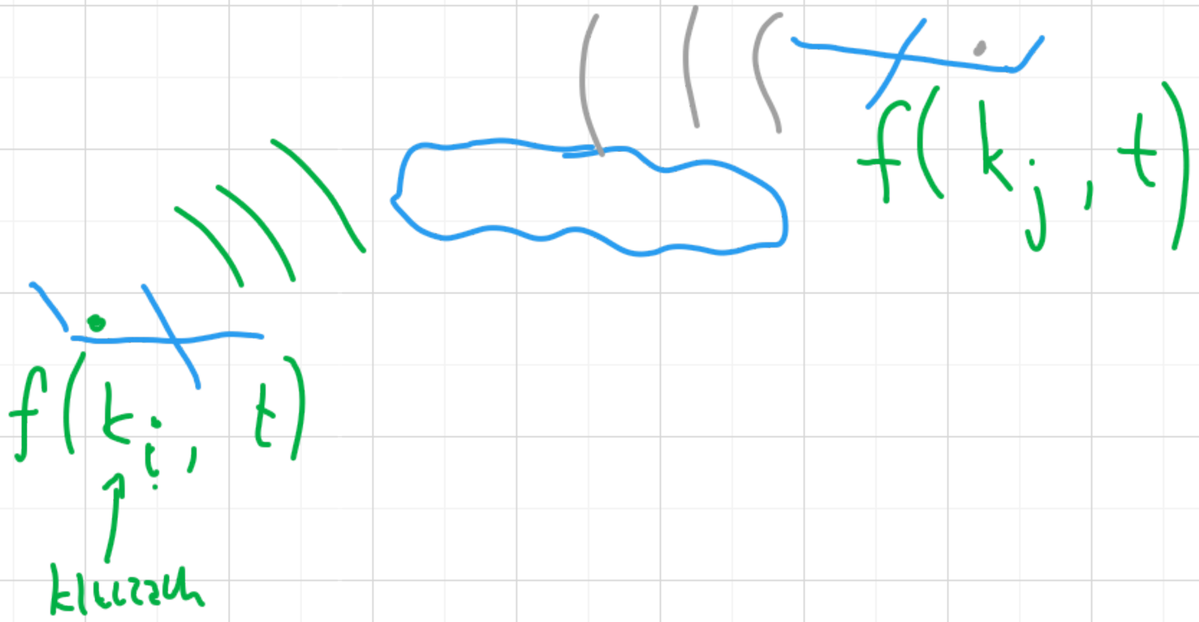
Diffie Hellman Key Exchange

W. Diffie



DHE

$\langle G, \circ \rangle, g$

Alice

① generuje $a \leftarrow_{losowo} \mathbb{Z}_{|G|}$

② oblicza $A = g^a$

A →

Bob

① generuje $b \leftarrow_{losowo} \mathbb{Z}_{|G|}$

② oblicza $B = g^b$

← B

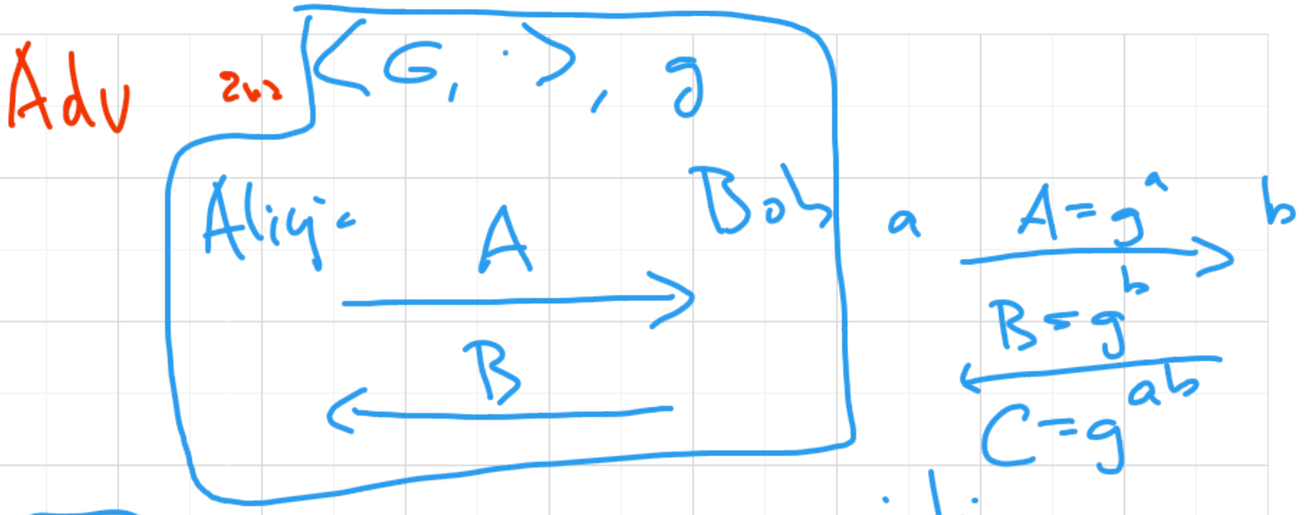
$C = B^a = (g^b)^a = g^{ba} = g^{ab}$

$K = h(g^{ab})$

$C = A^b = (g^a)^b = g^{ab}$

$K = h(C) = h(g^{ab})$

DHE bezpieczeństwo



- ważny jest wybór dobrej grupy
- gdyby istniał algorytm DL

$a \leftarrow DL(g, A)$

(takie, że $A = g^a$)

to byłby problem

DLP - discrete log problem

CDH - computational Diffie Hellman

DDH -

DHE jest bezpieczne jeżeli Adv nie potrafi obliczyć

$C \leftarrow COH[A, B, \langle G, \cdot \rangle, g]$

→ CDH

Pryktad

$\mathbb{Z}_p^+$, g

Alice Bob

$A = g \cdot a \bmod p$ →

← $B = g \cdot b \bmod p$

$C = B \cdot a = g \cdot a \cdot b = A \cdot b = C$

Adv zm: g → potrafi obliczyć a EGCD

MITM

Atak Man in the Middle