KRYPTOGRAFIA ASYMETRYCZNA I JEJ ZASTOSOWANIE W ALGORYTMACH KOMUNIKACJI

Krzysztof Bartyzel

Wydział Matematyki Fizyki i Informatyki,
Uniwersytet Marii Curii-Skłodowskiej w Lublinie

Streszczenie: Komunikacja oparta o otwarte kanały transmisyjne często wymaga użycia kryptograficznych metod w celu zapewnienia bezpieczeństwa. Artykuł przybliża zagadnienia związane z kryptografią klucza publicznego, podpisem cyfrowym, certyfikatem X.509 oraz szyfrowaną komunikacją.

Abstract: Cryptographic methods are often needed to assure security in communication over the open networks. This article approaches the technologies of public key cryptography, digital signature, public key certificate X.509 and encrypted communication.

Wstęp i podstawowe pojęcia

Słowo „kryptografia” pochodzi z greckiego „kryptós” „ukryty", „gráphein” „pisać" i można je przetłumaczyć jako „tajne pismo” lub „ukryte znaczenie”. Początkowo kryptografia opierała się na tajności sposobu przekazywania informacji oraz na steganograficznych sposobach ukrywania informacji w tekstach lub grafikach w taki sposób, aby nawet osoba przewożąca wiadomości nie wiedziała, że przewozi jakąś tajną wiadomość. Obecnie kryptografia zajmuje się przekształcaniem wiadomości w taki sposób, aby stała się niemożliwa do odczytania bez użycia specjalnego tajnego klucza.

Każdy algorytm kryptograficzny można zaliczyć do kryptografii symetrycznej albo do kryptografii asymetrycznej. Kryptografia symetryczna (Rys. 1) jest to taka kryptografia, w której zarówno do szyfrowania jak i do odszyfrowywania używamy tego samego klucza. Kryptografia asymetryczna (Rys. 2) jest to kryptografia, w której do szyfrowania używamy jednego klucza (tzw. Klucz publiczny) natomiast do odszyfrowywania używamy innego klucza (tzw. Klucz prywatny).

Rys. 1 Schemat algorytmu symetrycznego

Rys. 2 Schemat algorytmu asymetrycznego

Koncepcja kryptografii asymetrycznej została zaproponowana przez W. Diffie i M. Hellman w 1976 roku w pracy „New Directions in Cryptography”. Zaproponowany przez nich kryptosystem klucza publicznego (ang. *public key cryptosystem*) umożliwiał użycie publicznego kanału do transmisji kluczy, jednocześnie zapewniając bezpieczeństwo informacji zakodowanych za pomocą tego klucza. Zaproponowali oni użycie dwóch odmiennych kluczy, jednego E do szyfrowania wiadomości, drugiego D do ich

odszyfrowywania. Znajomość E w żaden sposób nie umożliwiała znalezienie D. To dało możliwość każdemu użytkownikowi umieszczenia w ogólnodostępnym miejscu swojego publicznego klucza E.

Do tej pory, aby zapewnić bezpieczeństwo komunikacji wymagane było użycie *(n-1)*n/2* kluczy zapewniając każdej parze użytkowników różną parę kluczy, natomiast stosując system Diffie i Hellman należało wygenerować zaledwie 2**n* kluczy.

Algorytm wymyślony przez W. Diffiego i M. Hellmana nie jest już bezpieczny, ale zapoczątkowana przez nich koncepcja kryptografii z kluczem publicznym była kontynuowana i zaowocowała powstaniem wielu bezpiecznych algorytmów. Najbardziej znanym i najczęściej używanym algorytmem asymetrycznym jest algorytm RSA.

Tabela 1. Porównanie ilości kluczy przy wykorzystaniu kryptografii symetrycznej i asymetrycznej w zależności od ilości użytkowników kryptosystemu.

Ilość użytkowników	***Kryptografia symetryczna***	***Kryptografia asymetryczna***
1	0	2
4	6	8
10	45	20
25	300	50
100	4 950	200
1 000	499 500	2 000
10 000	49 995 000	20 000

Algorytmy asymetryczne

Istnieje wiele różnych algorytmów asymetrycznych, jednakże wszystkie działają w w taki sposób, że w publicznym katalogu każdy użytkownik umieszcza procedurę szyfrowania i deszyfrowania *(ang. Encryption and decryption procedure)*. W katalogu zawarty jest również publiczny klucz E tego użytkownika. Klucz prywatny D jest przechowywany przez użytkownika i nikomu pod żadnym względem nie powinien być udostępniony. Metody szyfrowania i deszyfrowania są jawne, ponieważ bezpieczeństwo systemów z kluczem publicznych jest zapewnione dzięki trudności i ilości wymaganych obliczeń, a nie tajności zastosowanego sposobu zaszyfrowania wiadomości.
Procedury E i D muszą spełniać następujące cztery warunki:

a) Odszyfrowując zaszyfrowaną wiadomość musimy dostać oryginalną wiadomość:
   D(E(M))=M dla każdej wiadomości M;
b) Zarówno E jaki i D nie są obliczeniowo skomplikowane (są to funkcje o złożoności wielomianowej);
c) Publikując E użytkownik nie zmniejsza bezpieczeństwa wiadomości tj. nie istnieje prosta metoda wyznaczenia D za pomocą E. Oznacza to, że

użytkownik D jest jedyną osobą mogącą odszyfrować wiadomość zaszyfrowaną za pomocą E;

d) Jeśli wiadomość M zostanie najpierw „odszyfrowana", a następnie zaszyfrowana to powinniśmy otrzymać M:

$$E(D(M))=M \text{ dla każdej wiadomości } M.$$

Jeśli funkcja E spełnia warunki a), b) i c) to jest nazywana funkcją jednokierunkową z zapadką *(ang. trap-door one-way function)*. Ponadto, jeśli spełniony jest warunek d), to mamy do czynienia z permutacją jednokierunkową z zapadką *(ang. trap-door one-way permutation)*. Te funkcje nazywane są funkcjami z zapadką *(ang. trap-door)*, ponieważ są łatwe do wyliczenia, ale wyznaczenie odwzorowania odwrotnego jest bardzo trudne. Istnienie funkcji spełniających warunek d) stało się podstawą powstania podpisu cyfrowego.

Algorytm RSA

Kryptosystem RSA umożliwia zarówno szyfrowanie jak i dokonywanie podpisu cyfrowego. Został on opracowany przez Ronalda Rivesta, Adi Shamira i Leonarda Adlemana w 1977. Nazwa RSA powstała z pierwszych liter nazwisk jego wynalazców. Bezpieczeństwo oparte jest na problemie faktoryzacji dużych liczb oraz na problemie logarytmu dyskretnego. Ponieważ nie istnieją algorytmy umożliwiające szybkie rozwiązywanie tych problemów, a przy obecnych algorytmach czas rozwiązywania tego typu problemów rośnie wykładniczo wraz ze wzrostem wielkości stosowanych liczb, to do momentu ich odkrycia RSA jest bezpiecznym algorytmem.

Generacja kluczy

Weźmy dwie duże liczby pierwsze, p i q oraz obliczmy ich iloczyn $n=p*q$. Wybierzmy następnie liczbę e, mniejszą niż n względnie pierwszy z $(p-1)(q-1)$, co oznacza, że największym wspólnym dzielnikiem e i $(p-1)(q-1)$ jest 1. Następnie wyznaczmy liczbę d taką, aby $ed-1$ było podzielne przez $(p-1)(q-1)$, można to dokonać przy pomocy rozszerzonego algorytmu Euklidesa.

Liczby e i d są nazywane odpowiednio wykładnikiem publicznym i prywatnym. Klucz publiczny stanowi para (e,n), natomiast para (d,n) jest kluczem prywatnym. Czynniki p i q powinny być usunięte, bądź trzymane razem z kluczem prywatnym.

Obecnie trudne jest wyznaczenie wykładnika prywatnego d z klucza publicznego (e,n). Jednakże, jeśli zostanie odkryta metoda faktoryzacji liczby n (wchodzącej w skład klucza publicznego) na czynniki pierwsze p i q, to będzie możliwe ponowne wygenerowanie klucza prywatnego. Całe bezpieczeństwo algorytmu RSA opiera się o trudność faktoryzacji dużych liczb i odkrycie metody umożliwiającej łatwą faktoryzację liczb oznaczałaby definitywny koniec systemu RSA.

Szyfrowanie i deszyfrowanie

Przypuśćmy, że chcemy zaszyfrować wiadomość M, w tym celu wystarczy, że wyznaczymy szyfrogram o postaci:

$$C=M^e \bmod n.$$

Aby odszyfrować wiadomość wystarczy wykonać taka samą operacje, ale używając klucza publicznego:

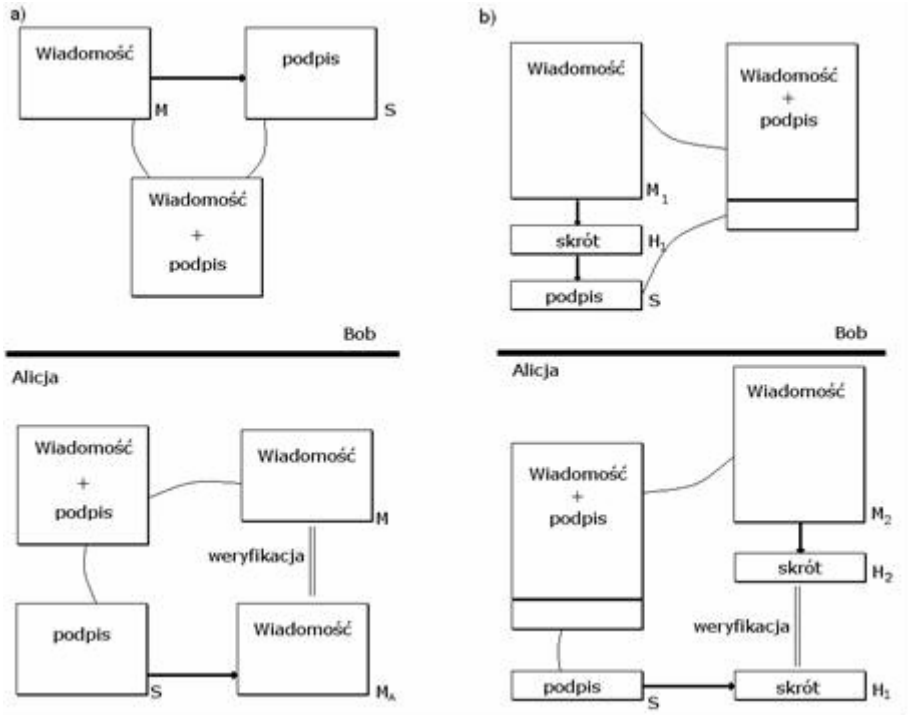
$$M=C^d \bmod n.$$

Podpis cyfrowy

Podpisu cyfrowy umożliwia potwierdzenie autentyczności dokumentu, weryfikację sygnatariusza, zapewnienie niezmienności treści od momentu podpisania oraz uniemożliwienia wyparcie się faktu podpisania dokumentu.

Podpis cyfrowy wykonywany jest przy pomocy klucza prywatnego, a weryfikowany za pomocą klucza publicznego. Oznacza to, że tylko jedna osoba może dokonać podpisu, właściciel klucza prywatnego, natomiast weryfikacji dokumentu może dokonać każdy, wystarczy, że z ogólnodostępnego katalogu pobierze klucz publiczny. Sytuacja jest odwrotna niż w przypadku szyfrowania. Podczas szyfrowania najpierw używamy klucza publicznego, a później klucza prywatnego. Gdy dokonujemy podpisu cyfrowego najpierw używamy klucza prywatnego później publicznego.

Istnieją dwa sposoby dokonania podpisu cyfrowego (Rys. 3). Model podpisu cyfrowego bez użycia funkcji skrótu jest bardzo uciążliwy w użytkowaniu. Powodem tego jest fakt, że w celu potwierdzenia autentyczności danego dokumentu musimy dołączyć do tego dokumentu jego podpis cyfrowy, którego wielkość jest porównywalna z wielkością dokumentu. W celu wyeliminowania tej niedogodności do algorytmu podpisu cyfrowego wprowadzono *jednokierunkowe funkcje skrótu.*



Rys 3 Schemat podpisu cyfrowego a) bez wykorzystania funkcji skrótu i b) z użyciem funkcji skrótu.

Działanie jednokierunkowych funkcji skrótu jest następujące:

a) Na podstawie pliku wejściowego, (przyjmijmy, że pracujemy z plikami, ale oczywiście mogą być to dane pochodzące z dowolnego źródła) o dowolnej wielkości, tworzony jest plik wynikowy (nazywany skrótem lub hasłem) zawsze o stałej wielkości niezależnie od rozmiaru pliku początkowego. W zależności od zastosowanej funkcji rozmiar pliku wynikowego może być inny, ale stosując jedną funkcję rozmiar skrótu zawsze będzie taki sam;
b) Nawet niewielkie zmiany w pliku wejściowym powinny powodować duże zmiany w pliku wynikowym;
c) Jest obliczeniowo trudne, aby znaleźć takie dwa pliki x i y, które po zastosowaniu na nich funkcji skrótu *H*, dawałyby takie same wartości tj., aby $H(x) \equiv H(y)$;
d) Ponadto jest obliczeniowo niewykonalne, aby znając funkcję skrótu jakiegoś pliku $H(x)$, umieć odtworzyć zawartość tego pliku *x*.

Podpis cyfrowy bez wykorzystania funkcji skrótu (Rys 3a)

Załóżmy, że Bob chce podpisaną wiadomość M przesłać do Alicji. Bob posiada klucz prywatny D, a klucz publiczny E jest umieszczony w publicznym katalogu. Aby podpisać wiadomość musi „zaszyfrować" wiadomość M za

pomocą swojego klucza prywatnego i otrzymany podpis wraz z oryginalną wiadomością przesłać do Alicji.

Alicja po otrzymaniu wiadomości i podpisu, „odszyfrowuje" podpis stosując klucz publiczny. Jeśli otrzymana wiadomość jest identyczna z wiadomością M otrzymana od Boba to powiadomienie jest autentyczne i następuje autoryzacja w przeciwnym razie należy uznać, że weryfikacja się nie powiodła.

Podpis cyfrowy z wykorzystaniem funkcji skrótu (Rys 3b)

Podobnie jak w poprzednim przypadku załóżmy, że Bob chce podpisaną wiadomość M przesłać do Alicji. Bob posiada klucz prywatny D, a klucz publiczny E jest umieszczony w publicznym katalogu. Aby podpisać wiadomość musi obliczyć skrót wiadomości M za pomocą ustalonej wcześniej funkcji skrótu. Tak otrzymany skrót „zaszyfruje" za pomocą swojego klucza prywatnego i otrzymany podpis wraz z oryginalną wiadomością przesłać do Alicji.

Alicja po otrzymaniu wiadomości i podpisu, „odszyfrowuje" podpis stosując klucz publiczny. Następnie oblicza skrót wiadomości M za pomocą tej samej funkcji skrótu co Bob. Jeśli otrzymany skrót wiadomości jest identyczny z odszyfrowanym podpisem to powiadomienie jest autentyczne i następuje autoryzacja, w przeciwnym razie weryfikacja się nie powiodła.

Certyfikaty

Standard X.509 opisuje budowę certyfikatu klucza publicznego. Może on zostać użyty, do przetransportowania różnych informacji związanych zarówno z procedurą szyfrowania jak i z weryfikacją podpisów. Duża część tej informacji jest opcjonalna, a zawartość obowiązkowych pól może się również zmieniać.

Certyfikat klucza publicznego jest ochroniony przez podpis cyfrowy wydawcy. Użytkownicy certyfikatów wiedzą, że jego zawartość nie została sfałszowana od momentu, gdy została podpisana, jeśli tylko podpis może zostać zweryfikowany. Certyfikaty zawierają grupę wspólnych pól, ponadto mogą zawierać opcjonalną grupę rozszerzeń. Jest dziesięć elementarnych pól: sześć obowiązkowych i cztery opcjonalne. Obowiązkowe pola to: numer seryjny, algorytm podpisu, nazwa wydawcy certyfikatu, okres ważności certyfikatu, klucz publiczny i nazwa podmiotu. Podmiot jest osobą, bądź organizacją, która jest w posiadaniu odpowiadającego klucza prywatnego. Opcjonalne pola to: numer wersji, dwa unikalne identyfikatory i rozszerzenie.

Protokół SSL

Protokół SSL *(ang. Secure Sockets Layer)*, opracowany przez firmę Nescape, stał się standardem komunikacji w Internecie. Został wprowadzony w celu zapewnienia prywatności komunikacji pomiędzy dwoma komputerami (serwerem i klientem) oraz dostarczenia autentyfikacji serwera i opcjonalnie

klienta. Swoje bezpieczeństwo opiera na bezpieczeństwie dostarczonym przez certyfikaty klucza publicznego.

SSL posługuje się protokołem komunikacyjnym, (np. TCP) przy wysyłaniu i odbieraniu wiadomości. Zaletą tego protokołu jest fakt, że jest on niezależny od aplikacji. Ustalenie bezpiecznego kanału transmisji może nastąpić przed przesłaniem pierwszej porcji danych przez inne protokoły (np. FTP, TELNET, HTTP). Wszystkie dane przesyłane za pomocą niezabezpieczonych protokołów, dzięki SSL, będą poufne.

Protokół SSL zapewnia **bezpieczny kanał** posiadający trzy podstawowe własności:

a) Kanał jest prywatny. Od momentu uzgodnienia klucza sesyjnego wszystkie wiadomości są szyfrowane;
b) Kanał jest autentyfikowany. Gwarantuje, że obie strony są naprawdę tymi za kogo się podają;
c) Kanał jest pewny. Transport wiadomości zawiera sprawdzanie integralności tych wiadomości.

Sesja SSL składa się z następujących kroków:

a) nawiązanie połączenia przez klienta;
b) wymiana informacji o metodzie szyfrowania;
c) uzgodnienie klucza sesyjnego;
d) przejście na połączenie szyfrowane;
e) zakończenie połączenia.

Szyfrowanie komunikacji

Istnieją trzy metody umożliwiające zapewnienie szyfrowanej komunikacji:

a) Szyfrowanie połączenia przy wykorzystaniu kryptografii asymetrycznej - jest to podejście zapewniające bardzo wysoki poziom bezpieczeństwa, ale ze względów praktycznych trudne do wykonania. Zazwyczaj szyfrowanie i deszyfrowanie przy wykorzystaniu kryptografii asymetrycznej trwa znacznie dłużej niż przy wykorzystaniu kryptografii symetrycznej;
b) Szyfrowanie połączenia przy pomocy kryptografii symetrycznej - jest to podejście zapewniające mniejszą wygodę (konieczność zapewnienia bezpiecznego kanału do przesłania klucza symetrycznego), jednakże szybkość jest znacząco wyższa niż w przypadku kryptografii asymetrycznej;
c) Metoda mieszana – metoda komunikacji umożliwiająca połączenie szybkości szyfrowania kryptografii symetrycznej z wygodą użytkowania kryptografii asymetrycznej. Po nawiązaniu połączenia następuje uzgodnienie klucza symetrycznego jednorazowego za pomocą kryptografii asymetrycznej, a następnie cała dalsza komunikacja odbywa się już za pomocą kryptografii symetrycznej. Jest to najczęściej

występująca metoda komunikacji. Została użyta m. in. w protokole SSL, PGP.

Podsumowanie

W obecnych czasach szyfrowane i autoryzowana komunikacja jest koniecznością. Kradzieże i wyłudzanie informacji, podszywanie się są na porządku dziennym i prowadzą do ogromnych strat szczególnie w bankowości. Użycie metod kryptograficznych do zapewnienia poufnej i pewnej komunikacji w znaczący sposób zwiększa nasze bezpieczeństwo. Znajomość tych metod umożliwia nam dobór poziomu zabezpieczeń odpowiadających naszym potrzebom.

Literatura

[1] Whitfield Diffie, Martin E. Hellman „New Directions in Cryptography"
[2] R.L. Rivest, A. Shamir, i L. Adleman„A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"
[3] RSA Laboratories. Crypto FAQ. http://www.rsasecurity.com/
[4] National Institute of Standards and Technology (NIST), „Introduction to Public Key Technology and the Federal PKI Infrastructure".
[5] RFC 2459, „Internet X.509 Public Key Infrastructure Certificate and CRL Profile"
[6] „SSL 2.0 PROTOCOL SPECIFICATION" www.nescape.com
[7] Daniel Rychcik „SSL - Teoria i zasada działania", http://www.ais.pl/~muflon/doc/progzesp/ssl.html