KRYPTOGRAFIA

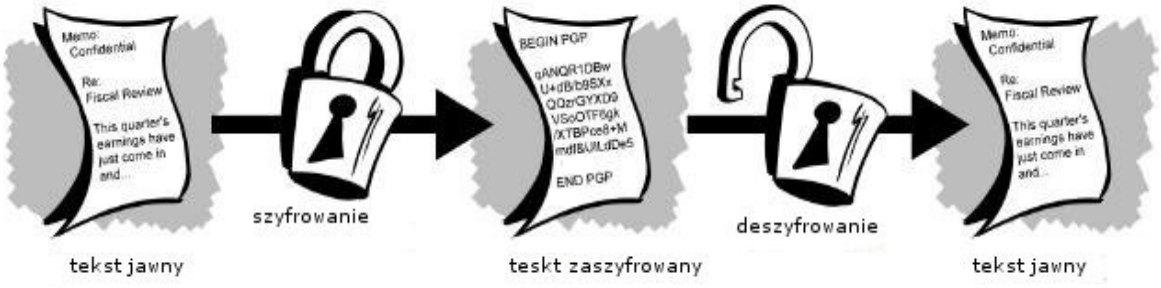
Wprowadzenie do Kryptografii

1 Podstawy Kryptografii

Kiedy Juliusz Cezar wysyłał wiadomości do swoich generałów, nie wierzył swoim kurierom. Zastępował każdą literę A w swojej wiadomości literą D, każdą B E i tak dalej przez cały alfabet. Tylko ktoś znał zasadę „przesunięcia o 3" mógł odszyfrować wiadomość.

SZYFROWANIE I DESZYFROWANIE

Dana która może być odczytana i zrozumiana bez specjalnych problemów jest nazywany *tekstem jawnym*. Metoda zamieniająca tekst jawny w taki sposób aby ukryć jego treść nazywana jest *szyfrowaniem*. Wynikowy tekst zaszyfrowany niemożliwy do odczytania nazywany jest tekstem zaszyfrowanym. Używamy szyfrowania aby upewnić się,że informacja jest ukryta przed każdym do kogo nie był skierowana, nawet tych którzy mogą zobaczyć dane zaszyfrowane. Proces odwracania zaszyfrowanego tekstu do jego pierwotnego testu jawnego jest nazywane deszyfrowaniem. Pokazuje to poniższy rysunek



CO TO JEST KRYPTOGRAFIA?

Kryptografia jest to nauka stosująca matematyki do szyfrowania i deszyfrowania danych. Kryptografia umożliwia przechowywanie wrażliwych informacji lub przenoszenia ich przez niezabezpieczone sieci (takie jak Internet) tak aby nie mogła ich odczytać osoba do której nie było to skierowane. Podczas gdy kryptografia jest nauką o zabezpieczaniu danych, kryptoanaliza jest nauką analizowania i łamania bezpieczeństwa komunikacji. Klasyczna kryptoanaliza łączy w sobie interesujące połączenie analitycznego wnioskowania, stosowania narzędzi matematycznych, dopasowywania wzorców, cierpliwości, determinacji i szczęścia. Kryptoanalitycy są też często zwani atakującymi. Kryptologia obejmuje zarówno kryptografię jak i kryptoanalizę. Powiązaną dyscypliną jest steganografia, która jest nauką ukrywania wiadomości zamiast czynienia ich nieczytelnymi. Steganografia to nie kryptografia; jest to postać kodowania. Opiera się na tajności mechanizmu używanego do ukrycia wiadomości. Jeśli, na przykład, zaszyfrowałeś poufną wiadomość przez wstawienie każdej litery jako pierwszej litery pierwszego słowa każdego zdania, jest to tajne do czasu aż ktoś się nie dowie jak szukać, a potem będzie miał to niezabezpieczone.

SILNA KRYPTOGRAFIA

„Są dwa rodzaje kryptografii na świecie: kryptografia która będzie powstrzymywać twoją siostrę

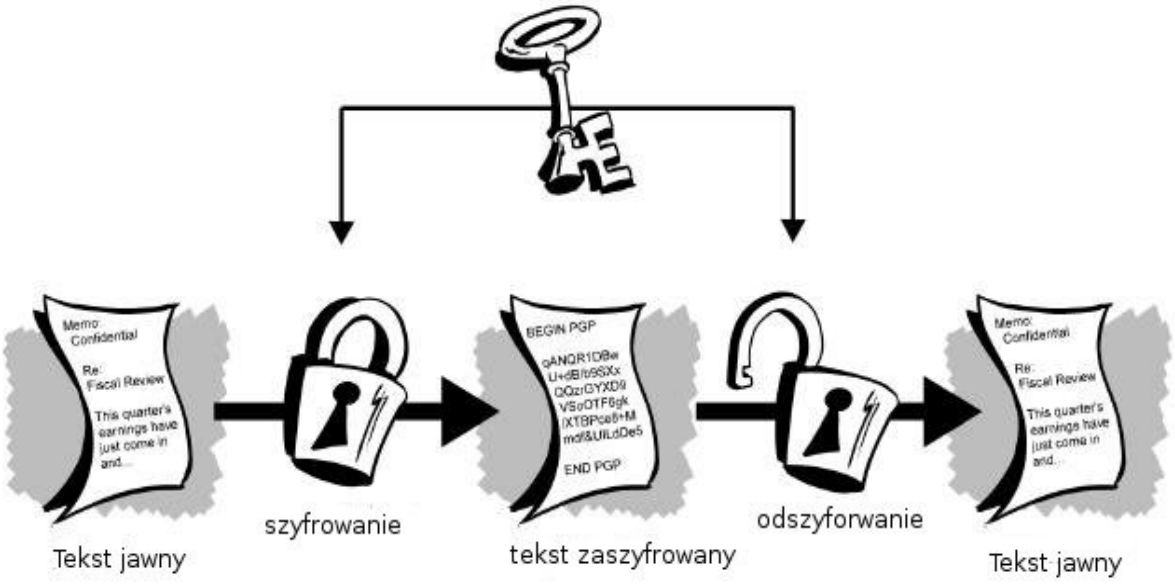
przed przeglądaniem twoich plików , i kryptografia która będzie powstrzymywać rządy przed czytaniem twoich plików”

Bruce Schneier ;Kryptografia Stosowana :Protokoły , Algorytmy i Kod Źródłowy w C

PGP należy do tej ostatniej kategorii.
Kryptografia może być silna lub słaba, jak wyjaśniłem powyżej. Siła kryptografii jest mierzona czasem i zasobami potrzebnymi dla uzyskania jawnego tekstu. Wynikiem silnej kryptografii jest tekst zaszyfrowany,który jest bardzo trudny do odszyfrowania bez posiadania odpowiedniego narzędzia deszyfrującego. Jak trudny? Mając moc wszystkich komputerów i nieograniczony czas – wykonywanie miliarda obliczeń na sekundę – nie jest możliwe odszyfrowanie wyniku silnej kryptografii przed końcem świata.. Ta sądzę ,że silna kryptografia powinna powstrzymać nawet najbardziej zdeterminowanych kryptoanalityków. Czy rzeczywiście? Nie ma dowodów na to ,że dzisiejsze silne szyfrowanie wytrzyma moc jutrzejszej mocy komputerowej. Jednak, silna kryptografia dostarczana przez PGP jest najlepszą dostępną dzisiaj. Czujność i konserwatyzm będą chronić cię lepiej niż domaganie się niedostępności.

Jak działa kryptografia?
Algorytm kryptograficzny, lub szyfr, jest funkcją matematyczną używaną w procesie szyfrowania i deszyfrowania. Algorytm kryptograficzny działa jako połączenie z klucze – słowem ,liczbą lub frazą – dla szyfrowania tekstu jawnego. Ten sam tekst jawny może być zaszyfrowany do różnych tekstów zaszyfrowanych różnymi kluczami. Bezpieczeństwo danych zaszyfrowanych jest całkowicie zależne od dwóch rzeczy : mocy algorytmu kryptograficznego i tajności klucza. Algorytm kryptograficzny , plus wszystkie możliwe klucze i wszystkie protokoły potrzebne do działania tworzą kryptosystem. PGP jest kryptosystmem

Kryptografia konwencjonalna
W kryptografii konwencjonalnej, zwanej również szyfrowaniem tajnym kluczem lub kluczem symetrycznym, jeden klucz jest używany zarówno do szyfrowania jak i deszyfrowania. Data Encryption Stnadard (DES) jest przykładem kryptosystemu konwencjonalnego, który został szeroko rozpowszechniony prze rząd USA jak i bankowość. Został on zastąpiony przez Advanced Encryption Standard (AES). Poniższy rysunek ilustruje proces konwencjonalnego szyfrowania



Szyfr Cezara
Najprostszym przykładem kryptografii konwencjonalnej jest szyfr podstawieniowy. Szyfr podstawieniowy zastępuje jeden fragment informacji innym. Jest to najczęściej robione przez przestawianie liter w alfabecie. Takim przykładem jest szyfr Cezara. Algorytmem jest tu przesunięcie alfabetu a kluczem liczba znaków do przesunięcia. Na przykład jeśli kodujemy słowo „TAJNE" używając klucza Cezara o wartości 3, przesuwamy alfabet tak, aby trzecia litera licząc w górę (D) zaczynała alfabet. Zacznijmy od

ABCDEFGHIJKLMNOPQRSTUVWXYZ

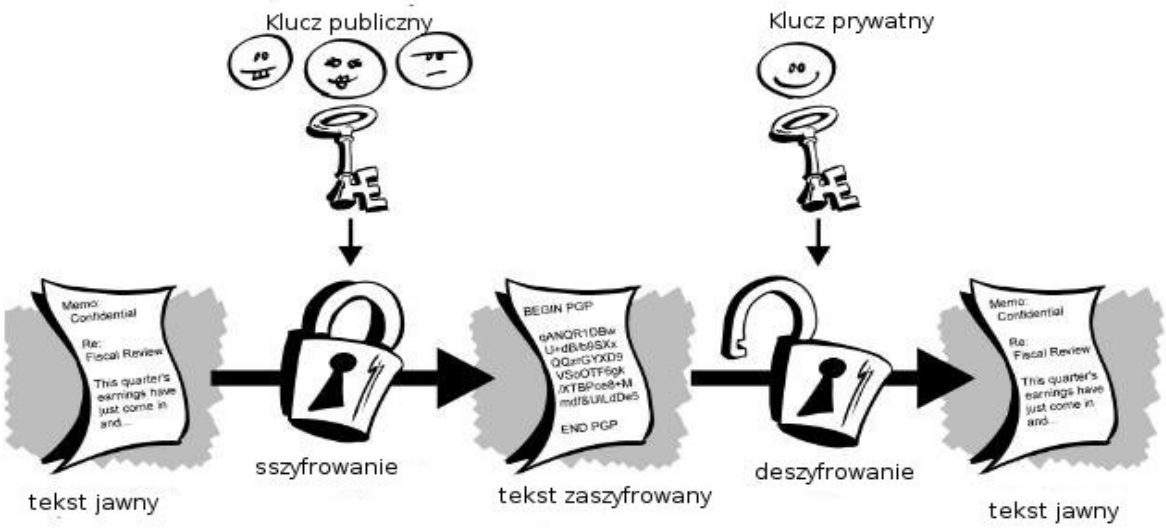
Teraz przewińmy wszystko o trzy aby uzyskać

DEFGHIJKLMNOPQRSTUVWXYZABC

gdzie D = A, E = B, F = c itd.
Używając tego schematu, tekst jawny „TAJNE" szyfrujemy jako „WDMQH" .Aby ktoś mógł odczytać ten tekst , należy mu powiedzieć , że kluczem jest 3. Oczywiście na dzisiejsze standardy jest to bardzo słaba kryptografia ,ale działała dla Cezara i ilustruje jak działa konwencjonalna kryptografia.

Zarządzanie kluczami a kryptografia konwencjonalna
Szyfrowanie konwencjonalne ma swoje zalety. Jest bardzo szybka, Jest szczególnie użyteczna dla szyfrowania danych które dalej nie pójdą, Jednak konwencjonalna kryptografia sama jako środek dla transmisji zabezpieczonych danych może kosztowne ze względu na bezpieczeństwo dystrybucji kluczy, Przypomnij sobie fragment ulubionego filmu szpiegowskiego: osoba z teczką przymocowaną do nadgarstka. Co jest w teczce? Prawdopodobnie nie jest to sam tajny plan. Jest to klucz służący do odszyfrowania tajnych danych. Nadawcy i odbiorcy zabezpieczonej komunikacji używających konwencjonalnej kryptografii, muszą zgodzić się na klucz i przechowywać go bezpiecznym między sobą. Jeśli są oni w różnych fizycznych miejscach, muszą zaufać kurierowi, lub innej formie bezpiecznego medium komunikacyjnego dla zabezpieczenia tajnego klucza przed ujawnieniem podczas transmisji. Każdy kto podsłuchał lub przejął klucz może potem odczytać , zmodyfikować i sfałszować wszystkie zaszyfrowane informacje lub uwierzytelnić tym kluczem. Problem jest tu dystrybucja kluczy: jak pobrać klucz przez odbiorcę bez narażania się na to ,że ktoś go przechwyci?

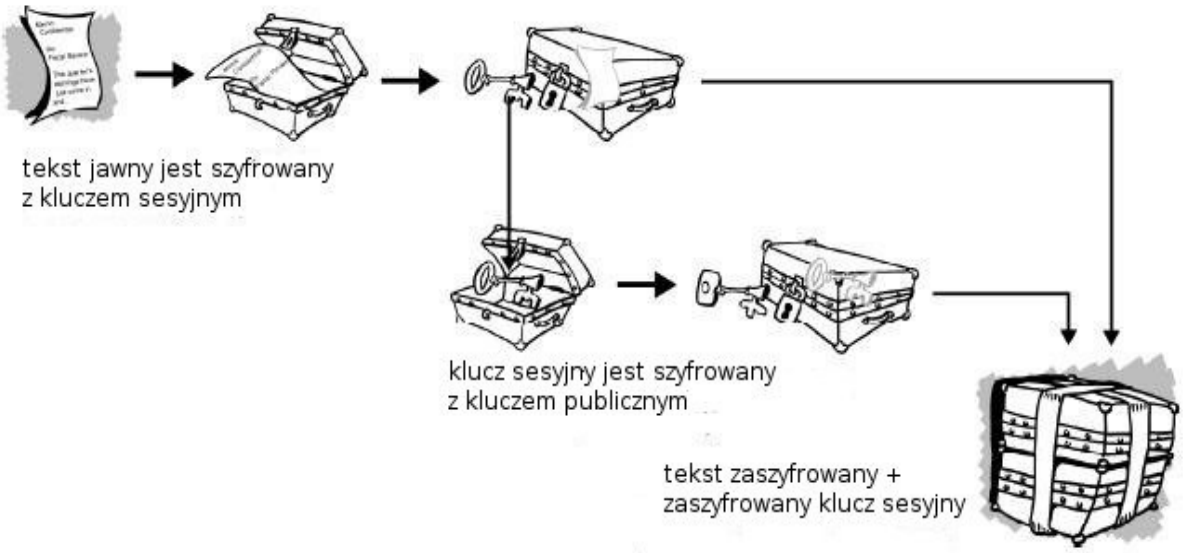
Krytpografia z kluczem publicznym
Problem z dystrybucją kluczy został rozwiązany przez kryptografię z kluczem publicznym, pojęcie wprowadzone przez Whitefilelda Diffie i Martina Hellmana w 1975 roku. Kryptografia z kluczem publicznym używa pary kluczy: klucza publicznego , który szyfruje dane i odpowiedniego klucza prywatnego, dla deszyfrowania. Ponieważ używa ona dwóch kluczy, czasami nazywana jest krytpografią asymetryczną. Upubliczniasz swój klucz publiczny podczas gdy zachowujesz w tajemnicy swój klucz prywatny. Każdy kto skopiuje twój klucz publiczny, może potem zaszyfrować informację, którą tylko ty możesz odczytać, nawet ludzie których nigdy nie spotkałeś. Jest obliczeniowo niewykonalne wydedukowanie klucza prywatnego z klucza publicznego. Ktoś kto ma klucz publiczny może szyfrować informacje ale nie może ich odszyfrować. Tylko osoba która ma odpowiedni klucz prywatny może odszyfrować tą informację.



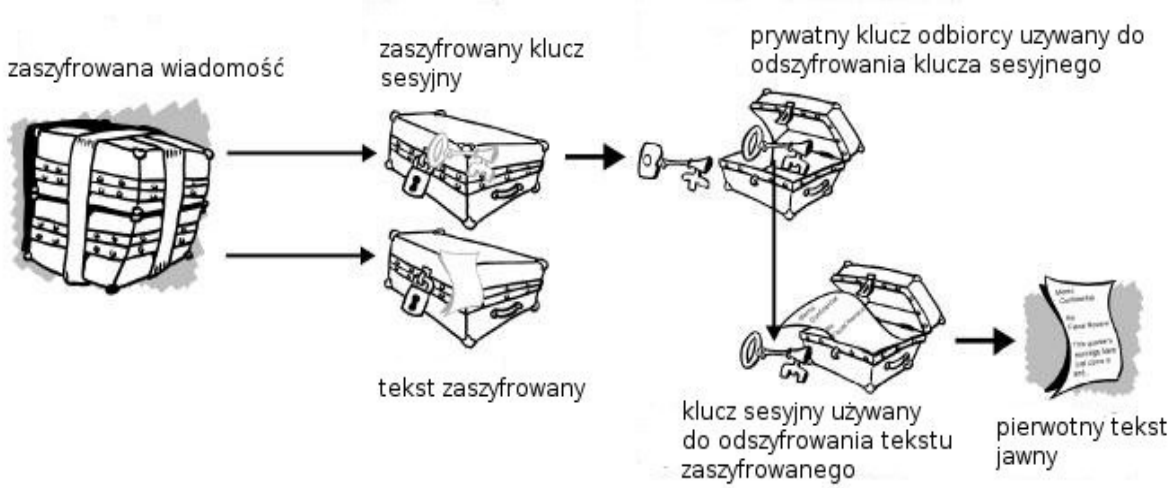
Podstawową zaletą kryptografii z kluczem publicznym jest to ,że pozwala ludziom nie mającym wcześniej układu bezpieczeństwa na zmianę bezpieczeństwa wiadomości. Wyeliminowana jest potrzeba współdzielenia przez nadawcę i odbiorcę tajnego klucza poprzez jakiś zabezpieczony kanał; cała komunikacja obejmuje tylko klucze publiczne, a żaden klucz prywatny nie jest transmitowany lub współdzielony. Przykłady kryptosystemu z kluczem publicznym to Elgamal(nazwany na cześć jego twócy, Tahera Elgamala), RSA (nazwany na cześć Rona Rivesta, Adi Shamira i Leonarda Adelmana) Diffie – Hellman (nazwany, jak zgadujesz ,na cześć jego twórców) iDSA, Digital Signature Algorithm (stworzony przez Davida Kravitza). Ponieważ kryptografia konwencjonalna była jedynym dostępnym środkiem dla przekazywania tajnych informacji, koszt zabezpieczonych kanałów i dystrybucje kluczy został przenoszony na tych którzy mogli go ponieść, czyli rządy i duże banki. Szyfrowanie z kluczem publicznym jest technologiczną rewolucją, która dostarcza silnej kryptografii dla dorosłych zastosowań. Pamiętaj ,że kuriera z teczką przymocowaną do nadgarstka? Szyfrowanie z kluczem publicznym wyłącza go z biznesu.

Jak pracuje PGP

PGP łączy w sobie najlepsze funkcje kryptografii konwencjonalnej i kryptografii z kluczem publicznym. PGP jest kryptosystemem hybrydowym. Kiedy użytkownik szyfruje tekst jawny PGP , PGP najpierw kompresuje tekst jawny. Dane skompresowane oszczędzają czas transmisji modemowej i przestrzeń na dysku , i co ważniejsze, wzmacnia bezpieczeństwo kryptograficzne. Większość technik kryptoanalitczynych wykorzystuje wzorce znajdowane w tekście jawnym dla złamania szyfru. Kompresja redukuje te wzorce w tekście jawnym, w skutek tego zwiększa się ochrona przed kryptoanalizą. (Pliki które są zbyt krótkie do kompresji lub które nie kompresują się dobrze , nie są kompresowane). PGP tworzy potem klucz sesyjny, który jest jednorazowym tajnym kluczem. Klucz ten jest losowo wygenerowaną liczbą z losowych ruchów myszki i uderzeń w klawisze. Klucz sesyjny działa z bardzo bezpiecznym, szybkim konwencjonalnym algorytmem szyfrowania dla szyfrowania tekstu jawnego; wynikiem jest tekst zaszyfrowany. Po zaszyfrowaniu danych, klucz sesyjny jest potem szyfrowany do klucza publicznego odbiorcy. Klucz sesyjny szyfrowania kluczem publicznym jest przekazywany wraz z zaszyfrowanym tekstem do odbiorcy.



Deszyfrowanie jest procesem odwrotnym. Kopia odbiorcy PGP używa odpowiedniego klucza prywatnego dla odzyskania klucza sesyjnego, którego potem PGP używa do odszyfrowania konwencjonalnie zaszyfrowanego tekstu szyfrowanego.



Połączenie tych dwóch metod szyfrowania łączy wygodę szyfrowania z kluczem publicznym z szybkością kryptografii konwencjonalnej. Szyfrowanie konwencjonalne jest około 10000 razy szybsze niż szyfrowanie z kluczem publicznym. Szyfrowanie z kluczem publicznym po kolei dostarcza rozwiązania dystrybucji kluczy i transmisji danych. Użyte razem, wydajność i dystrybucja kluczy są poprawione bez poświęcania bezpieczeństwa.

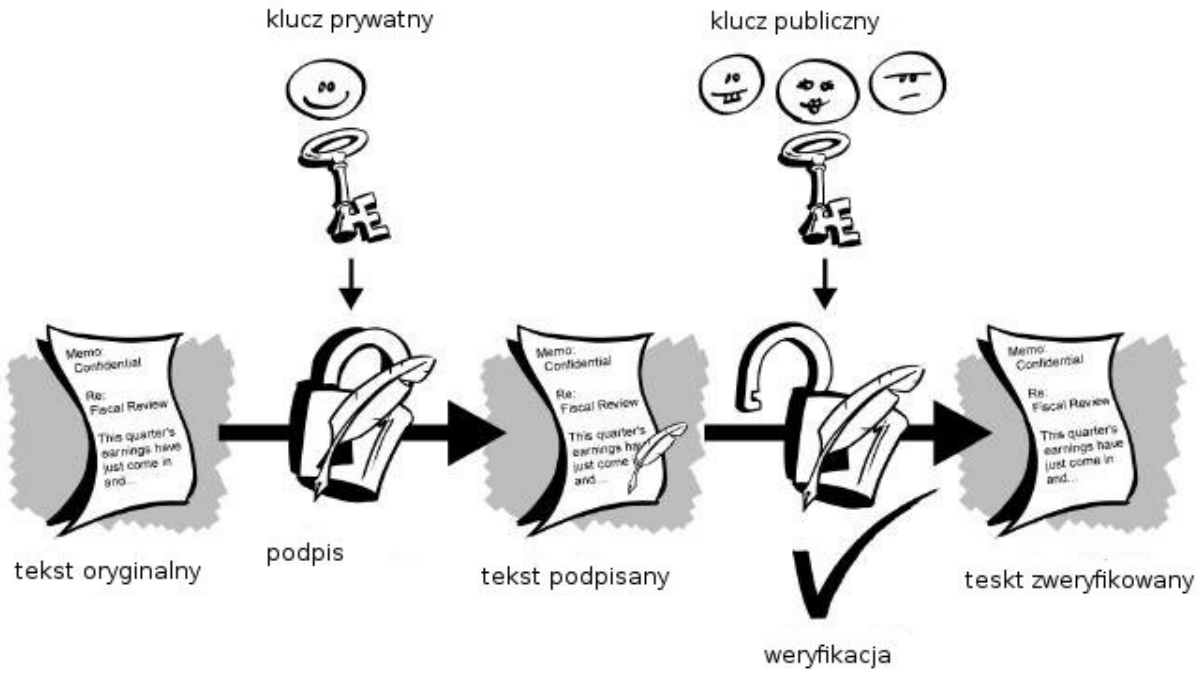
Klucze

Klucz jest wartością , która pracuje z algorytmem kryptoraficznym tworząc określony tekst zaszyfrowany. Klucze są zasadniczo bardzo, bardzo dużymi liczbami . Rozmiar klucza jest mierzony w bitach; liczba przedstawiająca 2048 bitowy klucz jest okropnie duży. W kryptografii z kluczem publicznym im większy klucz tym bardziej bezpieczny tekst. Jednak, rozmiar klucza publicznego i tajnego klucza konwencjonalnej kryptografii są całkowicie niepowiązane.

Konwencjonalny 80 bitowy klucz ma swój odpowiednik w silnym , 1024 bitowym kluczu publicznym . Konwencjonalny 128 bitowy klucz ma odpowiednik 3000 bitowego klucza publicznego. Ponownie, im większy klucz , większe bezpieczeństwo , ale algorytmy używane dla każdego typu kryptografii są bardzo różne a zatem trudno jest je porównać. Podczas gdy klucze publiczny i prywatny są powiązane matematycznie bardzo trudno wyprowadzić klucz prywatny z danego tylko klucza publicznego; jednak wyprowadzenie klucza prywatnego jest zawsze możliwe przy danej dużej ilości czasu i mocy komputerowej. Bardzo ważne jest wtedy wyprowadzenie klucza o właściwym rozmiarze; wystarczająco duży będzie bezpieczny, ale dość mały będzie znaleziony bardzo szybko. Dodatkowo musisz rozważyć kto może czytać twoje pliki ,jak określić kto to jest i jakie mogą być ich zasoby. Duże klucze będą kryptograficznie bezpieczne dłuższy czas. Jeśli to co chcesz zaszyfrować musi być ukryte wiele lat , możesz zechcieć użyć bardzo dużego klucza. Oczywiście nikt nie wie jak długo to co dzisiaj jest używane do szyfrowania, będzie bezpieczne jutro. Był czas kiedy 56 bitowy klucz symetryczny był uważany za wyjątkowo bezpieczny. Wierzyliśmy ,że do czasu komputerów kwantowych , 128 bitowy klucz będzie bezpieczny w nieskończoność. Wierzyliśmy, że nawet klucz 256 bitowy będzie bezpieczny w nieskończoność ,nawet jeśli ktoś wymyśli komputer kwantowy. Jest tak dlatego ,że AES zawiera opcję dla 128- i 256 bitowego klucza. Ale historia mówi ,że nic nie trwa wiecznie. Klucze są przechowywane w postaci zaszyfrowanej. PGP przechowuje klucze w dwóch plikach na dysku twardym; jeden dla klucza publicznego i jeden dla klucza prywatnego. Pliki te są nazywane bazą kluczy Jeśli używasz PGP , zazwyczaj dodajesz klucze publiczne swoich odbiorców do publicznej bazy kluczy. Twoje klucze prywatne są przechowywane w twojej prywatnej bazie kluczy. Jeśli zgubisz prywatną bazę kluczy , nie będziesz mógł odszyfrować żadnej informacji zaszyfrowanej kluczem z twojej bazy. Więc dobrym pomysłem jest tworzenie kopii zapasowej.

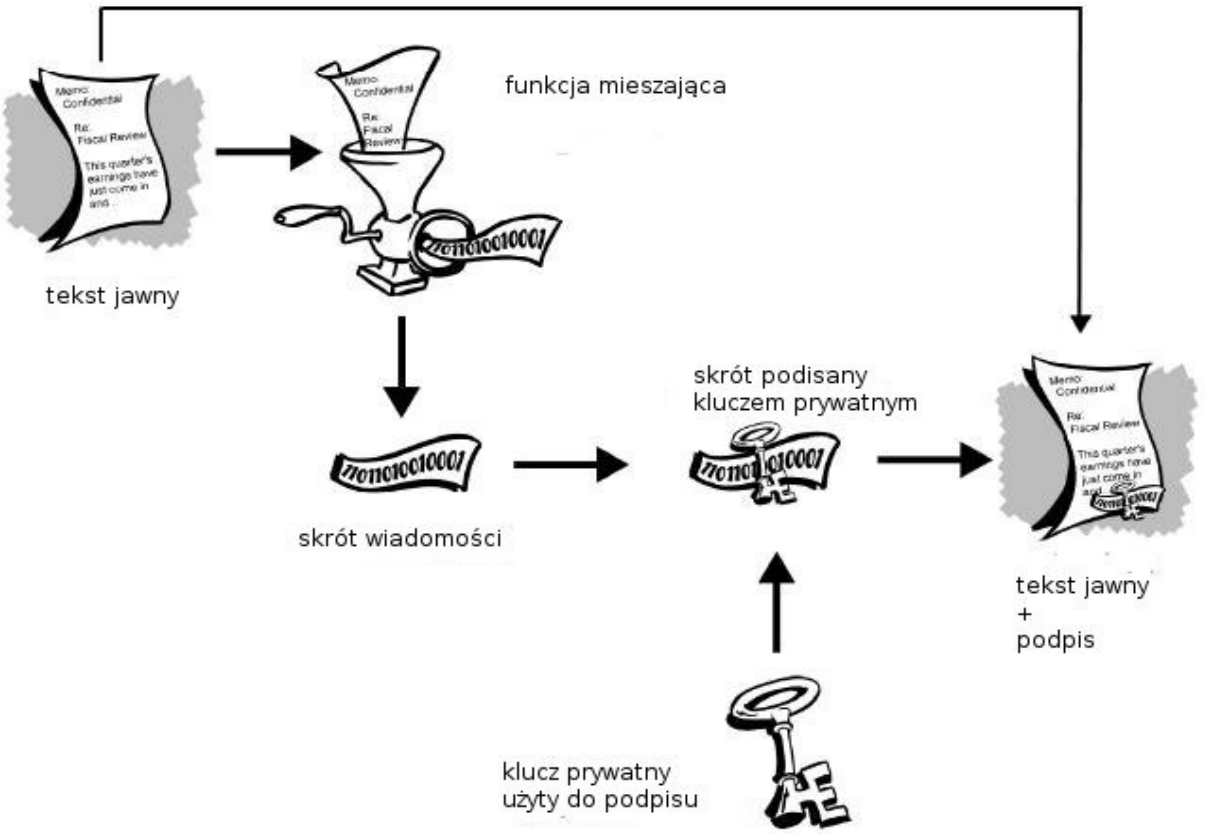
Podpisy cyfrowe

Główną zaletą kryptografii z kluczem publicznym jest to ,że dostarcza metody dla stosowania podpisów cyfrowych . Podpisy cyfrowe pozwalają odbiorcy informacji zweryfikować uwierzytelnienie informacji oryginalnej, jak również zweryfikować czy ta informacja nie została zmodyfikowana w czasie transmisji. Zatem cyfrowe podpisy klucza publicznego dostarczają uwierzytelnienia i integralności danych. Te funkcje są fundamentalne dla kryptografii i prywatności. Podpis cyfrowe służą temu samemu celowi co pieczątka na dokumencie lub podpis ręczny. Jednak z powodu sposobu w jaki jest tworzony, jest ważniejszy niż pieczęć lub podpis .Podpis cyfrowy nie tylko poświadcza tożsamość podpisującego, ale również pokazuje ,że zawartość podpisanej wiadomości nie została zmodyfikowana. Pieczęć fizyczna lub podpis ręczny tego nie robią .Jednak , jeśli pieczęć fizyczna , może być stworzona przez każdego kto ma sygnet, podpis cyfrowy może stworzyć ktoś z kluczem prywatnym z podpisywanej pary kluczy. Niektórzy ludzie mają tendencję do używania podpisów więcej niż tylko w szyfrowaniu. Podstawowy sposób w jaki są tworzone podpisy cyfrowe jest pokazany na poniższym rysunku. Algorytm podpisu używa twojego klucza prywatnego dla tworzenia podpisu i klucza publicznego dla jego weryfikacji. Jeśli informacja może być odszyfrowany kluczem publicznym, wtedy musi powstać u ciebie.



Funkcje mieszające

System opisany powyżej ma pewne problemy. Jest wolny i tworzy gigantyczne wolumeny danych – przynajmniej podwaja rozmiar pierwotnej informacji. Aby poprawić powyższy schemat, dodamy jednokierunkową funkcję mieszającą w procesie. Jednokierunkowa funkcja mieszająca pobiera długość zmiennej wejściowej – w tym przypadku, długość wiadomości, nawet tysiące lub miliony bitów – i tworzy daną wyjściową o stałej długości; powiedzmy 160 bitów. Funkcja mieszająca zapewnia ,że jeśli informacja zmienia się w jakiś sposób – nawet o jeden bit -tworzona jest całkiem inna dana wyjściowa. PGP używa silnej kryptograficznie funkcji mieszającej w tekście jawnym jaki podpisał użytkownik. To generuje daną o stałej długości znaną jako skrót wiadomości (I ponownie, dowolna zmiana informacji daje w wyniku całkowicie inny skrót). PGP używa skrótu i klucza prywatnego dla stworzenia „podpisu". PGP transmituje podpis i tekst jawny razem. Po uzyskaniu wiadomości, odbiorca używa PGP dla ponownego obliczenia skrótu, dlatego weryfikuje ten podpis. PGP może szyfrować tekst jawny lub nie; podpisany tekst jawny jest użyteczny jeśli jakiś odbiorca nie jest zainteresowany możliwością weryfikacji podpisu. Tak długo jak bezpieczna funkcja mieszająca jest używana, nie ma sposobu aby pobrać podpis z dokumentu i dołączenia do innego, lub zmodyfikować podpisaną wiadomość w dowolny sposób. Najmniejsza zmiana podpisanego dokumentu będzie powodowała błąd weryfikacji podpisu cyfrowego.



Podpisy cyfrowe odgrywają główną rolę w uwierzytelnianiu i walidacji kluczy innych użytkowników PGP

Certyfikaty cyfrowe

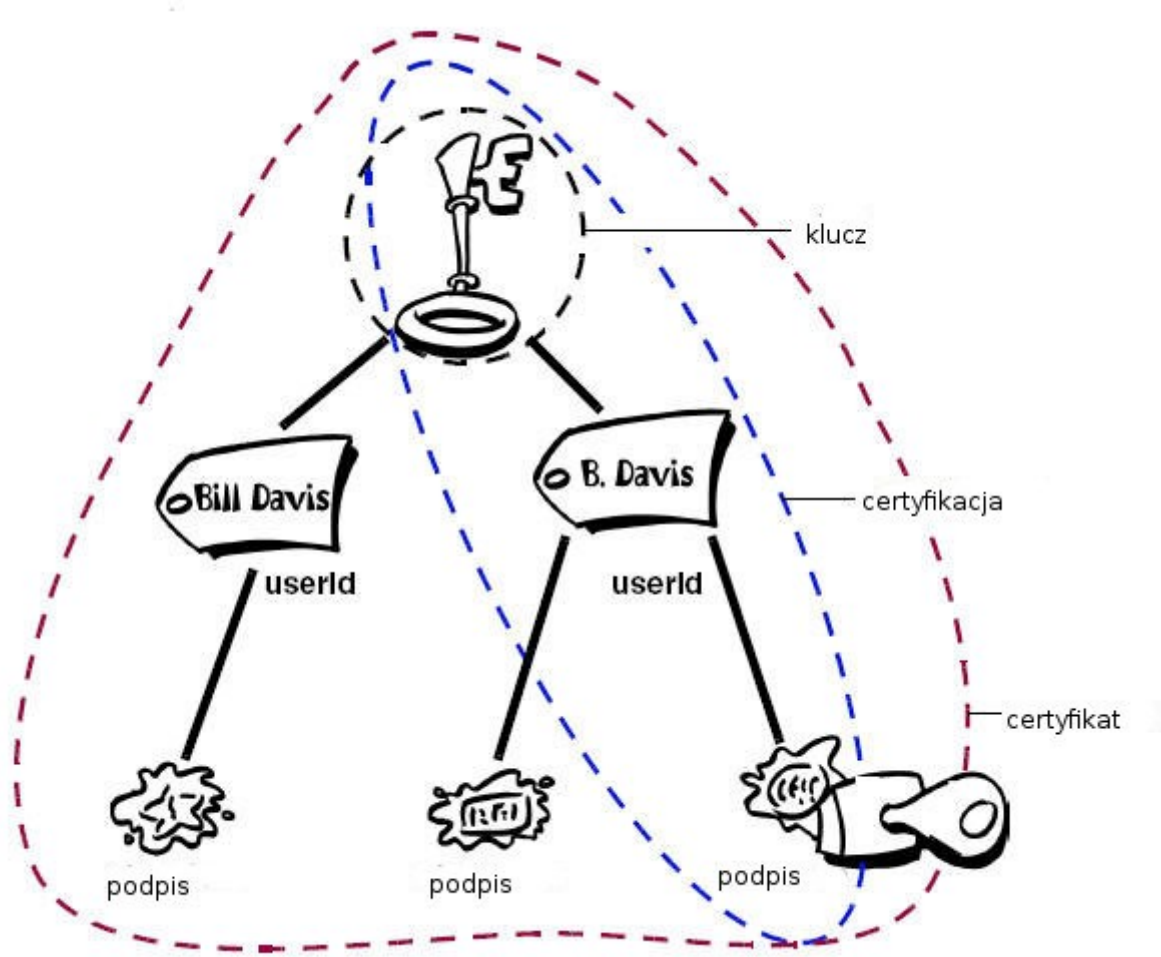
Jednym z problemów z kryptosystemami z kluczem publicznym jest to ,że użytkownicy muszą być ciągle czujni aby się upewnić ,że szyfrują klucz odpowiedniej osoby. W środowisku gdzie jest bezpieczna wymiana kluczy poprzez serwery publiczne , ataki man-in-the-middle są prawdopodobne. W tego typu ataku , ktoś wysyła fałszywy klucz z nazwą i ID użytkownika przeznaczone dla odbiorcy. Dana zaszyfrowana do – i przechwycone przez - prawdziwego właściciela fałszywego klucza jest teraz w złych rękach. W środowisku klucza publicznego , jest istotne abyś znał z pewnością ,że klucz publiczny którym szyfrujesz dane jest faktycznie kluczem publicznym odpowiedniego odbiorcy, a nie oszusta. Możesz po prostu zaszyfrować tylko te klucze, które fizycznie zostały ci dostarczone. Ale przypuśćmy ,że musisz wymienić informację z ludźmi z którymi się nigdy nie spotkałeś ; jak możesz być pewny ,że masz poprawny klucz? Certyfikaty cyfrowe upraszczają zadanie upewniania się ,że klucz publiczny naprawdę należy do stosownego właściciela. Certyfikat jest formą uwierzytelnienia .Innym rodzajem uwierzytelnienia jest prawo jazdy, ubezpieczenia społecznego. Każdy z nich ma jakąś informację identyfikującą cię i twoją tożsamość. Certyfikaty cyfrowe funkcjonują jako certyfikaty fizyczne. Podpis cyfrowy jest informacją zawartą z osobistym kluczem publicznym , który pomaga innym zweryfikować ten klucz czy jest poprawny. Certyfikaty cyfrowe są używane dla uniemożliwienia prób zastąpienia jedengo klucza osobistego innym.

Certyfikat cyfrowy składa się z trzech rzeczy :

- klucza publicznego
- certyfikowanej informacji (zazwyczaj „tożsamości” użytkownika, takie jak nazwisko, ID itd. Certyfikaty mogą również zawierać informacje uwierzytelniające o użytkowniku,)

- Jeden lub więcej podpisów cyfrowych

Celem podpisu cyfrowego na certyfikacie jest określenie ,że informacja certyfikująca została przetestowana przez osoby lub jednostki. Podpis cyfrowy nie potwierdza autentyczności certyfikatu jako całości; gwarantuje tylko ,że podpisana informacja tożsamości, przyszła wraz z , lub jest ograniczona, do klucza publicznego. Zatem certyfikat jest zasadniczo kluczem publicznym z jedną lub dwoma formami dołączonego ID, plus przyjacielskie potwierdzenie od innej zaufanej osoby.



Dystrybucja certyfikatów
Certyfikaty są używane kiedy jest konieczna wymiana kluczy publicznych z kimś. Dla małej grupy ludzi, którzy życzą sobie komunikować się bezpiecznie, łatwo jest ręcznie wymieniać dyskietki lub emaile zawierające klucz publiczny. To jest ręczna dystrybucja klucza publicznego i jest praktyczna tylko do pewnego punktu. Poza tym punktem, konieczny jest system który zapewnia mechanizm bezpieczeństwa, przechowywania i wymiany między współpracownikami czy partnerami biznesowymi . Może być to w postaci Serwerów Uwierzytelniania, lub systemów strukturalnych, które dostarczają dodatkowej funkcji zarządzania kluczami nazwanych Infrastrukturami Klucza Publicznego (PKI).

Serwery uwierzytelniania
Serwer uwierzytelniania jest bazą danych dostępną w sieci ,która pozwala użytkownikom odbierać i wysyłać certyfikaty cyfrowe. Często, serwery certyfikacji są również serwerami katalogów ogólnego przeznaczenia. Serwer certyfikacji może również dostarczać jakichś funkcji administracyjnych, które pomagają firmom na zarządzanie ich zasadami bezpieczeństwa.

Przykładem może być zezwalanie tylko na przechowywanie kluczy, które spełniają pewne wymagania. PGP Keyserver (znany poprzednio jako PGP Certificate Server) dostarcza tego, podczas gdy ogólne serwery katalogów nie.

Infrastruktura Klucza Publicznego (PKI)
PKI obejmują funkcję przechowywania certyfikatu serwera certyfikacji, ale również dostarcza usług i protokołów dla zarządzania kluczami publicznymi. To obejmuje możliwości publikowania , unieważniania i zaufania certyfikatom. Główna funkcją PKI jest wprowadzanie tego co jest znane jako komponenty Urzędu Certyfikacji (CA) i Urząd Rejestracji (RA). CA tworzą certyfikaty i podpisują je cyfrowo używając klucza prywatnego CA. Z powodu ich roli w tworzeniu certyfikatów , CA jest centralnym komponentem PKI. Używając klucza publicznego CA, każdy kto chce zweryfikować certyfikat uwierzytelniania weryfikuje podpis cyfrowy, a zatem, integralność zawartości certyfikatu. Zazwyczaj, RA odnosi się do ludzi, procesów i narzędzi używanych do obsługi rejestracji użytkowników z PKI (zarejestrowanie) i ciągłego administrowania użytkownikami. RA może wykonać badanie – proces weryfikacji czy dany klucz publiczny należy do odpowiedniego właściciela. RA jest jednostką ludzką - osobą, grupą, departamentem, firmą lub innym stowarzyszeniem. CA z drugiej strony, jest często oprogramowaniem, które jest używane dla zagadnienia rzeczywistej certyfikacji użytkownika komputera. Rola RA/CA jest analogiczna do Biura Paszportowego, gdzie niektórzy ludzie sprawdzają czy paszport jest potrzebny (funkcja RA) a inni tworzą paszport i wkładają go do oprawki (funkcja CA). Nie może być RA z CA, ale dostarcza podziału ról, które mogą być ważne w pewnych warunkach .

Formaty certyfikatów
Certyfikat cyfrowy jest zasadniczo zbiorem informacji o tożsamości razem z kluczem publicznym i podpisany przez zaufaną trzecią część udowadniającą ich autentyczność. Certyfikat cyfrowy może mieć jeden z kilku różnych formatów:
PGP rozpoznaje dwa różne formaty certyfikatów:

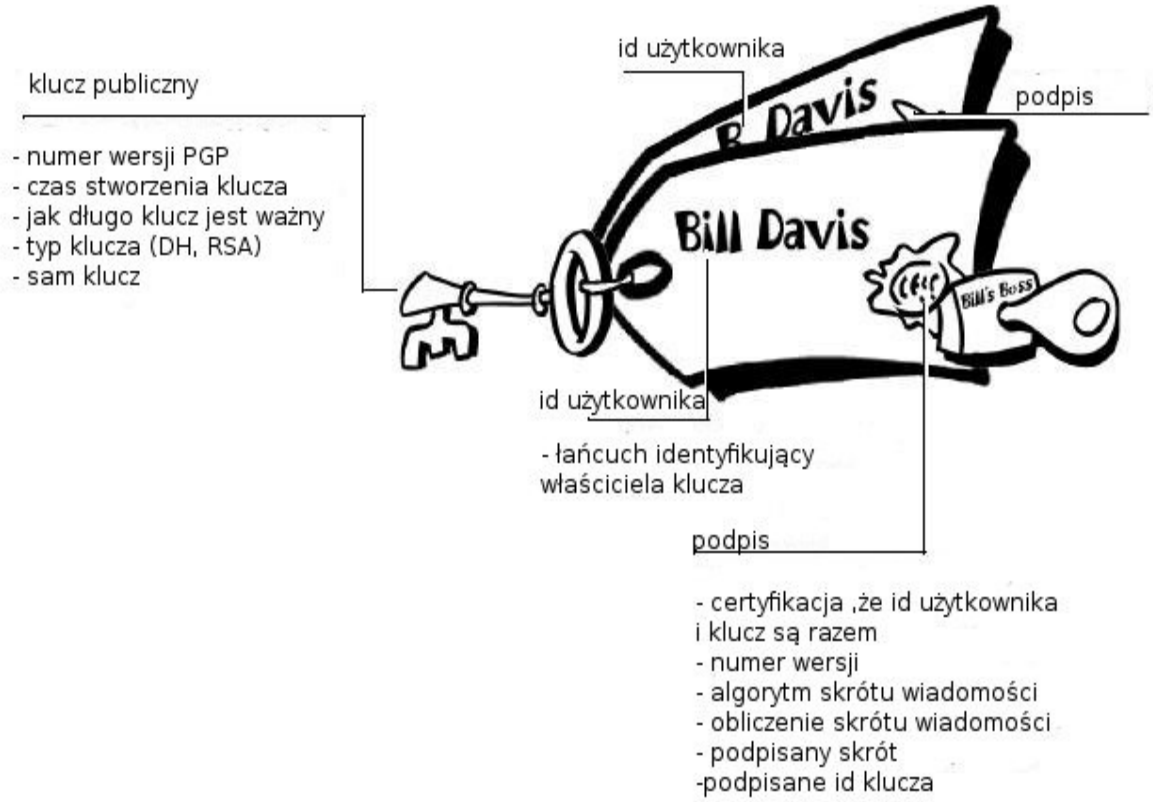
- Certyfikaty PGP (do którego odnosimy się po prostu jako klucze PGP
- Certyfikaty X.509

Formaty certyfikatów PGP
Certyfikat PGP obejmuje (ale nie jest to nich ograniczony) następujące informacje:

- Oprawkę certyfikatu klucza publicznego – publiczna część pary kluczy, razem z algorytmem klucza:: RSA, RSA Legacy, DH (Diffie – Hellman) lub DSA (Digital Signature Algorithm)
- Oprawkę informacji certyfikatu – składającą się z informacji „tożsamości" o użytkowniku, takie jak nazwisko, ID użytkownika, adres email, numer ICW, zdjęcie itp.
- Cyfrowy podpis właściciela certyfikatu – podpis używający klucza prywatnego z klucza publicznego związanego z tym certyfikatem
- Okres ważności certyfikatu -data / czas początku certyfikatu i data / czas jego ważności; wskazuje kiedy certyfikat straci ważność. Jeśli para kluczy zawiera podklucze, wtedy zawiera czas trwania każdego z zaszyfrowanych podkluczy.
- Preferowany algorytm symetrycznego szyfrowania dla tego klucza – wskazuje algorytm szyfrowania jaki preferuje właściciel certyfikatu aby mieć odszyfrowane informacje. Obsługiwane algorytmy to CAST, AES , IDEA Potrójny DES i Twofish.

Możesz myśleć o certyfikacie PGP jako kluczu publicznym z jedną lub więcej etykietami z nim związanym. Na tych „etykietach" znajdziesz informacje identyfikujące właściciela klucza i podpis właściciela klucza, co oznacza ,że klucz i identyfikacja idą razem (Ten szczególny podpis jest

nazywany self-signature; każdy certyfikat PGP zawiera self-signature). Unikalnym aspektem formatu certyfikatu PGP jest to ,że pojedynczy certyfikat może zawierać wiele podpisów. Kilku lub wielu ludzi może podpisać parę klucz / identyfikacja dla przetestowania ich własnej pewności ,że klucz publiczny definitywnie należy do określonego właściciela. Jeśli zajrzysz na publiczny serwer certyfikatów, możesz zauważyć ,że pewne certyfikaty zawierają wiele podpisów. Niektóre certyfikaty PGP składają się z klucza publicznego z kilkoma etykietami, każda zawierająca różne środki identyfikacji właściciela klucza (na przykład, nazwę właściciela i firmowe konto mailowe, nick właściciela i mail domowy, zdjęcie właściciela - wszystko w jednym certyfikacie). Lista podpisów każdej z tych tożsamości może się różnić; podpisy poświadczają autentyczność , tego ,że jedna z etykiet należy do klucza publicznego, a nie to ,że wszystkie etykiety są autentyczne.



Format certyfikatu X.509

X.509 jest innym formatem certyfikatu. Wszystkie certyfikaty X.509 spełniają międzynarodowy standard ITU-T X.509; zatem (teoretycznie) sertyfikaty X.509 tworzone dla jednej aplikacji mogą być użyte przez aplikację X.509 .W praktyce jednak, różne firmy tworzą własne rozszerzenia do certyfikatów X.509, które nie zawsze współpracują. Certyfikat wymaga kogoś kto potwierdzi ,że klucz publiczny i nazwa właściciela idą razem. W certyfikacie PGP , każdy może odgrywać rolę potwierdzają (chyba ,że ta opcja został jawnie ograniczona przez administratora firmy) Przy certyfikacie X.509, potwierdzający jest zawsze Urząd Certyfikacji lub ktoś wyznaczony przez Urząd (Pamiętaj ,że certyfikaty PGP również w pełni obsługuje strukturę hierarchiczną używającą CA dla potwierdzenie certyfikatów). Certyfikat X.509 jest zbiorem standardowych pól zawierających informacje o użytkowniku lub urządzeniu i ich odpowiednich kluczach publicznych. Standard X.509 definiuje jaka informacja znajduje się w certyfikacie i opisuje jak ją zakodować (format danych). Wszystkie certyfikaty X.509 ma następujące dane:

- **Oprawkę certyfikatu klucza publicznego** - oprawka certyfikatu klucza publicznego,

razem z algorytmem identyfikującym, , który określa do jakiego kryptosystemu należy klucz z parametry związane z kluczem.

- **Numer seryjny certyfikatu** – jednostka (aplikacja lub osoba), która tworząc certyfikat jest odpowiedzialna za przypisanie mu unikalnego numeru seryjnego dla odróżnienia go od innych certyfikatów. Informacja ta jest używana na różne sposoby; na przykład kiedy certyfikat jest unieważniany, jego numer seryjny jest umieszczany na Certificate Revocation List (CRL)
- **Unikalny identyfikator certyfikatu** (lub DN – nazwę rozróżnialną) – nazwa ta jest unikalna w Internecie. DN składa się wielu podsekcji i może wyglądać jak poniższy :

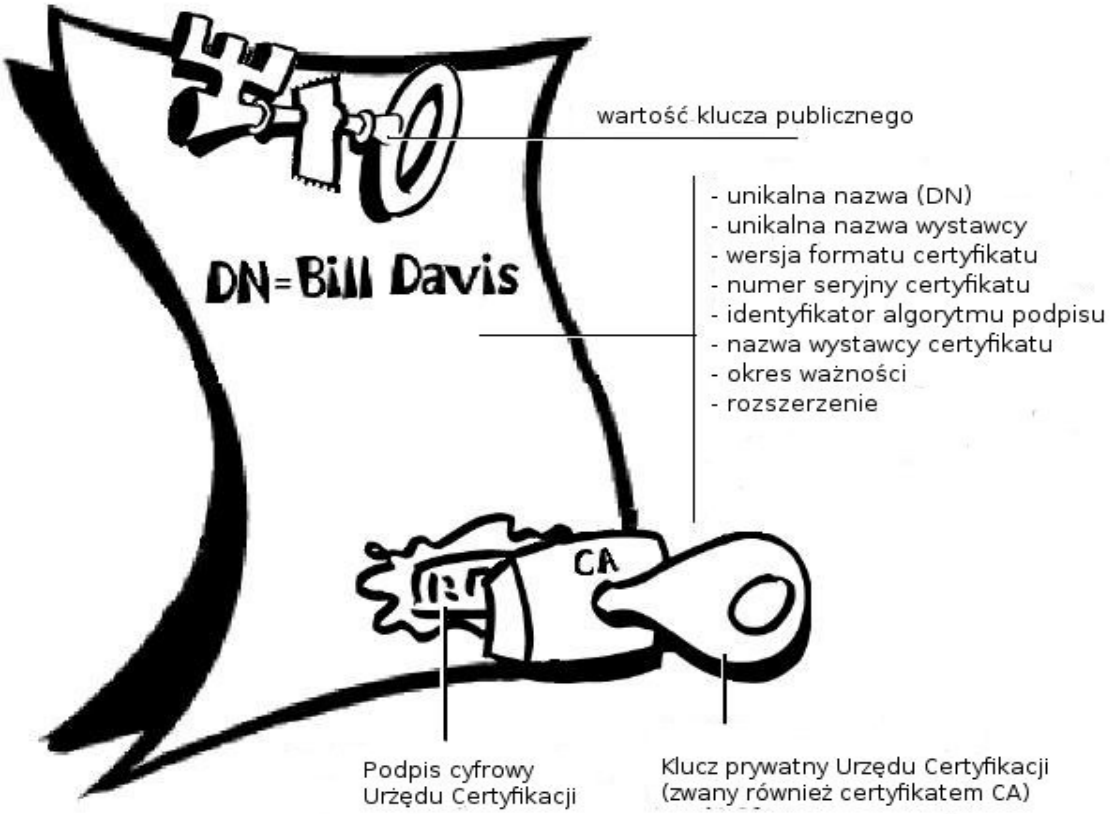
  CN = Bob Davis EMAIL=bdavis@pgp.com, OU= PGP Engineering, O = PGP Corporation, C = US)

- **Okres ważności certyfikatu** – data/czas startu certyfikatu i data / czas wygaśnięcia; wskazuje kiedy certyfikat wygaśnie.
- **Unikalna nazwa certyfikatu** – nazwa unikalna jednostki, która podpisała certyfikat. Zazwyczaj jest to CA. Użycie certyfikatu implikuje zaufanie do jednostki, która podpisała ten certyfikat.
- **Cyfrowy podpis wydawcy** – podpis używający klucza prywatnego jednostki, która wydała ten certyfikat.
- **Identyfikator algorytmu podpisu** - identyfikacja algorytmu używanego przez CA dla podpisania tego certyfikatu

Jest wiele różnic między certyfikatem X.509 a certyfikatem PGP, ale najważniejsze są następujące:

- możesz stworzyć swój własny certyfikat PGP; musisz poprosić o certyfikat X.509 Urząd Certyfikacji
- Certyfikaty X.509 naturalnie obsługują tylko pojedynczą nazwę dla właściciela klucza
- Certyfikaty obsługują tylko pojedynczy podpis cyfrowy dla poświadczenia poprawności klucza

Aby uzyskać certyfikat X.509, musisz poprosić o niego CA. Dostarczasz swój klucz publiczny, udowadniasz ,że posiadasz odpowiedni klucz prywatny i pewne informacje o sobie.. Potem cyfrowo podpisujesz informację i wysyłasz cały pakiet – żądanie certyfikatu – do CA CA wtedy wykonuje due diligence weryfikacji tej informacji jaką dostarczyłeś, jeśli jest poprawna, generuje ten certyfikat i zwraca ci go. Możesz myśleć ,że certyfikat X.509 wygląda jak standardowy certyfikat papierowy, z kluczem publicznym do niego dowiązanego. Masz swoją nazwę i pewne informacje o sobie, plus podpis osoby która stworzyła go dla ciebie.



Poprawność i zaufanie

Każdy użytkownik w systemie klucza publicznego jest podatny na fałszywy klucz (certyfikat). Poprawność jest wiarą w to , że certyfikat z kluczem publicznym należy do jego prawowitego właściciela. Poprawność jest istotna w środowisku klucza publicznego gdzie musisz stale konfrontować czy lub nie, określony certyfikat jest autentyczny. Jeśli gwarantujesz ,że klucz PGP należący do kogoś jest poprawny, możesz podpisać kopię bazy kluczy dla sprawdzenia faktu ,że jest on autentyczny. Jeśli chcesz aby inni wiedzieli ,że nadałeś temu certyfikatowi znak aprobaty, możesz wyeksportować podpis do serwera katalogów aby inni mogli go zobaczyć. Jak pisałem w sekcji o PKU, niektóre firmy projektują jeden lub więcej CA dla wskazania poprawności certyfikatu. W organizacji używającej PKI z certyfikatami X.509, zadaniem dla RA jest zatwierdzanie żądanego certyfikatu a zadaniem dla CA wystawienie certyfikatu użytownikowi. W organizacjach używających certyfikatów PGP bez PKI, zadaniem dla CA jest sprawdzenie autentyczności wszystkich certyfikatów PGP a potem podpisanie dobrego. Zasadniczo głównym celem CA jest powiązanie klucza publicznego z informacją identyfikującą zawartą w certyfikacie a zatem zapewnienie trzeciej części , że wszystkie środki zostały podjęty aby upewnić się ,że informacje identyfikujące i klucz jest poprawne .

Sprawdzenie poprawności

Jednym ze sposobów ustalenia poprawności jest przejście tego procesu ręcznie. Jest kilka sposobów wykonania tego. Możesz zażyczyć sobie od odbiorcy fizycznej kopii klucza publicznego. Ale czasami jest to niemożliwe i niewykonalne. Innym sposobem jest ręczne sprawdzenie odcisku palca certyfikatu. Podobnie jak unikalne są odciski palców człowieka, tak każdy odcisk palca certyfikatu PGP jest unikalny . Odcisk palca jest funkcją certyfikatu użytkownika i pojawia się jako właściwość certyfikatu. W PGP, odcisk palca może się pojawić jako liczba szesnastkowa lub szereg taka zwanych słów biometrycznych, które są fonetycznie różne i są używane dla uczynienia

procesu identyfikacji odcisku palca trochę łatwiejsze. Możesz sprawdzić czy certyfikat jest poprawny przez wywołanie właściciela klucza i poprosić właściciela o odczytanie odcisku palca klucza dla ciebie i zweryfikować ponownie odcisk palca aby uwierzyć ,że to prawda. To działa jeśli znasz głos właściciela, ale jak ręcznie weryfikować tożsamość kogoś kogo nie znasz? Niektórzy ludzie wstawiają odcisk palca swojego klucza na swojej wizytówce. Innym sposobem kontroli poprawności czyjegoś certyfikatu jest ufność ,że trzecia osoba przejdzie cały proces sprawdzania. CA , na przykład, jest odpowiedzialny za zapewnienie ,że przed wystawieniem certyfikatu, część klucza publicznego rzeczywiście należy do właściciela. Każdy kto zaufa CA będzie automatycznie rozważał certyfikaty podpisane przez CA za poprawne.

Ustanawianie zaufania
Zatwierdzasz certyfikaty. Ufasz ludziom. Dokładniej , ufasz ludziom zatwierdzającym certyfikaty innych ludzi.

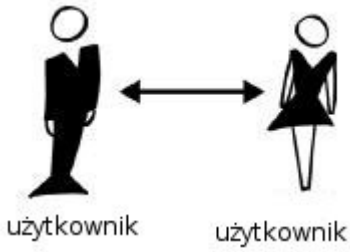
Meta i zaufani wprowadzający
W wielu sytuacjach, ludzie całkowicie ufają CA ustawiającym poprawne certyfikaty. Oznacza to, że każdy polega na CA przy ręcznym całym procesie walidacji Jest to dobre dla pewnej liczby użytkowników lub kilku działających stron, a potem jest nie możliwe dla CA zarządzanie na tym samym poziomie walidacji. W tym przypadku konieczne jest dodanie innych walidatorów do systemu. CA może być również meta – wprowadzającym. Meta wprowadzający nadaje nie tylko potwierdzenie kluczom ale nadaje możliwości ufania kluczom innych. Meta wprowadzający umożliwia innym działać jako zaufani wprowadzający. Ci zaufani wprowadzający mogą potwierdzać klucze z tym samym skutkiem co meta wprowadzający. Nie mogą jednak tworzyć nowych zaufanych wprowadzających. Meta wprowadzający i zaufany wprowadzający są terminami PGP .W środowisku X.509, meta wprowadzającym nazywany jest główny Urząd Certyfikacyjny (root CA) a zaufanym wprowadzającym podporządkowany CA. Root CAA używa klucza prywatnego związanego ze specjalnym typem certyfikatu nazywanym certyfikatem głównego CA do podpisania certyfikatów. Certyfikat podpisany przez certyfikat głównego CA jest widziany jako poprawny przez inne certyfikaty podpisane przez roota. Proces potwierdzania działa na dla certyfikatów podpisanych przez inne CA w systemie – tak długo jak certyfikat głównego CA podpisał podporządkowane certyfikaty CA, dowolny certyfikat podpisany przez CA jest rozpatrywany jako poprawny dla innych wewnątrz hierarchii.

Modele zufania
W relatywnie zamkniętych systemach, takich jak wewnątrz małej firmy, łatwo jest śledzić ścieżkę certyfikatu z powrotem do głównego CA. Jednak użytkownicy muszą często komunikować się z ludźmi spoza firmy, wliczając tych których nigdy nie spotkali. Ustanowienie zaufania do kogoś kto nie był wyraźnie zaufany dla CA jest trudne. Firmy postępują zgodnie z jednym z modeli zaufania, które dyktują użytkownikom jak ustanawiać poprawność certyfikatu. Są trzy różne modele:

- Zaufania bezpośredniego
- Zaufanie hierarchiczne
- Zaufanie sieciowe

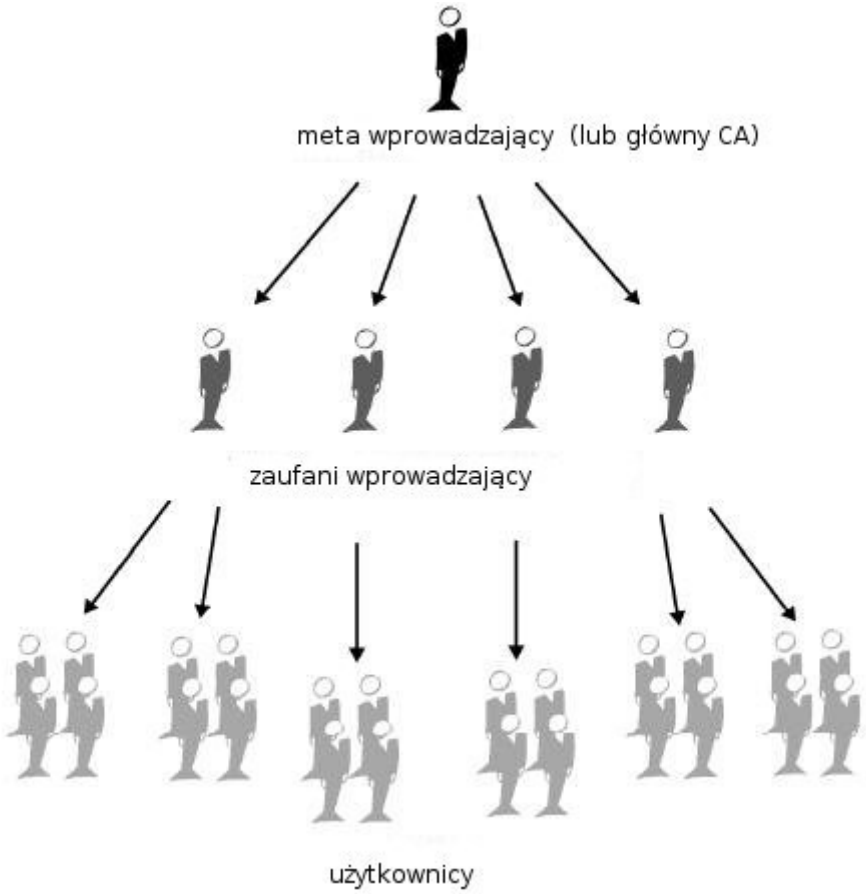
Bezpośrednie zaufanie
Bezpośrednie zaufanie jest najprostszym modelem zaufania. W modelu tym użytkownik wierzy ,że klucz jest poprawny ponieważ wiadomo skąd pochodzi. Wszystkie kryptosystemy używają tej formy zaufania w ten sposób. Na przykład, w przeglądarkach sieciowych, klucze głównego Urząd Certyfikacyjnego są bezpośrednio zaufane ponieważ zostały dostarczone przez wytwórcę. Jeśli jests jakaś forma hierarchii, rozwija się z tych bezpośrednich zaufanych certyfikatów. W PGP,

użytkownik który uwierzytelnia klucze i nigdy nie ustanawiał innego certyfikatu u zaufanego wprowadzającego ,używa zaufania bezpośredniego



Zaufanie hierarchiczne

W systemach hierarchicznych, jest kliku certyfikatów „głównych" z których wynika rozszerzone zaufanie.. Certyfikaty te mogą certyfikować certyfikaty, lub mogą certyfikować certyfikaty, które certyfikują jeszcze inne certyfikaty w łańcuchu. Rozważmy duże „drzewo" zaufania. „Liść" potwierdzania certyfikatu jest weryfikowany prze śledzenie zwrotne od certyfikującego do innego certyfikującego, dopóki nie zostanie znaleziony główny certyfikat.



Sieć zaufania

Sieć zaufania obejmuje powyższe modele ,ale również dodaje uwagę ,że zaufanie jest względne i pomysł ,że więcej informacji jest lepsze. Jest to zatem skumulowany model zaufania. Certyfikat może być zaufany bezpośrednio, lub zaufany w jakimś łańcuchu wracając z powrotem do bezpośrednio zaufanego certyfikatu głównego (meta wprowadzający), lub jakiejś grupy wprowadzających. Być może słyszałeś już o sześciu stopniach separacji, które sugerują ,że każda osoba na świecie może określić jakiś link do innej osoby na świecie używając sześciu , lub mniej innych ludzi jako pośredników. Jest to wprowadzanie sieciowe. Jest to również przegląd zaufania

PGP. PGP używa podpisów cyfrowych jaki formy wprowadzenia. Kiedy użytkownik podpisuje inny klucz, staje się on wprowadzającym dla tego klucza. Ponieważ proces trwa dalej, określ zaufanie sieciowe. W środowisku PGP,dowolny użytkownik może działać jako urząd certyfikujący. Dowolny użytkownik PGP może zatwierdzać certyfikat klucza publicznego innego użytkownika PGP. Jednak taki certyfikat jest tylko poprawny dla innego użytkownika jeśli pozostali rozpoznają zatwierdzającego jako zaufanego wprowadzającego (To znaczy , ufasz mi ,że pozostałe klucze są poprawne tylko jeśli uznasz mnie za zaufanego wprowadzającego)
Przechowywana baza kluczy publicznych każdego użytkownika wskazuje:

- czy lub nie, użytkownik uważa określony klucz jako poprawny
- poziom zaufania jaki użytkownik umieszcza w kluczu, który właścicielowi klucza może służyć jak certyfikator innych kluczy

Wskazujesz swoją kopią mojego klucza, co sądzisz o mnie.

Poziomy zaufania w PGP
Najwyższy poziom zaufania w kluczu, implikujące zaufanie, jest zaufaniem we własną parę kluczy. PGP zakłada,że jeśli twój własny klucz prywatny, musisz zaufać działaniu powiązanego z nim klucza publicznego. Dowolne klucze, podpisane przez bezpośrednio zaufany klucz , są poprawne. Są trzy poziomy zaufania jakie możesz przypisać komuś do klucza publicznego:

- Zaufanie całkowite
- Zaufanie marginalne
- Brak zaufania

Są również trzy poziomy wiarygodności:

- Wiarygodne
- Wiarygodność marginalna
- Niewiarygodne

Aby zdefiniować inny klucz jako zaufany wprowadzający:

1. Zacznij od poprawnego klucza :
   - podpisanego przez ciebie
   - podpisanego przez innego zaufanego wprowadzającego
2. Ustaw poziom zaufanie aby czuć ,że właściciel jest uprawniony

Na przykład, przypuśćmy ,że baza kluczy zawiera klucz Alicji. Uwiarygodniasz klucz Alicji i wskazujesz to przez podpisanie go. Wiesz ,że Alicja jest rzeczywiście pedantką przy potwierdzaniu innych kluczy. Dlatego przypisujesz jej kluczowi zaufanie całkowite. To czyni z Alicji Urząd Certyfikacji. Jeśli Alicja podpisze inny klucz, pojawi się jako Wiarygodny w twojej bazie kluczy. PGP wymaga jednego podpisanego całkowitego zaufania lub dwóch podpisanych marginalnych zaufań dla ustanowienia klucza jako wiarygodnego. Metody PGP rozważają dwa marginalne równe jednemu całkowitemu co jest podobne do sprzedawcy proszącego o dwie formy ID. Możesz rozpatrywać Alicję jako dosyć godną zaufania jak również rozpatrzyć Benka jako całkowicie godnego zaufania.

Unieważnianie certyfikatów
Certyfikaty są użyteczne tylko jeśli są zatwierdzone. Nie jest bezpiecznie upraszczać założenie ,że certyfikat jest zatwierdzony na zawsze. W większości organizacji i we wszystkich PKI, certyfikaty

mają ograniczony czas trwania. To ogranicza okres w jakim system jest zgodny z certyfikatem. Certyfikaty są zatem tworzone z planem okresu ważności: data / czas początkowy i data / czas końca. Oczekuje się ,że certyfikat będzie używany w całym okresie ważności (czasie życia). Kiedy certyfikat się kończy, nie będzie dłużej ważny, ponieważ uwierzytelnienie pary klucz / identyfikacja nie będzie dłużej zapewnione. (Certyfikat może być jeszcze bezpiecznie używany dla ponownego potwierdzenia informacji, która została zaszyfrowana lub podpisana w okresie jego ważności – jednak nie można zaufać zdaniom kryptograficznym wykonywanym wcześniej).
Są również sytuacje kiedy konieczne jest unieważnienie certyfikatu przed jego wygaśnięciem, tak jak kiedy certyfikat przechowuje termin zatrudnienia w firmie, lub oczekujemy ,że odpowiedni klucz prywatny certyfikatu został ustanowiony. Jest to wywołanie unieważnienia. Unieważniony certyfikat jest dużo bardziej niebezpieczny niż certyfikat który wygasł. Certyfikaty które wygasły są nieużywane, ale nie przenosi tego samego wątku co certyfikat unieważniony. Ktoś kto podpisał certyfikat , może unieważnić podpis na certyfiacie. Unieważniony podpis wskazuje ,że podpisujący nie wierzy ,że klucz publiczny i informacja identyfikacyjna nie idą już w parze. (lub odpowiedni klucz prywatny). Przy certyfikatach X.509, unieważniony podpis jest praktycznie taki sam jak unieważniony certyfikat, dodając,że tylko podpis na certyfikacie jest podpisem, który czyni go ważnym na pierwszym miejscu – podpis CA. Certyfikaty PGP dostarczają dodatkowej funkcji, którą możesz unieważnić certyfikat jednostki (nie tylko podpis na nim) jeśli czujesz ,że certyfikat powinien być cofnięty. Tylko właściciel certyfikatu (przechowujący odpowiedni klucz prywatny) lub ktoś kogo właściciel certyfikatu desygnował na unieważniającego może unieważnić certyfikat PGP. Tylko wydawca certyfikatu może unieważnić certyfikat X.509.

Komunikowanie ,że certyfikat został unieważniony
Kiedy certyfikat jest unieważniony, ważne jest aby poinformować użytkowników certyfikatu ,że nie będzie dłużej ważny. Z certyfikatami PGP, najpopularniejszym sposobem zakomunikowania ,że certyfikat został unieważniony, jest powiadomienie na serwerze certyfikatów, że nie używasz już tego klucza publicznego. W środowisku PKI komunikowanie o unieważnieniu certyfikatów jest dokonywane poprzez strukturę danych nazwaną Listą Unieważnionych Certyfikatów (CRL), która jest publikowana przez CA. CRL zawiera znacznik czasowy, listę zatwierdzonych wszystkich unieważnionych, certyfikaty które wygasły w systemie. Unieważnione certyfikaty pozostają na liście tylko dopóki nie straciły ważności, potem są usuwane z listy. CA dystrybuuje CRL do użytkowników w regularnych przedziałach czasu. Teoretycznie, zabezpiecza to użytkowników przed użycie wycofanego certyfiaktu. Możliwe jest że będzie czas między CRL'ami, kiedy nowszy wycofany certyfikat jest używany,

Co to jest długie hasło?
Większość ludzi zna ograniczenia przy dostępie do systemu komputerowego poprzez hasło ,które jest unikalnym łańcuchem znaków, które użytkownik wpisuje w kodzie identyfikacyjnym. Długie hasło jest dłuższą wersją hasła, i teoretycznie, bezpieczniejsze. Zazwyczaj składające się z wielu słów, długie hasło jest bezpieczniejsze przy standardowych atakach słownikowych, gdzie atakujący próbuje wszystkich słów w słowniku przy próbach określenia hasła. Najlepsze długie hasła są relatywnie długie i złożone i zawierają kombinację dużych i małych liter, cyfr i znaków interpunkcyjnych. PGP używa długiego hasła do szyfrowania twojego klucza na twojej maszynie. Twój klucz prywatny jest szyfrowany na twoim dysku używania mieszania długiego hasła jako tajnego klucza. Używasz długiego hasła do deszyfrowania i używania klucza prywatnego. Długie hasło powinno być trudne do zapomnienia i trudne dla innych do odgadnięcia. Powinno być to coś , co masz zakodowane w twojej długiej pamięci. Dlaczego? Ponieważ jeśli zapomnisz długiego hasła, nie będziesz szczęśliwy. Twój prywatny klucz stanie się całkowicie bezużyteczny bez długiego hasła.

Key splitting (podział klucza)
Mówi się ,że tajemnica nie jest tajemnicą jeśli jest znana więcej niż jednej osobie. Dzielenie pary kluczy prywatnych stwarza ten problem. Chociaż nie jest zalecane w praktyce, współdzielenie pary klucz prywatnych jest czasami konieczne. Corporate Signing Keys, na przykład, są prywatnymi kluczami używanymi przez firmy do podpidu – na przykład dokumentów prawnych, wrażliwych danych osobistych. W takim przypadku, warto mieć w posiadaniu dla wielu członków firmy dostęp do prywatnego klucza. W takim przypadku lepiej podzielić klucz między wielu ludzi w taki sposób aby jedna lub dwie osoby muszą przedstawić fragment klucza aby zrekonstruować go aby móc wykorzystać. Jeśli zbyt wiele fragmentów klucza są dostępne, wtedy nie można użyć klucza. Pewne przykłady dzielą na trzy fragmenty i wymagają dwóch z nich do zrekonstruowania klucza, lub dzielą na dwa fragmenty i wymagają obu. Jeśli jest używane połączenie bezpiecznej sieci podczas procesu rekonstrukcji, współwłaściciel klucza nie muszą być fizycznie obecni przy połączenia klucza.

2 Phil Zimmermann o PGP

Algorytmy symetryczne PGP
PGP oferuje wybór różnych algorytmów tajnych kluczy dla szyfrowania rzeczywistej wiadomości. Przez algorytm tajnego klucza, mamy na myśli konwencjonalny ,lub symetryczny szyfr blokowy, który używa tego samego klucza zarówno do szyfrowania jak i deszyfrowania. Symetryczny szyfr blokowy oferowany przez PGP to CAST, Potrójny -DES , IDEA i Twofish. Nie są one algorytmami „domowej roboty" Zostały one stworzone przez zespoły kryptografów o określonej reputacji. Z kryptograficznej ciekawości, możemy mówić dużo o tych algorytmach. CAST, Potrójny – DES i IDEA działają na 64 bitowych blokach tekstu jawnego i zaszyfrowanego. CAST i IDEA mają rozmiary 128 bitów, podczas gdy Potrójny - DES używa klucza 168 bitów. Podobnie jak Data Encrytpion Standarda (DES), te szyfry mogą być używane w trybach szyfrowego sprzężenia zwrotnego (CFB) i wiązania bloków zaszyfrowanych (CBC). PGP używa ich w 64 bitowym trybie CFB. PGP zawiera algorytm szyfrowania CAST ponieważ jest dobrym blokiem szyfrowym z 128 bitowym rozmiarem klucza, jest bardzo szybki i jest darmowy. Jego nazwa pochodzi od inicjałów projektantów, Carlisle'a Adamsa i Stanfforda Tavaresa z Northern Telecom (Nortel). CASt został dobrze zaprojektowany przez ludzi z dobrą reputacją na tym polu. Projekt jest oparty na formalnym podejściu z kilkoma formalnie dającymi się udowodnić założeniami dając dobry powód do wiary ,że prawdopodobnie wymaga wyczerpania klucza dla złamania jego 128 bitowego klucza. CAST nie jest słabym lub półsłabym kluczem. Są mocne argumenty ,że CAST jest całkowicie odporny zarówno na analizę liniową i różnicową kryptoanalizę, dwie najsilniejsze formy kryptoanalizy w publicznej literaturze. Projekt CAST i dobra reputacja jego twórców stał się celem krytpoanalitycznych ataków reszty akademickiej wspólnoty kryptografów. Szyfr blokowy IDEA (Internationa,l Data Encryptuon Alogrithm) jest oparty na koncepcji projektowej „mieszanych działań różnych grup algebraicznych". Został stworzony w ETH w Zurichu przez Jamesa L. Masseya i Xuejia Lai, i opublikowany w 1990 roku. Wcześniejsze publikacje dotyczyły algorytmu nazwanego IPES (Improved Proposed Encrytpion Standard), ale później zmieniono ją na IDEA. IDEA była odporna na ataki dużo lepiej niż wcześniejsze szyfry takie jak FEAL,REDOC-II, LOKI, Snefru i Khafre. IDEA jest również bardziej odporna niż DES na ataki kryptoanalityczne różniczkowe Bihama i Shamira, jak również ataki liniowe. Zaufanie w IDEA rośnie wraz z upływem czasu. Niestety, największą przeszkodą w akceptacji IDEA jako standardu jest fakt ,że Ascom Systec przechowuje patent na ten projekt i w przeciwieństwie do DES i CAST, IDEA nie może być dostępna dla każdego. Jako zabezpieczenie, PGP dołącza trzy kluczowy Potrójny – DES

w swoim repertuarze dostępnych szyfrów blokowych. DES został zaprojektowany przez IBM w połowie lat siedemdziesiątych. Chociaż został dobrze zaprojektowany, jest rozmiaru 56 bitów, co jest zbyt mały na dzisiejsze standardy. Potrójny – DES jest bardzo mocny i została konstruowany przez wiele lat, więc jest bezpieczniejszy niż nowsze szyfry takie jak CAST i IDEA. Potrójny – DES jest DES'em zastosowanym trzykrotnie do tego samego bloku danych, używając trzech różnych kluczy, z wyjątkiem drugiego działania DES wraca w trybie deszyfrowania. Ponieważ Potrójny – DES jest dużo wolniejszy niż CAST lub IDEA, szybkość nie jest zazwyczaj krytyczny dla aplikacji emailowych. Chociaż Potrójny – DES używa klucza o rozmiarze 168 bitów, efektywny silny klucz powienien mieć przynajmniej 112 bitów przeciwko atakującemu. Potrójny – DES nie jest chroniony przez patent. Począwszy od PGP w wersji 7.0, wprowadzono algorytm Twofish Bruce'a Schneier'a. Twofish był jednym z pięciu finalistów algorytmów w projekcie NIST Advanced Encryption Standard (AES). AES jest nowym szyfrem blokowym stworzonym z rozmiarem bloku 128 bitów i rozmiarami klucza 128 , 192 lub 256 bitów. Tymi pięcioma finalistami było Twofish, Serpent, Rijndael , RC6 i MARS. Klucze publiczne PGP generowane od wersji 5.0 PGP zawierały informacje osadzone w nim, które mówią nadawcy jaki szyfr blokowy użyty został, aby został zrozumiany przez oprogramowanie odbiorcy. Klucze publiczne Diffie-Hellman / DSS akceptuje CAST IDEA, AES Rijndael), Potrójny – DES lub Twofish są szyframi blokowymi, z CAST jako domyślnym wyborem. Tylko szyfr IDEA jest używany przez PGP do wysyłania komunikatów do kluczy RSA, ponieważ starsze wersje PGP obsługują tylko RSA i IDEA.

O podprogramach kompresji danych PGP

PGP zazwyczaj kompresuje jawny tekst przed jego zaszyfrowania go, ponieważ jest zbyt późno na kompresję jawnego tekstu po zaszyfrowaniu; dana zaszyfrowana nie jest kompresowalna. Dana skompresowana oszczędza na czasie przesłania i miejsce na dysku, i co ważniejsze, silniejsze bezpieczeństwo krytpograficzne. Większość technik kryptoanalitycznych wykorzystuje redundację znajdowaną w tekście jawnym dla złamania szyfru. Kompresja danych redukuje tą redundację w tekście jawnym,dlatego zwiększa się odporność na kryptoanalizę. Zajmuje to dodatkowy czas ale warto to zrobić z punktu widzenia bezpieczeństwa. Pliki które są zbyt krótkie dla kompresji, lub nie kompresują się dobrze, nie są kompresowane przez PGP. Dodatkowo, program rozpoznaje pliki stworzone w popularnych programach kompresujących, takiego jak PKZIP, i nie próbuje kompresować plików skompresowanych. Jako ciekawostka techniczna, program używa darmowego podprogramu kompresji ZIP napisanego przez Jean – Loup Gailly, Marka Adlera i Richarda B. Walesa. To oprogramowanie ZIP używa algorytmu kompresji, który jest funkcjonalnym odpowiednikiem używanym przez PKWare's PKZIP 2.x. To oprogramowanie kompresji ZIP zostało wybrane dla PGP głównie z powodu tego ,że ma rzeczywiście dobry współczynnik kompresji i ponieważ jest szybki.

O liczbach losowych używanych jako klucze sesyjne

PGP używa generatora kryptograficznego silnych pseudolosowych liczb dla tworzenia czasowych kluczy sesyjnych. Jeśli taki losowy plik nie istnieje, jest automatycznie tworzony i wypełniany prawdziwymi liczbami losowymi pochodzącymi z zebranych losowych zdarzeń przez program PGP od uderzeń w klawisze i ruchy myszki. Ten generator ponownie wypełnia plik za każdym razem kiedy jest używany, przez mieszanie w nim nowego materiału częściowo pochodzącego z czasu i innych rzeczywistych losowych zasobów. Używa algorytmu konwencjonalnego szyfrowania jako silnika dla generatora liczb losowych. Ten początkowy plik zawiera losowy materiał początkowy i materiał klucza losowego używanego w kluczu silnika szyfrowania konwencjonalnego dla generatora losowego. Ten początkowy plik losowy będą chroniony przed ujawnieniem, redukując ryzyko ataku pochodzącego z kolejnych lub poprzednich kluczy sesyjnych. Atakujący będzie miał trudno wyciągnąć coś użytecznego z przechwyconego tego pliku losowego, ponieważ plik jest

kryptograficznie wyprany przed i po każdym użyciu. Pomimo to, wydaje się że trzeba przechowywać go aby nie wpadł w niepowołane ręce. Jeśli to możliwe, uczyń plik czytelny tylko dla ciebie. Jeśli to niemożliwe, nie pozwalaj innym ludziom na kopiowanie plików ze swojego komputera.

O skrócie wiadomości

Skrót wiadomości jest kompaktowym (160 bitowym lub 128 bitowym) „destylatem" komunikatu lub sumy kontrolnej pliku. Możesz również myśleć o nim jako „odcisku palca" wiadomości lub pliku. Skrót wiadomości „przedstawia" twoją wiadomość, w taki sposób ,że jeśli wiadomość była modyfikowana w jakiś sposób, inne skróty wiadomości będą z niego obliczane. Czyni to możliwym wykrycie zmian dokonanych przez fałszerza. Skrót wiadomości jest obliczany przy użyciu silnej jednokierunkowej funkcji mieszającej wiadomości. Powinno być obliczeniowo niemożliwe dla atakującego wymyślić substytut wiadomości, która stwarzała by identyczny skrót wiadomości. W tym aspekcie, skrót wiadomości jest dużo lepszy niż suma kontrolna, ponieważ łatwo jest wymyśleć różne wiadomości , które tworzą taką samą sumę kontrolną . Ale podobnie jak w sumie kontrolnej, nie możesz wywnioskować oryginalnej wiadomości ze skrótu wiadomości. Algorytm skrótu wiadomości używany teraz w PGP jest nazywany SHA-1, co oznacza Secure Hash Algorithm, stworzony przez NSA dla National Institute of Standards and Technology (NIST). SHA-1 jest 160 bitowym algorytmem mieszającym. Niektórzy ludzie mogą uważać cokolwiek z NSA za podejrzane, ponieważ NSA jest znana z przechwytywania komunikacji i łamania kodów. Ale pamiętaj ,że NSA . Wszystkie nowe wersje PGP używają SHA-1 jako algorytmu skrótu wiadomości dla tworzenia podpisów z nowymi kluczami DSS, które jest zgodny z Digital Signature Standard NIST. Z powodów kompatybilności, nowsze wersje PGP używają jeszcze MD5 dla podpisów RSA, ponieważ starsze wersje PGP używają MD5 dla podpisów RSA. Algorytm skrótu wiadomości używany przez starsze wersje PGP to MD5, Message Digest Algorithm, umieszczony na publicznej domenie przez RSA Data Security, Inc. MD5 jest 128 bitowym algorytmem mieszającym. W 1996 roku, MD5 został złamany przez niemieckiego kryptografa Hansa Dobbertin. Chociaż MD5 nie został całkowicie złamany w danym czasie, odkryto ,że ma takie słabości, których nie używa się dla generowania podpisów

Jak chronić klucze publiczne przed zniekształceniem

W kryptosystemie kluczem publicznym , nie musisz chronić kluczy publicznych przed ujawnieniem, Faktycznie, lepiej jest jeśli są szeroko rozpowszechnione. Ale ważna jest ochrona kluczy publicznych przed zniekształceniem, aby upewnić się ,że klucz publiczny należy do osoby do której powinna należeć.Może to być największą słabością kryptosystemu z kluczem publicznym. Przypuśćmy ,że chcesz wysłać prywatną wiadomość do Alicji. Ściągasz certyfikat klucza publicznego Alicji z serwera kluczy. Szyfrujesz list do Alicji tym kluczem publicznym i wysyłasz go emailem. Niestety, bez wiedzy twojej lub Alicji inny użytkownik nazwany Karolem, zinfiltrował serwer kluczy i wygenerował własny klucz publiczny z ID Alicji dołączonym do niego. Podstępnie zastąpił fałszywy klucz w miejsce rzeczywistego klucza publicznego Alicji. Nieświadomie użyłeś fałszywego klucza należącego do Karola zamiast klucza publicznego Alicji. Wszystko wygląda normalnie ponieważ ten fałszywy klucz ma ID Alicji .Teraz Karol może odszyfrować tą wiadomość przeznaczoną dla Alicji ponieważ ma potrzebny klucz prywatny. Może nawet ponownie zaszyfrować odszyfrowana wiadomość z rzeczywistym kluczem publicznym i wysłać ją do ciebie abyś niczego nie podejrzewał. Co więcej może on nawet uczynić jawnym dobre podpisy od Alicji tym kluczem prywatnym ponieważ każdy może używać fałszywego klucza publicznego dla sprawdzenia podpisów Alicji. Jedyny sposób zabezpieczenia tego nieszczęścia jest zabezpieczenie przed zniekształceniem klucza publicznego. Jeśli otrzymałeś klucz publiczny bezpośrednio od Alicji , nie ma problemu. Ale może być to trudne jeśli Alicja jest tysiące kilometrów od ciebie. Być może mógłbyś otrzymać klucz publiczny Alicji od zaufanego przyjaciela Dawida, który wie , że

ma dobrą kopię klucza publicznego Alicji. Dawid może podpisać klucz publiczny Alicji, gwarantując integralność klucza publicznego Alicji. Dawid stworzył ten podpis swoim własnym kluczem prywatnym. Tak stworzony certyfikat podpisanego klucza publicznego, pokazujemy Alicji, i wiemy ,że nie został zniekształcony. Wymaga to abyś posiadał dobrą kopię klucza publicznego Dawida dla sprawdzenia jego podpisu. Być może Dawid dostarczył Alicji podpisaną kopię swojego klucza publicznego. Zatem Dawid może służyć jako „wprowadzający: między tobą a Alicją. Tak podpisany certyfikat klucza publicznego dla Alicji, może być uploadowany przez Dawida lub Alicję na serwer kluczy, a ty możesz go później ściągnąć. Potem możesz sprawdzić podpis przez klucz publiczny Dawida a zatem upewnisz się ,że jest to rzeczywisty klucz publiczny Alicji. Żaden oszust nie może zmusić cię do zaakceptowania swojego własnego fałszywego klucza jako Alicji ponieważ nie może sfałszować podpisu stworzonego przez Dawida. Zaufane osoby mogą nawet specjalizować się w dostarczaniu takiej usługi użytkownikom „wprowadzającym" przez dostarczenie podpisów dla ich certyfikatów klucza publicznego Takie zaufane osoby mogą być rozpatrywane jako „Urzędy Certyfikacji". Certyfikaty klucza publicznego noszące podpisy Urzędu Certyfikacji mogą być zaufane jak naprawdę należące do osoby do której przynależą. Wszyscy użytkownicy, którzy chcą w tym, partycypować, powinni znać dobrą kopię klucza publicznego Urzędu Certyfikacji, aby jego podpisy mogły być zweryfikowane. Zaufany , scentralizowany Urząd Certyfikacji jest szczególnie odpowiedni dla dużych bezosobowych sterowanych centralnie firm lub instytucji rządowych. Pewne środowiska instytucjonalne używają hierarchicznych Urzędów Certyfikacji. Dla bardziej zdecetralizowanych środowisk, zezwolenie wszystkim użytkownikom na działanie jako zaufani wprowadzający z przyjaciółmi i kolegami będzie prawdopodobnie lepsze niż zcentalizowany klucz urzędu certyfikacyjnego. Jedną z atrakcyjnych funkcji PGP jest to ,że może działać również w środowiskach zcentralizowanych z Urzędem Certyfikacji lub bardziej zdecentralizowanych środowiskach gdzie indywidualnie wymienia się klucze osobiste. Cała sprawa z ochroną klucza publicznego przed zniekształceniem jest najtrudniejszym problemem w praktycznych aplikacjach z kluczem publicznym. Jest to „pięta Achillesowa" kryptografii a kluczem publicznym. Powinieneś używać klucza publicznego tylko po tym jak upewnisz się ,że jest to dobry klucz publiczny, który nie został zniekształcony, i że rzeczywiście należy do osoby z którą został powiązany. Możesz być tego pewny jeśli otrzymasz certyfikat tego klucza publicznego bezpośrednio od właściciela, lub jeśli złożył podpis ktoś do kogo masz zaufanie, i od kogo dostałeś już dobry klucz publiczny.. Również, ID użytkownika powinno mieć pełną nazwę właściciela klucza, nie tylko jego imię. Niezależnie od tego jak jesteś ufny, nigdy nie powinieneś ulegać korzyścią i ufać kluczom publicznym ściągniętym z serwera kluczy lub strony WWW, chyba ,że jest podpisany przez kogoś komu ufasz. Ten nie certyfikowany klucz publiczny może być zniekształcony przez kogoś, być może nawet przez administratora systemu serwera kluczy lub strony WWW. Jeśli prosisz kogoś o podpisanie certyfikatu klucza publicznego, musisz mieć pewność ,że rzeczywiście należy on do osoby , której nazwisko figuruje w ID użytkownika tego certyfikatu klucza publicznego. Jest tak ponieważ twój podpis na jego certyfikacie klucza publicznego jest obietnicą daną przez ciebie ,że ten klucz publiczny na pewno należy do tej osoby. Inni ludzie którzy wierzą ci będą akceptować ten klucz publiczny ponieważ zawiera ona twój podpis Będzie nierozsądne polegać na pogłoskach; nie podpisuj klucza publicznego chyba ,że masz pewność ,że rzeczywiście należy on do niego. Najlepiej byłoby , gdybyś podpisał go tylko jeśli otrzymałeś go bezpośrednio od właściciela. Aby podpisać klucz publiczny, musisz być bardzo pewny właściciela klucza niż czy tylko chcesz użyć tego klucza do szyfrowania wiadomości. Aby być przekonanym co do ważności klucza aby go użyć, powinny być wystarczająca certyfikacja podpisów do zaufanych wprowadzających. Ale podpisując klucz, powinieneś wymagać wiedzy kto jest właścicielem klucza. Być może możesz zadzwonić do właściciela klucza i odczytać mu odcisk palca klucza, aby potwierdzić ,że klucz rzeczywiście do niego – i upewnić się ,że rzeczywiście rozmawiasz z właściwą osobą. Zapamiętaj ,że twój podpis na certyfikacie klucza publicznego nie gwarantuje integralności osoby, ale tylko gwarantuje

integralność osoby do której należy klucz publiczny. Nie ryzykuj wiarygodności przez podpisanie klucza publicznego socjopacie, nawet jeśli jesteś przekonany ,że klucz rzeczywiście należy do niego. Inni ludzie zaakceptują ten klucz jako należący do niego ponieważ podpisałeś go (zakładając ,że ci ufają), ale nie zaufają właścicielowi klucza. Zaufanie ,że klucz jest dobry nie jestem tym samym co zaufanie do właściciela klucza. Będzie dobrym pomysłem trzymać własny klucz publiczny ze zbiorem podpisanych certyfikatów dołączonych od różnych „wpropwadzających", w nadziei ,że większość ludzi będzie ufała przynajmniej jednemu z wprowadzających, który gwarantuje poprawność twojego klucza publicznego. Możesz przekazać klucz z dołączonym zbiorem podpisanych certyfikatów na różne serwerów kluczy. Jeśli podpiszesz jakiś klucz publiczny, zwracasz go do nich ze swoim podpisem tak aby, można dodać go do ich własnych zbiorów referencji dla ich własnych kluczy publicznych. Upewnij się ,że nikt nie zniekształcił twojej bazy kluczy publicznych. Sprawdzanie nowo podpisanego certyfikatu klucza publicznego musi ostatecznie zależeć od integralności zaufanych kluczy publicznych, które są już w twojej bazie kluczy publicznych. Lepiej zarządzać fizyczną kontrolą bazy kluczy publicznych z komputera zamiast na zdalnym systemie, tak jak zrobiłbyś dla klucza prywatnego. Jest to ochrona przed zniekształceniem, nie przed ujawnieniem, Utrzymuj zaufaną kopię zapasową bazy kluczy publicznych a klucza prywatnego na medium chronionym przed zapisem. Ponieważ twój własny zaufany klucz publiczny jest używany jako końcowy uwierzytelniający dla bezpośredniego i pośredniego certyfikowania wszystkich pozostałych kluczy w twojej bazie kluczy, jest najważniejszym kluczem do ochrony przed zniekształceniem. Możesz chcieć przechowywać kopię zapasową na dyskietce chronionej przed zapisem. PGP generalnie zakłada , że będziesz zarządzał fizycznym bezpieczeństwem swojego systemu i bazy kluczy, jak również swoją kopią PGP. Jeśli intruz może zniekształcić to co masz na dysku, wtedy teoretycznie może zanieczyścić sam program. Jednym ze skomplikowanych sposobów na ochronę całej bazy kluczy publicznych przed zanieczyszczeniem jest podpis całego bazy twoim własnym prywatnym kluczem. Możesz to zrobić przez osobno podpisany certyfikat bazy kluczy publicznych.

Jak PGP śledzi który klucz jest poprawny?

Przed przeczytaniem tej sekcji , powinieneś przeczytać sekcję poprzednią. PGP śledzi jakie klucze w bazie kluczy publicznych są właściwie certyfikowane z podpisami od wprowadzających do których mamy zaufanie. Wszystko co musisz zrobić to powiedzieć PGP jacy ludzie, jakim ufasz , są wprowadzającymi, i certyfikować ich klucze własnym zaufanym kluczem. PGP może pobrać go automatycznie walidując inne klucze, które będą podpisane przez desygnowanych wprowadzających. I oczywiście osobiście możesz podpisać więcej kluczy. Są dwa całkowicie oddzielne kryteria jakich używa PGP dla osądzenia użyteczności klucza publicznego:

Czy klucz rzeczywiście należy do osoby która pojawia się jako właściciel? Innymi słowy , czy jest podpisany zaufanym podpisem?

Czy należy do kogoś komu ufasz aby certyfikował inne klucze?

PGP może wykalkulować odpowiedź na pierwsze pytanie. Odpowiedzi na drugie pytanie musisz udzielić PGP wyraźnie. Kiedy dostarczysz odpowiedzi na pytanie 2, PGP wykalkuluje odpowiedź na pytanie 1 dla innych kluczy podpisanych przez wprowadzającego, którego desygnowałeś jako zaufanego. Klucze ,które certyfikowałes przez zaufanego wprowadzającego są uznawane za poprawne przez PGP. Klucze należące do zaufanych wprowadzających muszą same być certyfikowane albo przez ciebie albo przez innych zaufanych wprowadzających. PGP pozwala również na możliwość posiadania kilku cieni zaufania dla ludzi działających jako wprowadzających. Twoje zaufanie dla właściciela klucza działającego jako wprowadzający nie odzwierciedla twojego szacunku dla ich osobistej integralności; powinno również odzwierciedlać jak kompetentni są w zrozumieniu zarządzania kluczami i używania dobrego osądu przy podpisywaniu kluczy . Możesz desygnować osobę jako nie zaufaną, marginalnie zaufaną lu całkowicie zaufaną dla certyfikacji innych kluczy publicznych. Ta informacja zaufania jest

przechowywana w twojej bazie kluczy z ich kluczem ale kiedy mówisz PGP aby skopiował klucz z bazy kluczy, PGP nie kopiuje informacji zaufania wraz z kluczem, ponieważ twoje prywatne zdanie na temat zaufania jest postrzegane jako poufne. Kiedy PGP szacuje poprawność klucza publicznego, bada poziom zaufania wszystkich dołączonych podpisów certyfikowanych. Oblicza wzmocniony wynik poprawności; na przykład dwa marginalnie zaufane podpisy są uważane za wiarygodne jak jeden w pełni zaufany podpis. Sceptycyzm programu jest regulowany – na przykład, może wymusić na PGP aby wymagał dwóch w pełni zaufanych podpisów lub trzech marginalnie zaufanych podpisów dla ustanowienia klucza jako poprawnego. Twój własny klucz jest „aksjomatycznie" poprawny dla PGP, nie potrzebujący podpisu wprowadzającego dla udowodnienia jego ważności. PGP wie które klucze publiczne są twoje przez spojrzenie na odpowiednie klucze prywatne w kluczu prywatnym. PGP zakłada również ,że sam sobie zaufałeś całkowicie certyfikując inne klucze.
Standardowe schematy zarządzania kluczem publicznym stworzone przez rząd lub inne monolityczne instytucje , takie jak Internet Privacy Enhamced Mail (PEM), które są oparte na scentralizowanej kontroli i obowiązkowo scentralizowanym zaufaniu. Schematy standardowe polega na hierarchii Urzędu Certyfikacji które dyktują kto musi być zaufany. Program decentralizuje metody probabilistyczne dla określania legalności klucza publicznego, co jest fragmentem architektury zarządzania klucza. PGP pozwala ci samemu wybrać komu zaufać, ustawiając cię na górze twojej piramidy prywatnych certyfikatów. PGP jest dla ludzi którzy wolą sami składać swój spadochron. Zwróć uwagę ,że chociaż to podejście zdecentralizowane, do zwykłych członków organizacji jest tu akcentowane, nie oznacza to ,że PGP nie wykonuje się równie dobrze w bardziej hierarchicznych, scentralizowanych schematach zarządzania kluczem publicznym. Duże korporacje będą chciały mieć centralną osobę, która podpisze wszystkie klucze pracowników. PGP obsługuje taki scenariusz scentralizowany jako szczególny przypadek bardziej ogólnego modelu zaufania.

Jak chronić klucze prywatne przed ujawnieniem
Aby ochronić klucz prywatny, możesz zacząć od fizycznej kontroli nad nim. Trzymanie go w komputerze jest OK. Jeśli musisz używać komputera firmowego, nad którym nie zawsze masz fizyczną kontrolę nad nim, wtedy przechowuj bazy kluczy prywatnych i publicznych na zabezpieczonym, chronionym przed zapisem, dysku i nie pozostawiać go , kiedy wychodzisz z biura. Nie jest dobrym pomysłem pozwalać aby rezydował on w systemie takim jak system dial-up UNIX. Ktoś może podsłuchiwać linię modemową i przechwycić twoje długie hasło a potem uzyskać twój aktualny klucz prywatny ze zdalnego systemu. Powinieneś używać tylko klucza prywatnego na maszynie która jest pod twoją fizyczna kontrolą. Nie przechowuj długiego hasła na komputerze na którym masz swój plik z prywatnym kluczem. Przechowywanie ich razem jest bardzo niebezpieczne. Nie chciałbyś aby wpadły w niepowołane ręce. Zrób kopię klucza prywatnego – pamiętaj ,masz tylko kopię klucza prywatnego a zgubienie go będzie powodować bezużyteczność wszystkich kopi klucza publicznego jakie rozsiałeś po całym świecie
Zdecentralizowane, nie instytucjonalne podejście , jakie obsługuje PGP dla zarządzania kluczami publicznymi ma swoje zalety, ale niestety również oznacza ,że nie możesz oprzeć się na pojedynczej centralnej liście na której zostały zawarte klucze. Czyni to trochę trudniejszym zawarcie uszkodzenia klucza prywatnego.
Jeśli zdarzy się gorszy przypadek – jeśli zarówno klucz prywatny i długie hasło są naruszone – będziesz musiał dokonać „unieważnienie klucza" certyfikatu. Ten rodzaj certyfikatu jest używany dla ostrzegania innych ludzi aby zatrzymać używanie klucza publicznego. Możesz użyć PGP dla stworzenia takiego certyfikatu przez użycie polecenia Revoke z menu PGPkeys lub przez Designated Revoker do tego. Wtedy musisz wysłać to do serwera certyfikatu aby inni mogli go znaleźć. Ich własne oprogramowanie PGP zainstaluje ten certyfikat unieważnionego klucza w ich bazie kluczy publicznych i automatycznego zabezpieczenia ich przed przypadkowym użyciem

klucza publicznego ponownie. Możesz potem wygenerować nową parę kluczy prywatny/publiczny i opublikować nowego klucza publicznego. Możesz wysłać jeden pakiet zawierający zarówno nowego klucza publicznego i certyfikat unieważnionego klucza dla starego klucza.

Co jeśli zgubisz swój klucz prywatny ?
Zazwyczaj, jeśli chcesz unieważnić swój klucz prywatny, możesz użyć polecenia Revoke z menu PGPkeys aby unieważnić certyfikat, podpisany twoim kluczem prywatnym. Ale co możesz zrobić jeśli zgubisz swój klucz prywatny , lub twój klucz został usuniety, lub zapomniałeś swoje długie hasło? Nie możesz unieważnić go sam, ponieważ musisz używać swojego klucza prywatnego do jego unieważnienia. Jeśli nie musisz desygnować unieważniającego dla twojego klucza, każdy kto PGP określił , może unieważnić klucz , musisz poprosić każdą osobę która podpisała twój klucz aby zwolnić ich certyfikat. Wtedy ktoś kto próbuje użyć klucza opartego o zaufanie do jednego z twoich wprowadzających nie będzie wiedział o zaufaniu do twojego klucza.

GLOSARIUSZ

A5
Algorytm kryptograficzny używany w europejskich komórkach

Acces control (Kontrola dostępu)
Metoda ograniczenia dostępu do zasobów, pozwalająca na dostęp tylko jednostkom uprzywilejowanym

Additional recipient request key
Specjalny klucz, którego obecność wskazuje, że wszystkie zaszyfrowane wiadomości do powiązanego klucza bazowego, powinny być również szyfrowane do niego.

AES (Advanced Encryption Standard)
Standard rządu USA dla algorytmu zastępującego starszy DES. AES ma 16 bajtowe bloki i może działać na kluczach 128, 192 lub 256 bitowych.

AKEP (Authentication Key Exchange Protocol)
Przekazanie klucza oparte o szyfrowanie symetryczne pozwalające dwóm jednostkom wymieniać współdzielony tajny klucz, bezpiecznie przed atakującymi pasywnymi.

Algorytm (szyfrowanie)
Zbiór zasad matematycznych (logika) używanych w procesie szyfrowania i deszyfrowania.

Algorytm (mieszanie)
Zbiór zasad matematycznych (logika) używanych w procesie tworzenia skrótu wiadomości i generowania klucza / podpisu

Anonimowość
Maskowanie tożsamości jednostki

ANSI (American National Standards Institute)
Standard stworzony przez różne komitety Accredited Standards Committees (ASC). Komitet X9 skupił się na standardach bezpieczeństwa dla usług przemysłowych.

API (Application Programming Interface)

Środek wykorzystujący funkcje oprogramowania, pozwalając niepodobnym produktom oprogramowania na wzajemną interakcję.

ASN.1 (Abstract Syntax Notation One)

Standard ISO/IEC dla kodowania zasad używany w certyfikatach ANSI X.509;są dwa typy – DER (Distinguished Encoding Rules) i BER (Basic Encoding Rules).

Asymetryczne klucze

Oddzielny ale zintegrowana para kluczy, składająca się z jednego klucza publicznego i jednego klucza prywatnego. Każdy klucz jest jednokierunkowy, co oznacza ,że klucz używany do szyfrowania informacji może nie być użyty do odszyfrowania tej samej danej.

Authentication (uwierzytelnienie)

Proces demonstrujący czy jednostka jest tym czym jest

Authorization certificate (Certyfikat autoryzacji)

Elektroniczny dokument ustalający dostęp lub prawa uprzywilejowania.

Autoryzacja

Proces określania co jednostka może wykonać

Blind signature (Ślepy podpis)

Możliwość podpisania dokument bez wiedzy o jego zawartości, podobnie do notariusza.

Blokowy szyfr

Szyfr symetryczny działający na blokach tekstu jawnego i tekstu zaszyfrowanego, zazwyczaj 64 lub 128 bitowy.

Blowfish

64 bitowy symetryczny szyfr blokowy składający się z ekspansji klucza i szyfrowania danych. Szybki, prosty i kompaktowy algorytm w domenie publicznej napisany przez Bruce;a Schneiera

CA (Urząd Certyfikacyjny)

Trzecia strona godna zaufania (TTP) która tworzy certyfikaty składające się z zapewnienia o różnych atrybutach i łączy je jednostce i / lub z jej kluczem publicznym

CAPI (CryptoAPI)

Kryptografia Microsoft API dla systemu operacyjnego opartego o Windows i aplikacje

Capstone

Stworzony przez NSA chip kryptograficzny , który zaimplementował rząd USA jak możliwości Key Escrow

CAST

Szyfr blokwowy z 8 bajowymi blokami i 128 bitowym kluczem. Sworzony w Kanadzie prze Carlisle'a Adamsa i Stafforda Tavaresa

CBC (Cipher Block Chaining – Wiązanie Bloków Zaszyfrowanych)

Proces XORowania tekstu jawnego z poprzednim blokiem tekstu zaszyfrowanego przed szyfrowaniem, zatem dodaje mechanizm sprzężenia zwrotnego do szyfru blokowego

CERT (Computer Emergency Repsonse Team)

Bank informacji bezpieczeństwa, który promuje świadomość bezpieczeństwa. CERT dostarcza 24 godzinnej pomocy technicznej dla komputerów sieci z zajściami związanymi z bezpieczeństwem. CERT znajduje się przy Software Engineering Institute prze Uniwersytecie Carnegie Mellon w Pittsburgu.

Certyfikat (cyfrowy certyfikat)

Dokument elektroniczny składający się z klucza publicznego, informacji o kluczu i podpis cyfrowy łączący klucz i informację razem. To jest dokument, który stanowi ,że podpisujący wierzy ,że informacja i klucz są razem. Łączenie nazw, adresy email , tworzą klucz jako Certyfikat Tożsamości.

CFM (Cipher Feedback Mode - Tryb Sprzężenia Zwrotnego Szyfru)

Szyfr blokowy, który jest implementowany jako samo synchronizujący szyfr strumieniowu

CDSA (Common Data Security Architecture)

Laboratoryjna Architektura Intela (IAL) tworząca środowisko dla adresowania problemów bezpieczeństwa danych odziedziczonych z Internetu i Intranetu , dla użycia w produktach Intela lub innych internetowych

Certyfikacja

Aprobata informacji przez zaufaną jednostkę

Ciphertext (Tekst zaszyfrowany)

Dane wyjściowe szyfru. Szyfr zaczyna się od tekstu jawnego i używa klucza dla stworzenia tekstu zaszyfrowanego

Confidentiality (Poufność)

Utrzymywanie czegoś prywatnego lub tajnego w tajemnicy przed innymi, al ci którzy są uwierzytelnieni widzą je

Cookie

Plik lub token , przekazywany z serwera sieciowego do klienta sieciowego (przeglądarki), który jest używany do identyfikacji ciebie i zapisania informacji takich jak ID i hasła, adresy mailowe, numer karty kredytowej i inne informacje

Credentials (Uwierzytelniania)

Coś co dostarcza podstaw dla wierzytelności lub poufności

CRL (Certificate Revocation List – Lista Unieważnionych Certyfikatów)

Online, aktualna lista certyfikatów, które nie są dłużej ważne.

Cross – certification (Certyfikacja wzajemna)

Dwie lub więcej organizacje lub Urzędy Certyfikacji, które współdzielą poziom

zaufania.

Cryptoanalysis (Kryptoanaliza)

Odwrotność krytpografii, kryptoanaliza jest sztuką i nauką łamania szyfrów, tekstów zaszyfrowanych lub klucz

CRYPTOKI

Znane również jako PKCS#11, standard API dla używania tokenów kryptograficznych zawierających małe karty i akceleratory.

Cryptography (Kryptografia)

Sztuka lub nauka tworzenia wiadomości które są połączeniem prywatnych, podpisanych nie zmodyfikowanych z niezaprzeczalnością.

Cryptosystem (Kryptosystem)

System składający się z algorytmów kryptograficznych, wszystkich możliwych tekstów jawnych, zaszyfrowanych kluczy.

Data integrity (Integralność danych)

Metoda zapewnienia, że informacji nie została modyfikowana prze nieautoryzowane lub nieznane środki

Deszyfrowanie

Proces przetwarzania tekstu zaszyfrowanego z powrotem na tekst jawny.

DES (Data Encryption Standard)

64 bitowy szyfr blokowy, algorytm symetryczny znany również jako Data Encryption Algorithm (DEA) przez ANSI i DEA-1 przez ISO. Używany przez 20 lat, zaadoptowany w 1976 roku jako FIPS 46.

Dictionary attack (Atak słownikowy)

Obliczeniowy atak brute force dla uzyskania hasła, przez wypróbowanie oczywistych i logicznych kombinacji słów.

Diffie - Hellman

Pierwszy algorytm z kluczem publicznym, stworzony w 1976 roku, korzystający z logarytmów dyskretnych w polach skończonych.

Digital cash (Elektroniczne pieniądze)

Elektroniczne pieniądze która jest przechowywana i transferowana przez różne złożone protokoły.

Direct trust (Bezpośrednie zaufanie)

Ustalenie zaufania między partnerami

Dyskretny logarytm

Matematyczny problem używany w / przez algorytmy asymetryczne, podobnie jak Diffie – Hellman czy Krzywa Eliptyczna. Jest odwrotnością wykładnika modularnego, który jest funkcją jednokierunkową.

DMS (Defense Messaging System)

Standard stworzony przez Departament Obrony USA dla przekazywania wiadomości dla rządu i agencji wojskowych

DNSSEC (Domain Name System Security Working Group)

Zaproponowany projekt IETF, który będzie określał poprawki do protokołu DNS chroniąc DNS przed nieautoryzowanymi modyfikacjami danych i maskaradą danych pierwotnych.Będzie dodawał integralność danych i uwierzytelnienie do DNS poprzez podpisy cyfrowe.

DSA (Digital Signature Algorithm)

Algorytm klucza publicznego tylko z podpisem, używany w Digital Signature Standard. DSA jest wariantem algorytmu Elgamala.

Digital signature (podpis cyfrowy)

Elektroniczna identyfikacja osoby lub rzeczy stworzony przy użyciu algorytmu klucza publicznego. W zamiarach, weryfikacja odbiorcy integralności danych i tożsamości nadawcy danej.

DSS (Digital Signature Standard)

Federal Information Processing Standard (FIPS) USA dla podpisów cyfrowych, używający DSA i SHA-1

ECC (Elliptic Curve Cryptosystem – Kryptosystem Krzywej Eliptycznej)

Wariant algorytmów z kluczem publicznym rodziny Diffie – Hellmana, działający na innych zbiorach niż liczby całkowite i dający mniejsze, szybciej wykonujące się klucze,

EDI (Electronic Data Interchange)

Bezpośrednia, ustandaryzowana wymiana komputer – z – komputerem, dokumentów biznesowych, między organizacją a jej dostawcami i klientami.

Elgamal

Wariant Diffie – Hellmana, który pozwala na szyfrowanie kluczem publicznym podobnym do szyfrowania RSA. Klucze Diffie – Hellmana w PGP są kluczami Elgamal

Elgamala schemat

Używany do podpisów cyfrowych i szyfrowania, oparty na logarytmach dyskretnych w polach skończonych; może być użyty z funkcją DSA.

Encryption (Szyfrowanie)

Proces maskowania wiadomości w taki sposób aby ukryć jej zawartość

Entropia

Matematyczna miara ilości niepewności i losowości

FEAL

Szyfr blokowy używający 64 bitowych bloków i 64 bitowego klucza, stworzony przez A.Shimizu i S.Miyaguchi w japońskim NTT .

Filtr

Funkcja, zbiór funkcji, lub połączenie funkcji które stosują jakąś liczbę transformacji na zbiorze wejściowym, tworząc zbiór wyjściowy zawierający tylko te elementy zbioru wejściowego, które spełniają kryteria transformacji. Wybrane elementy mogą albo nie, być dalej transformowane do wynikowego zbioru wyjściowego. Przykładem może być wyszukiwanie funkcji, która akceptuje wiele łańcuchów mających związki lgiczne ((jak a lub jak b) ale nie zawierające c), i opcjonalnie wymusza przypadek znalezionych łańcuchów w danych wynikowych.

Finerprint (Odcisk palca)

Unikalny identyfikator dla klucza, który jest uzyskiwany przez mieszanie określonej części danych klucza.

FIPS (Federal Information Processing Standard)

Rządowy standard USA wydany przez NIST

Firewall

Połączenie sprzętu i oprogramowania, które chronią granice sieci publicznej / prywatnej przeciwko pewnym atakom ,zapewniając pewien stopień bezpieczeństwa.

GAK (Government Access to Keys)

Metoda dla rządu do przechowywania indywidualnych kluczy prywatnych

Gost

64 bitowy symetryczny szyfr blokowy używający 256 bitowego klucza , stworzony w dawnym Związku Radzieckim.

GSS-API (Generic Security Services API)

Wysokopoziome bezpieczne API oparte o IETF RFC 1508, które izoluje kod aplikacji zorientowany sesyjnie przed szczegółami implementacji.

Hash function (Funkcja mieszająca)

Jednokierunkowa funkcja mieszająca – funkcja która tworzy skrót wiadomości, który nie może być odwrócony dla stworzenia oryginału.

HMAC (Hash-based Message Auhentication Code)

Mechanizm używający funkcji mieszającej, takiej jak SHA-1 dl stworzenia MAC opartego o klucz współdzielony.

Hierarchiczne zaufanie

Szereg stopni jednostek, które dystrybuują zaufanie w organizacji, powszechnie używając certyfikatu uwierzytelnienia ANSI X.509. Meta wprowadzający PGP są mechanizmem dla stosowania zaufania hierarchicznego zaufania z certyfikatami PGP.

HTTP (HyperText Transfer Protocol)

Protokół używany dla transferowania dokumentów między serwerami lub z serwera do klienta.

IDEA (International Data Encryption Standard)

64 bitowy symetryczny szyfr blokowy używający 128 bitowych kluczy oparty o mieszaniu różnych grup algebraicznych. Uznawany za silny algorytm.

IETF (Internet Engineering Task Force)

Duża , otwarta międzynarodowa społeczność projektantów sieciowych, operatorów, sprzedawców i badaczy, skupiona na ewolucji architektury Internetu i działań w nim.

Identyfikacyjny certyfikat

Podpisana instrukcja, która łączy klucz z pojedynczą nazwą i ma w zamierzeniu służyć delegowaniu uwierzytelniania od nazwy pojedynczej do klucza publicznego.

Inicjujący wektor (IV)

Blok danych , które służą jako punkt startowy dla szyfru blokowego używający trybu łańcuchowego sprzężenia zwrotnego

Integralność

Założenie ,że dana nie jest zmodyfikowana (przez nieuprawnioną osobę) podczas przechowywania lub transmisji.

IPsec

Schemat szyfrowania warstwy TCP/IP wewnątrz IETE

ISO (International Organization for Standardization)

Odpowiedzialny za szeroki zakres stnadardó, takich jak model OSI i międzynarodowe związki z ANSI w X.509 .

ITU-T (International Telecommunication Union-Telecommunication)

Formalnie CCITT (Consultative Committee for International Telegraph and Telephone), organizacja standardyzacji technologii telekomunikacyjnych.

Kerberos

System uwierzytelnia oparty o serwer stworzony w MIT, Microsoft wbudował wariant Kerberosa do systemu domen.

Klucz

Liczba używana w szyfrze do szyfrowania jawnego tekstu do tekstu zaszyfrowanego.

Klucza deponowanie

Mechanizm odzyskiwanie klucza, który działa przez proste utrzymywanie kopii kluczy

Klucza wymiana

Schemat dla dwóch lub więcej węzłów dla transferu tajnego klucza sesyjnego poprzez niezabezpieczony kanał.

Klucza długość

Liczba bitów przedstawiająca rozmiar klucza; im dłuższy klucz tym jest on silniejszy.

Kluczami zarządzanie

Proces i procedury dla bezpiecznego przechowywania i dystrybuowania dokładnych kluczy kryptograficznych;ogólnie proces generowania i dystrybuowania klucza krytpograficznego dla uwierzytelnienia odbiorcy w bezpieczny sposób.

Kluczy odzyskiwanie

Mechanizm dla odtwarzania kluczy kryptograficznych z ostateczną możliwością odszyfrowania tekstu zaszyfrowanego nim

Klucza rozbijanie

Proces dzielenia na części pojedynczego klucza między wiele części, żadna nie mająca możliwości rekonstrukcji całego klucza.

LDAP (Lightweight Directory Access Protocol)

Prosty protokół , który obsługuje dostęp do operacji wyszukiwania w katalogach zawierających informacje takie jak nazwy, numery telefonów, i adresy, w niekompatyblinych systemach poprzez Internet.

MAA (Message Authenticator Algorithm)

Standard ISO, który tworzy 32 bitowy hash, stworzony dla mainframe'ów IBM

MAC (Message Authentication Code)

Ekwiwalent klucza symetrycznego podpisu cyfrowego.MAC'i nie ukrywają danych, ale pozwalają komuś kto zna klucz, poznać czy nie był zmodyfikowany.

MD2 (Message Digest 2)

128 bitowa , jednokierunkowa funkcja mieszająca stworzona przez Rona Rivesta, uzależniona od losowej permutacji bajtów.

MD4 (Message Digest 4)

128 bitowa , jednokierunkowa funkcja mieszająca stworzona przez Rona Rivesta, używająca prostego zbioru manipulacji bitowych na 32 bitowych operandach

MD5 (Message Digest 5)

Poprawiona, bardziej złożona wersja MD4, ale jeszcze 128 bitowa, jednokierunkowa funkcja mieszająca.

Message digest (Skrót wiadomości)

Liczba która jest pochodną z wiadomości. Zmiana pojedynczego znaku w wiadomości powoduje ,że wiadomość będzie miała inny skrót wiadomości.

MIC (Message Integrity Check)

Pierwotnie zdefiniowane w PEM dla uwierzytelniania używając MD2 lub MD5. Micalg (message integrity calculation) jest używane w bezpiecznej implementacji MIME

MIME (Multipurpose Internet Mail Extension)

Dostępny za darmo zbiór specyfikacji, które oferują sposób wymiany tekstu w językach z różnymi zbiorami znaków, i multimediami email wśród różnych systemów komputerowych, które używają standardowej poczty Internetu.

MMB (Modular Multiplication-based Block)

Oparty o IDEA, Joan Daemen stworzył ten 128 bitowy klucz / 128 bitowy rozmiar bloku algorytmu symetrycznego, nie używany z powodu jego podatności na kryptoanalizę liniową.

MOSS (MIME Object Security Service)

Zdefiniowany w RFC 1848, możliwość szyfrowania i usług podpisu dla MIME, wliczając zarządzanie kluczem w oparciu o techniki asymetryczne.

MSP (Message Security Protocol)

Wojskowy odpowiednik PEM, protokół poziomu aplikacji kompatybilny X.400 dla zabezpieczenia emaili, stworzony przez NSA w latach osiemdziesiątych.

MTI

Jednoprzebiegowy protokół uzgadniania klucza Matsumoto, Takashimy i Imai, który dostarcza wzajemnego uwierzytelniania klucza bez potwierdzania klucza lub uwierzytelniani jednostki.

NAT (Network Address Translator)

RFC 1631, połączenie routera dwóch sieci razem; jedna przeznaczona jako wewnętrzna, jest adresowana albo prywatnym lub przestarzałymi adresami, które muszą być skonwertowane do poprawnego adresu przed tym pakietami są wysyłane do sieci (przeznaczone jako zewnętrzne).

NIST (National Institute for Standards and Technology)

Dział Departamentu Handlu USA, który wydał otwarty, standard FIPS

Non – repudation (Niezaprzeczalność)

Wiara ,że po podpisie lub weryfikacji MAC, właściciel klucza nie może zaprzeczyć ,że go stworzył

One -time pad (Szyfr z kluczem jednorazowym)

Duży, niepowtarzalny zbiór prawdziwie losowych liter klucza używanych do szyfrowania, rozważany jako jeden doskonały schemat szyfrowania, wymyślony przez J.Mauborgne'a i G. Vernam'a w 1917 roku.

One-way hash (Mieszanie jednokierunkowe)

Funkcja zmiennej łańcuchowej dla stworzenia wartości o stałej długości przedstawiająca oryginalny pre – obraz, również znana skrótem wiadomości, odciskiem palca, sprawdzeniem integralności wiadomości (MIC)

OpenPGP

Standaryzacja IETF dla PGP. Składa się z dwóch RFC, RFC 2440 i RFC 3156

Open PGP/MIME

Standard IETF (RFC 3156) który dostarcza prywatności i uwierzytelnienia używająca zawartości bezpieczeństwa Mulripurpose Internet Mail Extension (MIME) opisanego w RFC 1847.

PAP (Password Authentication Protocol)

Protokół uwierzytelniania , który pozwala użytkownikowi PPP dla uwierzytelniania innych, nie zabezpiecza przed nieautoryzowanym dostępem ale jedynie identyfikuje zdalny koniec.

Passphrase (Długie hasło)

Łatwa do zapmiętania fraza używana do lepszego zabezpieczenia niż pojedyncze hasło; wyliczanie klucza konwertuje go do klucza losowego.

Password (Hasło)

Sekwencja znaków lub słów wysyłanych do systemu dla celów uwierzytelniania, walidacji lub weryfikacji

PCT (Private Communication Technology)

Protokół szyfrowania sieciowego podobny do SSL, stworzony przez Microsoft i VISA. . IEFT połączył PCT z SSL tworząc TLS.

PEM (Privacy Enhanced Mail)

Protokół dostarczający zabezpieczenia maili (RFC 1421-1424) zawierająca usługi dla szyfrowania, uwierzytelniania, integralności wiadomości i zarządzania kluczem. PEM używa certyfikatów ANSI X.509.

Prmitive filter (Filtr podstawowy)

Funkcja która stosuje pojedynczą transformację do zbioru wejściowego, tworząc zbiór wyjściowy zawierający tylko te elementy zbioru wejściowego, które spełniają kryteria transformacji. Przykład może być funkcja wyszukiwania, która akceptuje tylko pojedynczy łańcuch a dane wyjściowe listę numerów linii gdzie łańcuch został znaleziony.

Pretty Good Privacy (PGP)

Aplikacja i protokół (RFC 2440) dla bezpieczeństwa e-mail i szyfrowania pliku stworzony przez Phila R. Zimmermanna. Pierwotnie wydany jako darmowy, kod źródłowy zawsze był dostępny publicznie. PGP używa różnych algorytmów, takich jak IDEA ,RSA, DSA, MD5, SHA-1 dla szyfrowania, uwierzytelniania , integralności wiadomości i zarządzanie kluczami. PGP jest oparty o model „Zaufanie Sieciowe" i rozpropagowany na świecie.

PKCS (Public Key Crypto Standards)

Zbiór de facto standardów dla kryptografii z kluczem pulicznym stworzonym w kooperacji z nieformalnym konsorcjum (Apple, DEC, Lotus, Microsoft, MIT, RSA i Sun), które obejmują implementację standardu określonego algorytmu i algorytmu niezależnego. Specyfikacje definiują składnię wiadomości i innych protokołów kontrolowanych przez RSA Data Security Inc

PKI (Public Key Infrastructure)

Szeroko dostępny system certyfikatów dla uzyskania klucza publicznego jednostki, z jakimś stopniem pewności ,że masz „prawy' klucz i ,że nie został unieważniony

Plaintext (Tekst otwarty)

Dane wejściowe szyfru. Szyfr zaczyna się od tekstu otwartego i używa klucza do stworzenia tekstu zaszyfrowanego

Pseudo – losowych liczb generator

Proces matematyczny który daje wyraźnie liczby losowe

Prywatny klucz

Prywatnie przechowywany „tajny" koponent zintegrowanej asymetrycznej pary kluczy, często odnosimy się do niego jako klucza deszyfrującego.

Publiczny klucz

Publicznie dostępny komponent zintegrowanej asymetrycznej pary kluczy, często odnosimy się do niego jako klucza szyfrującego.

Random number (Liczba losowa)

Ważny aspekt wielu kryptosystemów, i konieczny element w generowaniu unikalnego klucza (-y), które są nieprzewidywalne dla przeciwnika. Prawdziwe liczby losowe są zazwyczaj dziedziczone z zasobów naturalnych

RC2 (Ron's Cipher 2)

Zmienny rozmiar klucza, 64 bitowy symetryczny szyfr blokowy, tajny przechowywany przez RSA, SDI.

RC4 (Ron's Cipher 4)

Zmienny rozmiar klucza szyfru strumieniowego, z właściwym algorytmem RSA Security Inc.

RC5 (Ron's Cipher 5)

Szyfr blokowy z różnymi argumentami, rozmiar bloku, rozmiar klucza i liczbę rund.

RIPE – MD

Algorytm zaprojektowany dla projektu RIPE, stworzony dla ochrony przed znanymi atakami kryptoanalitycznymi i tworzy 128 bitową wartość mieszającą, wariacja MD4.

REDOC

Opatentowany w USA algorytm szyfru blokowego stworzony przez M.Wooda, używający 160 bitowego klucza i 80 bitowego bloku.

Revocation (Unieważnienie)

Anulowanie certyfikacji lub uwierzytelnienia

RFC (Request for Comment)

Dokument IETF, albo FYI (For Your Information) RFC pod serie, które są omówieniem i wprowadzeniem lub STD RFC po serie, które identyfikują określone standardy Internetowe. Każdy RFC ma numer RFC po którym jest indeksowany i przez który może być znajdowany.

Rijndael

Szyfr blokowy stworzony przez Joan Daemen i Vincenta Rijmena, wybrany jako nowy Advanced Ecryption Standard (AES). Jest zarówno szybszy i mniejszy niż jego konkurenci. Rozmiar klucza i rozmiar bloku mogą być 128-, 192- lub 256 bitowy albo być zwiększany o 32 bity.

ROT-13 (Szyfr obrotowy)

Prosty kod zastępujący (Cezar), obracając każdą z 26 liter na 13 miejscach.

RSA

RSA Security Inc lub odniesienie do Rona Rivesta ,Adi Shamira i Lena Adlemana; lub odniesienie do algorytmu jaki stworzyli. Algorytm RSA jest używany w krptografii z kluczem publicznym i oparty na fakcie, że jest łatwo pomnożyć dwie duże liczby pierwsze razem.

SAFER (Secure And Fast Encryption Routine)

Nie zastrzeżony algorytm klucza szyfrującego szyfrem blokowym 64 bitowym. Nie jest opatentowany, dostępny jest za darmo i został stworzony przez Masseya, który również stworzył IDEA

Salt

Łańcuch losowy, który jest łączony z hasłami (lub liczbami losowymi) przed działaniem na funkcji jednokierunkowej. To połączenie skutecznie wydłuża i chroni hasło, czyniąc tekst zaszyfrowany mniej wrażliwym na ataki słownikowe.

SDSI (Simple Distibuted Security Infrastruccture)

Nowe PKI zaproponowane przez Ronalda L. Rivesta (MIT) i Butlera Lampsona (Microsoft). Dostarcza środków definiowania grup i elementów grup, list kontroli dostępu i zasada bezpieczeństwa.

SEAL (Software – optimized Encryption Algorithm)

Szybki szyfr strumieniowy dla maszyn 32 bitowych stworzony przez Rogawaya i Coppermitha.

Secret key (klucz tajny)

Albo „klucz prywatny” w algorytmach z kluczem publicznym (asymetrycznych) lub „klucz sesyjny” w algorytmach symetrycznych.

Secure channel (bezpieczny kanał)

Środek komunikowania wiadomości od jednej jednostki do drugiej tak ,że przeciwnik nie ma możliwości przeporządkowania, usunięcia, wstawienia lub odczytania (SSL, IPSec, podsłuch)

Self – signed key

Klucz publiczny, który został podpisany przez odpowiedni klucz prywatny dla udowodnienia właścicielstwa.

SEPP (Secure Electronic Payment Protocol)

Otwarta specyfikacja dla bezpiecznych transakcji bankowych przez Internet. Stworzony przez IBM, Netscape, GTE, Cybercash i MasterCard.

SESAME (Secure European System for Applications in a Multi-vendor Enviroment)

Europejski projekt badawczo rozwojowy, który rozszerza Kerberosa przez dodanie uwierzytelniania i dostępu do usług.

Sesyjny klucz

Tajny klucz (symetryczny) używany do szyfrowania każdego zbioru danych na podstawowych transakcjach. Różne klucze sesyjne są używane dla każdej sesji komunikacyjnej.

SET (Secure Elctronic Transaction)

Zapewnia bezpieczną wymianę numerów kart kredytowych poprzez Internet.

SHA-1 (Secure Hash Algorithm)

160 bitowa funkcja mieszająca; część DSS

SKIP (Simple Key for IO)

Proste zarządzanie kluczami dla protokołów internetowych stworzone przez Sun Microsystems.

Skipjack

Algorytm szyfrowania 80 bitowym kluczem zawarty w chipie Clipper NSA

SKMP (Secure key Management Protocol)

Architektura zaproponowana przez IBM, odzyskiwania kluczy, która używa techniki hermetyzacji klucza dla zapewnienie odzyskania klucza i wiadomości dla zaufanej trzeciej strony.

S/MIME (Secure Multipurpose Mail Extension)

Standard stworzony przez Deming Software i RSA Data Security dla szyfrowania i/lub uwierzytelnionych danych MIME. S/MIME definiuje format dla danych MIME, algorytmy, które muszą być użyte dla interoperacyjności (RSA, RC2, SHA-1) i dodatkowych działa takich jak certyfikaty ANSI X.509 i przenoszenie przez Internet .

SNAPI (Secure Network API)

API Netscape dla bezpieczeństwa usług, które zapewniają sposób dla zasobów aby były chronione przeciwko nieautoryzowanym użytkownikom, dla komunikacji szyfrowanej i uwierzytelnionej, i dla integralności informacji.

SPKI (Simple Public Key Infrastructure)

Propozycja IETF projektu standardu (Ellisona, Frantza i Thomasa) formatu certyfikatu klucza publicznego, powiązanego z podpisami i innymi formatami i protokołem gromadzenia kluczy.

SSH (Secure Shell)

Protokół IETF dla bezpieczeństwa warstwy przenoszenia przez dostarczenie szyfrowania, kryptograficznego uwierzytelnienie hosta i ochrony integralności.

SSL (Secure Socket Layer)

Stworzony przez Netscape dla zapewnienia bezpieczeństwa i prywatności w Internecie. Obsługuje uwierzytelnienie serwera i klienta i zarządza bezpieczeństwem i integralnością kanału transmisyjnego.

SST (Secure Transaction Technology)

Bezpieczny protokół płatności stworzony przez Microsoft i Visę jako towarzyszący protokołowi PCT.

Stream cipher (Szyfr strumieniowy)

Klasa symetrycznego klucza szyfrującego gdzie transformacja może być zmieniana dla każdego symbolu tekstu jawnego będącego szyfrowanym, użyteczne dla środowiska z małą pamięcią bufora danych.

STU-III (Secure Telephone Unit0

NSA zaprojektował telefon dla bezpiecznego głosu i wolnej komunikacji danych dla

użytku przez Departament Obrony USA i jego kontrahentów.

Substitution cipher (Szyfr podstawieniowy)

Znaki tekstu jawnego są zastępowane innymi znakami do postaci tekstu zaszyfrowanego

S/WAN (Secure Wide Area Network)

Specyfikacja RSA Data Security, Inc dla implementowania IPSec aby zapewnić interoperacyjność między firewallem a TCP/IP. Celem S/WAN jest użycie IPsec aby pozwalał firmom na mieszanie firewalla i TCP/IP dla zbudowania opartej o Internet Virtual Private Networks(VPN).

Symetryczny algorytm

Znany również jako konwencjonalny, tajny klucz i algorytm pojedynczego klucza; klucz szyfrowania i klucz deszyfrowania są takie same lub mogą być wyliczane jedne z drugiego. Istnieją dwie kategorie : Blok i Strumień.

TACACS+ (Terminal Access Controller Access Control System)

Protokół, który zapewnia dostęp do zdalnego uwierzytelniania, autoryzacji i powiązania usług konta i logowania, używany przez Cisco Systems.

Timestamping (Znacznik czasu)

Zapis czasu stworzenia lub istnienia informacji

TLS (Transport Layer Security)

Standaryzacja IETF dla SSL, łączona z PCT.

TLSP (Transport Layer Security Protocol)

ISO 10736, projekt standardu międzynarodowego

Transposition cipher (Szyfr przestawieniowy)

Tekst otwarty pozostaje ten sam ale porządek znaków jest przestawiony

Triple DES (Potrójny DES)

Konfiguracja szyfrowania w której algorytm DES jest użyty trzykrotnie z trzema różnymi kluczami.

Trust (Zaufanie)

Firma wierzy w uczciwość, rzetelność, sprawiedliwość i/lub niezawodność osoby, firmy lub innej jednostki.

TTP (Trust Third-Party, Zaufana Trzecia Część)

Odpowiedzialna część na którą wszyscy uczestniczący zgadzają się z góry, zapewnia usługi lub funkcje takie jak certyfikacja, przez przypisanie klucza publicznego do jednostki ,znacznika czasowego lub deponowanie kluczy.

Twofish

Nowy, 256 bitowy szyfr blokowy z algorytmem symetrycznym. Twofish ma jeden z pięciu algorytmów, jakich używa National Institute of Standarda and Technology (NIST) USA dla Advanced Ebcryption Standard

Validation (Walidacja)

Środek zapewniający aktualność autoryzacji używający manipulacji informacją lub zasobami.

Verification (Weryfikacja)

Uwierzytelnienie, potwierdzenie lub ustanowienie trafności.

VPN (Virtual Private Network)

Pozwala sieciom prywatnym na przejście od końcowego użytkownika, poprzez sieć publiczną (Internet) bezpośrednio do bramki domowej, takiej jak firmowy Intranet.

WAKE (Word Auto Key Encrytpion)

Tworzy strumień 32 bitowego słowa, które może być XOR'owane ze strumieniem tekstu jawnego dla stworzenia tekstu zaszyfrowanego, stworzony przez Davida Wheeler'a

Web of Trust (Sieć zaufania)

Rozproszony model zaufania używany przez PGP dla walidacji właściciela klucza publicznego, gdzie poziom zaufania jest skumulowany, oparty na indywidualnej wiedzy „wprowadzającego”

W3C (World Wide Web Consortium)

Miedzynarodowe konsorcjum założone w 1994 roku, przygotowujące protokołu dla ewolucji World Wide Web

XOR (Exclusive OR)

Matematyczne działanie na parze jedynek i zer. Daną wyjściową XOR jest zero, jeśli

obie dane wejściowe są takie same, albo jeden albo zero. Jest jedynką, jeśli pojedyncze wejście jest jedynką a drugie zerem.

X.509v3

Certyfikat cyfrowy ITU-T który jest wewnętrznie rozpoznawany w dokumentach elektronicznych, używany do udowodnienia tożsamości i właściciela klucza publicznego poprzez komunikację sieciową.. Zawiera nazwisko wystawcy, informacje identyfikujące użytkownika i podpis cyfrowy wydawcy.

X9.17

Specyfikacja ANSI , która uszczegóławia metodologię generowania liczb losowych i pseudolosowych.