Spis treści

0.1 Wstęp

Wraz ze wzrostem zapotrzebowania na pozyskanie nowych klientów, a tym samym kontraktów oraz z naciskami ze strony organizacji ochrony środowiska, aby zredukować liczbę drukowanych dokumentów, coraz więcej firm decyduje się na generowanie i wymianę dokumentów między pracownikami (i/lub swoimi oddziałami) w formie elektronicznej. Jeśli wymiana tych dokumentów dokonywana jest w wąskim gronie pracowników, możemy być w 100% pewni, że dokument jest autentyczny i w formie niezmienionej. Problem zaczyna się, gdy musimy wymieniać dokumenty z naszymi pracownikami lub partnerami handlowymi w różnych miastach lub nawet krajach. Wtedy nie możemy mieć pewności, że dokument wysłany jest tym samym dokumentem, który otrzymaliśmy. Przy dzisiejszej technologii dokument taki mógł zostać przechwycony przez osoby niepowołane (trzecie) i/lub zmieniony w celu zmylenia adresata lub korzyści majątkowych.

Rozwiązaniem problemu stwierdzenia autentyczności dokumentu oraz pewności, że nadawca jest tym, za kogo się podaje, jest podpis elektroniczny (cyfrowy). Narzędziem, które nam to w prosty sposób umożliwia jest język XML, a dokładniej *XML Signature*.

0.2 Cel pracy

Praca ma na celu zaprezentowanie możliwości, jakie daje kryptografia oraz język XML w zakresie podpisu elektronicznego.

ZA MAŁO!

0.3 Struktura pracy

0.1 - ten rozdział, ...

Dalsza część struktury pracy powstanie po napisaniu pracy.

Rozdział 1

Początek...

Na początku było pismo wykształcone niezależnie w wielu kulturach stanowiło niezbadaną tajemnicę dla tych, którzy nie potrafili czytać. Szybko jednak zrodziła się konieczność ukrycia informacji również przed tymi, którym umiejętność ta nie była obca. Najbardziej oczywistym rozwiązaniem było schowanie tajnej wiadomości przed ludźmi, którzy mogliby ją odczytać. Takie zabiegi wkrótce jednak przestały wystarczać. Wiadomość mogła zostać odnaleziona podczas wnikliwego przeszukania, a wtedy tajne informacje dostałyby się w ręce wroga. A gdyby udało się napisać list działający na zasadzie „drugiego dna"? Z pozoru zawierałby on błahe treści, jednak jeśli adresat wiedziałby, gdzie i jak szukać, mógłby dotrzeć do „mniej niewinnych" informacji. Tak narodziła się steganografia.

1.1 Steganografia

Steganografia to ogół metod ukrywania tajnych przekazów w wiadomościach, które nie są tajne. Jej nazwa wywodzi się od greckich słów: *steganos* (ukryty) oraz *graphein* (pisać). W przeszłości stosowano wiele wymyślnych sposobów osiągnięcia tego efektu. Popularny niewidzialny atrament to jeden z najbardziej znanych przykładów steganografii. Pierwsze zapiski na temat stosowania tej sztuki znaleźć można już w księgach z V wieku p.n.e. Przykładem może

być opisana przez Herodota historia Demaratosa, Greka, który ostrzegł Spartan przed przygotowywaną przeciw nim ofensywą wojsk perskich. Nie mógł on wysłać oficjalnej wiadomości do króla, zeskrobał więc wosk z tabliczki i wyrył tekst w drewnie. Następnie ponownie pokrył tabliczkę woskiem i wręczył posłańcowi. Czysta tabliczka nie wzbudziła podejrzeń perskich patroli i bezpiecznie dotarła do celu. Tam, co prawda, długo głowiono się nad jej znaczeniem, wkrótce jednak żona spartańskiego wodza Leonidasa wpadła na pomysł zeskrobania wosku, co pozwoliło odkryć tajną wiadomość.

W miarę postępu technicznego, a także rozwoju samej steganografii, powstawały coraz wymyślniejsze metody ukrywania wiadomości. Znana jest na przykład metoda ukrywania wiadomości w formie kropki w tekście drukowanym, stosowana podczas II wojny światowej. Wiadomość była fotografowana, a klisza pomniejszana do rozmiarów około mm^2 i naklejana zamiast kropki na końcu jednego ze zdań w liście. Obecnie bardzo popularne jest ukrywanie wiadomości w plikach graficznych. Kolejne przykłady można mnożyć, jednak nawet najbardziej wymyślne z nich nie gwarantują, iż wiadomość nie zostanie odkryta. Koniecznością stało się zatem wynalezienie takiego sposobu jej zapisywania, który gwarantowałby tajność nawet w przypadku przechwycenia przez osoby trzecie.

1.2 Kryptografia

Nazwa *kryptografia* również wywodzi się z języka greckiego (od wyrazów *kryptos* — ukryty i *graphein* — pisać). Jej celem jest utajnienie znaczenia wiadomości, a nie samego faktu jej istnienia. Podobnie jak w przypadku steganografii, data jej powstania jest trudna do określenia. Najstarsze znane przykłady przekształcenia pisma w formę trudniejszą do odczytania pochodzą ze starożytnego Egiptu, z okresu około 1900 roku p.n.e. Pierwsze tego typu zapisy nie służyły jednak ukrywaniu treści przed osobami postronnymi, a jedynie nadaniu napisom formy bardziej ozdobnej lub zagadkowej. Skrybowie zapisujący na ścianach grobowców historie swych zmarłych panów świado-

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

Tabela 1.1: Tablica Polibiusza

mie zmieniali niektóre hieroglify, nadając napisom bardziej wzniosłą formę. Często celowo zacierali ich sens, zachęcając czytającego do rozwiązania zagadki. Ten element tajemnicy był ważny z punktu widzenia religii. Skłaniał on ludzi do odczytywania epitafium i tym samym do przekazania błogosławieństwa zmarłemu. Nie była to kryptografia w ścisłym tego słowa znaczeniu, zawierała jednak dwa podstawowe dla tej nauki elementy — przekształcenie tekstu oraz tajemnicę.

Na przestrzeni kolejnych 3000 lat rozwój kryptografii był powolny i dosyć nierówny. Powstawała ona niezależnie w wielu kręgach kulturowych, przybierając różne formy i stopnie zaawansowania. Zapiski na temat stosowania szyfrów znaleziono na pochodzących z Mezopotamii tabliczkach z pismem klinowym. Ich powstanie datuje się na 1500 rok p.n.e. W II w. p.n.e. grecki historyk Polibiusz opracował system szyfrowania oparty na tablicy przyporządkowującej każdej literze parę cyfr (tabela 1.1). W późniejszych czasach tablica ta stała się podstawą wielu systemów szyfrowania. Przekształcenie liter w liczby dawało możliwość wykonywania dalszych przekształceń za pomocą prostych obliczeń lub funkcji matematycznych. Metodę Polibiusza uzupełnioną kilkoma dodatkowymi utrudnieniami kryptoanalitycznymi zastosowała między innymi niemiecka armia przy opracowywaniu wspomnianego na wstępie systemu szyfrującego ADFGX oraz jego udoskonalonej wersji ADFGVX.

Pierwsze wzmianki dotyczące stosowania kryptografii w celach politycznych pochodzą z V w. p.n.e. z Indii. Wymieniana jest ona jako jeden ze

sposobów zdobywania informacji przez przebywających za granicą ambasadorów. Sekretne pismo wspomniane jest również w słynnej Kamasutrze — figuruje tam jako jedna z 64 sztuk, które kobieta powinna znać.

Ogólnie stosowane w starożytności metody kryptografii można podzielić na dwa rodzaje — przestawianie i podstawianie. W pierwszym przypadku następowała zamiana szyku liter w zdaniach, czyli, innymi słowy, tworzony był anagram. Przykładem szyfrowania przestawieniowego jest pierwsze znane urządzenie szyfrujące — *spartańska scytale* z V w. p.n.e. Miała ona kształt pręta o podstawie wielokąta, na który nadawca nawijał skórzany pas. Wiadomość pisana była wzdłuż pręta, po czym odwijano pas, na którym widać było tylko pozornie bezsensowną sekwencję liter. Potem goniec przenosił list do adresata, stosując czasem steganograficzne sztuczki, na przykład opasując się nim i ukrywając tekst po wewnętrznej stronie. Odczytanie wiadomości było możliwe przy użyciu scytale o takiej samej grubości, jaką miał pręt nadawcy.

Druga, bardziej popularna metoda polegała na podstawianiu za litery tekstu jawnego innych liter bądź symboli. Za przykład może tu posłużyć szyfr Cezara, najsłynniejszy algorytm szyfrujący czasów starożytnych (jego twórcą był Juliusz Cezar). Szyfr ten opierał się na zastąpieniu każdej litery inną, położoną o trzy miejsca dalej w alfabecie. W ten sposób na przykład wiadomość o treści Cesar przekształca się w Fhvdu. Adresat znający sposób szyfrowania w celu odczytania wiadomości zastępował każdą literę tekstu tajnego literą położoną o trzy miejsca wcześniej w alfabecie.

Szyfry przyporządkowujące każdej literze alfabetu jawnego dokładnie jedną literę, kombinację cyfr lub symbol nazywamy szyframi monoalfabetycznymi. W przypadku szyfru Cezara układ alfabetu tajnego zawsze pozostawał ten sam. Znacznie bezpieczniejszym rozwiązaniem było dokonywanie w nim okresowych zmian tak, aby znajomość metody szyfrowania nie wystarczała do odczytania wiadomości.

Stanowiło to jednak utrudnienie również dla adresata. Musiał on dodatkowo posiadać klucz (układ liter lub symboli w alfabecie tajnym). Tak powstał największy problem w historii kryptografii — dystrybucja klucza. Raz

przechwycony klucz stawał się bezużyteczny, gdyż wiadomości szyfrowane za jego pomocą nie były już bezpieczne. O ile w przypadku wymiany wiadomości między dwiema osobami nie była to z reguły duża przeszkoda (wystarczyło ustalić nowy klucz), o tyle w przypadku szyfrowania na potrzeby wojskowe rodziło to bardzo wiele problemów. Trzeba było dostarczyć nowy klucz do wszystkich jednostek i to możliwie szybko, gdyż każda przechwycona przez wroga wiadomość stawała się dla niego łatwa do odczytania.

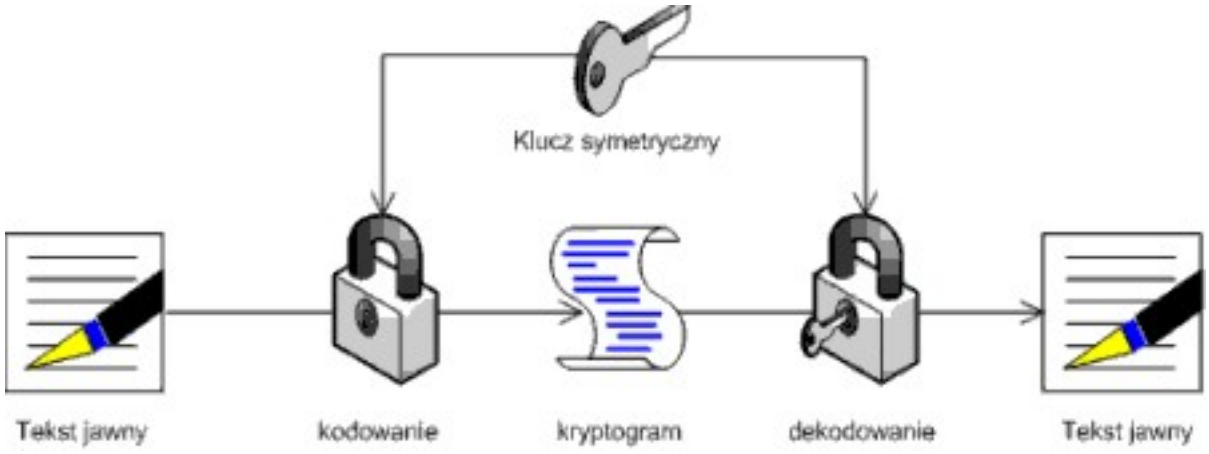
Istnieją dwie podstawowe grupy algorytmów szyfrowania.

1.3 Szyfry z kluczem symertycznym

Przy szyfrowaniu wiadomości kluczem symertycznym, klucz używany do jej zaszyfrowania jest identyczny z kluczem wymaganym do ich odszyfrowania (rys. 1.1). Oznacza to, że najpierw nadawca i odbiorca muszą wspólnie określić klucz, jakiego będą używać do szyfrowania korespondencji między sobą. Oznacza to, że przy korespondencji z np. 10 kontrahentami musimy posiadać 10 różnych kluczy, co może stanowić problem z określeniem, który klucz powinniśmy użyć. Globalnie oznacza to, że dla np. 10 osób trzeba wygenerować aż 45 różnych kluczy, ale przy np. 100 osobach już trzeba wygenerować 4950 różnych kluczy.

1.4 Szyfry z kluczem asymertycznym

W algorytmach szyfrowania asymetrycznego klucze szyfrowania i deszyfracji są różne i są w posiadaniu różnych osób (rys. 1.2). Oznacza to, że każda osoba chcąca szyfrować wiadomości musi posiadać dwa klucze, **publiczny** i **prywatny**. Jak sama nazwa wskazuje klucz publiczny jest udostępniany wszystkim zainteresowanym, natomiast klucz prywatny musi pozostać tany. Zaletą szyfrowania asymetrycznego jest to, że każda osoba musi posiadać jeden klucz prywatny (swój) oraz klucze publiczne osób, z którymi chce korespondować. Oznacza to, że musimy posiadać mniejszą ilość kluczy niż w



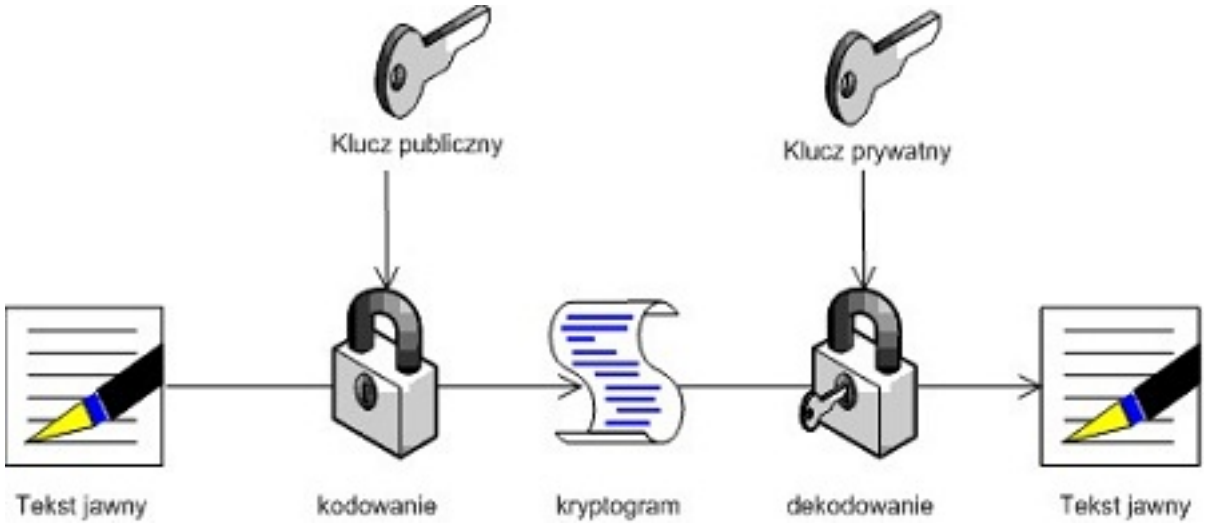
Rysunek 1.1: Schemat szyfrowania kluczem symetrycznym. Źródło [5]

przypadku szyfrowania kluczem symetrycznym. Globalnie oznacza to, że dla np. 10 osób trzeba wygenerować tylko 20 kluczy, a dla np. 100 osób tych kluczy potrzeba wygenerować tylko 200. Jak widać różnica w liczbie generowanych kluczy jest kolosalna, dlatego obecnie na świecie sposób ten jest najczęściej stosowany.

1.5 Podpis cyfrowy

Podpis cyfrowy jest to matematyczny sposób potwierdzania autentyczności cyfrowego dokumentu. Istnieje wiele schematów podpisów cyfrowych, obecnie jednak najpopularniejszym jest schemat podpisu dokumentów cyfrowych w systemach kryptograficznych z kluczem publicznym i jednokierunkową funkcją skrótu - w systemie tym do oryginalnej wiadomości dołączany jest skrót dokumentu, zaszyfrowany prywatnym kluczem nadawcy. Potwierdzenie autentyczności wiadomości jest możliwe po odszyfrowaniu skrótu kluczem publicznym nadawcy i porównaniu go z wytworzonym skrótem odebranego dokumentu [4].

Podpisywanie się pod dokumentami jest nieodłączną częścią handlu. Wraz z rozwojem handlu elektronicznego narodziła się potrzeba opracowania elek-



Rysunek 1.2: Schemat szyfrowania kluczem asymetrycznym. Źródło [5]

tronicznych odpowiedników podpisów. Protokoły podpisu elektronicznego są próbą rozwiązania tego problemu. W Polsce prace nad wprowadzeniem podpisu elektronicznego ruszyły na początku roku 2001. Odpowiednia ustawa została uchwalona 18 września tego samego roku. Kolejny rok zajęło wprowadzanie odpowiednich aktów wykonawczych, w wyniku czego oficjalnie w polskim prawie podpis elektroniczny funkcjonuje dopiero od 16 sierpnia 2002. Powstało kilka Centrów Certyfikacji pozwalających na wyrobienie certyfikatu niezbędnego do wykonywania podpisów elektronicznych.

Podobnie jak w przypadku pozostałych protokołów, najpierw trzeba się zastanowić, jakie warunki musi spełniać poprawnie wykonany podpis elektroniczny. Dopiero wtedy można zacząć myśleć nad zastosowaniem konkretnych mechanizmów kryptograficznych. Z pewnością podpis powinien jednoznacznie wskazywać na tożsamość podpisującego. Ponadto powinien być niepodrabialny. Osoba podpisująca nie może później wyprzeć się złożonego podpisu, jak również zmienić treści podpisanego dokumentu. Wreszcie sam podpis nie może zostać użyty po raz drugi, ani też przeniesiony na inny dokument.

W protokołach podpisu cyfrowego powyższe zadania są realizowane przy

użyciu kryptografii asymetrycznej oraz jednokierunkowych funkcji skrótu. Są to funkcje jednokierunkowe, generujące jako wynik skrót o określonej długości. Innymi słowy dla dowolnie długiej wiadomości (nieprzekraczającej limitu wyznaczonego dla danego algorytmu) wynik będzie miał zawsze ten sam rozmiar (na przykład 160 bitów). Jest to bardzo przydatna właściwość, ponieważ często podpisywane dokumenty mają dość spore rozmiary. Bez funkcji skrótu obliczenia konieczne do wykonania podpisu znacznie by się wydłużały. Podpisywanie skrótu wiadomości trwa natomiast o wiele krócej.

Wygenerowany skrót wiadomości podpisywany jest z wykorzystaniem klucza prywatnego użytkownika. Umożliwia to każdemu, kto ma dostęp do odpowiedniego klucza publicznego, zweryfikowanie tożsamości podpisującego. Zmiana treści dokumentu uniemożliwi weryfikację podpisującego, a samego podpisu nie można przenieść na inny dokument.

Opisana procedura to „klasyczny" protokół podpisu cyfrowego. W zależności od potrzeb tworzone są również inne rozwiązania. Poniżej Autor podaje niektóre z nich.

1.5.1 Niezaprzeczalne podpisy cyfrowe

Nazwa tego typu protokołów może być nieco myląca, ponieważ protokoły niezaprzeczalne (oprócz tradycyjnej funkcji podpisywania dokumentów) uniemożliwiają weryfikację podpisu bez zgody podpisującego. Wiąże się ona jednak z tym, iż podpisujący nie może się również wyprzeć swojego podpisu. Protokół tego typu przebiega w następujący sposób:

- Użytkownik A przedstawia użytkownikowi B dokument wraz z wykonanym przez siebie podpisem.
- Użytkownik B generuje liczbę losową i przesyła ją do użytkownika A.
- Użytkownik A dokonuje przekształcenia otrzymanej liczby w oparciu o swój klucz prywatny. Przekształcenie to jest dosyć zawiłe matematycznie, najważniejszy jednak jest fakt, iż uzyskanie poprawnego (pasują-

cego do podpisu) wyniku jest możliwe tylko przy wykorzystaniu klucza prywatnego osoby podpisującej.

- Użytkownik A wysyła wynik obliczeń do użytkownika B.
- Następuje weryfikacja podpisu.

Mimo wrażliwości na ataki typu Man in the Middle protokoły tego typu znajdują liczne zastosowania ze względu na możliwość kontrolowania procesu weryfikacji przez osobę podpisującą dokument. Dodatkowe podprotokoły pozwalają na dowodzenie autentyczności podpisów lub uniemożliwiają wypieranie się ich.

Przykładowe algorytmy realizujące protokół podpisu niezaprzeczalnego to:

- *Algorytm Chauma* — oparty na potęgowaniu modulo liczba pierwsza p,
- *Algorytm Boyar-Damagarda* — oparty na algorytmie podpisu cyfrowego EIGamala,
- *Algorytm Harna-Yanga* — dla niezaprzeczalnych podpisów grupowych.

1.5.2 Niepodrabialne podpisy cyfrowe

Najpierw wypada się zastanowić, jakie cechy musiałby posiadać podpis niepodrabialny. Ponieważ technologia podpisu opiera się na wykorzystaniu par kluczy publiczny-prywatny, ewentualne fałszerstwo wymagałoby znalezienia (lub odtworzenia) odpowiedniego klucza prywatnego. Taka operacja wymaga ogromnej mocy obliczeniowej porównywalnej ze złamaniem szyfru asymetrycznego. Niemniej jednak nie można wykluczyć tego typu ataków. Jak im przeciwdziałać? Otóż jest to niemożliwe. Fałszerstwu nie da się zapobiec, można je jednak wykryć. Służą temu protokoły podpisów niepodrabialnych. Dla każdego klucza publicznego istnieje wiele pasujących kluczy

prywatnych. Aby dokonać fałszerstwa, atakujący musiałby znaleźć ten właściwy, będący w posiadaniu osoby wykonującej podpis. Tymczasem o wiele większe jest prawdopodobieństwo uzyskania innego klucza prywatnego pasującego do badanych podpisów i klucza publicznego. Podpisy wykonane tym kluczem faktycznie będą weryfikowane jako należące do osoby, której podpis jest podrabiany. Niemniej jednak, jeśli zajdzie taka konieczność, łatwo będzie udowodnić, że doszło do fałszerstwa, ponieważ wykonano je przy użyciu innego klucza prywatnego. Podpisy są w takim przypadku odmienne, chociaż pasują do tego samego klucza publicznego.

W ten sposób zniwelowane zostaje ryzyko skutecznego ataku ze strony przeciwnika dysponującego dużą mocą obliczeniową, nadal jednak istnieje możliwość podrobienia podpisu poprzez kradzież właściwego klucza prywatnego.

1.5.3 Podpisy ślepe

Ślepe podpisy cyfrowe opracowano z myślą o sytuacjach, w których podpisujący nie powinien poznać treści podpisywanego dokumentu. Być może wydaje się to niedorzeczne, a jednak w pewnych okolicznościach może okazać się przydatne.

Wyobraźmy sobie sytuację, w której jeden z uczestników protokołu występuje w charakterze notariusza. Potwierdza swoim podpisem dostarczenie pewnego dokumentu przez innego użytkownika. Jednocześnie dostarczyciel chciałby mieć pewność, iż notariusz nie pozna informacji zawartych we wspomnianym dokumencie.

Najprostszym rozwiązaniem w takiej sytuacji jest wykorzystanie tzw. czynnika zaciemniającego. Jest to wybrana losowo zmienna, przez którą użytkownik A mnoży wysyłane do podpisu dane. Użytkownik B (notariusz) składa podpis pod tak przekształconym dokumentem, nie mając możliwości uzyskania żadnych informacji co do jego treści (o ile zmienna wybrana była w sposób naprawdę losowy), a następnie odsyła go użytkownikowi A. Ten usuwa zaciemnienie i otrzymuje pierwotny dokument wraz z podpisem. Takie

rozwiązanie ma jednak pewną wadę. Użytkownik B nie ma żadnej możliwości sprawdzenia, czy tak naprawdę nie podpisuje zobowiązania wpłaty sporej sumy na konto użytkownika A. Aby temu zapobiec, udoskonalono całą procedurę w poniżej opisany sposób. Użytkownik A przygotowuje dokument do podpisu, po czym wykonuje n jego kopii. Wszystkie kopie, każda po przemnożeniu przez inny czynnik zaciemniający, przesyłane są do użytkownika B. Ten prosi użytkownika A o dostarczenie czynników zaciemniających dla n-1 dokumentów. Wszystkie te dokumenty sprawdzane są pod kątem potencjalnego oszustwa. Jeśli okażą się formalnie poprawne, podpis jest składany pod jedynym nieodszyfrowanym plikiem. Aby móc oszukać tak skonstruowany protokół, użytkownik A musiałby przewidzieć (a raczej zgadnąć), o które czynniki zaciemniające poprosi go użytkownik B. Prawdopodobieństwo takiego wydarzenia wynosi $1/n$. Innymi słowy im większe n, tym większe prawdopodobieństwo wykrycia złych zamiarów ze strony wysyłającego dokument. Jeśli dodamy do tego surową karę za wszelkie próby oszustwa, protokół powinien zapewnić duże bezpieczeństwo.

1.5.4 Inne warianty podpisu cyfrowego

Oprócz powyższych wymienić można również inne protokoły dokonywania podpisów cyfrowych, opierające się na podobnych rozwiązaniach:

- *Podpisy pośrednie* (ang. **proxy signatures**) pozwalają na wstawianie podpisów przez użytkownika B w imieniu użytkownika bez znajomości jego klucza prywatnego,

- *Podpisy z wyznaczonym potwierdzającym* (ang. **designated confirmer signatures**) umożliwiają weryfikację podpisu przez osobę trzecią. Dzięki temu potwierdzenie poprawności podpisu jest możliwe nawet w sytuacji, kiedy osoba podpisująca jest niedostępna (na przykład ze względu na chorobę lub wyjazd), a także w przypadku utraty przez nią klucza prywatnego

- *Podpisy grupowe* (ang. **group signatures**) służą nie tyle sprawdzeniu tożsamości podpisującego, ile jego przynależności do danej grupy. Innymi słowy protokół obsługuje przyznawanie uprawnień w obrębie określonego zbioru użytkowników. Podpisy sprawdzane są jedynie pod kątem przynależności danego użytkownika do wspomnianego zbioru. Jego tożsamość może być jednak ujawniona, jeśli zachodzą wątpliwości co do autentyczności podpisu.

Rozdział 2

Infrastruktura klucza publicznego

Skrót PKI oznacza *infrastrukturę klucza publicznego* (ang. **Public Key Infrastructure**) i odnosi się do rozwiązań mających na celu zarządzanie kluczami publicznymi użytkowników. O ile bowiem wymiana zaszyfrowanej korespondencji między znajomymi nie wymaga specjalnego systemu zarządzania kluczami szyfrującymi, o tyle w przypadku rozwiązań na większą skalę system taki jest konieczny. Mamy wówczas do czynienia z większą liczbą użytkowników i konieczne jest rozwiązanie problemu bezpiecznej dystrybucji kluczy. Jaką mamy bowiem gwarancję, że pobrany przez nas z serwera klucz publiczny faktycznie należy do danej osoby? Może mamy do czynienia z atakiem Man in the Middle? Konieczne staje się zatem utworzenie zaufanej instytucji, która potwierdzałaby przynależność kluczy do poszczególnych osób i organizacji. Tu pojawia się PKI.

2.1 PKI w teorii...

PKI jest rozwiązaniem pozwalającym na przypisywanie użytkownikom kluczy i uniemożliwianie fałszerstw opartych na ich podmienianiu. Jak jednak miałoby to działać? Na początek Autor przedstawia model teoretyczny.

PKI zakłada istnienie centralnej instytucji obdarzonej powszechnym zaufaniem, której zadaniem byłoby wydawanie, przechowywanie i udostępnianie kluczy publicznych oraz udzielanie informacji o nich. Instytucję taką nazywamy centrum certyfikacji (stosuje się również skrót CA pochodzący od angielskiej nazwy **certification authority**). Każdy nadesłany klucz publiczny podlega procesowi certyfikacji — użytkownik, który go nadesłał, proszony jest o podanie swoich danych osobowych, a te są przez centrum weryfikowane. Jeśli podane informacje okażą się prawdziwe, do klucza zostaje przypisany odpowiedni certyfikat, w którym potwierdza się, iż klucz ten należy do danego użytkownika. Certyfikat zawiera podpis elektroniczny centrum certyfikacji, dzięki czemu każdy może zweryfikować jego autentyczność. Jedynym warunkiem jest tutaj ogólna dostępność klucza publicznego danego centrum. Klucze użytkowników są przechowywane w centrum certyfikacji i powszechnie udostępniane. W każdej chwili możliwe jest usunięcie własnego klucza z bazy danych (na przykład w przypadku kompromitacji klucza prywatnego).

Przedstawione rozwiązanie wygląda elegancko i sprawia wrażenie bezpiecznego. Mamy oto zaufaną instytucję umożliwiającą wszystkim bezpieczną komunikację z użyciem kryptografii asymetrycznej. Rzeczywistość, jak zwykle, wygląda nieco inaczej.

2.2 ...i w praktyce

Opisany powyżej model PKI nie ma prawa zaistnieć w realnym świecie. Rozwiązania stosowane w praktyce znacznie różnią się od idealnego modelu. W tym rozdziale Autor wskaże najważniejsze przeszkody stojące na drodze do jego konstrukcji oraz ich wpływ na kształt rzeczywistych struktur PKI.

2.2.1 Złożoność

Nasz idealny model zakładał istnienie centralnego urzędu certyfikacji obsługującego wszystkich użytkowników. Jeśli weźmie się pod uwagę potencjalną liczbę tych użytkowników, od razu staje się jasne, dlaczego model taki nie

ma prawa poprawnie działać. Szacuje się, że do internetu ma dostęp ponad miliard ludzi. Do tego doliczyć należy osoby prawne (przedsiębiorstwa, banki itp.). Być może nie każdy użytkownik będzie chciał korzystać z PKI, ale niektórzy będą potrzebować więcej niż jednego klucza. Takie centrum musiałoby przypisać każdemu z nich unikalną nazwę powiązaną z odpowiednim kluczem. Nazwa ta powinna umożliwiać innym użytkownikom jednoznaczną identyfikację właścicieli kluczy.

Jest to problem praktycznie nierozwiązywalny. Wiele krajów wprowadziło numery identyfikacyjne dla swoich obywateli (przykładem może być PESEL), tu jednak mamy do czynienia z systemem identyfikacji w skali globalnej. Wykorzystanie numerów identyfikacyjnych nadanych w poszczególnych krajach nie wchodzi w rachubę z dwóch powodów — po pierwsze rozwiązanie to nie funkcjonuje wszędzie, a po drugie w niektórych krajach wykorzystywanie takich danych jest zabronione przez prawo o ochronie danych osobowych.

Już ta jedna przeszkoda uniemożliwia powołanie ogólnoświatowego centrum certyfikacji. Na tym jednak nie koniec.

2.2.2 Zaufanie

Kolejny problem wynika bezpośrednio z poprzedniego. W jaki sposób skłonić wszystkich użytkowników, aby zaufali naszemu centrum? Należy pamiętać, że mamy do czynienia z dziesiątkami, albo nawet setkami milionów ludzi na całym świecie. Ustanowienie instytucji, której ufaliby wszyscy, jest po prostu niemożliwe. Jest to o tyle istotne że w wielu przypadkach certyfikowane klucze służą do ochrony ważnych transakcji handlowych. Zaufanie i pewność co do tożsamości drugiej strony jest tutaj podstawową sprawą.

Rozwiązaniem powyższych problemów jest odejście od koncepcji uniwersalnego PKI na rzecz struktury rozproszonej. Główne centra certyfikacji podpisują certyfikaty regionalnych, te z kolei mogą potwierdzać certyfikaty jeszcze niższego szczebla, itd. W ten sposób powstaje tzw. ścieżka certyfikacji, a więc lista kolejnych centrów potwierdzających dany certyfikat. Przykładowa ścieżka certyfikacji przedstawiona została na rysunku

Wstawić rysunek z Podstawy kryptografii rys. 4.72 ze s.217 lub podobny

. Na samej górze znajduje się główne centrum (ang. **Global Sign Root CA**), poniżej zaś kolejne, aż do tego, które bezpośrednio podpisało nasz certyfikat.

Takie rozwiązanie znacznie ułatwia organizację wydawania certyfikatów. Dzięki istnieniu centrów certyfikacji w poszczególnych krajach i regionach o wiele prostsza staje się obsługa większej liczby użytkowników, a przeszkody związane z brakiem zaufania zostają w znaczny sposób ograniczone.

Istnieje jednak pewna wada takiego rozwiązania. Otóż struktura wielopoziomowa jest bardziej podatna na fałszerstwa niż struktura scentralizowana. Każdy punkt w ścieżce certyfikacji to potencjalne miejsce ataku. Złożoność zawsze źle wpływa na bezpieczeństwo i podobnie jest również w tym przypadku. Ciekawe rozwiązanie tego problemu podano w książce Kryptografia w praktyce: regionalne centrum podpisuje certyfikat użytkownika, a następnie wysyła go do centrum głównego. Tam sprawdzana jest poprawność ścieżki certyfikacji i, jeśli przebiegnie ona poprawnie, wystawiany jest nowy certyfikat, podpisany bezpośrednio przez tę instytucję. Takie rozwiązanie rokuje pewne nadzieje, jednak jak dotąd nie jest stosowane w praktyce.

2.2.3 Cykl życia klucza

Inny problem, przed jakim stają projektanci i użytkownicy PKI, związany jest z cyklem życia kluczy. Generalnie wyróżnić tu można sześć etapów:

- utworzenie,
- certyfikacja,
- rozprowadzanie,
- użytkowanie aktywne,
- użytkowanie pasywne,

- unieważnienie klucza.

Tworzenie klucza i jego certyfikacja do stosunkowo krótkie i proste etapy. Problemy związane z wystawianiem zaufanego certyfikatu przedstawiono we wcześniejszej części tego rozdziału. Kolejnym etapem jest rozprowadzanie klucza zarówno przez jego właściciela, jak i przez centrum certyfikacji (klucz jest umieszczany na serwerze, skąd każdy może go pobrać). Użytkowanie aktywne oznacza etap, w którym użytkownik korzysta ze swojego klucza prywatnego do szyfrowania wiadomości, a pozostali deszyfrują je kluczem publicznym. Użytkowanie pasywne rozpoczyna się w momencie wycofania z użytku klucza prywatnego. Bywa to na ogół spowodowane jego zmniejszonym bezpieczeństwem. Może się ono wiązać z jego kompromitacją lub zbyt długim okresem użytkowania. Okres taki może trwać kilka miesięcy lub nawet kilka lat, w zależności od przypadku. Im cenniejsze informacje chroni klucz, tym częściej należy go zmieniać. Powszechną praktyką jest wyznaczanie limitu określającego ilość danych, które można bezpiecznie zaszyfrować danym kluczem. Po jego przekroczeniu pojawia się ryzyko wycieku chronionych informacji (sytuacja taka bywa również określana jako zmęczenie klucza). W związku z powyższym w systemach przetwarzających duże ilości tajnych danych stosuje się rozdzielanie kluczy. Polega ono na przypisywaniu osobnych kluczy do poszczególnych typów danych, osób czy zastosowań. Dzięki temu zmniejszana jest ilość informacji szyfrowanych pojedynczym kluczem, co wydłuża okres jego użytkowania. Dodatkową zaletą tego rozwiązania jest ograniczenie strat związanych z ewentualną kompromitacją klucza.

Warto tu również zaznaczyć, iż decyzja w kwestii unieważnienia klucza niekoniecznie musi zależeć od właściciela klucza. Centra certyfikacji często wyznaczają okres ważności certyfikatu, po którym przypisany mu klucz publiczny przestaje być ważny. Również same centra muszą co jakiś czas zmieniać swoje klucze.

Po wycofaniu klucza następuje z reguły kilkumiesięczny okres, w trakcie którego użytkownik nadal będzie odbierał zaszyfrowane nim wiadomości, jednak sam nie będzie już szyfrował niczego odpowiadającym mu kluczem

prywatnym. Klucz jest nadal akceptowany, dzięki czemu można zakończyć wszelkie rozpoczęte wcześniej operacje. Po tym okresie klucz zostaje unieważniony. I w tym miejscu zaczynają się problemy.

Unieważniony certyfikat umieszczony zostaje na specjalnej liście CRL (lista odwołań certyfikatów). Każdy użytkownik, który chce wykorzystać do szyfrowania pobrany wcześniej z serwera klucz publiczny, powinien najpierw sprawdzić, czy klucz ów nie znajduje się na tej liście. Teoretycznie jest to dobre rozwiązanie. W rzeczywistości może ono rodzić liczne problemy.

Po pierwsze zablokowanie dostępu do bazy CRL uniemożliwi sprawdzenie ważności kluczy. Może to nastąpić w wyniku awarii lub ataku typu DoS. W konsekwencji nieważny klucz publiczny będzie ponownie wykorzystywany. Tworzenie rozproszonej bazy CRL jest z kolei rozwiązaniem bardzo kosztownym.

Po drugie samo istnienie takiej bazy nie spowoduje, iż ludzie posiadający unieważniony certyfikat nagle zdadzą sobie sprawę z jego nieprzydatności. Pozostanie on nadal w użytku, ponieważ mało kto zadaje sobie trud regularnego sprawdzania ważności posiadanych certyfikatów. Mówiąc krótko, niemożliwe jest dostarczenie informacji o unieważnieniu certyfikatu do wszystkich jego posiadaczy.

Pojawiają się również inne problemy związane z użytkowaniem certyfikatów. Liczne zarzuty są wysuwane na przykład wobec standardu x.509 (powszechnie używanego w Polsce). Można wskazać tu również trudności związane ze strukturą certyfikatu i jego kompatybilnością z przeglądarkami internetowymi. W Polsce swego czasu pojawiły się problemy z certyfikatami niektórych banków internetowych, które były rozpoznawane jako nieważne przez przeglądarkę Internet Explorer. Winny wszystkiemu był błąd w przeglądarce. Opracowano stosowną aktualizację i certyfikaty znów są poprawnie weryfikowane.

PKI jest świetnym przykładem na to, jak ważne jest odpowiednie zastosowanie opracowanych mechanizmów kryptograficznych. Złe rozwiązanie strukturalne może narazić na szwank teoretycznie solidny system bezpieczeństwa.

Jest to jednak bardziej kwestia odpowiedniej organizacji niż kryptografii, dlatego Autor nie będzie się szerzej rozpisywać na ten temat.

Rozdział 3

Język XML

To jest rozdział o XML.

3.1 XML Signature

To sekcja o XML Signature[3].

3.1.1 Struktura dokumentu

Tu jest opis struktury elementu XML Signature.

```
<Signature ID?>
    <SignedInfo>
        <CanonicalizationMethod/>
        <SignatureMethod/>
        (<Reference URI? >
            (<Transforms>)?
            <DigestMethod>
            <DigestValue>
        </Reference>)+
    </SignedInfo>
    <SignatureValue>
   (<KeyInfo>)?
   (<Object ID?>)*
</Signature>
```

Prosty przykład zastosowania.

```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
   <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
         <Transforms>
            <Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
         </Transforms>
         <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
         <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK.../DigestValue>
      </Reference>
   </SignedInfo>
   <SignatureValue>...</SignatureValue>
   <KeyInfo>
      <KeyValue>
         <DSAKeyValue>
            <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
         </DSAKeyValue>
      </KeyValue>
   </KeyInfo>
</Signature>
```

Element *SignedInfo*

Element *SignatureValue*

Element *KeyInfo*

Element *Object*

3.1.2 Elementy dodatkowe

Element *Manifest*

Element *SignaturePropeties*

Rozdział 4

Zakończenie

To już jest koniec! Nie ma już nic, jesteśmy wolni, możemy iść!!!

Bibliografia

[1] Karbowski M., *Podstawy kryptografii*, Wydanie II, Helion, Gliwice 2008

[2] Kazienko P. Gwiazda K., *XML na poważnie*, Helion, Gliwice 2002

[3] XML Signature Syntax and Processing (Second Edition) *http://www.w3.org/TR/xmldsig-core/*, październik 2010, dostępna online

[4] Strona internetowa Wikipedia.pl *http://pl.wikipedia.org/wiki/Podpis_cyfrowy*, październik 2010, dostępna online

[5] Adres strony internetowej z której pochodzą obrazki schematu klucza symetrycznego i asymetrycznego *http://vpn.svera.pl/szyfry.php*

Spis rysunków

Spis tabel