Diffie-Hellman algoritam

– Tehničko i naučno pisanje –

Jana Vuković, Sofija Janevska, Lazar Nikolić, Dunja Milenković

Matematički fakultet
Univerzitet u Beogradu

Beograd, 2022.

Osnove Diffie-Hellman algoritma

- Kriptografija javnog ključa
- Vitfild Difi i Martin Helman - "Novi pravci u kriptografiji"
- Dva ključa
- Jednosmerne matematičke funkcije

Koraci Algoritma

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	$b, B, A,$ $K = A^b \mod p$ $= g^{ab} \mod p$

Tabela: Šematski prikaz razmena promenljivih tokom algoritma

Problemi oslonci

Sve u cikličnoj grupi G reda q

- Problem diskretnog logaritma

  Pronalaženje k, $0 \leq k \leq q-1$ tako da $x = g^k$

- 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* $C = g^{ab}$

Primer Diffie-Hellman algoritma

- Neka je izabrani prost broj $q = 353$. Prost koren za ovu vrednost je $\alpha = 3$.
- Tajni ključevi: $X_A = 97$, $X_B = 233$.
- Javni ključevi: $Y_A = 3^{97} \mod 353 = 40$, $Y_B = 3^{233} \mod 353 = 248$.
- Razmena javnih ključeva Y_A i Y_B; Izračunavanje tajnog ključa K.
- Anastasija tajni ključ izračunava po formuli:

$$K = (Y_B)^{X_A} \mod 353 = 248^{97} \mod 353 = 160$$

- Boban tajni ključ izračunava po formuli:

$$K = (Y_A)^{X_B} \mod 353 = 40^{233} \mod 353 = 160$$

ElGamal

- Zasnovan je na kompleksnosti izračunavanja vrednosti diskretnih logaritama.
- Sastoji se iz tri glavne tačke - generisanje ključa, enkripcija i dekripcija.
- $q = 19$, $\alpha = 10$.
- $X_A = 5$, $Y_A = \alpha^{X_A} \mod q = 10^5 \mod 19 = 3$.
- $M = 17$, $k = 6$.
- $K = Y_A^k \mod q = 3^6 \mod 19 = 7$.
- $C1 = \alpha^k \mod q = 10^6 \mod 19 = 5$.
- $C2 = KM \mod q = 7 \cdot 17 \mod 19 = 5$
- $K = C_1^{X_A} \mod q = 11^5 \mod 19$
- $7 \cdot K^{-1} \equiv 1 \mod 19 \implies K^{-1} = 11$
- $M = (C_2 K^{-1}) \mod q = 5 \cdot 11 \mod 19 = 17$

Napadi i primena

- Čovek u sredini
  $g^{a'}$, $g^{b'}$, $ENC_{g^{ab'}}(m)$, $ENC_{g^{a'b}}(m')$
- Autsajder (eng. *Outsider*) napad
- Insider napad
  $g^a = 1$ tj. $g^{ab} = 1$; $g^a = g$
- DoS (eng. *Denial of Service*)
- Primene na bezbednosnim protokolima (SSL, SSH, IPSec)

Literatura

- Maryam Ahmed, Baharan Sanjabi, et al. Diffie-Hellman and Its Application in Security Protocols, (IJESIT), 2012.
- E. Rescorla (June 1999) Diffie-Hellman Key Agreement Method
- Kevin S. McCurley (1990). The Discrete Logarithm Problem
- A. Joux, K. Nguyen (2003). Separating Decision Diffie-Hellman from Computational Diffie-Hellman in Cryptographic Groups
- J. F. Raymond, A. Stiglic (2000). Security Issues in the Diffie-Hellman Key Agreement Protocol
- T.Elgamal (1985). A public key cryptosystem and a signature scheme based on discrete logarithms