RSA

A | B

$\boxed{p, q \text{ - l. prvočísla}}$ ← dvě

$n = pq$

$b \in \{1, \dots, n-1\}$ $\quad NSD(b, \varphi(n)) = 1$, $\quad \varphi(n) = (p-1)(q-1)$

$a = b^{-1} \mod \varphi(n)$ ← rozš. Eukl.

$K_B^{pub} = (n, b)$ $\quad K_B^{priv} = a$

$m \in \{0, 1, \dots, n-1\}$

$e_{K_B^{pub}}(m) = m^b \mod n$

$d_{K_B^{priv}}\left(e_{K_B^{pub}}(m)\right) = \left(e_{K_B^{pub}}(m)\right)^a \mod n = m$

p, q dvě

p, q ~ 1024 b → 2048 b

p, q ~ 2048 b → 4096 b

---

p 2048 b. ~ 2^{2048}

E n

$n = pq$

Generowanie liczb pierwszych

1) Losujemy liczbę $\underline{n}$ (dużą).

2) $\underbrace{\text{Sprawdzamy}}_{\text{JAK???}}$, $\underbrace{\text{czy } n \text{ jest liczbą pierwszą.}}$

To nie jest problem rozkładu na czynniki!!!

$\underbrace{\text{Test Millera-Rabina}}$ (70'), $\underbrace{\text{Test AKS}}$ (2002)

Małe twierdzenie Fermata:

n - l. pierwsza, $n \nmid a$

n nie jest dzielnikiem a

$$a^{n-1} \equiv 1 \pmod n$$

$$\boxed{\begin{array}{l} n \text{ - l. pierwsza} \\ a^{n} \equiv a \pmod n \end{array}}$$

$n = 341 = 11 \cdot 31$

$2^{340} \equiv 1 \pmod{341}$ 341 przeszło test Fermata

$3^{340} \equiv 56 \pmod{341}$ $\Rightarrow$ 341 jest l. złożoną

$56 \not\equiv 1$

(ALE nie znamy rozkładu 341 na czynniki pierwsze)

Liczby Carmichaela

$561 = 3 \cdot 11 \cdot 17$

$a^{561} \equiv a \pmod{561}$ dla dowolnego a

$a^{560} \equiv 1 \pmod{561}$ dla dowolnego $a \neq 3, 11, 17$

Test Millera - Rabina

$x^2 \equiv 1 \pmod{n}$ $\quad x \in \{0, 1, \dots, n-1\}$

l. pierwsza

$x^2 - 1 \equiv 0 \pmod{n}$

$(x-1)(x+1) \equiv 0 \pmod{n}$

$(x-1)(x+1) = k \cdot n$

$n \mid (x-1)(x+1)$

Jeżeli n jest liczbą pierwszą, to

$n \mid x-1$ lub $n \mid x+1$.

$x - 1 = i \cdot n \qquad x+1 = j \cdot n$

$x = 1 + in \qquad x = -1 + j \cdot n$

$x \equiv 1 \pmod{n} \qquad x \equiv -1 \pmod{n}$

$\boxed{x = 1 \quad \text{lub} \quad x = n-1}$

$n = 561 = 3 \cdot 11 \cdot 17$

$2^{560} \equiv 1 \pmod{561}$

$(\underbrace{2^{280}}_{x})^2 \equiv 1 \pmod{561}$

$\boxed{x^2 \equiv 1 \pmod{561}}$

$2^{280} \equiv 1 \pmod{561}$

$(\underbrace{2^{140}}_{x})^2 \equiv 1 \pmod{561}$

560
280
140
70
35

$2^{140} \equiv 67 \pmod{561} \Longrightarrow$ 561 NIE jest liczbą pierwszą!

$n \in \mathbb{N}$, n - nieparzyste

$\boxed{n - 1 = 2^d m}$

m – nieparzyste

$561 - 1 = 2^{\overset{d}{4}} \cdot \underset{m}{35}$

Losujemy $a \in \{2, 3, \dots, n-1\}$

	a^m	a^{2m}	a^{4m}	$\dots$	$a^{2^k m}$	$a^{2^{k+1} m}$	$\dots$	$a^{2^{d-1} m}$	$a^{\overset{n-1}{2^d m}}$	
1)		...	...	...	...	...	...	...	$\neq 1$	✗
2)	1	1	1	1	1	1	1	1	1	✓

3)	157	15	13	...	$\boxed{-1}$	1	1	1	1
					przed pierwszą	1			
4)	8	13	4	...	$\neq -1$	1	1	1	1

$\boxed{67}$

$x^2 \equiv 1 \pmod{561}$

$\boxed{a=2}$

35 70 140 280 560

... 67 1 1

$\mathbb{P}$(n jest złożone i n przechodzi test Millera dla losowego a) $\leq \frac{1}{4}$

Jeżeli a losujemy (niezależnie) k razy:

$\mathbb{P}$(n jest złożone i n przechodzi k testów Millera dla k losowych a) $\leq \frac{1}{4^k}$

$\boxed{k = 10, \boxed{20}}$

$\leq \frac{1}{4^{20}} = \frac{1}{2^{80}}$

Problem logarytmu dyskretnego,
protokół Diffiego-Hellmana,
kryptosystem ElGamala.

$\log_a b = c \iff \boxed{a^c = b}$ w $\mathbb{Z}_p$

PLD (DLP)

IN: p, g, a, istnieje x, dla którego $\boxed{g^x \equiv a \pmod p}$ $x = ?$

OUT: x $x = \log_g a \pmod p$

Protokół D-H

$A \xleftrightarrow{K\,?} B$

$A \xleftrightarrow{p,\ g} B$

p – l. pierwsza, g – generator w $\mathbb{Z}_p$

dla dowolnego $a \in \mathbb{Z}_p$ istnieje x, dla którego $g^x \equiv a \pmod p$

$g^x \equiv a \pmod p$

tajne wyłącznie Alicji

$a \in \mathbb{Z}_p$ $b \in \mathbb{Z}_p$

$A = g^a \bmod p$ $B = g^b \bmod p$

$A \longrightarrow$

$\longleftarrow B$

$B^a = (g^b)^a \bmod p = \boxed{g^{ab} \bmod p}$ ← K → $A^b = (g^a)^b \bmod p = \boxed{g^{ab} \bmod p}$

$E: \ p, g, A, B$

$B^{a} = K$

$A^{b} = K$

$a = ?$

$b = ?$

$\underline{g}^{a} = \underline{A} \pmod{\underline{p}}$

PLD

$g^{b} = B \pmod{p}$

$b = ?$

PLD

Kryptosystem ElGamala (ElGamal)

$\mathcal{P} = \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ $\quad$ p - duża liczba pierwsza

$\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^* = \{(x,y) : x, y \in \mathbb{Z}_p^*\}$

$\mathcal{K} = \{(p, g, x, \alpha) : g^x \equiv \alpha \pmod{p}\}$

generator w $\mathbb{Z}_p^* \iff \{g^x : x \in \mathbb{N}\} = \mathbb{Z}_p^*$

(p, g, x, α)

Klucz publiczny: $(p, g, \alpha) = K$

Klucz prywatny: $x = (p, g, x)$