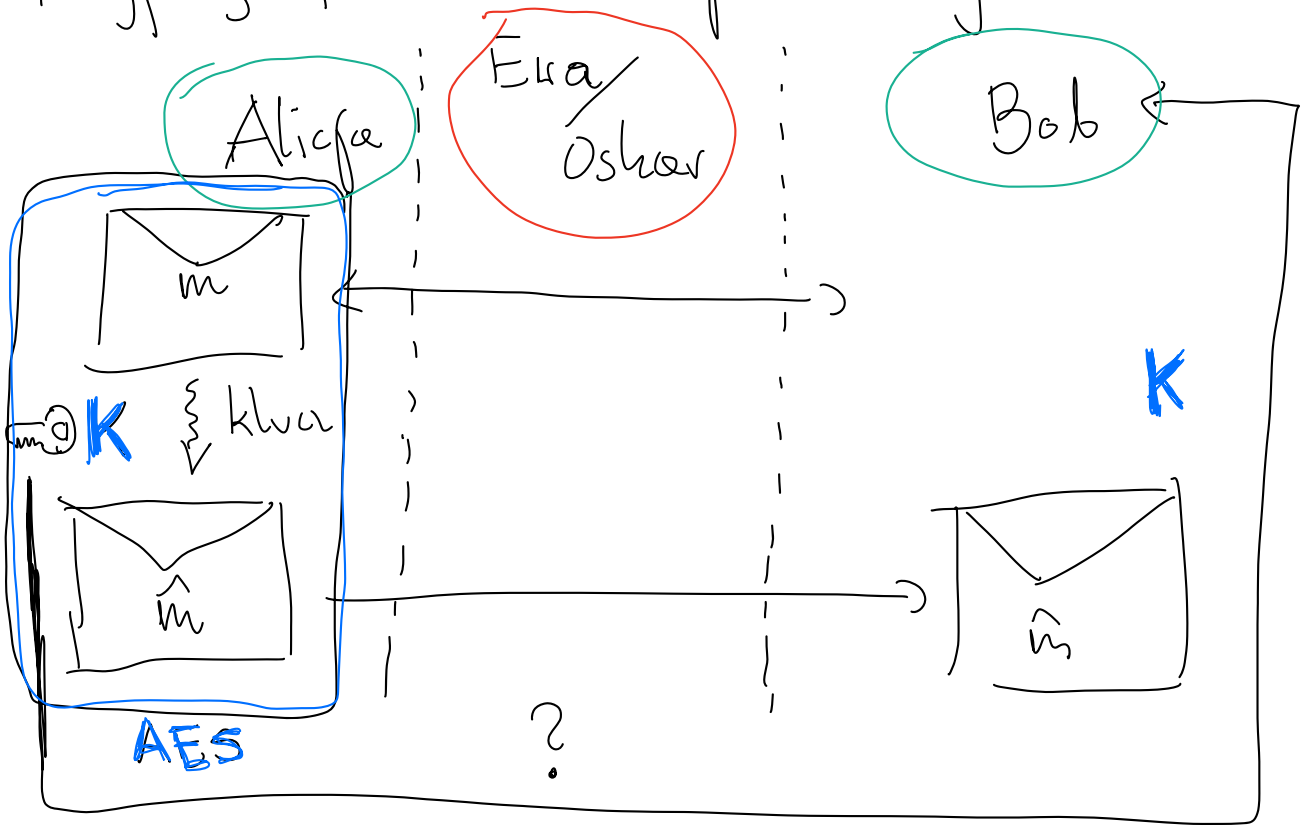
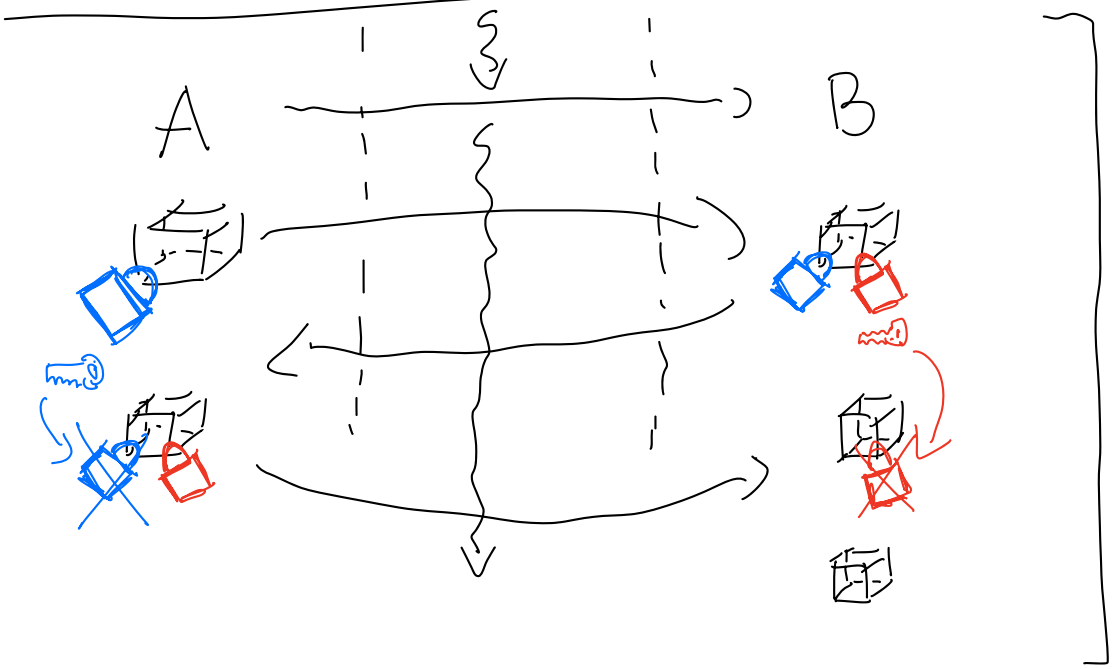
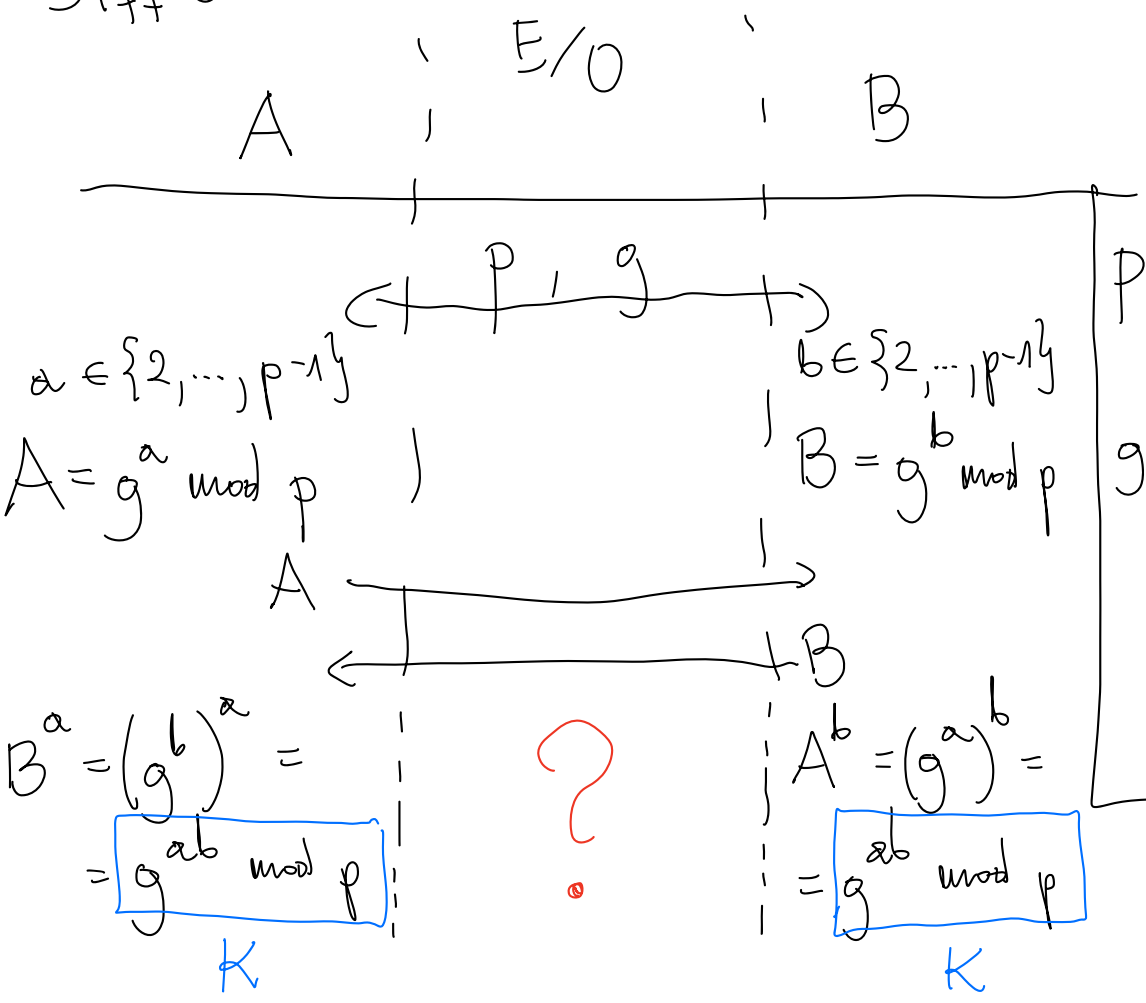
Kryptografia klucz publicznego



1970' Protokół Diffiego-Hellmana 1973
System RSA 1976



Diffie-Hellman



p - duża liczba pierwsza

$g \in \{2, 3, \dots, p-2\}$

$g^{p-1} \equiv 1 \pmod p$

$g^m \neq 1 \pmod p$ dla $m < p-1$

E/O: p, g, A, B

$K = A^{(b)} = B^{(a)}$

a? b?

$A = g^a \bmod p$

$\begin{cases} g^x = A \pmod p \\ x = ? \end{cases}$

$g^x = A \quad |\log_g()$

$x = \log_g A$

$p = 61 \qquad g = 2$

$g^x = 41 \pmod{61} \qquad x = ?$

Problem logarytmu dyskretnego

p	$O(\sqrt{p})$	$O(\log p)$

RSA Rivest, Shamir, Adleman

A

m

B

p, q – duże duże liczby pierwsze

$n = pq$

$e \in \{3, 4, \dots, n\}$

$NWD(e, \varphi(n)) = 1$

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

$d = e^{-1} \bmod \varphi(n)$ [RAE]

$d \cdot e = 1 \pmod{\varphi(n)}$

(n, e) – klucz publiczny

d – klucz prywatny

A

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

$m^e \bmod n$

$\hat{m}$ → $\hat{m}$

$(\hat{m})^d = (m^e)^d = m^{ed}$

E/O

d?

$d = e^{-1} \mod \varphi(n)$

RAE

?

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

? ?

$n = pq$

Problem faktoryzacji

$\sqrt{n}$ $\sqrt[3]{n}$ $\sqrt[4]{n}$

$p, q \sim 2000b$

$n \sim 4000b$

$\sqrt{n} \sim 2000b$

$\sqrt[4]{n} \sim 500b$

$de \equiv 1 \pmod{\varphi(n)}$

$de = 1 + k\varphi(n)$

$m^{ed} = m^{1+k\varphi(n)} =$

$= m \cdot m^{k\varphi(n)} = m \cdot (m^{\varphi(n)})^k$

tw. Eulera

$= m \cdot 1^k \equiv m \pmod{n}$

tw. Eulera (o ile $NWD(m,n) = 1$)

$n = pq$

Jeśli $p|m$ lub $q|m$

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

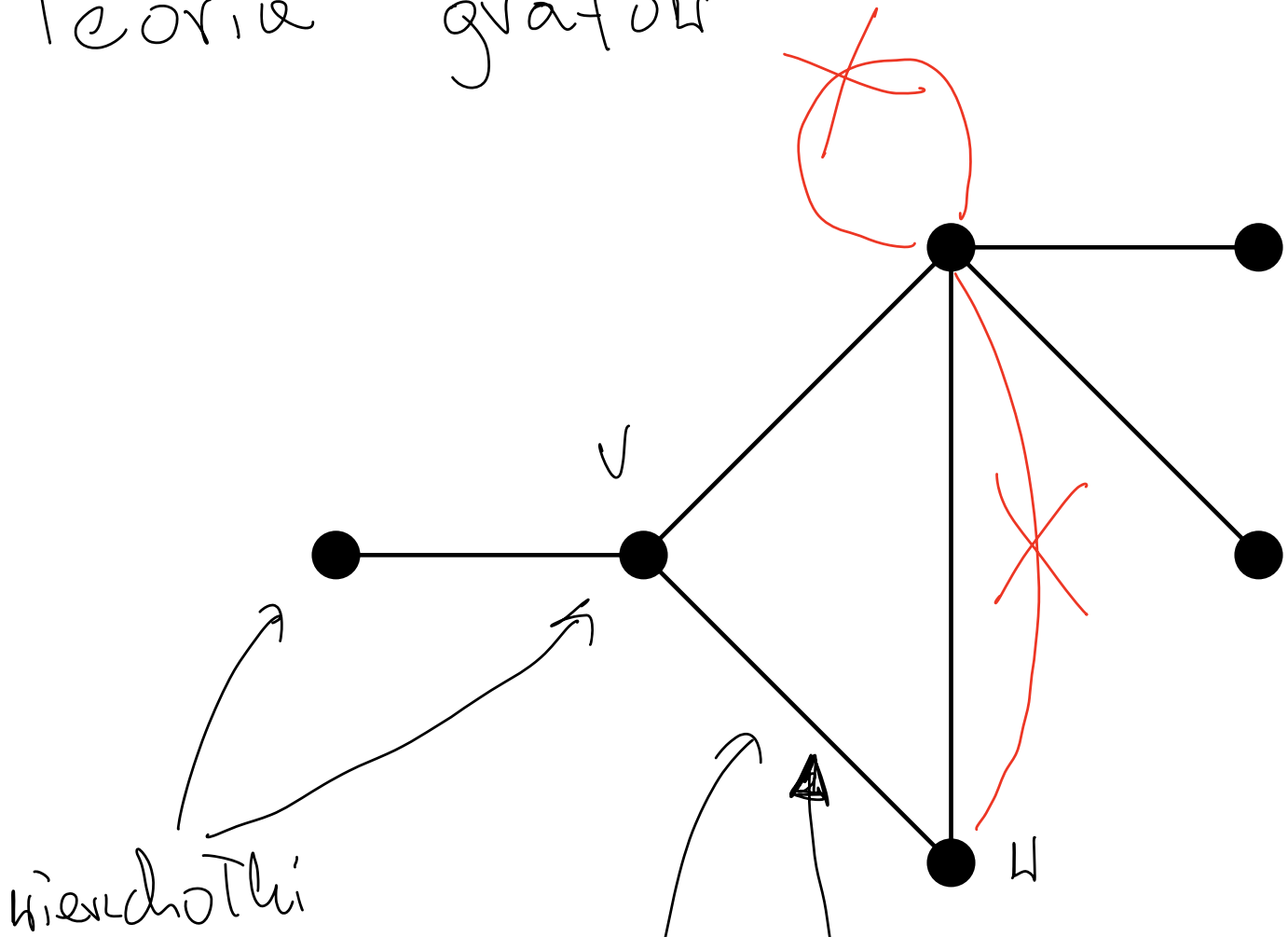
nie mocy MTF + CTR

$m^{\varphi(n)} = m^{(p-1)(q-1)}$

ch.

$m^e \longrightarrow (m^e)^d = m$

Teoria grafów

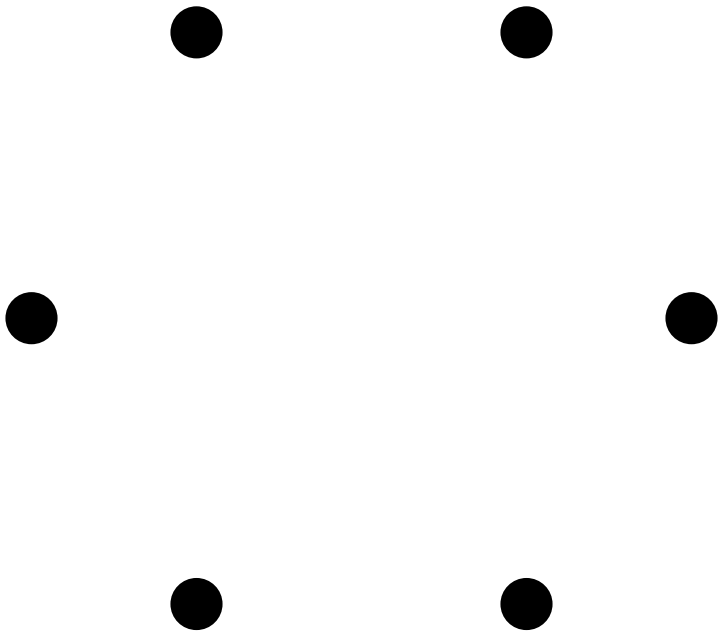


$G = (V, E)$

$V = \{v_1, \ldots, v_n\}$ zb. wierzchołków

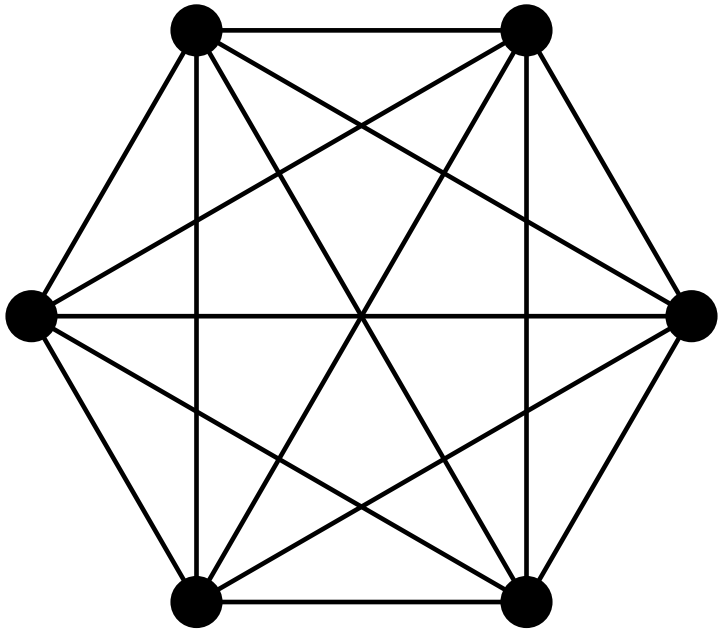
$E \subset \{\{v, u\} : v, u \in V\}$

Graf pusty



Graf pełny

K_n

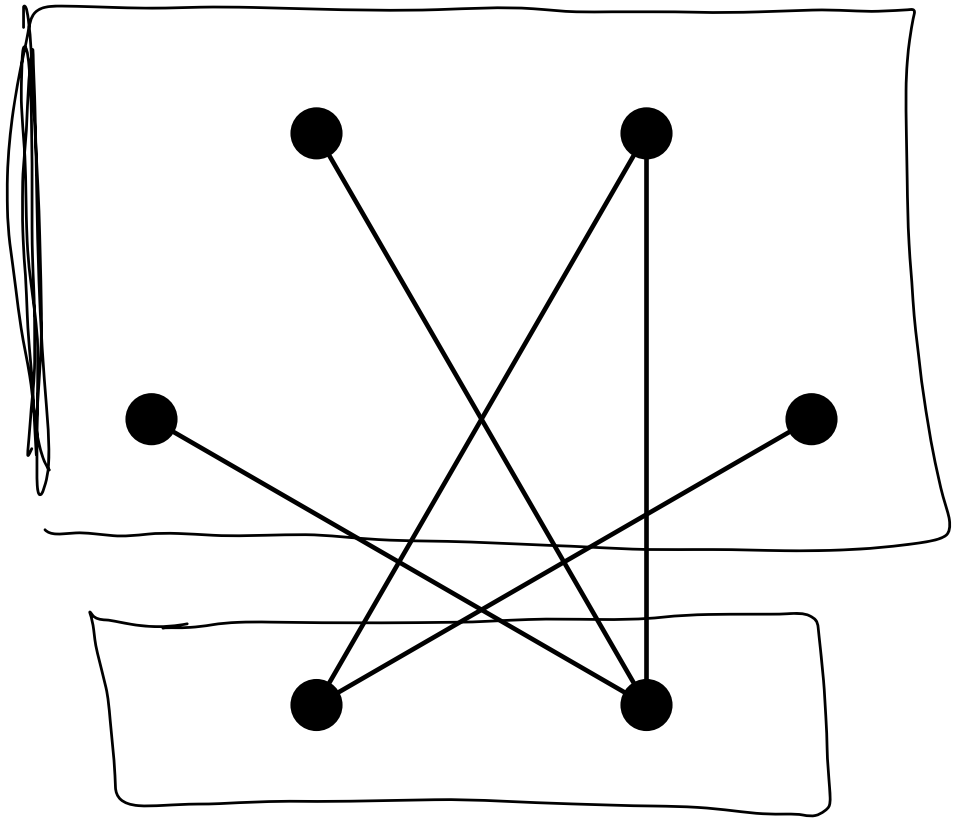


$\frac{n(n-1)}{2}$

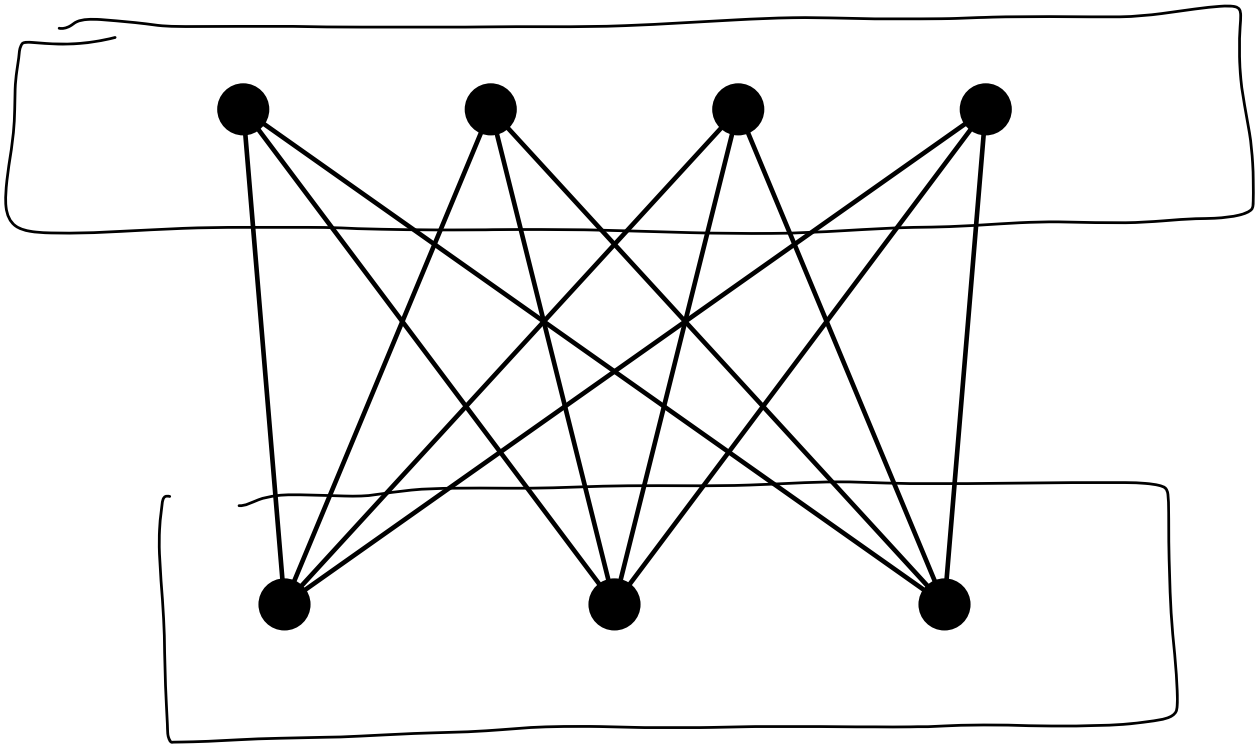
$\leftarrow K_6$

n $\binom{n}{2} = \frac{n(n-1)}{2}$

Graf dwudzielny

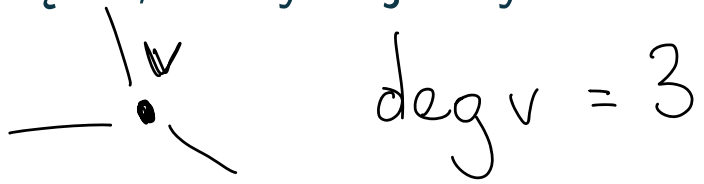


Pełny graf dwudzielny



Podstawowe definicje

- **Stopień wierzchołka**: liczba krawędzi, których jednym z końców jest dany wierchołek.



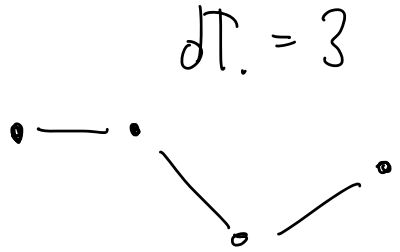
- **Spacer** od v do w:

$$vv_1,\ v_1v_2,\ \ldots,\ v_{k-1}w.$$

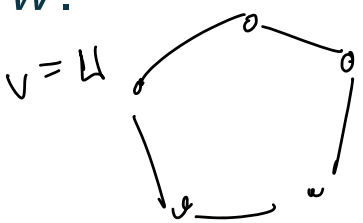
Oznaczenie:

$$v \to v_1 \to v_2 \to \cdots \to v_{k-1} \to w.$$

- **Długością** spaceru jest liczba jego krawędzi.



- **Spacer zamknięty**: $v = w$.

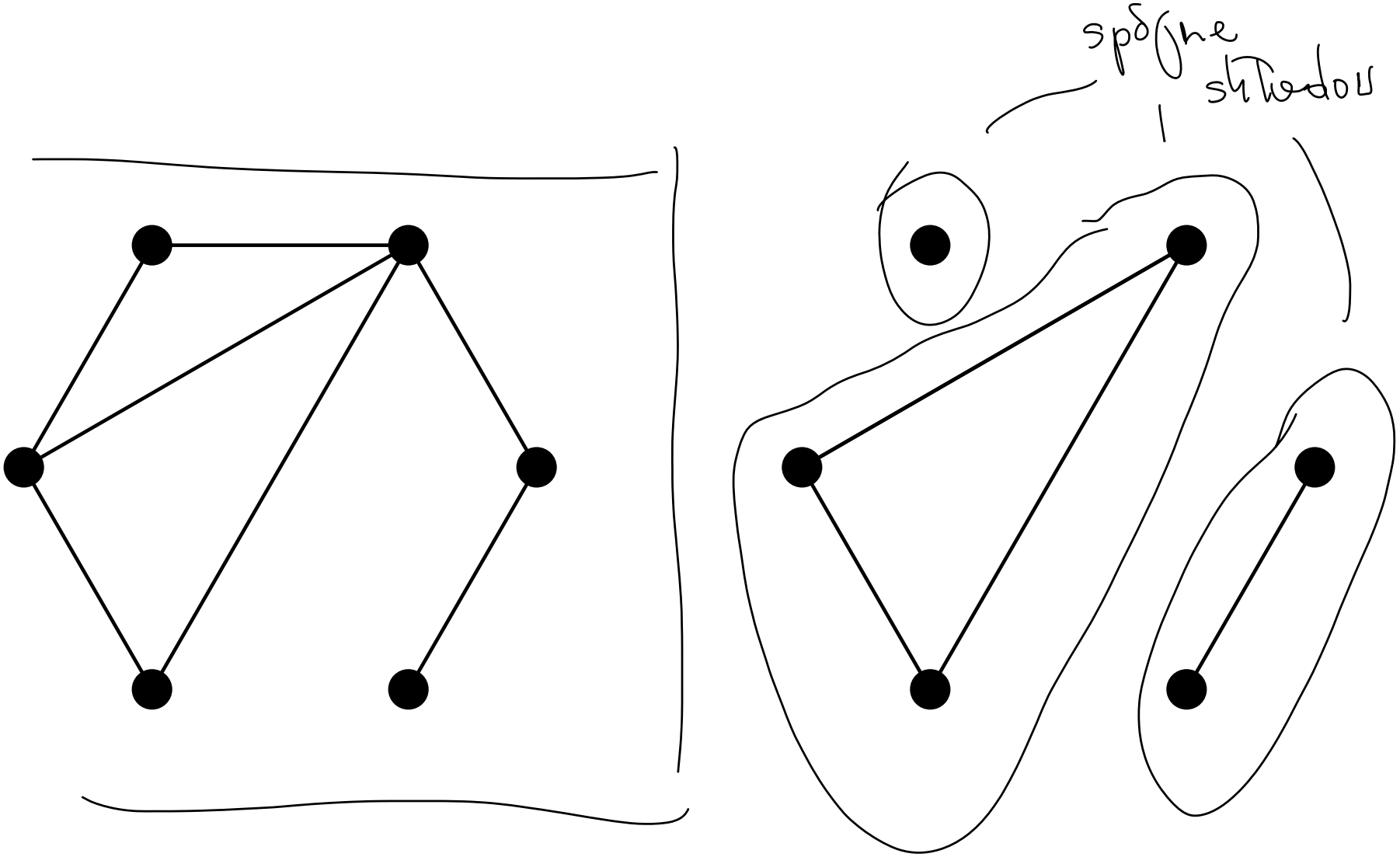


Podstawowe definicje

- **Droga**: spacer bez powtarzających się krawędzi.
- **Ścieżka**: spacer bez powtarzających się wierzchołków.
- **Cykl**: ścieżka długości $\geqslant 2$, w której pierwszy i ostatni wierzchołek są połączone krawędzią.

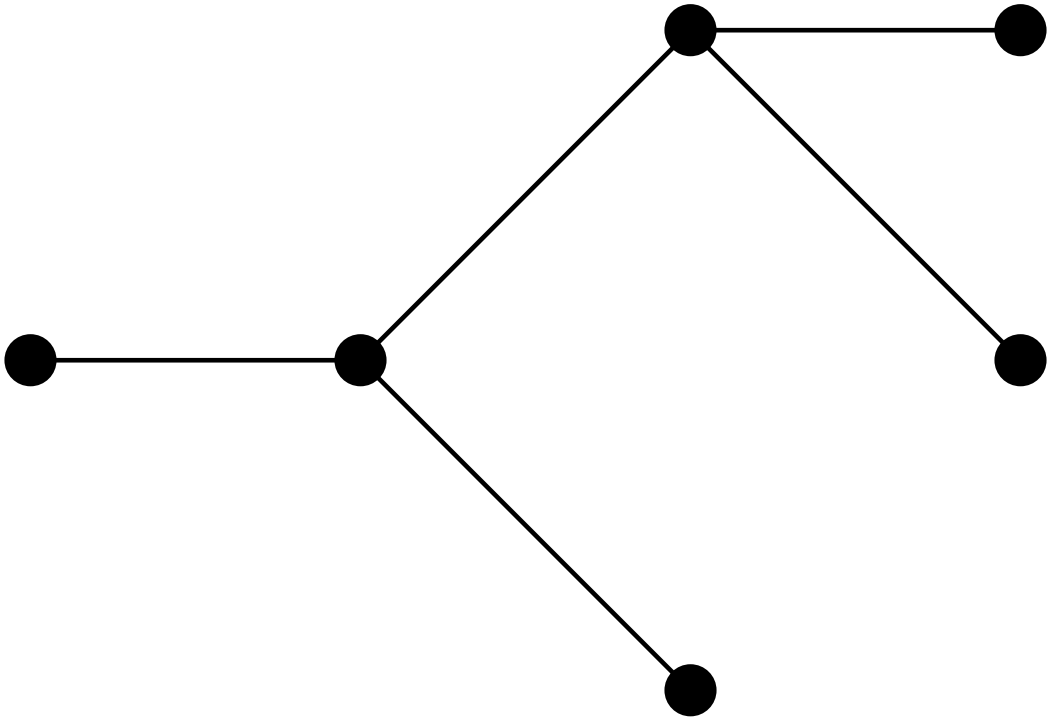
Podstawowe definicje

⇝ **Graf spójny**: między każdymi dwoma wierzchołkami istnieje spacer.



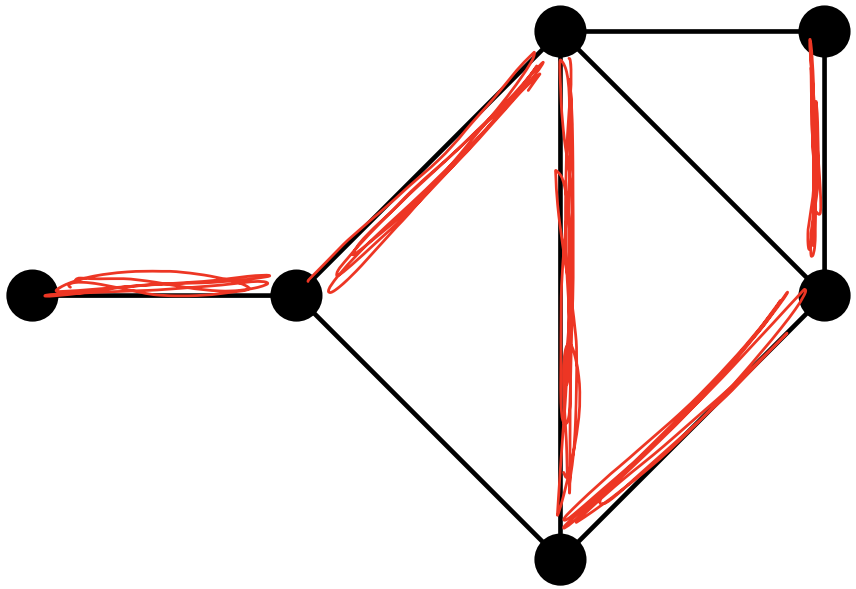
Podstawowe definicje

⇝ **Drzewo**: graf spójny bez cykli.



Podstawowe definicje

- **Drzewo rozpinające**: podgraf, który zawiera wszystkie wierzchołki i jest drzewem.



Algorytm Kruskala

Mosty królewieckie