Elementy kryptografii

Kryptografia klucza publicznego

Wprowadzenie

Przedmiot poszukiwań

Znalezienie takiego przekształcenia, w którym szyfrowanie dokonywane jest innym kluczem niż deszyfracja

⇩

Klucz asymetryczny

Szyfrowanie $C = f_e(M)$ **Deszyfracja** $M = f_d(C)$

M **- wiadomość** C **- kryptogram**

f_e **- Klucz szyfrowania** f_d **- Klucz deszyfracji**

Znajomość jednego z kluczy nie może pomóc w odgadnięciu drugiego klucza

Wprowadzenie

Arytmetyka modularna

Dziedzina - liczby całkowite

Operacja ‘modulo’ - reszta z dzielenia

$$y = a \circ b \oplus n, \qquad \circ \Rightarrow \begin{cases} + \\ - \\ * \end{cases}$$

Przykłady $40 \oplus 7 = (5*7+5) \oplus 7 = 5$ $5^3 \oplus 7 = (5*5*5) \oplus 7 = 125 \oplus 7 = (17*7+6) \oplus 7 = 6$

Wybrane właściwości arytmetyki modularnej

- Istnienie odwrotności $ab \oplus n = 1 \Rightarrow a = \ldots$ $a*3 \oplus 5 = 1 \Rightarrow a = 2$
- Możliwość upraszczania obliczeń (redukcja)

$ab \oplus n = (a \oplus n)(b \oplus n) \oplus n$ $(17*19) \oplus 7 = (17 \oplus 7)(19 \oplus 7) \oplus 7 = (3*5) \oplus 7 = 1$

Kryptografia klucza publicznego - RSA

Szyfrowanie

$$C = M^e \oplus n$$

M - wiadomość

C - kryptogram

- $n = pq$ p, q - wielocyfrowe liczby pierwsze
- e - pewna wielocyfrowa liczba dobierana na podstawie p i q

e,n - parametry przekształcenia szyfrującego - klucz kodowania

Deszyfracja

$$M = C^d \oplus n$$

- d - pewna wielocyfrowa liczba dobierana na podstawie p,q

d,n - parametry przekształcenia szyfrującego - klucz dekodowania

Kryptosystem RSA (1977)

Aby złożenie przekształcenia kodującego i dekodującego było tożsamością (pozwalało na odtworzenie zaszyfrowanego tekstu), to znaczy:

$$M = C^d \oplus n = (M^e \oplus n)^d \oplus n$$

liczby e (klucz kodowana) i d (klucz dekodowania) trzeba dobrać, by:

$$ed \oplus (p-1)(q-1) = 1$$

Procedura tworzenia kluczy

1. **Wybieramy liczby pierwsze** $p = 5,\ q = 7$ ➡ $n = 35$
2. **Wybieramy e** $e < \alpha = (p-1)(q-1), \gcd(\alpha, e) = 1$ ➡ $e = 11$
3. **Określamy d** $ed \oplus (p-1)(q-1) = 1 \Rightarrow 11d \oplus 24 = 1$ ➡ $d = 11$

*p , q - **tajne** (ale nie trzeba przechowywać)*

Kryptosystem RSA

Procedura szyfrowania wiadomości

$e = 11$ $n = 35$

A. **Zamieniamy szyfrowany tekst na ciąg liczb (mniejszych od n)**

Szyfrowany tekst - ‘dąb’ ➡ **06 02 03**

B. **Szyfrujemy (własność redukcji działań arytmetyki modularnej)**

$$6^{11} \oplus 35 = (6^2 6^2 6^2 6^2 6^2 6) \oplus 35 = 6$$

$$2^{11} \oplus 35 = (2^6 2^5) \oplus 35 = ((64 \oplus 35) \cdot 32) \oplus 35 = (29 * 32) \oplus 35 = 928 \oplus 35 = 18$$

$$3^{11} \oplus 35 = (3^4 3^4 3^3) \oplus 35 = ((81 \oplus 35)(81 \oplus 35) \cdot 27) \oplus 35 = (11 \cdot 11 \cdot 27) \oplus 35 =$$
$$(16 \cdot 27) \oplus 35 = 432 \oplus 35 = 12$$

C. **Tworzymy kryptogram** ➡ **06 18 12**

Kryptosystem RSA

Procedura deszyfracji wiadomości $d = 11$ $n = 35$

a **Wiadomość do deszyfracji** ➡ **06 18 12**

B **Deszyfrujemy (własność redukcji działań arytmetyki modularnej)**

$$6^{11} \oplus 35 = (6^2 6^2 6^2 6^2 6^2 6) \oplus 35 = 6$$

$$18^{11} \oplus 35 = (18^2 18^2 18^2 18^2 18^2 18) \oplus 35 = (9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 18) \oplus 35 = 2$$

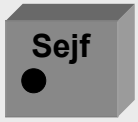
$$12^{11} \oplus 35 = (12^2 12^2 12^2 12^2 12^2 12) \oplus 35 = (4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 12) \oplus 35 = 3$$

C **Tworzymy tekst:** **06 18 12** ➡ **dąb**

Korzystanie z RSA

Uczestnicy komunikacji D G

Generacja kluczy

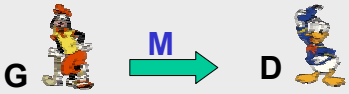


Klucz dekodowania - klucz prywatny (tajny)

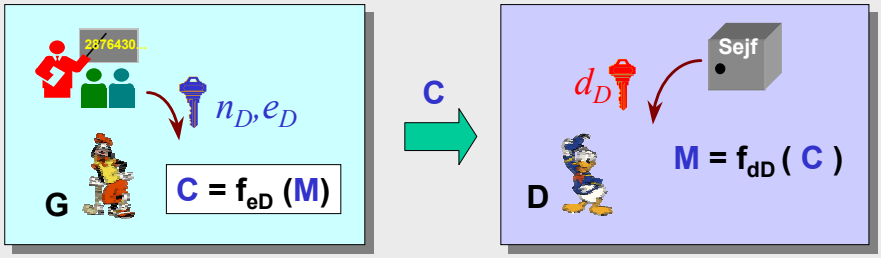
Klucz kodowania - klucz publiczny jawny

Korzystanie z RSA

Cel: G chce przesłać wiadomość do D



Procedura szyfrowania



$M = f_{dD}(f_{eD}(M))$ $\quad$ $M = f_{eD}(f_{dD}(M))$

Kryptosystem RSA

Bezpieczeństwo szyfru

Klucz publiczny e i klucz prywatny d to para liczb o własności - jeżeli zaszyfruję tekst jedną z nich, to odtworzę go tylko i wyłącznie używając drugiej

Czy mając dane n i e można znaleźć d ?

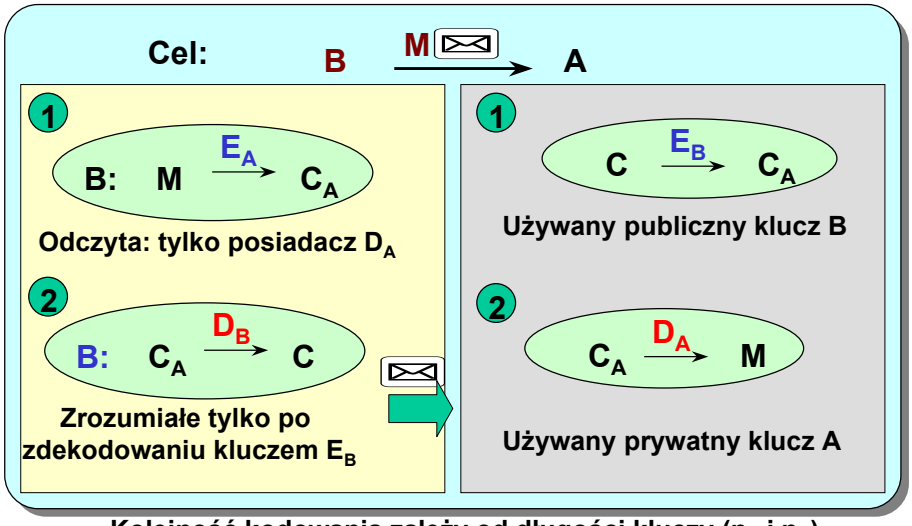
Jedyna znana metoda postępowania - rozkład liczby n na czynniki pierwsze (faktoryzacja)

Problem NP-zupełny

1998: udana faktoryzacja liczby 160 cyfrowej

Zalecenie: $n \geq 1024$ *bity* *(308 cyfr)*

Jednoczesna ochrona poufności i autentyczności przy użyciu metody RSA



Kolejność kodowania zależy od długości kluczy (n_A i n_B)

Kryptosystem RSA

➡ Złożoność obliczeniowa algorytmu szyfrowania

P-1.4GHz: 240kbit / s (S), 2Mbit/s (H)
(1024b) (970b)

Szyfrowanie komunikacji przy użyciu metod klucza publicznego jest o wiele wolniejsze niż w przypadku metod klucza symetrycznego

⬇

Podstawowa wada systemów szyfrowania z kluczem publicznym

Powszechne zastosowanie metody szyfrowania

⬇

Wymiana klucza dla szyfrowania szyfrem symetrycznym (klucza sesyjnego)

Współczesne szyfry z kluczem asymetrycznym - podsumowanie

Technika szyfrowania

- Własności arytmetyki modularnej (i tzw. ciała Galois)
- Szyfry blokowe

Bezpieczeństwo szyfrów

- Atak metodą prób i błędów (wrażliwość na tekst spreparowany)
- Złożoność - wykładnicza funkcja długości klucza
  (1024 bity w RSA to odpowiednik ok. 80b szyfru symetrycznego, 128 bitów klucza szyfru symetrycznego to ok. 3000 bitów RSA)

Stosowane metody

- RSA
- Szyfry 'plecakowe' (Merklego-Hellmana ...)

Ustalanie klucza sesyjnego

Diffie-Hellman

Wymiana kluczy przez publiczną sieć

Problem - jak ustalić klucz tajny komunikacji uzgadniając go za pośrednictwem sieci publicznej

- Dane są: liczba pierwsza p i liczba całkowita g
- D wybiera a, takie że $0<a<p-1$
- G wybiera b, takie że $0<b<p-1$
- D oblicza $J= g^a \bmod p$ i wysyła J do G
- G oblicza $K = g^b \bmod p$ i wysyła K do D
- D oblicza $X = K^a \bmod p$
- G oblicza $Y = J^b \bmod p$

$X = g^{ab} = Y$ ⇒ klucz

Klucz jest wypadkową liczb generowanych przez obie strony

Ustalanie klucza sesyjnego

Diffie-Hellman

$X = g^{ab} = Y$

Publicznie znane p, g, J i K nie pozwalają na znalezienie X - jest to problem z klasy NP

Metoda wymiany kluczy Diffie-Hellmana jest wrażliwa na atak typu 'Man-in-the-middle"

Do ustalenia klucza sesyjnego stosuje się w praktyce albo technikę RSA albo modyfikacje metody Diffie-Hellmana

Kryptosystem RSA

Przykładowy klucz 1024 bitowy

mQCNAzGvwGAAAAEEAMQXI06gfdoZzy2Ngdqua6Zf6q4Bfdotc8qGHk9RncuEHSB
f 2DrqYrkVmn6cANJp/HdBkJH39LcKybOGbxiahmjVnngPp+PzvX8+Wi7kQ5NP267S0
JIituePxuklEQ5pqywHw8yxtOGIqLjkJtb/pRvZyiC0Cyw1bjnbPFHw2SetAAUR tCZSb2J
pbiBXaGl0dGxlIDxmaXJzdHByQG96ZW1haWwuY29tLmF1PokAlQMFEDGv wGE52z
xR8NknrQEBbV0D/1gJSldscj2bFJ0uD9LOY+LSTj71yxdONZ3cycPZ+3zpShCNcsqNAG
vHXDtqcGQrNrxHmYqnKBaJ/+46n/FSkDnt/bvEAb105m+6T5oTK8h+ MaaVuvdcphwKf
IPQbIoI6LcmtwSd0cyBBndp+O+02x0xhcd2Qx7Gni7J+fz8mm0y =Yjno