10 - Discrete Log I Diffie-Hellman

Wednesday, 19 June 2024 15:05

Discrete Log

Mamy skończoną grupę przemienną (?) G oraz $a, b \in G$.

Chcemy znaleźć $x \in \mathbb{Z}$: $a^x = b$.

Złożoność: jest w NP, nie wiadomo czy NPC.

Diffie Hellman

Mamy grupę G oraz elementy g^x i g^y. Znaleźć g^{xy}.

Złożoność: Discrete-Log $\leq$ Diffie-Hellman.

Protokół Diffiego-Hellmana

Wybieramy grupę G i generator g.

Alicja wybiera a, wysyła g^a

Bob wybiera b, wysyła g^b.

Wspólna wartość: g^{ab}.