

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 - Koraci Algoritma

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

Tabela: Tajnost promenljivih u toku algoritma

Slajd 4



Slajd 5



Slajd 6



Slajd 7



Slajd 8

