

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 - Problemi oslonci

Sve u cikličnoj grupi G reda q

- Problem diskretnog logaritma

U cikličnoj grupi G reda q , pronalaženje k ,
 $0 \leq k \leq q - 1$ tako da $x = g^a$

- Komputacioni Diffie-Hellman

$a, b \in \mathbb{Z} \setminus q\mathbb{Z}$, $A = g^a$, $B = g^b$. Pronalaženje g^{ab} ako znamo A, B

- Odlučujući Diffie-Hellman

$a, b, c \in \mathbb{Z} \setminus q\mathbb{Z}$, $A = g^a$, $B = g^b$, $C = g^c$ ili $C = g^{ab}$

Slajd 5



Slajd 6



Slajd 7



Slajd 8

