PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
SERIA: Edukacja Techniczna i Informatyczna 2012 z. VII

Mikhail Selianinau, Piotr Kamiński
Akademia im. Jana Długosza w Częstochowie

SCHEMAT ZABEZPIECZENIA WYMIANY INFORMACJI POMIĘDZY TRZEMA UŻYTKOWNIKAMI KRYPTOGRAFICZNYM SYSTEMEM RSA

Streszczenie. Wymagania bezpieczeństwa informacji w sieciach telekomunikacyjnych różnych zastosowań to główne motywacje kryptografii asymetrycznej. We współczesnych warunkach bezpieczeństwo systemów informacyjnych jest wspierane przez metodę kryptograficzną z kluczem publicznym posiadającym większą funkcjonalnością. Metody te są coraz częściej stosowane w systemach łączności i przetwarzania informacji i są traktowane jako obiecujący kierunek szyfrowania i uwierzytelniania danych. W uogólnionym modelu asymetrycznego kryptosystemu z kluczem publicznym źródłowy tekst jest szyfrowany za pomocą klucza publicznego adresata i jest przekazywany do niego. Deszyfrowanie tekstu jest możliwe przy użyciu tajnego klucza znanego tylko przez adresata. Główne wymagania dla systemów klucza publicznego dla niezawodnej wymiany danych są: nieodwracalność przekształcenia tekstu źródłowego i niemożność odzyskania tekstu za pomocą klucza publicznego, niemożliwe jest przy obecnym poziomie technologii określenie klucza tajnego na podstawie klucza publicznego. Wśród teoretycznych i praktycznych problemów związanych z najpopularniejszymi algorytmami kryptografii asymetrycznej większą uwagę poświęca się na system szyfrowania RSA z kluczem publicznym oraz na zbudowane na jego podstawie schematy podpisu elektronicznego i systemu uwierzytelniania. W tym artykule omówiono realizację schematu wymiany informacji zabezpieczonej kryptograficznym systemem RSA dla wielu użytkowników.

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

Powszechne stosowanie sieci telekomunikacyjnych wymaga zabezpieczenia przesyłanych wiadomości za pomocą określonego algorytmu szyfrowania. Kryptografia zajmuje się metodami przetwarzania informacji, które nie pozwoliłyby niepożądanym osobom je uzyskać z przechwyconych wiadomości.

Obecnie dostępne są różne metody szyfrowania, utworzono teoretyczną i praktyczną podstawę do ich stosowania. Zdecydowaną większość z tych metod można skutecznie stosować do ochrony informacji [1–7].

W celu zapewnienia wymaganego poziomu kryptograficznej ochrony informacji nowoczesne systemy kryptograficzne muszą spełniać następujące wspólne wymagania:

- zaszyfrowana wiadomość może być zdolna do odczytu tylko wtedy, gdy posiadamy klucz;
- liczba operacji potrzebnych do określenia używanego klucza szyfrującego nie powinna być mniejsza niż całkowita liczba możliwych kluczy;
- liczba operacji potrzebnych do odszyfrowania danych, próbując wszystkich możliwych kluczy, musi wykraczać poza możliwości współczesnych komputerów (w tym możliwości korzystania z komputerów w sieci);
- znajomość algorytmu szyfrowania nie powinna mieć wpływu na niezawodność ochrony danych;
- drobna zmiana w kluczu powinna doprowadzić do znaczącej zmiany w treści zaszyfrowanej wiadomości;
- długość szyfrogramu musi być równa długości tekstu źródłowego;
- nie powinno być prostych i łatwych do znalezienia zależności pomiędzy kluczami konsekwentnie używanych w procesie szyfrowania;
- dowolny klucz z wielu możliwych musi zapewniać bezpieczeństwo informacji;
- zmiana długości klucza nie powinna prowadzić do pogorszenia jakości algorytmu szyfrującego.

Cały zestaw kryptograficznych środków bezpieczeństwa informacji można podzielić na dwie duże grupy.

Podstawą pierwszej grupy są metody kryptografii zbudowane na bazie symetrycznego algorytmu szyfrowania. Cechą charakterystyczną tych systemów jest użycie tego samego klucza do operacji szyfrowania i deszyfrowania. Wykorzystanie systemów z kluczem symetrycznym jest następujące:

- bezpiecznie jest tworzony, dystrybuowany i przechowywany klucz symetryczny;
- nadawca używa symetrycznego algorytmu szyfrowania z tajnym kluczem do otrzymania zaszyfrowanego tekstu;
- nadawca wysyła zaszyfrowany tekst, ale symetryczny tajny klucz nigdy nie jest transmitowany przez niepewne kanały.

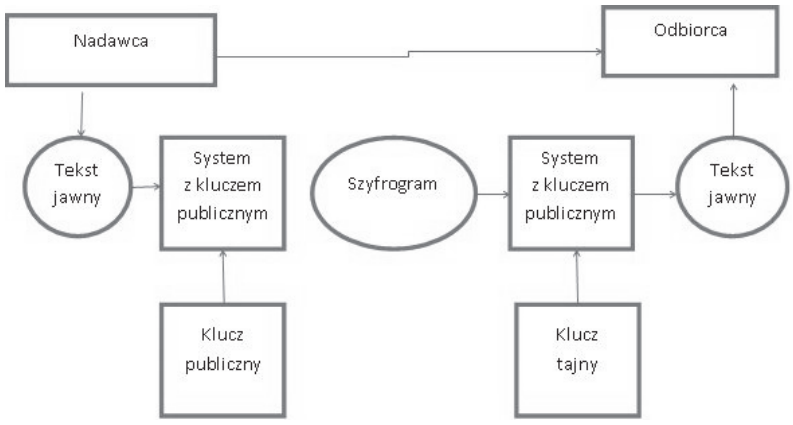
Aby otrzymać tekst jawny, odbiorca używa tego samego klucza do szyfrogramu. Główną wadą kryptografii symetrycznej jest to, że tajny klucz musi być znany zarówno nadawcy, jak i odbiorcy, co tworzy problem dystrybucji klucza.

Druga grupa obejmuje systemy kryptograficzne z wykorzystaniem asymetrycznych algorytmów szyfrujących. Wymagania bezpieczeństwa informacji

w sieciach telekomunikacyjnych różnych zastosowań to główne motywacje kryptografii asymetrycznej.

We współczesnych warunkach bezpieczeństwo systemów informacyjnych jest wspierane przez metodę kryptograficzną z kluczem publicznym posiadającym większą funkcjonalność. Metody te są coraz częściej stosowane w systemach łączności i przetwarzania informacji i są traktowane jako obiecujący kierunek szyfrowania i uwierzytelniania danych.

W uogólnionym modelu asymetrycznego kryptosystemu z kluczem publicznym źródłowy tekst jest szyfrowany za pomocą klucza publicznego adresata i jest przekazywany do niego. Deszyfrowanie tekstu jest możliwe przy użyciu klucza tajnego znanego tylko przez adresata.



Rys. 1. Uogólniony model asymetrycznego kryptosystemu

Różnorodność asymetrycznych systemów kryptograficznych jest generowana przez zbiór tak zwanych funkcji jednokierunkowych (nieodwracalnych). Funkcja jednokierunkowa jest to taka funkcja, której wartość możemy łatwo obliczyć, natomiast dla znanej wartości funkcji obliczenie argumentu funkcji jest zagadnieniem wyjątkowo bardzo trudnym. Inaczej mówiąc, dla funkcji jednokierunkowych znamy funkcje, natomiast nie potrafimy skonstruować funkcji do nich odwrotnych.

Nowoczesne asymetryczne systemy kryptograficzne oparte są na jednym z jednostronnych przekształceń matematycznych:

- faktoryzacja dużych liczb na czynniki pierwsze,
- obliczanie logarytmu dyskretnego,
- znalezienie pierwiastków równań algebraicznych

i mogą być stosowane jako samodzielny sposób bezpieczeństwa danych, dystrybucji kluczy i uwierzytelniania użytkowników.

Główne wymagania dla systemów klucza publicznego dla niezawodnej wymiany danych, to:
- nieodwracalność przekształcenia tekstu źródłowego i niemożność odzyskania tekstu za pomocą klucza publicznego;
- niemożliwe jest przy obecnym poziomie technologii określenie klucza tajnego na podstawie klucza publicznego.

Wśród teoretycznych i praktycznych problemów związanych z najpopularniejszymi algorytmami kryptografii asymetrycznej większą uwagę poświęca się na system szyfrowania RSA z kluczem publicznym oraz na zbudowane na jego podstawie schematu podpisu elektronicznego i systemu uwierzytelniania.

W systemie szyfrowania RSA klucz szyfrujący jest powszechnie znany i umożliwia zaszyfrowanie wiadomości przez nadawcę informacji w taki sposób, aby odbiorca informacji mógł ją odszyfrować, a jednocześnie nikt niepowołany (również znający ten klucz) nie mógł odczytać zaszyfrowanego tekstu.

W kryptosystemie RSA klucz (który nazywa się kluczem asymetrycznym) składa się z dwóch części:
1) części jawnej (publicznej) K_e, która służy tylko do szyfrowania i znana jest wszystkim użytkownikom kryptosystemu,
2) części tajnej (prywatnej) K_d, która służy tylko do deszyfrowania i znana tylko odbiorcy wiadomości.

Klucze do szyfrowania K_e i deszyfrowania K_d są różne.

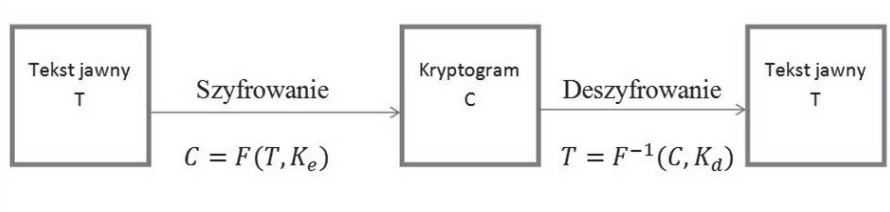
Szyfrowanie kluczem publicznym może być opisane wzorem

$$C = F(T, K_e)$$

a deszyfrowanie – wzorem

$$T = F^{-1}(C, K_d)$$

gdzie: C – kryptogram, T – tekst jawny, K_e – klucz publiczny, K_d – klucz prywatny.



Rys. 2. Szyfrowanie i deszyfrowanie

Generowanie klucza w systemie RSA polega na przeprowadzeniu następujących kroków:
1) wybieramy dwie duże liczby pierwsze p_1, p_2;
2) obliczamy ich iloczyn $n = p_1 \cdot p_2$ nazywany modułem algorytmu;

3) wybieramy liczbę $e \in N$ mniejszą niż n i względnie pierwszą z $\varphi(n) = (p_1 - 1) \cdot (p_2 - 1)$; e jest publicznym wykładnikiem;
4) obliczamy liczbę d, która jest odwrotnością liczby e modulo $\varphi(n)$, to znaczy: $ed \equiv 1 \bmod \varphi(n)$; d jest prywatnym wykładnikiem;
5) kluczem szyfru RSA jest trójka liczb (n, e, d), przy czym para (n, e) jest kluczem publicznym K_e, kluczem prywatnym K_d jest para (n, d).

Nadawca szyfruje wiadomość kluczem publicznym K_e, tworząc kryptogram

$$C = T^e \bmod n$$

Odbiorca chcąc deszyfrować wiadomość od nadawcy kluczem prywatnym K_d oblicza

$$T = C^d \bmod n$$

Rozważmy realizację schematu wymiany informacji zabezpieczonej kryptograficznym systemem RSA dla wielu użytkowników. Mianowicie, gdy moduł n jest iloczynem trzech dużych liczb pierwszych $p_1,\ p_2,\ p_3$, tj.:

$$n = p_1 \cdot p_2 \cdot p_3;$$

$$\varphi(n) = (p_1 - 1) \cdot (p_2 - 1) \cdot (p_3 - 1)$$

Wybieramy klucz publiczny $K_e = (n, e)$ oraz dwa klucze tajne $K_{d_1} = (n, d_1)$ i $K_{d_2} = (n, d_2)$. Liczby $e, d_1, d_2 \in N$ spełniają następujący warunek:

$$e \cdot d_1 \cdot d_2 \equiv 1 \bmod \varphi(n)$$

Więc klucz tajny K_d jest podzielony na dwie części K_{d_1} i K_{d_2}, co jest niezbędne w przypadkach, gdy użytkownicy nie ufają sobie nawzajem.

Schemat wymiany informacji polega na przeprowadzeniu następujących kroków:

1) w celu zaszyfrowania tekstu jawnego T za pomocą klucza publicznego K_e nadawca (pierwszy użytkownik) używa funkcji szyfrującej $F(T, K_e)$;
2) kryptogram $C_1 = T^e \bmod n$ otrzymany od nadawcy jako sekwencja liczb jest przekształcany przez drugiego użytkownika w kryptogram $C_2 = {C_1}^{d_1} \bmod n$ za pomocą klucza tajnego K_{d_1} używając funkcji $F^{-1}(C_1, K_{d_1})$;
3) w celu deszyfrowania kryptogramu C_2 za pomocą drugiej części klucza tajnego K_{d_2} trzeci użytkownik (adresat) używa funkcji deszyfrującej

$F^{-1}(C_2, K_{d_2})$; w wyniku deszyfrowania odbiorca otrzymuje tekst jawny $T = {C_2}^{d_2} \bmod n$.

W celu zapewnienia wymaganego poziomu kryptograficznej ochrony informacji liczby pierwsze p_1, p_2, p_3 wykorzystywane do konstrukcji klucza należy wybrać tak, aby były tzw. mocnymi liczbami pierwszymi, czyli liczbami pierwszymi, których iloczyn jest wyjątkowo trudny do faktoryzacji za pomocą znanych aktualnie algorytmów [1, 2]. Dlatego liczby te muszą spełniać następujące podstawowe warunki:

- liczby p_1, p_2, p_3 są wybrane losowo,
- liczba $n = p_1 \cdot p_2 \cdot p_3$ ma co najmniej 512 bitów (około 150 cyfr dziesiętnych).

Literatura

[1] Menezes A.J., P.C. van Oorschot, Vanstone S.A., Handbook of Applied Cryptography, CRCPress, NewYork 1997.

[2] Stinson D.R., Kryptografia w teorii i w praktyce, WNT, Warszawa 2005.

[3] Kutyłowski M., Strothmann W.B., Kryptografia: Teoria i praktyka zabezpieczania systemów komputerowych, Wyd. READ ME, Warszawa 1999.

[4] Schneier B.,. Kryptografia dla praktyków, WNT, Warszawa 2002.

[5] Buchmann J.A., Wprowadzenie do kryptografii, PWN, Warszawa 2006.

[6] Bauer F.L., Sekrety kryptografii, Helion, Gliwice 2002.

[7] Wobst R., Kryptologia. Budowa i łamanie zabezpieczeń, RM, Warszawa 2002.

[8] Koblitz N., Wykład z teorii liczb i kryptografii, WNT, Warszawa 2006.

Mikhail Selianinau, Piotr Kamiński
Akademia im. Jana Długosza w Częstochowie

THE SCHEME FOR THE SECURITY EXCHANGE OF INFORMATION BETWEEN THE THREE USERS USING RSA CRYPTOGRAPHIC SYSTEM

Abstract

Information security requirements of telecommunication networks of the various applications are the main motivations of asymmetric cryptography. In modern conditions security of information systems is supported by the methods of public-key cryptography

which have a higher functionality. These methods are increasingly used in communication systems and information processing, and are regarded as a promising direction of data encryption and authentification. In a generalized model of asymmetric public-key cryptosystem the source text is encrypted using the recipient's public key and is passed to him. Text decryption is possible using a secret key known only to recipient. The main requirements for public-key systems for reliable data exchange are: the irreversible transformation of the source text and the inability to recover the text using public key; it is impossible at the present level of technology to determine the secrete key from the public key.Among the theoretical and practical problems associated with the most popular cryptography algorithms more attention is paid to the RSA encryption with public key and built on the its basis schemes of electronic signature and authentification.This article discussed the implementation of the secure information exchange scheme for multiple users on the base of RSA cryptographic system.

Keywords: information security, RSA cryptosystem, cryptogram, encryption, public key, private key, prime numbers