# 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**

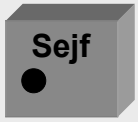




# Korzystanie z RSA

**Uczestnicy komunikacji** **D** **G**

**Generacja kluczy**




$d_D$

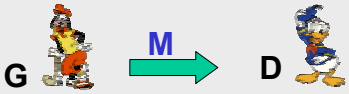
$n_D, e_D$


**Klucz dekodowania - klucz prywatny (tajny)**

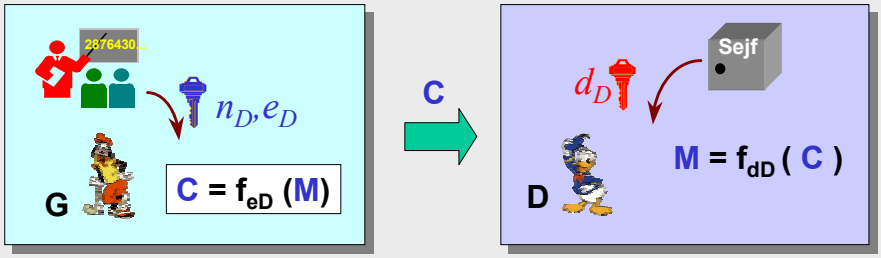
**Klucz kodowania - klucz publiczny jawny**

# 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)**

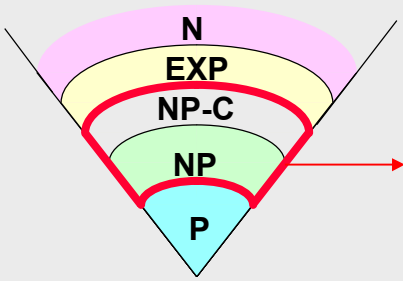
**Problem NP-zupełny**

*1998: udana faktoryzacja liczby 160 cyfrowej*

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

# Problemy NP -zupełne

## Klasy złożoności problemów




**Przedmiot zainteresowań kryptografii**

**Poszukiwanie rozwiązania:**
**czas wykładniczy** $t = 2^n - 1$

**Weryfikacja rozwiązania:**
**czas wielomianowy** $t = 9n + 7$

**'Klasyczne' problemy NP-zupełne**

- **Problem podróżującego akwizytora**
- **Kolorowanie map, układanki ...**





# Liczby pierwsze

- **Rozkład liczby na czynniki pierwsze to problem NP**
- **Szacunkowo N/log(N) liczb pierwszych mniejszych od danej N**

**168 mniejszych od 1000, około 51 milionów mniejszych od miliarda, jedna na 300 dla liczb 200-cyfrowych, jedna na 600 dla liczb 300-cyfrowych**

## Generacja liczb pierwszych

**Nieznany algorytm pewnej generacji inny od sprawdzania podzielności**

↓

**Czyli - dane N - podziel przez wszystkie od 2 do N/2**

↓

**Wykładniczo rosnący czas obliczeń**

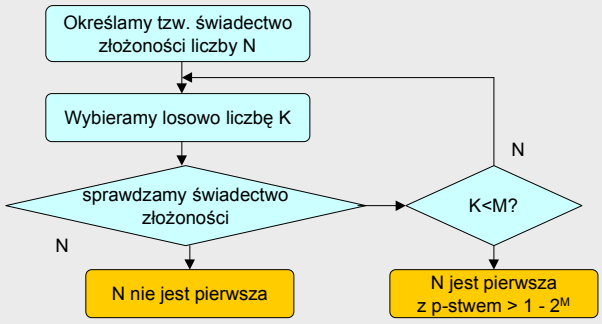
**Modyfikacje - omijanie wielokrotnych podzielników itp. - niewiele zmieniają**

# Liczby pierwsze

**Istnieje algorytm sprawdzania, czy dana liczba jest liczbą pierwszą oparty na hipotezie Riemana (a więc nie udowodniony)**

**W praktyce stosowane są probabilistyczne algorytmy sprawdzania**

**Sprawdzenie czy wylosowana liczba jest pierwsza to problem klasy P**

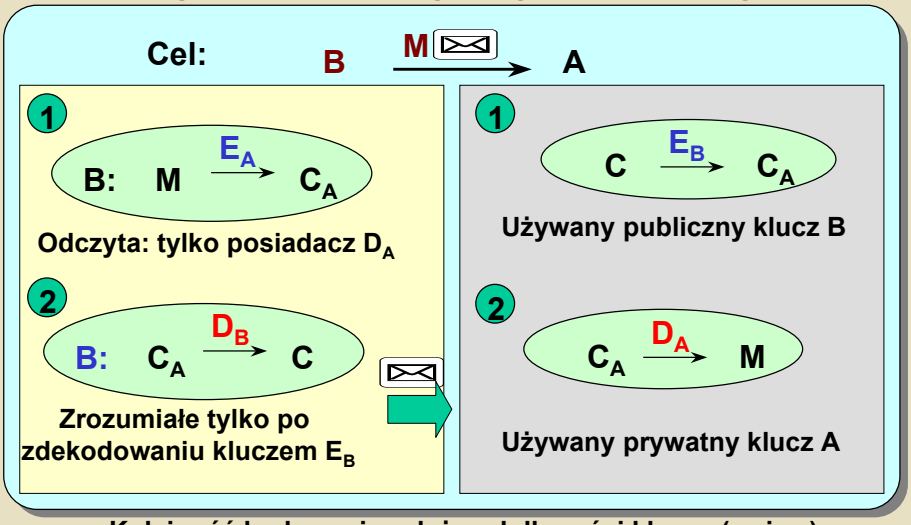



**1996 - najdłuższa znana liczba pierwsza: > 420 tysięcy cyfr**





# 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



Bezpieczeństwo systemów informatycznych

# 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

Krzysztof Ślot © 2002

# Kryptosystem RSA

## Obliczanie odwrotności

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

**Dane** $e,z$ **Cel - obliczyć** $d$

**Rozważmy wyrażenia (każdą liczbę można wyrazić w taki sposób)**

$z = c_0 * e + r_1$ $e = c_1 * r_1 + r_2$ $r_1 = c_2 * r_2 + r_3$ ... $r_{n-1} = c_n * r_n + 1$

**W końcu zawsze dojdziemy do reszty 1**

$$1 = r_{n-1} - c_n r_n = r_{n-1} - c_n (r_{n-2} - c_{n-1} r_{n-1}) =$$
$$= r_{n-1}(1 + c_{n-1}) - c_n r_{n-2} = (r_{n-3} - c_{n-2} r_{n-2})(1 + c_{n-1}) - c_n r_{n-2} =$$
$$= \alpha \cdot z - \beta \cdot e \Rightarrow d = \beta$$

**bo** $ed \oplus z = 1 \Leftrightarrow \alpha \cdot z - ed = 1$





# Kryptosystem RSA

## Obliczanie odwrotności - przykład

**Dane** $p=53,\ q=61$ ⇒ $n=3233,\ z=52*60=3120$

**Załóżmy, że** $e=71$ ⇒ $d = ?$

$z = c_0 * e + r_1$ ⇒ $3120 = c_0 * 71 + r_1$ ⇒ $c_0 = 43, r_1 = 67$

$e = c_1 * r_1 + r_2$ ⇒ $71 = c_1 * 67 + r_2$ ⇒ $c_1 = 1, r_2 = 4$

$r_1 = c_2 * r_2 + r_3$ ⇒ $67 = c_1 * 4 + r_3$ ⇒ $c_2 = 16, r_3 = 3$

$r_2 = c_3 * r_3 + r_4$ ⇒ $4 = c_1 * 3 + r_3$ ⇒ $c_3 = 1, r_4 = 1$

# Kryptosystem RSA

## Obliczanie odwrotności - przykład

$$1 = r_2 - c_3 r_3 = r_2 - c_3(r_1 - c_2 r_2) = r_2(1+c_2) - c_3 r_1 = (e - c_1 r_1)(1+c_2) - c_3 r_1 =$$

$$= -r_1(c_1 + c_1 c_2 + c_3) + e(1+c_2) = -(z - c_0 e)(c_1 + c_1 c_2 + c_3) + e(1+c_2) =$$

$$= -z(c_1 + c_1 c_2 + c_3) + e(1 + c_2 + c_0 c_1 + c_0 c_1 c_2 + c_0 c_3)$$

$$d = 1 + c_2 + c_0 c_1 + c_0 c_1 c_2 + c_0 c_3 = 17 + 43 \cdot 18 = 791$$



Bezpieczeństwo systemów informatycznych

# 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

Krzysztof Ślot © 2002