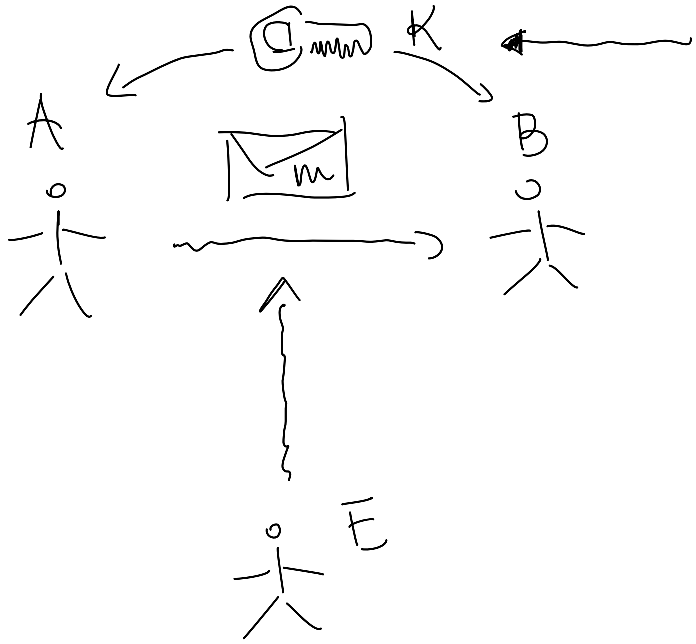
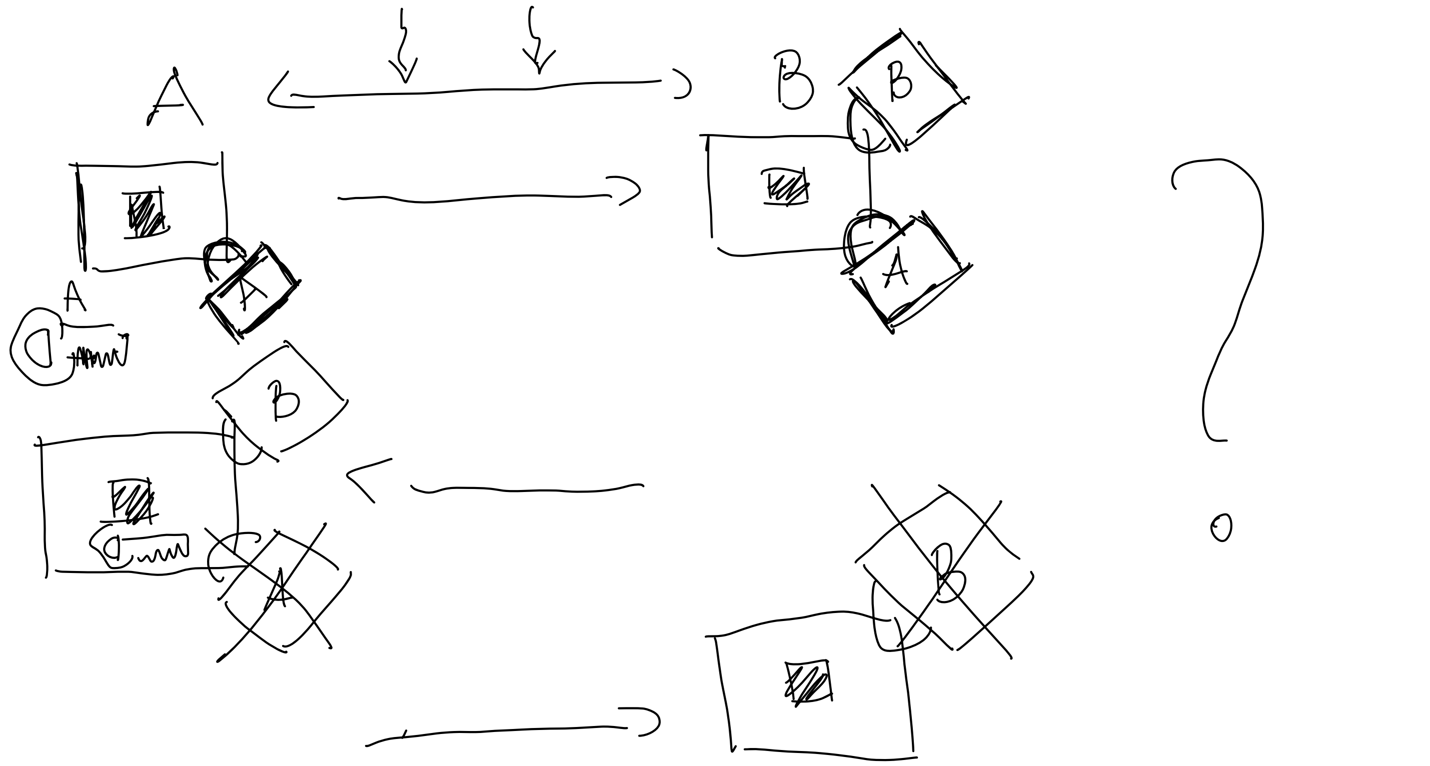


Problem dystrybucji klucze



W. Diffie 1970' M. Hellman

E

$A \longleftrightarrow B$

1. $7, \ 11$

2. $a = 4$ | $b = 8$

$A = 7^a = 7^4 \equiv 3 \pmod{11}$ | $B = 7^b = 7^8 \equiv 9 \pmod{11}$

3. $\xrightarrow{A} 3$

$9 \xleftarrow{B}$

4. $B^a = 9^4 \equiv \boxed{5} = K$ | $A^b = 3^8 \equiv \boxed{5} = K$

$B^a = (7^b)^a = 7^{ba} \pmod{11}$ | $A^b = (7^a)^b = 7^{ab} \pmod{11}$

$m, \ n$

$a, \ b$

$A = m^a \pmod{n}$

$B = m^b \pmod{n}$

$B^a = \ldots$

$A^b = \ldots$

E: $7, \ 11$

$A = 3, \ B = 9$ $\quad a? \quad b?$

$a: \ 7^a \equiv 3 \pmod{11}$?

$b: \ 7^b \equiv 9 \pmod{11}$?

$$mx \equiv a \pmod{n}$$ ✓

$$m^x \equiv c \pmod{n}$$ m, c, n - znane

$$x = ?$$

$$m^x = c \quad | \log_m$$

$$\boxed{x = \log_m c}$$

$$\boxed{\begin{array}{l} m^x \equiv c \pmod{n} \\ x \in \mathbb{Z}\,! \end{array}}$$ Problem logarytmu dyskretnego

GCHQ

1971/1972 Clifford Cocks

2000'

1973 - 1976 RSA (Rivest - Shamir - Adleman)

A B

B: 1. Wybiera dwie (duże) liczby pierwsze.

p, q

2. $n = p \cdot q$

3. Wybiera $e \geq 3$, dla którego

$NWD(e, (p-1)(q-1)) = 1$

4. Ogłasza światu klucz publiczny:

(n, e).

5. Wylicza (RAE)

$d = e^{-1} \pmod{(p-1)(q-1)}$

Klucz prywatny Boba:

d

A: $m \in \mathbb{Z}$ $(m \in \{0, 1, \dots, n-1\})$

$$A \longrightarrow B$$

$$\hat{m} = m^e \bmod n \longrightarrow B$$

$$(\hat{m})^d = ?$$

$$(\hat{m})^d = (m^e)^d = m^{ed} = m^{1+(p-1)(q-1)k} =$$

$d = e^{-1} \pmod{(p-1)(q-1)}$

$de \equiv 1 \pmod{(p-1)(q-1)}$

$\pmod n$ 1 $\equiv$ TE

$$= m \cdot \underbrace{\boxed{m^{(p-1)(q-1)}}^{k}}_{?} = m \cdot \left(m^{(p-1)(q-1)}\right)^k \overset{TE}{=} m \cdot 1 \equiv$$

$$\equiv m \pmod n$$

TE: $\boxed{NWD(m,n) = 1}$? $\Rightarrow m^{\varphi(n)} \equiv 1 \pmod n$

$n = pq$ $\quad \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$m^{(p-1)(q-1)} \equiv 1 \pmod{\overset{n}{\overset{\shortparallel}{pq}}}$

MTF

Ćw. Co zrobić, gdy $NWD(m,n) > 1$?

E: $\underset{pq}{\overset{\shortparallel}{n}}, e$ $\quad \hat{m} = m^e \pmod n$ $\quad m = ?$

$d = e^{-1} \pmod{(p-1)(q-1)}$?

$$(p-1)(q-1) = \underbrace{pq}_{n}\,\underbrace{-p-q}_{?}+1$$

Ewa nie umie (szybko) rozłożyć n na czynniki pierwsze!