Diffie-Hellman algoritam

– Tehničko i naučno pisanje –

Jana Vuković, Sofija Janevska, Lazar Nikolić, Dunja Milenković

Matematički fakultet
Univerzitet u Beogradu

Beograd, 2022.

Slajd 1

- ...

Slajd 2

- ...

Slajd 3

Trenutni korak	Anastasija zna	Javno poznato	Boban zna
Početak algoritma		g, p	
Svako računa svoj ključ	$a, A = g^a \mod p$	g, p	$b, B = g^b \mod p$
Razmena javnih ključeva	a, A, B	g, p, A, B	b, B, A
Svako računa isto, tajno K	$a, A, B,$ $K = B^a \mod p$ $= g^{ab} \mod p$	g, p, A, B	$b, B, A,$ $K = A^b \mod p$ $= g^{ab} \mod p$

Table: **Tajnost promenljivih u toku algoritma**

Slajd 4

- ...

Slajd 5

- ...

Slajd 6

- ...

Slajd 7

- ...

Slajd 8

- ...