# Protokół Diffiego-Hellmana

# Protokół Diffiego-Hellmana

Protokół Diffiego-Hellmana (D-H) jest jedna z pierwszych praktycznych metod ustalania wspólnego klucza pomiedzy dwiema stronami, które nie musza wcześniej wymieniać sie tajnymi informacjami.

- Klucz wygenerowany przez te dwie strony może być nastepnie użyty do szyfrowania komunikacji w standardowych kryptosystemach symetrycznych.
- Protokół opiera sie na trudności obliczeniowej problemu dyskretnego logarytmowania.

# Etapy protokołu Diffiego-Hellmana

- Alice i Bob publicznie ustalaja liczbe pierwsza p oraz baze g (generator).
- Alice wybiera prywatny numer $a$, oblicza ( $A = g^a \mod p$) i publicznie przekazuje $A$ do Boba.
- Bob wybiera prywatny numer $b$, oblicza ( $B = g^b \mod p$ ) i publicznie przekazuje $B$ do Alice.
- Alice oblicza ( $k = B^a \mod p$ ).
- Bob oblicza ( $k = A^b \mod p$ ).
- Uzyskany klucz $k$, ( $k = g^{ab} \mod p$) jest wspólny dla Alice i Boba.

# Przykład

- Ustalone parametry:p $= 7$ i g $= 2$.
- Wybrane sekrety:
  - Alice: ( a $= 5$ )
  - Bob: ( b $= 4$ )
- Obliczenia:
  - Alice: ( $A = 2^5 \mod 7 = 32 \mod 7 = 4$ )
  - Bob: ( $B = 2^4 \mod 7 = 16 \mod 7 = 2$ )
- Wspólny klucz:
  - Alice oblicza: ( $k = 2^5 \mod 7 = 4$ )
  - Bob oblicza: ($k = 4^4 \mod 7 = 4$ )

# Zadanie 1 i 2

- Zaimplementuj funkcje $powmod(a, b, c)$, która oblicza ($a^b$ mod $c$) korzystajac z algorytmu szybkiego potegowania modułowego.
- Napisz program, który symuluje działanie jednej ze stron w protokole Diffiego-Hellmana. Program powinien pozwolić użytkownikowi na wprowadzenie wartości $p$, $g$, $a$, a nastepnie obliczyć $A$, przyjać wartość $B$ od użytkownika i obliczyć wspólny klucz $k$.