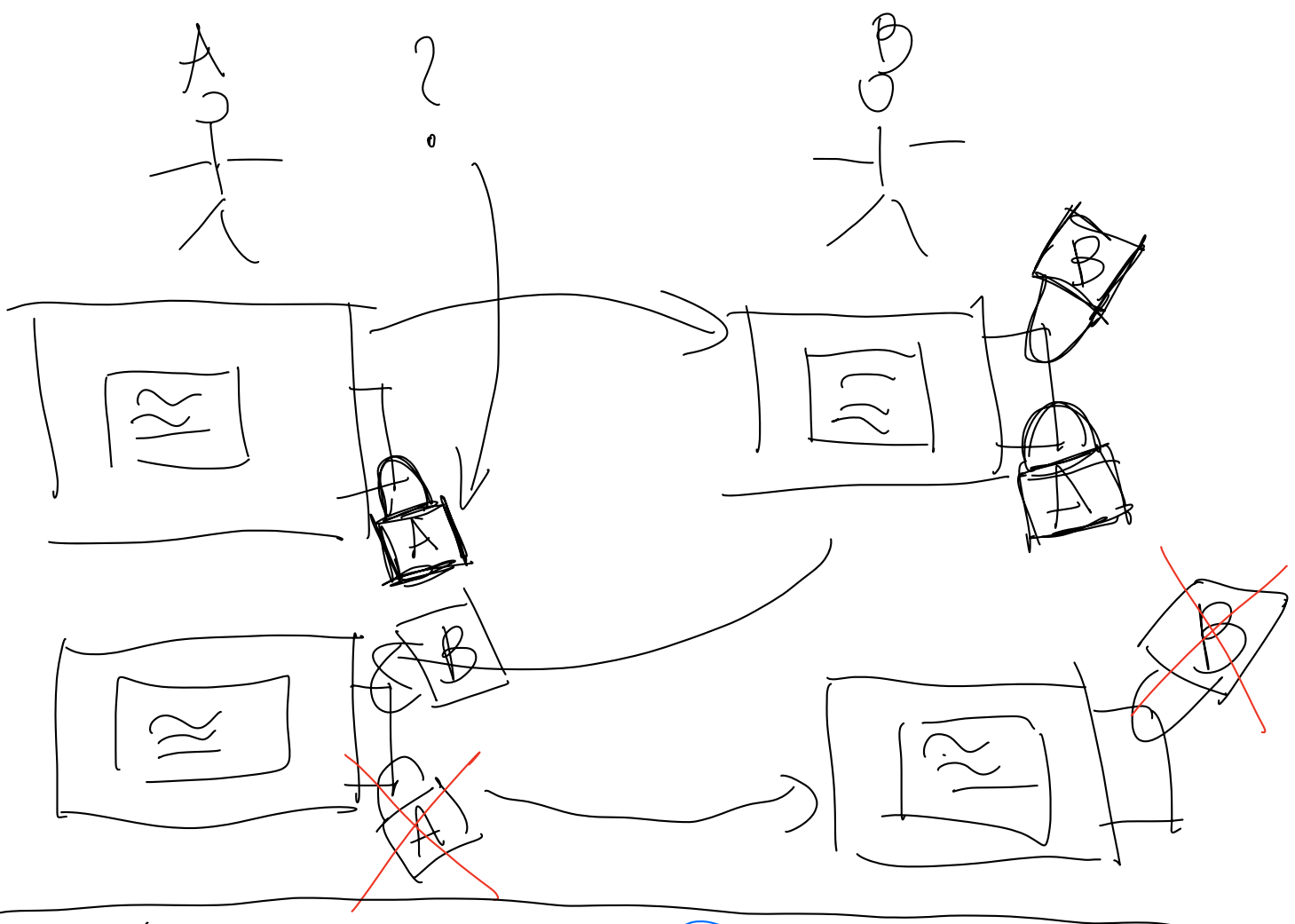


1970'

E

$y^x \bmod 11$

A

B

7 , 11

$7^2 = 49 \equiv_{11} 5$

$7^4 = 5^2 \equiv_{11} 3$

$a = 4$ ← ?

$7^x \equiv_{11} 4$

? → $b = 8$

$A = y^a = 7^4 \bmod 11 = 3$

$B = 7^8 \equiv_{11} 9$

$B = 9$

$B^a = 9^4 \equiv_{11} (-2)^4 \equiv_{11} 5$

$A^b = 3^8 \equiv_{11} 5$

$(a^b)^c = (a^c)^b$

k	$3^k \bmod 11$
1	3
2	9
3	5
4	1
5	3
6	9
7	5
8	1

$A = 3$

Problem logarytmu dyskretnego.

$7^x \equiv 4 \pmod{11}$

$x := \log_7 4$ ~~$\pmod{11}$~~

$7^x = 4 \mid \log_7()$

$x = \log_7 4$

$$1037597722881^x \equiv 13811899 \pmod{98766655544411}$$

Kryptografia z kluczem publicznym

- ⇝ Od „zwasze”

  umieć zaszyfrować = umieć odszyfrować

- ⇝ Whitfield Diffie i Martin Hellman (1975 r.)

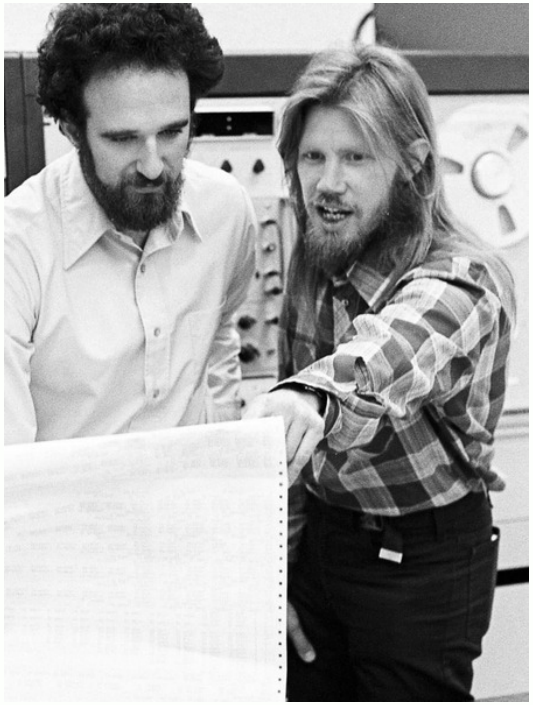
  klucz trzeba podzielić!

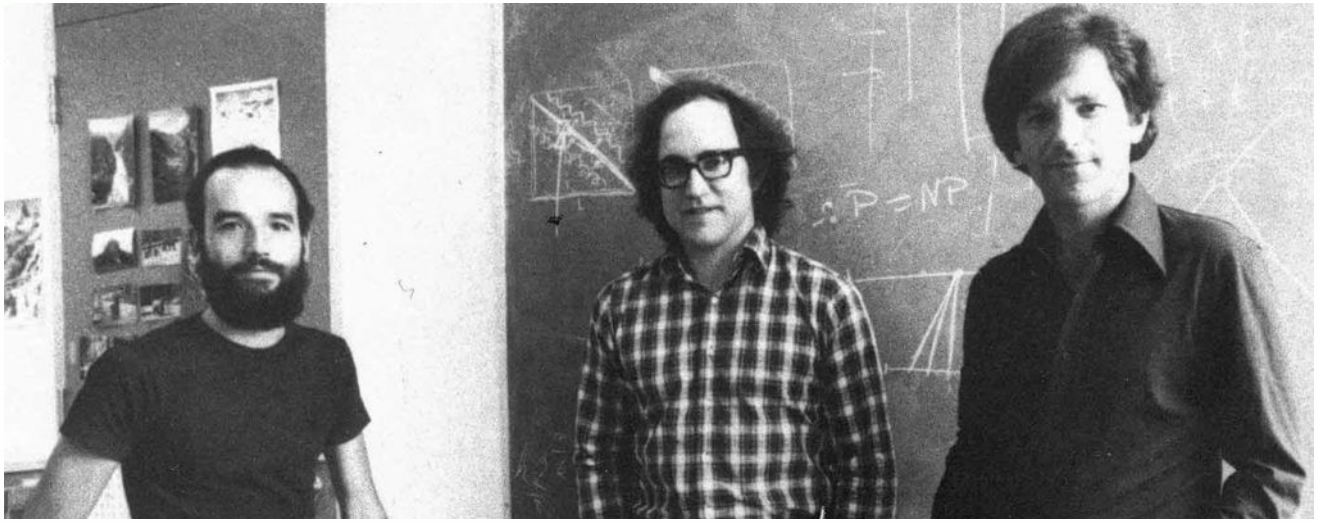
- ⇝ Ronald Rivest, Adi Shamir i Leonard Adleman (1977 r.)

  kryptosystem RSA

1975 GCHQ

2000 Clifford Cocks





System RSA

- ⇝ Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.

$p, q \sim 4096$ bitów $\quad p \neq q$

$q \ldots$

System RSA

- ⇝ Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.
- ⇝ Wybierz $e < n$ względnie pierwsze z $(p-1)(q-1)$.

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

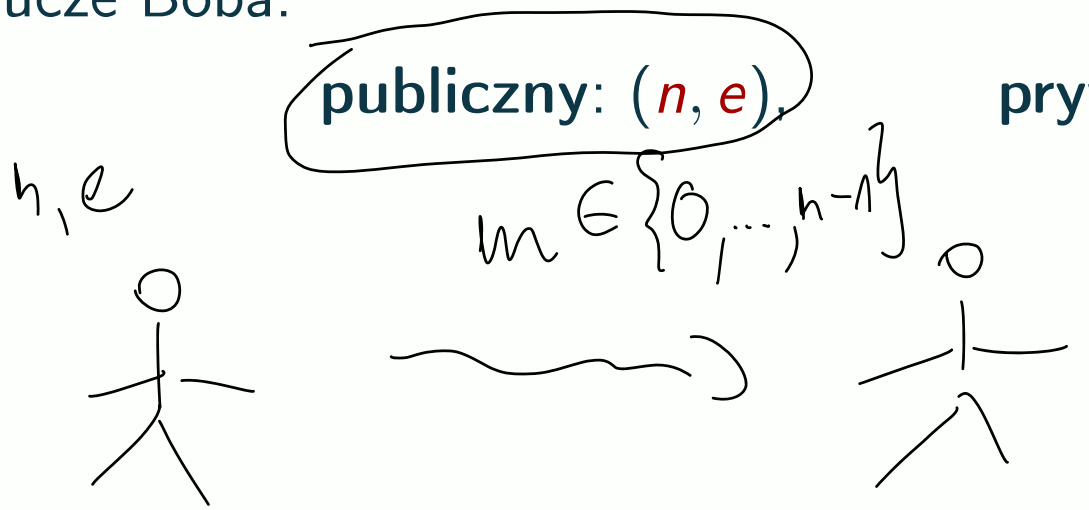
System RSA

- ⇝ Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.
- ⇝ Wybierz $e < n$ względnie pierwsze z $(p-1)(q-1)$.
- ⇝ Znajdź $d = e^{-1}$ względem $(p-1)(q-1)$. $de \equiv 1 \pmod{(p-1)(q-1)}$

System RSA

- ⇝ Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.
- ⇝ Wybierz $e < n$ względnie pierwsze z $(p-1)(q-1)$.
- ⇝ Znajdź $d = e^{-1}$ względem $(p-1)(q-1)$.
- ⇝ Klucze Boba:

publiczny: (n, e). **prywatny**: d.



System RSA

- Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.
- Wybierz $e < n$ względnie pierwsze z $(p-1)(q-1)$.
- Znajdź $d = e^{-1}$ względem $(p-1)(q-1)$.
- Klucze Boba:

  publiczny: (n, e), **prywatny**: d.
- Alicja szyfruje wiadomość m:

$$m \mapsto \hat{m} = \underbrace{m^e \bmod n.}_{\text{szyfrowanie}}$$

System RSA

- Wybierz dwie duże liczby pierwsze p i q. Oblicz $n = pq$.
- Wybierz $e < n$ względnie pierwsze z $(p-1)(q-1)$.
- Znajdź $d = e^{-1}$ względem $(p-1)(q-1)$.
- Klucze Boba:

  publiczny: (n, e), **prywatny**: d.
- Alicja szyfruje wiadomość m:

$$m \quad \mapsto \quad \hat{m} \quad = \quad m^e \bmod n.$$

- Bob odczytuje wiadomość:

$$\hat{m} \quad \mapsto \quad (\hat{m})^d \bmod n \quad = \quad m^{de} \bmod n \quad = \quad m.$$

desyfrowanie

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

$de = 1 + (p-1)(q-1)k$

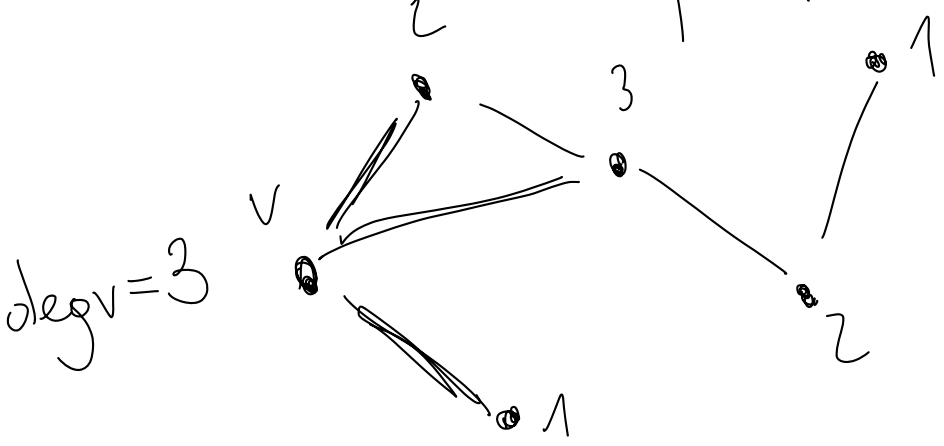
$m^{1+(p-1)(q-1)k} = m \cdot \left(m^{(p-1)(q-1)}\right)^k$

$a^{\varphi(n)} \equiv 1 \pmod{n}$

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

$TE \Rightarrow 1$

Teoria Grafów



$\deg v = 3$

$\sum \deg v = 12$

$|E| = 6$

$G = (V, E)$

zbiór wierzchołków (dowolny zbiór skończony)

zbiór krawędzi

$V = \{v_1, v_2, v_3, \dots, v_n\}$

$\{v_i, v_j\}, \quad v_i \neq v_j$

krawędź $v_i v_j$

$E \subset \{\{v, w\} : v, w \in V, \ v \neq w\}$

$v \in V$

stopień wierzchołka $v \overset{\text{ozn.}}{=} \deg v =$ liczba krawędzi, których jednym z końców jest v.

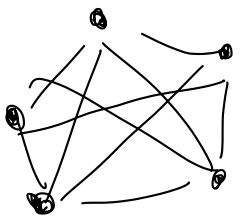
Tw.

$$\sum_{v \in V} \deg v = 2|E|$$

- Graf pusty

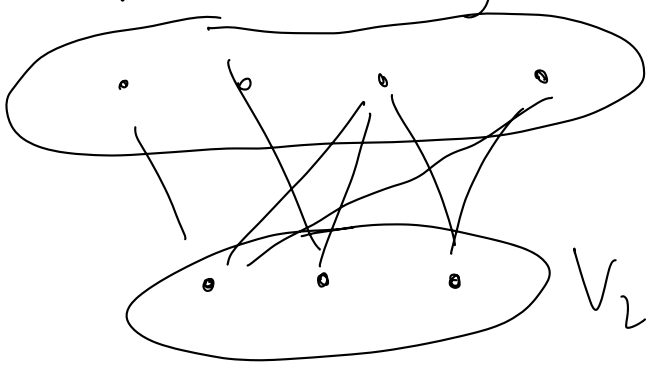
$V = \{v_1, \dots, v_n\}$, $E = \emptyset$

- Graf pełny



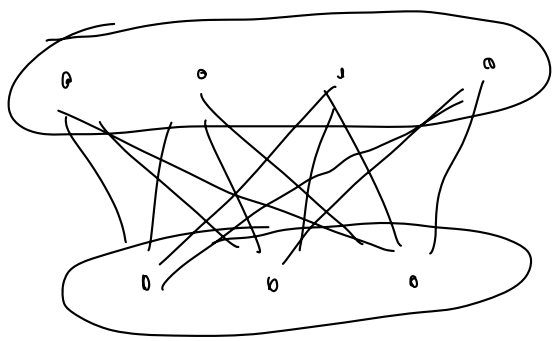
K_n

- Graf dwudzielny



- Pełny graf dwudzielny

$K_{n,m}$



$K_{3,4}$