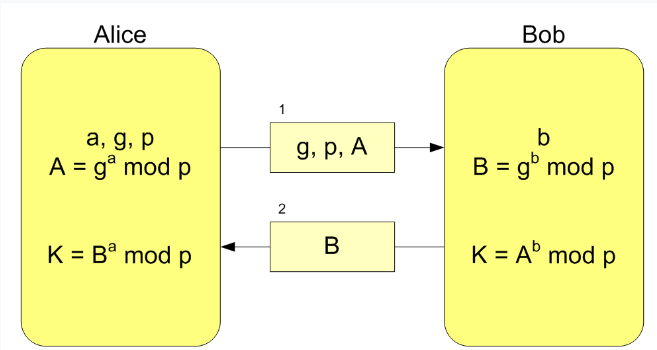
Datu aizsardzība

## **Diffie-Helman atslēgu apmaiņa**

**Arturs Davidenko**

**ITIA 1**

Jelgava 2024

****

**1 uzdevums**

**Difī-Hellmana** (Diffie-Hellman) protokols ļauj divām pusēm, kurām nav iepriekš kopīgi lietota noslēpuma, izveidot kopīgu slepeno atslēgu, izmantojot nedrošu saziņas kanālu. Pēc tam šo kopīgo noslēpumu var izmantot šifrētu ziņojumu sūtīšanai.

1.Pirmkārt, abas puses vienojas izmantot kopīgu bāzi g un kopīgu moduli p, kas nav slepeni. Pieņemsim, g = 2, p = 11.

2. Tad katra puse izvēlas slepenu skaitli, kuru tā neatklāj. Pieņemsim, ka Alise izvēlas slepeno skaitli a = 3, bet Bobs izvēlas slepeno skaitli b = 7.

3. Katra puse aprēķina publisko vērtību, ko nosūta otrai pusei. 

Tādējādi Alise aprēķina  un nosūta šo skaitli Bobam.

Bobs aprēķina un nosūta šo skaitli Alisei.

Tad Alise un Bobs, izmantojot viens otram dotos skaitļus, aizstāj formulu un iegūst skaitli, kuram jābūt vienādam gan Alisei, gan Bobam. Mūsu piemērā koplietojamā slepenā atslēga būs 2.

**Alise:**

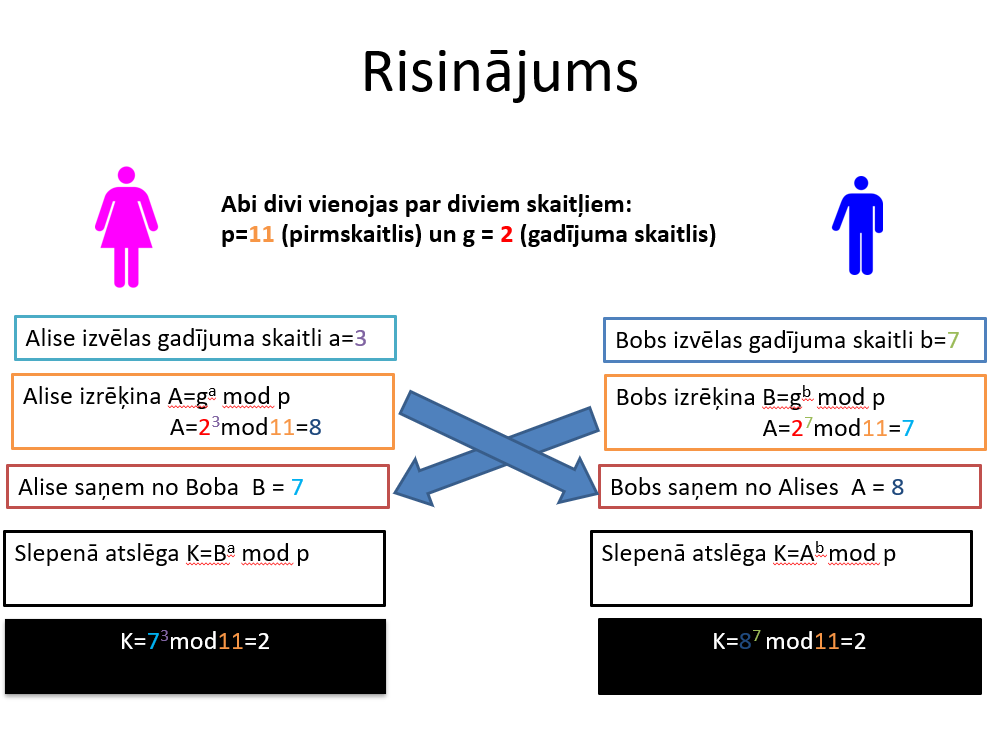
****

**Bob:**

****

Difī-Hellmana protokols aizsargā pret noklausīšanos diskrētā logaritma problēmas sarežģītības dēļ. Pat ja iebrucējs pārtver kopīgo g un p, kā arī abu pušu publiskās atslēgas, viņš joprojām nevar viegli aprēķināt kopīgo slepeno atslēgu, nezinot slepenos skaitļus a vai b.

**Tas vizuāli parāda, kā piemērs darbojas ar maniem skaitļiem:**

****

**2 uzdevums**

Diffie-Hellman protokols ir jutīgs pret **Man-In-The-Middle (MITM)** uzbrukumu.

Iebrucējs (sauksim viņu par Artūru) ir gatavs pārtvert un mainīt ziņojumus, kas tiek pārsūtīti starp Alisi un Bobu.

Hakera (Artūra) uzbrukuma būtība ir pārtvert un izveidot savus ģenerētos datus kopā ar Alisi un Bobu. Šādi rīkojoties, Alise un Bobs domās, ka viņi sazinās viens ar otru.

Kad Alise nosūta savu publisko vērtību Bobam, Artūrs to pārtver un aizstāj ar savu publisko vērtību, kas izveidota, izmantojot viņa slepeno numuru. Pēc tam Artūrs nosūta šo publisko vērtību Bobam, uzdodoties par Alisi. Tas pats tiek darīts ar Bobu, kad viņš nosūta Alisei datus.

Šādā veidā Artūrs var atšifrēt un modificēt jebkurus ziņojumus, ko Alise un Bobs sūta viens otram, jo viņš sazinās ar katru no viņiem, izmantojot atsevišķu kopīgo slepeno atslēgu. Alise un Bobs domā, ka viņi sazinās tieši viens ar otru, lai gan patiesībā visi viņu ziņojumi iet caur Artūru.