ale jeszcze nie oficjalnie przyjętym, przez Internetową Radę ds. Działań w celu zapewnienia bezpiecznej poczty elektronicznej przez Internet. Zaprojektowany do pracy z aktualnymi formatami internetowych wiadomości e-mail, PEM obejmuje szyfrowanie, uwierzytelnianie i zarządzanie kluczami oraz umożliwia korzystanie z kryptosystemów z kluczem publicznym i tajnym kluczem. Obsługiwanych jest wiele narzędzi kryptograficznych: dla każdej wiadomości e-mail określony jest określony algorytm szyfrowania, algorytm podpisu cyfrowego, funkcja skrótu itd. W nagłówku. PEM wyraźnie obsługuje tylko kilka algorytmów kryptograficznych; inne można dodać później. DES w trybie CBC jest obecnie jedynym obsługiwanym algorytmem szyfrowania wiadomości, a do zarządzania kluczami są

obsługiwane zarówno RSA, jak i DES. PEM wspiera również korzystanie z certyfikatów, potwierdzając standard CCITT X.509 dla struktury certyfikatu. Szczegóły PEM można znaleźć w Internetowych dokumentach RFC (Żądania Komentarze) od 1421 do 1424. PEM prawdopodobnie zostanie oficjalnie przyjęty przez Radę ds. Działań Internetowych w ciągu jednego roku. Trusted Information Systems opracował bezpłatną niekomercyjną implementację PEM, a wkrótce będą również dostępne inne implementacje.

8.8 Czym jest RIPEM?

RIPEM to program opracowany przez Marka Riordana, który umożliwia bezpieczną internetową pocztę elektroniczną; zapewnia zarówno szyfrowanie, jak i podpisy cyfrowe, używając RSA i procedur DES z RSAREF (patrz Pytanie 8.10). RIPEM nie jest w pełni zgodny z PEM; na przykład obecnie nie obsługuje certyfikatów. Jednak przyszłe wersje będą zawierać certyfikaty i będą w pełni zgodne ze standardem PEM. RIPEM jest dostępny bezpłatnie do użytku niekomercyjnego w USA i Kanadzie. Aby uzyskać RIPEM, uzyskaj konto ftp na stronie ripem.msu.edu.

8.9 Czym jest PKCS?

PKCS (Public Cryptography Standards) to zestaw standardów do implementacji kryptografii z kluczem publicznym. Został wydany przez RSA Data Security, Inc. we współpracy z konsorcjum przemysłu komputerowego, w tym Apple, Microsoft, DEC, Lotus, Sun i MIT. PKCS jest cytowany przez OIW (Warsztat wdrożeniowy OSI) jako metoda wdrażania standardów OSI. PKCS jest kompatybilny z PEM, ale wykracza poza PEM. Na przykład, gdy PEM może obsługiwać tylko dane ASCII, to PKCS jest również przeznaczony dla danych binarnych. PKCS jest również zgodny ze standardem CCITT X.509. PKCS obejmuje zarówno standardy implementacji algorytmów, jak i niezależne od algorytmów. Obsługiwane są określone algorytmy: wymiana kluczy RSA, DES i Diffie-Hellman. Definiuje również niezależną od algorytmu składnię podpisów cyfrowych, kopert cyfrowych (do szyfrowania) i certyfikatów; to pozwala komuś implementującemu dowolny algorytm kryptograficzny dostosować się do standardowej składni, a tym samym zachować interoperacyjność. Dokumenty wyszczególniające standardy PKCS można uzyskać wysyłając wiadomość e-mail na adres pkcs@rsa.com lub anonimowy ftp na adres rsa.com.

8.10 Co to jest RSAREF?

RSAREF to zbiór procedur kryptograficznych w przenośnym kodzie źródłowym C, dostępny bezpłatnie w RSA Laboratories, oddział RSA Data Security, Inc. Obejmuje on RSA, MD2, MD5 i DES; Wymiana klucza Diffiego-Hellmana zostanie zawarta w najbliższej wersji. Obejmuje to zarówno podprocedury niskiego poziomu, takie jak modułowe potęgowanie, jak i wysokopoziomowe funkcje kryptograficzne, takie jak weryfikacja podpisów cyfrowych. Procedury arytmetyczne mogą obsługiwać liczby całkowite o dużej dokładności, a procedury algorytmów RSA mogą obsługiwać zmienne wielkości kluczy. RSAREF jest w pełni kompatybilny ze standardami PEM i PKCS. RSAREF jest dostępny dla obywateli USA i Kanady oraz dla stałych mieszkańców USA. Może być używany w osobistych, niekomercyjnych aplikacjach, ale nie może być używany komercyjnie lub wysyłany poza USA i Kanadę. Licencja RSAREF zawiera więcej szczegółów na temat dozwolonego użycia i niedozwolonego. RSAREF jest dostępny w Internecie, wysyłając wiadomość e-mail na adres rsaref@rsa.com lub przez ftp na adres rsa.com.