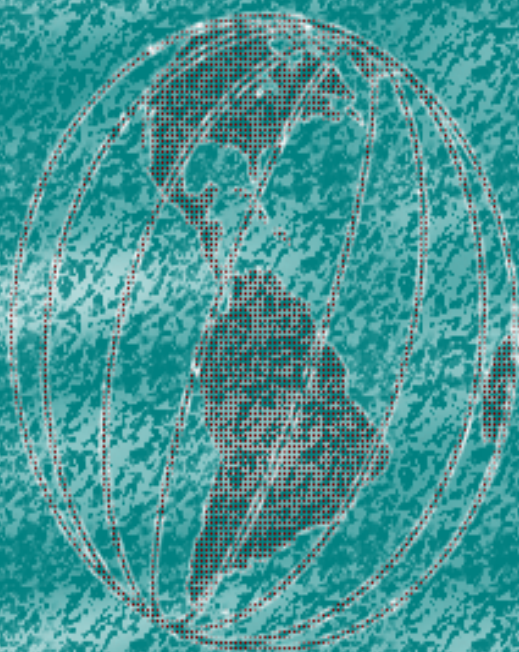


11010 10100100 00111010 10100100 00111010 10100100 00
11010 10100100 00111010 10100100 00111010 10100100 00
11010 10100100 00111010 10100100 00111010 10100100 00

Cebulski Kamil

PODPISY

GYFROWIE



0 00111010 10100100 00111010 10100100 00111010 10100
0 00111010 10100100 00111010 10100100 00111010 10100
0 00111010 10100100 00111010 10100100 00111010 10100

PODPISY CYFROWE

Kamil Cebulski



Jędrzejów 2002

Wszelkie prawa zastrzeżone!

Niniejsza publikacja może być kopiowana, oraz dowolnie rozprowadzana tylko i wyłącznie w formie dostarczonej przez Wydawcę. Zabronione są jakiegokolwiek zmiany w zawartości publikacji bez pisemnej zgody wydawcy. Zabrania się dalszej odsprzedaży tej publikacji.

SPIS TREŚCI

WSTĘP 3

1. KRYPTOGRAFIA SYMETRYCZNA 6

Schemat działania 8

2. KRYPTOGRAFIA ASYMETRYCZNA. 11

Schemat działania 11

3. UWIERZYTELNIANIE 12

Jednokierunkowa funkcja skrótu. 12

4. PRZYKŁADY 16

5. ZAKOŃCZENIE 19

BIBLIOGRAFIA 20

Wstęp

Podpis elektroniczny wymaga zastosowania określonej technologii. Najbardziej znaną jest technologia oparta o kryptografię. Podpis wygenerowany tą metodą nazywa się podpisem cyfrowym. Na potrzeby pracy wykorzystam schematy działań i zastosowań algorytmów do szyfrowania, zarządzania kluczami i podpisów cyfrowych stosowane przez pakiety produktów uważanych za najlepsze jak PEM oraz PGP. Zapewniają one poufność, uwierzytelnienie pochodzenia danych, spójność wiadomości, uniemożliwienie nie przyznania się autorstwa wiadomości i zarządzania kluczami.

Szyfrowanie ogólnie mówiąc to przekształcenie czytelnej informacji, czyli tekstu jawnego w niezrozumiały ciąg znaków. Opiera się na dwóch podstawach: algorytmie i kluczu. Algorytm jest przekształceniem matematycznym, za pomocą którego tekst jawny jest przekształcany w ciąg nieczytelnych znaków i odwrotnie. Klucz to losowy ciąg bitów, którego używa się łącznie z algorytmem. Każdy klucz powoduje inny sposób pracy algorytmu. Są różne rodzaje algorytmów i różne rodzaje kluczy, jedne i drugie mają różne zastosowanie. Z uwagi na ich różną złożoność, szybkość i bezpieczeństwo są wykorzystywane do różnych celów jak np. do szyfrowania dokumentów, zarządzania kluczami, podpisów cyfrowych. W tej części pracy zostaną przedstawione podstawowe rodzaje kryptografii, wybrane algorytmy, oraz zaprezentowane zostaną schematy i zastosowania poszczególnych rodzajów kryptografii.

Kryptografia – jest zbiorem metod wykorzystywanych do zabezpieczenia informacji. Dzięki kryptografii możemy przekształcić normalny, zrozumiały tekst lub innego typu wiadomości w taki sposób, iż stanie się ona niezrozumiała dla nieupoważnionego odbiorcy.

Kryptografia narodziła się tysiące lat temu – w starożytnej Grecji i Rzymie, generałowie używali jej do szyfrowania wiadomości, na polach bitew. Pierwsze systemy kryptografii opierały się na dwóch technikach: podstawiania oraz przestawiania. Technika podstawiania jak sama nazwa wskazuje, opiera się na zasadzie zamiany każdego znaku w przesyłanej wiadomości na wybrany inny znak. W tzw. Szyfrze Cezara litera „a” zamieniana była na literę „d”, litera „b” na literę „e” i tak dalej. Niektóre szyfry wykorzystujące podstawianie używają takich samych schematów zamiany dla każdej litery w tekście, inne wykorzystują różne schematy dla różnych liter.

Transpozycja polega na zamianie kolejności znaków znajdujących się w tekście oryginalnej wiadomości. Jeden z systemów przestawiania polega na zapisywaniu wiadomości w wierszach tabeli i odczytywaniu jej kolumn. Metoda podwójnego przestawiania sprowadza się do dwukrotnego przeprowadzenia takiej operacji.

1. Kryptografia symetryczna

Algorytmem wykorzystywanym w kryptografii symetrycznej jest m.in. algorytm DES. Algorytm DES (ang. Data Bureau of Standards – Narodowe Biuro Standardów obecnie NIST – National Institute of Standards and Technology) jako rządowy standard szyfrowania, jest stosowany w prawie wszystkich rodzajach łączności elektronicznej i przechowywania danych. DES jest algorytmem blokowym. Oznacza to, że całość danych dzielona jest na określone części – bloki. W przypadku DES blok ma 8 bajtów – cały dokument jest dzielony na takie 8 bajtowe części. Na raz algorytm szyfruje 8 bajtów tekstu jawnego i powstaje 8 bajtów tekstu zaszyfrowanego. Deszyfruje również w porcjach po 8 bajtów. Algorytm składa się z 16 powtarzających się prostych funkcji zwanych iteracjami. Im większa liczba iteracji lub cykli zapewnia większe bezpieczeństwo. Dodanie dalszych iteracji algorytmowi DES nie poprawi w sposób znaczący jego bezpieczeństwa, które jest i tak bardzo wysoko oceniane. Złamany może być tylko przez łamanie brutalne. Łamanie brutalne to łamanie tekstu zaszyfrowanego i tak samo małego odpowiadającego mu tekstu jawnego. Istota polega na tym, że metodą prób i błędów eliminuje się po kolei wszystkie możliwe klucze, aż do znalezienia tego właściwego, którego tekst odszyfrowany będzie w 100% zgodny z tekstem jawnym. Jest to ewidentne wskazanie, że jest to klucz właściwy i można odszyfrować resztę tekstu. Łamanie brutalne jest na tyle niebezpieczne, że dla odszyfrowania tekstu będą wykorzystywane wszystkie możliwe klucze, aż do znalezienia tego właściwego. Skoro nie można zapobiec łamaniu to można spróbować zniechęcić do łamania poprzez podniesienie kosztów tego ataku w kwestii czasu i pieniędzy. Oprócz wyżej zaprezentowanego algorytmu są jeszcze inne.

Wybierając algorytm należy pamiętać o dwóch kwestiach: o bezpieczeństwie i szybkości. Bezpieczeństwo algorytmu szyfrującego opiera się na bezpieczeństwie klucza. Poniżej tabela podsumowująca aspekt bezpieczeństwa wybranych algorytmów stosowanych w kryptografii symetrycznej z uwzględnieniem długości klucza i atakiem na nie.

Algorytm	Długość klucza	Najlepszy atak	Uwagi
DES	56 bitów	Łamanie brutalne	Łamanie brutalne wykonalne
Potrójny DES	112 bitów	Łamanie brutalne	Łamanie brutalne niewykonalne
IDEA	128 bitów	Łamanie brutalne	Zbyt nowy algorytm
RC2	Zmienna	Nieznany	Szczegóły algorytmu nie są znane
RC4	Zmienna	Nieznany	Szczegóły algorytmu nie są znane

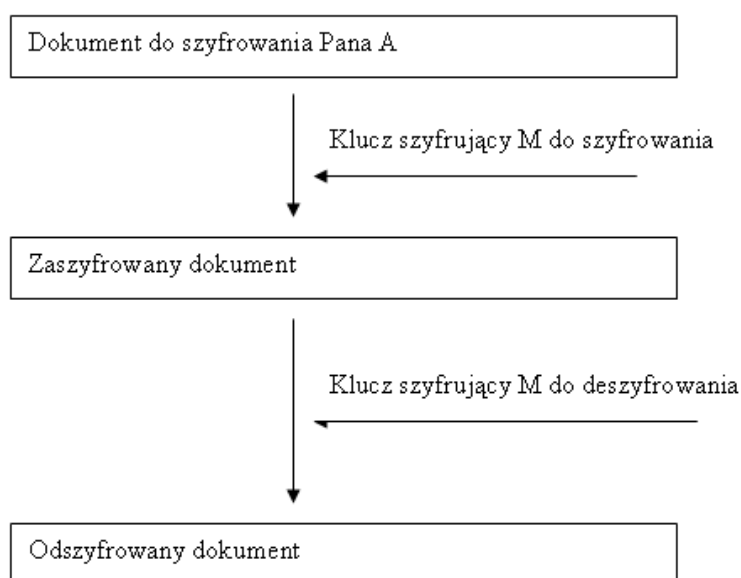
Komentując zamieszczone w tabelce informacje widzimy, że jeżeli chodzi o bezpieczeństwo to najlepszym algorytmem zdaje się być potrójny DES. Jest on uważany za bardzo silny, ponieważ nikomu nie udało się go złamać. Niemniej nie można udowodnić ponad wszelką wątpliwość, że ten algorytm jest niełamanalny, ale istnieje olbrzymia ilość dowodów, że tak właśnie jest. Wadą tego algorytmu jest jego powolność. Jest on najwolniejszy z trzech czołowych z tabeli algorytmów.

W literaturze podkreśla się, że nie ma stu procentowo bezpiecznych algorytmów. Wszystkie dadzą się złamać – to kwestia sprzętu i czasu. Nawet te, które uznane są za najbezpieczniejsze nikt nie zaryzykuje twierdzenia, że są one stuprocentowo bezpieczne, albowiem co do zasady nie została udowodniona niełamanalność żadnego algorytmu. Niemniej jest jeden wyjątek – algorytm z kluczem jednorazowym. Jest jedynym schematem szyfrującym, w którym można udowodnić, że jest absolutnie nieprzełamywalny. Największą popularnością cieszy się on w środowisku szpiegowskim z uwagi na fakt, że po pierwsze nie wymaga żadnego sprzętu do implementacji i po drugie jest całkowicie bezpieczny. Wymaga on wytworzenia wielu zestawów pasujących do siebie ciągów kluczy szyfrujących. Każdy z tych ciągów składa się z pewnej liczby losowych znaków klucza. Te znaki klucza nie są generowane przez jakiegokolwiek rodzaju kryptograficzny generator klucza, a wybierane za pomocą prawdziwie losowego procesu. Każda strona otrzymuje dopasowany zestaw ciągu. Każdy znak klucza w ciągu jest używany do zaszyfrowania jednego tekstu jawnego, po czym już nigdy nie zostaje użyty ponownie. Jest to istota nieprzełamywalności klucza. Mimo pewności co do bezpieczeństwa algorytm ten nie jest używany, ponieważ jest niepraktyczny. Liczba kluczy jednorazowych, którą trzeba wygenerować musi być co najmniej równa rozmiarowi tekstu jawnego, a klucze te muszą być zmieniane z upływem czasu. Z tym można

pracować w programach użytkowych o małej szybkości transmisji, ale nie w nowoczesnych systemach komunikacyjnych o dużej szybkości.

Schemat działania

Kryptografia symetryczna opiera się na kluczu pojedynczym, który musi być znany przez zainteresowane strony, a nie może być udostępniony pod żadnym pozorem osobom trzecim. Strony te posługują się tym samym kluczem do zaszyfrowania jak i odszyfrowania wiadomości. Poniżej schemat działania.



Pan A chce przesłać Panu B dokument, szyfruje wiadomość przy pomocy klucza szyfrującego M. Pan B chcąc odczytać wiadomość od A deszyfruje ją tym samym kluczem M. Klucz M musi pozostać dla bezpieczeństwa przesyłanych danych w tajemnicy, bowiem kto nie zna klucza nie może odszyfrować wiadomości i poznać treści dokumentu.

Jeżeli natomiast ktoś chciałby poznać treść wiadomości dla Pana B, musiałby użyć metody siłowej (brutalnej). Skuteczność przeprowadzenia ataku taką metodą zależy od długości klucza. Algorytm DES posiada 56 bitowy klucz. Każdy bit może mieć dwie wartości 1 lub 0, oznacza to, że istnieje 2^{56} (około 72 057 594 037 900 000) możliwych kluczy. Zatem, jeżeli, ktoś posiada nowoczesny, szybki komputer, który potrafi sprawdzić miliard kluczy na sekundę, atak będzie trwał nie dłużej niż 834 dni. Jeżeli natomiast Pan A użyłby kodowania opartego na 128 bitowym kluczu, haker posiadający miliard komputerów, z których każdy potrafiłby sprawdzić miliard kluczy na sekundę, złamałby kod w ciągu 10^{13} lat, co stanowi prawie tysiącrotnie więcej niż szacowany wiek wszechświata. Zatem można powiedzieć, że klucz 128 bitowy jest bardzo bezpieczny, należy jednak pamiętać, że przy bardzo tajnych dokumentach wykorzystuje się klucze 2024 bitowe!

Mankamentem tego systemu jest to, że trzeba uzgadniać klucz tajny, przechowywać go w bezpiecznym miejscu i współdzielić ze wszystkimi osobami, z którymi będą wymieniane się zabezpieczonymi wiadomościami. Atakując mechanizm zarządzania kluczami osiągnie się znacznie więcej niż przez atak algorytmów. Wynaleziono inny rodzaj kryptografii, gdzie te problemy zostaną wyeliminowane lub zniwelowane. Jest to kryptografia asymetryczna.

Do szyfrowania informacji metodą asymetryczną, wykorzystuje się zarówno metodę podstawiania, jak i metodę zamiany. Do algorytmu wykorzystuje się wiele funkcji matematycznych, których, które można odwrócić, tzn. dla dokładnie jednego x z danego przedziału, przyporządkowane jest 1 y i odwrotnie, każdemu y przypada tylko 1 x . Własność ta potrzebna jest do wykorzystywania jednego algorytmu do szyfrowania jak i deszyfrowania wiadomości. Wykorzystuje się zatem funkcje liniowe lub hiperboliczne. Do szyfrowania wykorzystuje się, tylko w określonej dziedzinie funkcji, funkcje sinusoidalne, hiperbole oraz tangensoidy.

Aby zapewnić wysokie bezpieczeństwo algorytmu, wszystkie funkcje jak i dziedziny i przeciwdziedziny są ze sobą logicznie powiązane. Przeważnie wykorzystuje się schemat, że przeciwdziedzina jednej funkcji jest dziedziną drugiej (algorytm DES), lub część przeciwdziedziny pierwszej funkcji jest dziedziną drugiej, a pozostała część albo nie podlega dalszemu szyfrowaniu, lub stanowi dziedzinę kolejnej funkcji.

Jeszcze większe bezpieczeństwo zapewnia łączenie części dziedziny w kolejny, tym razem pojedynczy argument logiczny. Aby wszystko to przybliżyć, posłużę się kilkoma przykładami, kodującymi liczbę **847068214947**.

Na początku do wszystkich cyfr w liczbie dodamy po 1, w przypadku cyfry 9, otrzymujemy 0, otrzymamy zatem **958179325058**. Następnie, wykorzystamy funkcje $y=2x$, aby jeszcze bardziej zaszyfrować wiadomość. Jeżeli otrzymania liczby jednocyfrowej, w miejsce dziesiątek wstawiamy 0. Otrzymujemy zatem: **181016021418060410001016**. Teraz jeżeli obok siebie występują 3 takie same cyfry, 2 z nich stojące po lewej stronie zamieniamy na literę a. Otrzymujemy: **18101602141806041a01016**. Postępując w ten sposób używając dziesiątek funkcji, sprawiamy, że nasz algorytm jest bezpieczniejszy, gdyż znalezienie pierwszych funkcji wykorzystywanych do kodowania, nie powoduje odkrycie całego algorytmu i nie pomaga w odczytywaniu informacji.

Jeżeli będziemy postępować w sposób odwrotny, po serii obliczeń otrzymamy liczbę początkową, gdyż każdą literę a, zamienimy na 2 znaki stojące po jej prawej stronie, następnie wszystkie liczby podzielimy przez 2, likwidując przy tym wszystkie zera, poza przypadkiem, w którym istnieją dwa zera, wtedy kasujemy tylko jedno. Następnie odejmujemy od każdej cyfry 1 i nasza wiadomość została odszyfrowana.

2. Kryptografia asymetryczna.

Algorytmem wykorzystywanym w kryptografii asymetrycznej jest m. in. Algorytm RSA. Nazwa pochodzi od pierwszych liter nazwisk autorów: Rona Rivesta, Adi Shamira i Leny Adlemana. Na istotę składa się godny uwagi aspekt matematyczny i jak zwykle bezpieczeństwo oraz szybkość szyfrowania i deszyfrowania. Z punktu widzenia matematycznego, algorytm RSA oparty jest o liczby pierwsze. Wytworzenie klucza jawnego wymaga pomnożenia dwóch dużych liczb pierwszych, aby uzyskać iloczyn tych liczb. Działanie matematyczne stosunkowo proste. Z dwóch liczb uzyskuje się trzecią. Jednakże uzyskanie klucza prywatnego z klucza jawnego (czyli z tej trzeciej dokładnie te dwie, które były na początku) jest związane z rozłożeniem tego iloczynu na czynniki pierwsze (czyli proces niejako odwrotny). Jeżeli iloczyn jest liczbą wystarczająco dużą, to rozłożenie go na czynniki pierwsze nie jest zadaniem łatwym do wykonania, niemniej jednak możliwym. Kwestią kluczową jest tu nie możliwość, a czas dokonania tej operacji. Chodzi tu o to, aby cała potęga sprzętu i najtęższe w tej dziedzinie umysły nie były w stanie dokonać tego w rozsądnym terminie. W rzeczywistości w dalekiej przyszłości takie obliczenia mogą okazać się absurdem.

Schemat działania

Kryptografia z kluczem jawnym oparta jest o parę kluczy jawny (publiczny) i tajny (prywatny). Konkretny klucz jawny pasuje do konkretnego klucza prywatnego. Nie można wyliczyć jednego klucza na podstawie drugiego. Klucz jawny jest kluczem publicznym, czyli powszechnie dostępnym. W związku z czym każdy może otrzymać jego kopię. W interesie posiadacza pary kluczy jest aby jak najwięcej podmiotów posiadało kopię jego klucza publicznego. Osoba A (czyli podmiot zainteresowany korespondencją z B) chcąc wysłać zaszyfrowaną wiadomość B sięga do klucza publicznego, aby tym kluczem zaszyfrować dla niego informację. B za pomocą swojego klucza prywatnego może ją odszyfrować. Nawet przechwycona wiadomość nie jest czytelna dla nieuczciwego C, ponieważ nie posiada on klucza prywatnego B. Może posiadać klucz publiczny B, ale nie pomoże to w deszyfracji wiadomości. W ogólnym skrócie została przedstawiona istota kryptografii z kluczem jawnym. W rzeczywistości jest to bardziej skomplikowany proces.

3. Uwierzytelnianie

Ważne jest dla adresata, że dokument, który do niego przychodzi drogą elektroniczną pochodzi od osoby, która podaje się za nadawcę tego dokumentu. Uwierzytelnianie nadawcy odbywa się za sprawą koncepcji podpisu cyfrowego.

Z technicznego punktu widzenia jest to sekwencja bitów dołączona do dokumentu cyfrowego, na podstawie którego można potwierdzić autentyczność nadawcy. Wbrew pozorom i odmiennie niż w przypadku podpisu odręcznego dla każdego dokumentu podpis cyfrowy jest inny. Dzieje się to z prostej przyczyny, że zachodzą inne procesy niż przy zwykłym podpisywaniu dokumentu.

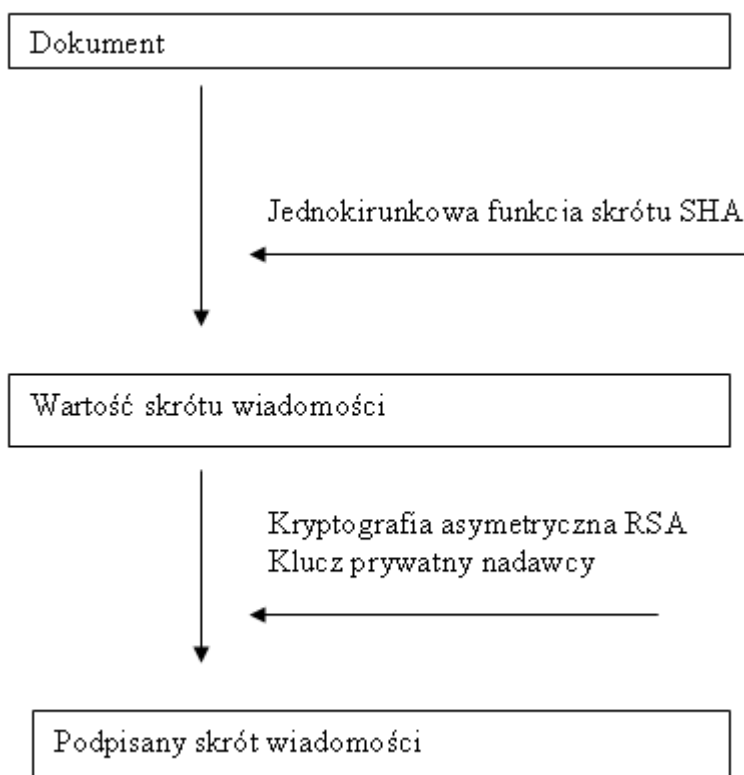
Podpis cyfrowy spełnia następujące kryteria:

- a) **niepodrabialny** – nikt nie może wygenerować oryginalnego podpisu cyfrowego jak tylko nadawca
- b) **autentyczny** – pochodzi od osoby, która podaje się za nadawcę
- c) **nie może być użyty kilkakrotnie** - podpis cyfrowy jest używany tylko raz i za każdym razem jest inny
- d) **niezmienialny** – po podpisaniu nie można zmienić podpisu, w przeciwnym wypadku traci ważność
- e) **nie można się go wyprzeć** – prawidłowo podpisany dokument stanowi dowód, że pochodzi on od nadawcy, a nadawca nie może się go wyprzeć.

Jednokierunkowa funkcja skrótu.

Jednokierunkowa funkcja skrótu (inaczej skrót, funkcja ściągająca, funkcja kompresująca, kryptograficzna suma kontrolna, kontrola spójności danych, kod spójności danych, kod wykrywania ingerencji, kod uwierzytelniania wiadomości) jest specjalną funkcją kryptograficzną do przekształcania wiadomości o dowolnych rozmiarach w niezrozumiały tekst. Nie jest to szyfrowanie, bowiem poddanie wiadomości tej operacji „niszczy” wiadomość a działanie przeciwne nie jest możliwe. Ponadto funkcja nie korzysta z klucza. Te właściwości sprawiają, że jest ona wykorzystywana do identyfikacji wiadomości.

W wyniku poddania wiadomości działaniu tej funkcji tworzy się skrót wiadomości. Jest on wystarczająco długi, dzięki temu szansa na to, aby dwa różne dokumenty dały ten sam skrót jest dosłownie nikła. Następnie wykorzystuje się algorytm podpisów cyfrowych kryptografii z kluczem jawnym i klucz prywatny podpisania skrótu wiadomości. Poniżej schemat obrazujący ten proces.



Szyfrowanie zapewnia bezpieczeństwo i poufność korespondencji, a podpisy cyfrowe dają uwierzytelnianie nadawcy. Połączenie wszystkich tych procesów szyfrowania i tworzenia podpisów cyfrowych daje dopiero pożądane bezpieczeństwo czyli

- a) **poufność wiadomości** – mamy pewność, że nikt nie ma wglądu do przesłanych dokumentów, nie może zapoznać się z ich treścią
- b) **nienaruszalność danych** – nikt nie może zmieniać, poprawiać, ani w żadne sposób naruszać treści tych wiadomości w sposób, który nie zostanie zauważony
- c) **pewność** - co do tego, od kogo pochodzą dokumenty, nikt nie może się wyprzec tego, że to on jest nadawcą.

Za pomocą specjalnej matematycznej funkcji zwanej jednokierunkową funkcją skrótu, tworzy się skrót tej wiadomości. Następnie wykorzystuje się algorytm podpisów cyfrowych kryptografii z kluczem jawnym jak np. RSA i klucz prywatny do podpisania skrótu wiadomości. Należy połączyć wiadomość i podpis cyfrowy. W celu podpisania tej wiadomości należy wygenerować klucz szyfrujący za pomocą algorytmu konwencjonalnego jak np. DES. W celu zaszyfrowania klucza pobiera się klucz jawny odbiorcy wiadomości i szyfruje się, poczym łączy wiadomość z zaszyfrowanym kluczem i w ten sposób końcową zabezpieczoną wiadomość można przesłać nadawcy.

Nadawca aby odczytać rozdziela zaszyfrowaną wiadomość od zaszyfrowanego klucza losowego, deszyfruje losowy klucz za pomocą algorytmu z kluczem jawnym i używa swojego klucza prywatnego. Deszyfruje wiadomość za pomocą algorytmu konwencjonalnego i odszyfrowanego klucza. Oddziela wiadomość od podpisu i za pomocą jednokierunkowej funkcji skrótu oblicza wartość skrótu wiadomości. Pobiera klucz jawny nadawcy i deszyfruje podpis za pomocą algorytmu podpisów cyfrowych z kluczem jawnym i klucza jawnego odbiorcy. Porównuje odszyfrowany podpis nadawcy z wartością skrótu wiadomości. Jeżeli są takie same to podpis uznaje i akceptuje wiadomość jako oryginalną.

W przypadku algorytmów wykorzystywanych przez kryptografię z kluczem pojedynczym zostały omówione wady i zalety. Jeżeli natomiast chodzi o kryptografię asymetryczną problem został celowo pominięty. Z uwagi na złożoność i ważność zagadnienia postanowiłem poświęcić temu więcej miejsca.

W ogromie użytkowników uczestniczących w wymianie elektronicznej, w obliczu ogromnego postępu technologicznego, żeby nie narazić się na oszustwa, zachodzi potrzeba poddania niejako kontroli kluczy jawnych użytkowników, neutralnego zabezpieczenia zarządzania kluczami jawnymi i potwierdzeniu, że dany klucz należy do danego podmiotu i nie jest używany przez żaden inny podmiot. Do tego potrzebny jest ktoś, kto będzie zajmował się tym i tylko tym przez cały czas – Zaufana Trzecia Strona.

Strony wymiany elektronicznej dążą do uzyskania certyfikatu – czyli swego rodzaju zaświadczenia potwierdzającego identyfikację danej osoby i zawierającego jej klucz publiczny. Zaświadczenie to jest podpisywane przez specjalny organ do tego upoważniony,

który wydaje certyfikaty. Od stopnia zaufania tego organu zależy czy będziemy mieli zaufanie do wydanego przez niego certyfikatu, że jest dostatecznie sprawdzony i że jest poprawny.

Do budowania algorytmów opartych na kryptografii asymetrycznej, używa się dowolnych funkcji, które co najmniej dla dwóch x , przyjmują tę samą wartość y , zatem na szeroka skale wykorzystuje się sinusoidy, tangensoidy, hiperrbole i podobne. Ma to na celu, stworzenie takiego algorytmu, którego odwrócenie byłoby niemożliwe, bądź trudne do odwrócenia. Na przykład poddając liczbę **3245346**, operacji, która ma na celu dodanie do cyfr mniejszych bądź równych cyfrze 3, jedności, spowoduje powstanie liczby **4345446**. Natomiast z tej liczby nie możemy już otrzymać liczby poprzedniej, gdyż nie wiemy, czy poszczególne cyfry cztery, powstała z dodania jedności do cyfry 3, czy też na początku była cyfrą 4.

Mimo, iż odnalezienie pierwotnej liczby, wydaje się być trudne, jest możliwe do zrobienia, gdyż istnieją 4 cyfry o wartości 4, każda z nich może przybrać 2 wartości 4 lub 3, zatem istnieje 2^4 możliwości wszystkich kombinacji. Stosując tę metodę odnalezienie liczby pierwotnej jest możliwe ale zajmuje bardzo dużo czasu, gdyż może istnieć bardzo wiele kombinacji.

4. Przykłady

Wszystkie omawiane przeze mnie algorytmy, są objęte patentami i są chronione prawem autorskim, dlatego niemożliwe jest abym przedstawił dokładny schemat działania tych algorytmów. Na potrzeby pracy stworzyłem nowe, bardzo proste algorytmy.

a) kodowanie symetryczne

Kodowanie symetryczne stanowi najprostszą metodą kodowania tekstu. W przykładzie weźmiemy pod uwagę tekst złożony z liter alfabetu polskiego, znaków interpunkcyjnych oraz kilku liczb. Oto tekst, który chcemy zakodować.

ALA MA 2 KOTY.

Aby zakodować powyższy tekst, zamieniamy poszczególne znaki, które nie są literami, na liczby, a liczby na litery, zatem nasz algorytm przybierze następującą postać.

A=01 B=02 C=03 D=04 E=05 F=07 G=08 H=09 I=10 J=11 K=12 L=13
M=14 N=15 O=16 U=17 P=18 R=19 S=20 T=21 U=22 W=23 Y=24 Z=25
. =26 [spacja]=27 1=a 2=b 3=c 4=d 5=e 6=f 7=g 8=h 9=i 0=j

Zamieniając powyższy tekst według wskazówek, otrzymujemy ciąg znaków, który nam nic nie mówi.

01130127140127b271216212426

Jeżeli chcemy odkodować wiadomość, musimy znać ten sam klucz, który został użyty do zakodowania tekstu.

b) kodowanie asymetryczne

Kodowanie asymetryczne charakteryzuje się tym, iż klucz używany do kodowania i rozkodowywania różnią się od siebie. Chcąc więc zakodować tekst, musimy wygenerować 2 klucze. Pierwszy klucz służący do zakodowania informacji, będzie wyglądał podobnie do klucza we punkcie a), jednak do każdej cyfry zakodowanego tekstu dodamy 1, a jeżeli występuje litera, zastępujemy ją występującą w alfabecie o 1 pozycje niżej, z tym że literę „a” zastępujemy literą „z”. Zatem zakodowana informacja prezentuje się w następujący sposób.

12241238251238a382327323537

Natomiast do odkodowania wiadomości używamy innego klucza, który wygląda następująco:

A=12 B=13 C=14 D=15 E=16 F=18 G=19 H=10 I=21 J=22 K=23 L=24
M=25 N=26 O=27 U=28 P=29 R=30 S=31 T=32 U=33 W=34 Y=35 Z=36
. =37 [spacja]=38 1=z 2=a 3=b 4=c 5=d 6=e 7=f 8=g 9=h 0=i

Korzystając z tego klucza możemy odkodować tekst. Jeżeli natomiast użyjemy go do zakodowania tekstu, powstanie co prawda ten sam ciąg znaków, ale jeżeli będziemy postępować z tym kluczem jak z kluczem zakodowywującym, czyli dodamy po 1 do każdej cyfry, a każdą wartość litery zmniejszymy o 1, to za pomocą w ten sposób powstałego klucza nie otrzymamy prawidłowo odkodowanego tekstu.

c) uwierzytelnianie

Uwierzytelnianie, jest bardzo podobne do kodowania asymetrycznego, jednak w tym wypadku kodowanie samo przez siebie nie ma na celu zaszyfrowania wysyłanej wiadomości.

Jeżeli chcemy coś uwierzytelnić, musimy wykonać skrót wiadomości. Naszym skrótem będzie co drugi znak w naszym przykładowych tekście. Otrzymujemy zatem po skróceniu:

AAM OY

Tak otrzymany skrót poddajemy kodowaniu asymetrycznemu z punktu b). Otrzymujemy:

121225382735

Teraz wysłana przez nas wiadomość powinna wyglądać tak:

121225382735

„ALA MA 2 KOTY”

Aby sprawdzić autentyczność, trzeba rozszyfrować skrót wiadomości, oraz używając algorytmu, tworzenia skrótu, sprawdzić, czy korzystając z załączonej wiadomości można zrobić identyczny skrót.

5. Zakończenie

Współczesna epoka to epoka społeczeństwa informatycznego, którego częścią stajemy się z wyboru, albo za sprawą nakładanych na nas obowiązków. W tej epoce nie tylko w Polsce, ale i na świecie wciąż jedyną nie tyle znaną, co wykorzystywaną metodą generowania podpisu elektronicznego jest metoda kryptograficzna. To jej podporządkowany jest aparat administracyjny w poszczególnych regulacjach i przepisy prawne dotyczące administracyjno – prawnych aspektów podpisu elektronicznego.

Przemierzając materiał zawarty w pracy, porównując różne systemy prawne można dojść do określonych wniosków.

1. Podpis Elektroniczny o odpowiednim stopniu zabezpieczenia jest praktycznie nie do podrobienia. Podpis elektroniczny wbrew pozorom i ogólnemu pogładowi na podpis nie jest stały, a za każdym razem inny. Dla każdej wiadomości jest generowany inny podpis i nie jest on taki sam jak ten wygenerowany przed chwilą dla innej wiadomości. Wynika to z zastosowania techniki, metody generowania podpisu i zastosowania algorytmów z kluczem pojedynczym i publicznym oraz jednokierunkowej funkcji skrótu. A zatem można powiedzieć, że jest bezpieczniejszy niż podpis odręczny. Na bezpieczeństwo to składają się ten i kilka innych aspektów. Jednakże w tym stwierdzeniu też można doszukać się kilku „ale”, kilku „pod warunkiem” niezgodności.
2. Przede wszystkim trzeba mieć świadomość, że zabezpieczenie dokumentu podpisem elektronicznym dotyczy tylko danego dokumentu, tylko danej wiadomości, a nie dotyczy komputera, za pomocą którego łączymy się z siecią i wysyłamy podpisaną wiadomość. Komputer, z którego wychodzimy na zewnątrz tj. do sieci musi być zabezpieczony różnymi programami antywirusowymi, różnej klasy firewall'ami i innymi środkami. Ponadto niezbędne jest zabezpieczenie klucza prywatnego. Najlepiej ważne dane i klucze przechowywać na innym komputerze nie podłączonym do sieci. Niezastosowanie się chociażby do jednego z powyższych zaleceń może skutkować zniwelowaniem zabezpieczenia dokumentu podpisem elektronicznym. W wieku technologii cyfrowych, gdzie nawet termin „wojna” jest na nowo definiowany, odpowiedzialność podpisujących jest bardzo duża, z której nie zawsze można zdawać sobie sprawę.

BIBLIOGRAFIA

1. Dyrektywa 97/7/EC parlamentu Europejskiego i Rady z 20 maja 1997r w sprawie ochrony konsumentów w odniesieniu do umów zawieranych na odległość,
2. Ustawa polska o podpisie elektronicznym z 27.07.2001r,
3. Wytyczne w sprawie kryptografii (Guidelines for Cryptography Policy) – dokument OECD (Organization for Economic Co-operation and Development) z dnia 27.03.1997,
4. Simson Garfinkel, Gene Spafford, WWW Bezpieczeństwo I handle, O'Reilly, NewYork 1999.

