PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Mikhail Selianinau
Akademia im. Jana Długosza
Al. Armii Krajowej 13/15, 42-200 Częstochowa,
e-mail: m.selianinov@ajd.czest.pl

SCHEMAT ZABEZPIECZONEGO OTWARTEGO KANAŁU ŁĄCZNOŚCI BEZ PRZEKAZYWANIA KLUCZY

Streszczenie. Obecny etap rozwoju nauki i społeczeństwa charakteryzuje się zwiększeniem różnorodności problemów powstających podczas przetwarzania i przekazywania informacji. Powszechnie wiadomo, że aktualnie zwiększa się znaczenie metod i środków ochrony informacji. Jednym z najważniejszych elementów bezpieczeństwa informacji jest kryptografia.
Najbardziej skutecznym sposobem ochrony informacji jest szyfrowanie. Główną zaletą stosowania technologii szyfrowania jest poufność danych. Zwykły tekst wejściowy przekształca się w tekst zaszyfrowany, który ukrywa znaczenie wiadomości i może być przesłany za pomocą kanału publicznego.
W artykule opisany został algorytm kryptograficzny, który umożliwia wysyłanie wiadomości przy użyciu otwartego kanału łączności bez uprzedniego przekazywania kluczy pomiędzy użytkownikami. Zaproponowany schemat wymiany informacji jest podobny do skrzynki zamkniętej za pomocą jednego lub dwóch zamków. W tym algorytmie procedura szyfrowania jest procesem kolejnego „zawieszania zamków" na tekst jawny przez nadawcę i odbiorcę informacji.

Słowa kluczowe: bezpieczeństwo informacji, kryptosystem, kryptogram, szyfrowanie, klucz publiczny, klucz prywatny, liczby pierwsze.

Wstęp

Obecny etap rozwoju nauki i społeczeństwa charakteryzuje się zwiększeniem różnorodności problemów powstających podczas przetwarzania i przekazywania informacji. Właściwy dobór metod i środków oraz ocena ich skuteczności i kosztów możliwe są tylko we współpracy z ekspertami w różnych dziedzinach wiedzy. Zapewnienie bezpieczeństwa informacji jest ciągłym procesem analizy, projektowania, eksploatacji i oceny systemów bezpieczeństwa informacji.

Powszechnie wiadomo, że aktualnie zwiększa się znaczenie metod i środków ochrony informacji. W ciągu życia jednego pokolenia nastąpiła jakościowa zmiana sytuacji w tym obszarze. Wcześniej problemami bezpieczeństwa informacji zajmowali się tylko eksperci służb specjalnych. A teraz krąg osób, w ten czy inny sposób związanych z bezpieczeństwem informacji, jest bardzo szeroki i trwa proces jego dalszego rozszerzenia.

Jednym z najważniejszych elementów bezpieczeństwa informacji jest kryptografia. Na początku XXI wieku techniki kryptograficzne są coraz częściej stosowane w życiu codziennym. Nowe praktyczne zastosowania kryptografii są źródłem jej rozwoju. Współczesna kryptografia wykorzystuje metody algebry abstrakcyjnej, teorii liczb oraz rachunku prawdopodobieństwa [1–9].

Szyfrowanie informacji

W ostatnim czasie komputer stał się jednym z głównych narzędzi pracy. Przechowuje różne dane: informacje o klientach, dane finansowe, prezentacje i inne ciągle wymagane dokumenty. Część z tych informacji ma zasadnicze znaczenie i charakter poufny. Najbardziej skutecznym sposobem ochrony informacji jest szyfrowanie [3, 6, 7]. Główne zalety stosowania technologii szyfrowania są następujące:

- poufność danych: zwykły tekst wejściowy przekształca się w tekst zaszyfrowany, który ukrywa znaczenie wiadomości i może być przesłany za pomocą kanału publicznego;
- integralność danych: kryptograficzną sumę kontrolną można obliczyć na dowolnym tekście zdefiniowanym przez użytkownika w celu ochrony integralności danych; w efekcie odbiorca może mieć pewność, że dane są w postaci, w której zostały utworzone;
- elektroniczne podpisy cyfrowe: podpis cyfrowy zapewnia odbiorcę, że wiadomość jest autentyczna i została wysłana przez nadawcę.

Tak więc zastosowanie systemu szyfrowania pozwala na przekazywanie ważnych dokumentów za pomocą sieci telekomunikacyjnych, zmniejszając jednocześnie czas przetwarzania informacji. Ponadto znacznie zmniejsza się ryzyko i potencjalne straty podczas próby kradzieży informacji.

Systemy kryptograficzne

Obecnie jednym z głównych celów bezpieczeństwa informacji jest wykrywanie i zapobieganie zagrożeniom. Oczywiście efektywność systemu ochrony informacji przed nieautoryzowanym dostępem jest możliwa tylko na podstawie wszechstronnego zastosowania zabezpieczenia informacji.

Spośród tych metod szczególne znaczenie ma kryptografia [1–9]. Wykorzystanie technik kryptograficznych w celu ochrony systemów informacyjnych jest teraz najbardziej istotne. Wynika to z faktu, że zwiększa się wykorzystanie sieci komputerowych, w tym Internetu, przenoszących duże ilości informacji o charakterze prywatnym, które nie muszą być dostępne dla osób nieupoważnionych.

Obecnie stosowane systemy kryptograficzne mają swoje wady i zalety. W celu zapewnienia bezpieczeństwa informacji należy użyć kombinacji różnych algorytmów kryptograficznych [2–4, 6, 7]. Wybór metody szyfrowania dla konkretnego systemu informacyjnego w dużym stopniu zależy od jej charakteru i powinien opierać się na wszechstronnej analizie wymagań dotyczących systemu ochrony informacji.

Aktualnie termin „kryptografia asymetryczna" oznacza dużą grupę mechanizmów, algorytmów, protokołów i pomysłów stosowanych w rozwoju systemów bezpieczeństwa informacji. Pojęcie funkcji jednokierunkowej było podstawą dla kryptografii asymetrycznej [7]. Faktycznie to, że obliczanie pewnej funkcji i jej odwrócenie wymaga różnej informacji wejściowej (pewnej asymetrii), określa nazwę tego kierunku w kryptografii.

Nadawca i odbiorca wiadomości współdziałające w sieci komputerowej powinni przestrzegać pewnych zasad w celu wykonania sekwencji czynności pomiędzy nimi. Reguły te są nazywane protokołem, który zapewnia nie tylko bezpieczeństwo informacji, ale również uwierzytelnianie korespondentów [6, 7]. Protokół kryptograficzny to taki sposób interakcji abonentów, w wyniku którego osiągają oni swoje cele, a ich przeciwnicy nie. Taka definicja nieformalna obejmuje prawie wszystkie ciekawe sposoby wykorzystania kryptografii asymetrycznej:

- protokoły publiczne dystrybucji kluczy;
- protokoły klucza publicznego;
- protokoły podpisu cyfrowego;
- protokoły uwierzytelniania dokumentów i osób;
- ochrona prywatności korespondencji elektronicznej;
- pieniądze cyfrowe.

Podstawą rozwoju kryptografii asymetrycznej bez wątpienia są potrzeby praktyki. W związku z dynamicznym rozwojem systemów informacyjnych oraz rozszerzeniem ich infrastruktury potrzeby praktyczne stwarzają nowe wyzwania dla algorytmów kryptograficznych. W chwili obecnej główne motywacje kryptografii asymetrycznej mogą być zgrupowane w następujący sposób:

- potrzeby rozwoju sieci telekomunikacyjnych różnego rodzaju, w tym o złożonej topologii;
- potrzeba zapewnienia bezpieczeństwa informacji w globalnej sieci Internet;

– potrzeby systemów bankowych, w tym przy użyciu kart inteligentnych.

Asymetryczne systemy kryptograficzne wykorzystują tak zwane funkcje nieodwracalne lub jednokierunkowe, które mają tę właściwość, że dla danej wartości x jest stosunkowo łatwo obliczyć wartość $f(x)$, a jeśli jest znana wartość funkcji $Y = f(x)$, to nie istnieje prosty sposób obliczania wartości x [5–8]. Nieodwracalność funkcji w kryptografii jest rozumiana nie jako nieodwracalność teoretyczna, lecz jako praktyczna niemożliwość obliczania odwrotności za pomocą wykorzystania nowoczesnych narzędzi obliczeniowych w ciągu przewidzianego okresu czasu.

Ogólnie rzecz biorąc, powszechnie stosowane asymetryczne algorytmy kryptograficzne są oparte na następujących problemach matematycznych, które wiążą się z nieodwracalnymi przekształceniami, są to:

1. rozkład dużych liczb na czynniki pierwsze;
2. obliczanie logarytmu dyskretnego;
3. obliczanie pierwiastków równań algebraicznych.

Problem dystrybucji kluczy

Bez względu na to, jak zaawansowane i niezawodne są systemy kryptograficzne, ich słabością w praktycznej realizacji jest problem dystrybucji kluczy. Ogólnie oznacza to, że wymiana kluczy także wymaga użycia systemu kryptograficznego. Aby rozwiązać ten problem, były zaproponowane systemy kryptografii asymetrycznej z kluczem publicznym [4, 6–8]. Ich istotą jest to, że każdy adresat generuje dwa klucze, które są połączone ze sobą przez pewne reguły. Jeden klucz jest kluczem publicznym, a drugi prywatnym. Klucz publiczny jest dostępny dla każdego, kto chce wysłać wiadomość do odbiorcy. Klucz prywatny jest tajemnicą.

Tekst wiadomości jest szyfrowany za pomocą klucza publicznego adresata i wysyłany do niego. Szyfrogramu w zasadzie nie można odszyfrować za pomocą tego samego klucza publicznego. Deszyfrowanie wiadomości jest możliwe tylko za pomocą klucza prywatnego, który jest znany tylko odbiorcy.

W celu zapewnienia ochrony systemów informacyjnych kryptografia asymetryczna ma dwa ważne i oczywiste wymagania:

– transformacja wiadomości oryginalnej powinna być nieodwracalna i wykluczyć jej odzyskanie na podstawie klucza publicznego;
– wyznaczanie klucza prywatnego na podstawie klucza publicznego również nie powinno być możliwe przy obecnym poziomie technologii; pożądane jest, aby znać dokładne dolną granicę złożoności (liczbę operacji) do ujawnienia szyfru.

W 1976 r. Diffie i Hellman zaproponowali użycie dyskretnego potęgowania do tworzenia systemów kryptograficznych. Był to pierwszy algorytm

klucza publicznego [4, 6, 7]. Jego bezpieczeństwo jest oparte na trudności obliczania dyskretnych logarytmów w odróżnieniu od lekkości dyskretnego potęgowania. Algorytm Diffiego-Hellmana eliminuje potrzebę bezpiecznego kanału łączności do przekazywania kluczy. Mimo że ten algorytm pozwala unikać problemu bezpiecznej wymiany kluczy, pozostaje jeszcze potrzeba uwierzytelniania. Przy użyciu tego algorytmu musi być zapewnione, że użytkownik A otrzymuje klucz publiczny od użytkownika B i odwrotnie. W tym przypadku pozostaje niebezpieczeństwo imitacji.

W ogóle problem zarządzania kluczami jest problemem znalezienia takiego protokołu dystrybucji kluczy, który zapewnia możliwość rezygnacji z centrum dystrybucji kluczy, wzajemne uwierzytelnianie uczestników sesji, potwierdzenie wiarygodności sesji za pomocą mechanizmu „zapytanie – odpowiedź", użycie oprogramowania lub sprzętu. Oprócz tego mamy następujące wymagania ogólne:

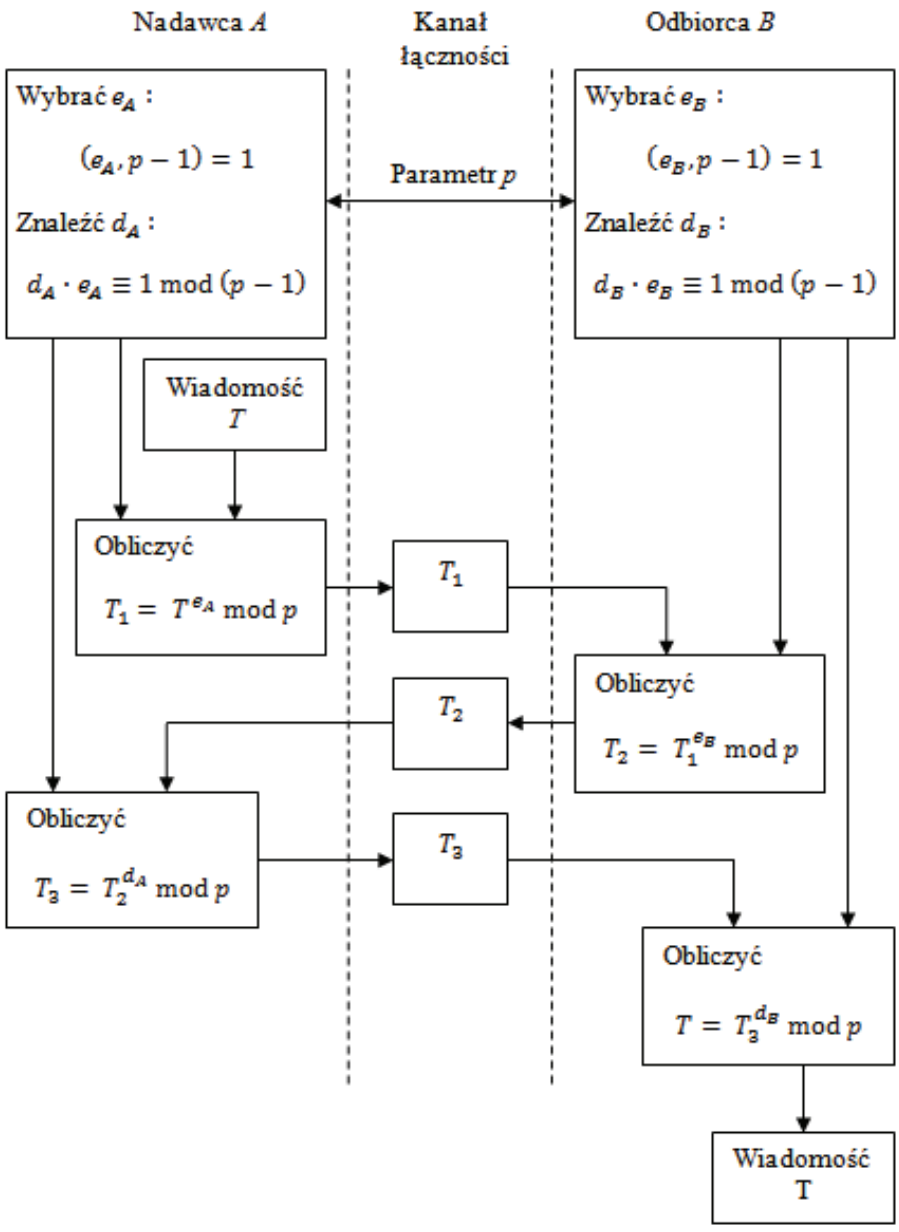
- nie powinno być prostych i łatwych do znalezienia związków między kluczami stosowanymi w procesie szyfrowania;
- każdy klucz ze zbioru możliwych kluczy powinien zapewnić niezawodną ochronę informacji;
- zmiana długości klucza nie powinna prowadzić do pogorszenia jakości algorytmu szyfrowania.

Algorytm wymiany informacji bez przekazywania kluczy

Poniżej opisany zostanie algorytm kryptograficzny, który umożliwia wysyłanie wiadomości przy użyciu otwartego kanału łączności bez uprzedniego przekazywania kluczy pomiędzy użytkownikami. Zaproponowany schemat wymiany informacji jest podobny do skrzynki zamkniętej za pomocą jednego lub dwóch zamków. W tym algorytmie procedura szyfrowania jest procesem kolejnego „zawieszania zamków" na tekst jawny przez nadawcę i odbiorcę informacji.

Użytkownicy A (nadawca) i B (odbiorca) jako „zamki" stosują cze $K_A = (e_A, d_A)$ i $K_B = (e_B, d_B)$, do generowania których wykorzystywana została duża liczba pierwsza p nazywana modułem algorytmu. Liczba ta jest parametrem otwartym.

Schemat algorytmu kryptograficznego został pokazany na rysunku.



Rys. 1. Algorytm kryptograficzny bez przekazywania kluczy

Rozważmy realizację algorytmu wymiany informacji bez przekazywania kluczy pomiędzy użytkownikami.

Proces generowania kluczy użytkowników *A* i *B* polega na przeprowadzeniu następujących kroków:

1. nadawca *A* i odbiorca *B* wybierają dużą liczbę pierwszą p;
2. nadawca *A* wybiera liczbę $e_A \in N$ mniejszą niż p i względnie pierwszą z $\varphi(p) = p - 1$; e_A jest pierwszą częścią klucza K_A, która służy tylko do szyfrowania wiadomości;
3. dalej nadawca *A* oblicza liczbę d_A, która jest odwrotnością liczby e_A modulo $\varphi(p)$, to znaczy: $d_A e_A \equiv 1 \bmod \varphi(p)$; d_A jest drugą częścią klucza K_A, która służy tylko do deszyfrowania;
4. analogicznie do kroku 2, odbiorca *B* wybiera liczbę $e_B \in N$ mniejszą niż p i względnie pierwszą z $\varphi(p) = p - 1$; e_B jest pierwszą częścią klucza K_B, która służy tylko do szyfrowania wiadomości;
5. następnie odbiorca *B* oblicza liczbę d_B, która jest odwrotnością liczby e_B modulo $\varphi(p)$, to znaczy: $d_B e_B \equiv 1 \bmod \varphi(p)$; d_B jest drugą częścią klucza K_B, która służy tylko do deszyfrowania.

Ogólnie, jeśli użytkownik ma wygenerowany klucz $K = (e, d)$, to może on zaszyfrować wiadomość T (tekst jawny) kluczem *e*, tworząc kryptogram

$$C = F(T, K) = T^e \bmod p$$

Do rozszyfrowania wiadomości użytkownik stosuje klucz *d*, obliczając

$$T = F^{-1}(C, K) = C^d \bmod p$$

Liczby $e,\ d \in N$ spełniają następujący warunek:

$$e \cdot d \equiv 1 \bmod \varphi(p)$$

Schemat wymiany informacji pomiędzy użytkownikami *A* i *B* bez przekazywania kluczy jest następujący:

1. w celu zaszyfrowania tekstu jawnego T za pomocą klucza e_A nadawca (użytkownik *A*) używa funkcji szyfrującej $F(T, K_A)$ i oblicza kryptogram $T_1 = T^{e_A} \bmod p$, który wysyła do odbiorcy (użytkownika *B*);
2. zaszyfrowany tekst T_1 otrzymany od nadawcy jako sekwencja liczb jest przekształcany przez użytkownika B w tekst $T_2 = {T_1}^{e_B} \bmod p$ za pomocą klucza e_B , przy użyciu funkcji $F(T_1, K_B)$, i odsyłany z powrotem do użytkownika *A*;
3. w celu pierwszego deszyfrowania kryptogramu T_2 za pomocą drugiej części d_A klucza K_A użytkownik *A* używa funkcji deszyfrującej $F^{-1}(T_2, K_A)$; w wyniku deszyfrowania otrzymuje on tekst
$$T_3 = {T_2}^{d_A} \bmod p = {T_1}^{d_A e_B} \bmod p = T^{e_A d_A e_B} \bmod p = T^{e_B} \bmod p$$
i wysyła do użytkownika *B*.

4. użytkownik B w celu ostatecznego deszyfrowania tekstu T_3 za pomocą drugiej części d_B klucza K_B używa funkcji deszyfrującej $F^{-1}(T_3, K_B)$; wynikiem deszyfrowania jest tekst jawny ${T_3}^{d_B} \bmod p = T^{d_B e_B} \bmod p = T$.

W celu zapewnienia wymaganego poziomu kryptograficznej ochrony informacji liczbę pierwszą p wykorzystywaną do generowania kluczy $K_A = (e_A, d_A)$ i $K_B = (e_B, d_B)$ należy wybrać tak, aby miała co najmniej 512 bitów (około 150 cyfr dziesiętnych).

Kryptoanalityk nie może uzyskać tekstu jawnego T na podstawie znanych tekstów T_1, T_2, T_3 z powodu złożoności rozwiązania problemu obliczania logarytmu dyskretnego.

Literatura

[1] Bauer F.L., Sekrety kryptografii, Helion, Gliwice, 2003.
[2] Buchman J.A., Wprowadzenie do kryptografii, PWN, Warszawa, 2006.
[3] Karbowski M., Podstawy kryptografii. Wydanie II, Helion, Gliwice, 2008.
[4] Koblitz N., Wykład z teorii liczb i kryptografii, WNT, Warszawa, 2006.
[5] Koblitz N., Algebraiczne aspekty kryptografii, WNT, Warszawa, 2009.
[6] Menezes A.J. i in., Kryptografia stosowana, WNT, Warszawa, 2005.
[7] Schneier B., Kryptografia dla praktyków, WNT, Warszawa, 2002.
[8] Stinson D.R., Kryptografia, WNT, Warszawa, 2005.
[9] Wobst R., Kryptologia. Budowa i łamanie zabezpieczeń, Wyd. RM, Warszawa, 2002.

Mikhail Selianinau
Akademia im. Jana Długosza w Częstochowie

THE SCHEME OF THE SECURE OPEN COMMUNICATION CHANNEL WITHOUT TRANSFER OF KEYS

Abstract

The current stage of development of science and society is characterized by an increasing variety of problems that generated during the processing and transmission of information. It is well known that at present increases the importance of methods and means of information protection. One of the main elements of information security is cryptography.

The most effective way to protect information is encryption. The main advantage of the use of encryption technology is confidentiality. Input plain text is converted into ciphertext that hides the meaning of a message and can be sent using the public channel. The article describes the cryptographic algorithm that allows sending messages using an open communication channel without transmission of keys between users. The proposed scheme of the information exchange is similar to a closed box with just one or two locks. In this algorithm the encryption procedure is a process of sequential "hanging locks" on the plain text by the sender and recipient.

Keywords: Information security, cryptosystem, cryptogram, encryption, public key, private key, prime numbers.