Diffie-Hellman algoritam

Seminarski rad u okviru kursa
Tehničko i naučno pisanje
Matematički fakultet

Dunja Milenkovic
mi22056@alas.matf.bg.ac.rs

Jana Vukovic
mi22124@alas.matf.bg.ac.rs

Lazar Nikolic
mi22164@alas.matf.bg.ac.rs

Sofija Janevska
mi22035@alas.matf.bg.ac.rs

15. novembar 2022.

Sažetak

U ovom tekstu je ukratko prikazana osnovna forma seminarskog rada. Obratite pažnju da je pored ove .pdf datoteke, u prilogu i odgovarajuća .tex datoteka, kao i .bib datoteka korišćena za generisanje literature. Na prvoj strani seminarskog rada su naslov, apstrakt i sadržaj, i to sve mora da stane na prvu stranu! Kako bi Vaš seminarski zadovoljio standarde i očekivanja, koristite uputstva i materijale sa predavanja na temu pisanja seminarskih radova. Ovo je samo šablon koji se odnosi na fizički izgled seminarskog rada (šablon koji *morate* da ispoštujete!) kao i par tehničkih pomoćnih uputstava.

Sadržaj

1 Uvod

Sve rasprostranjenija upotreba interneta širom sveta donosi sa sobom, kako značajne prednosti u načinu istraživanja, rada, povezivanja i sl. tako i povećan rizik od nebezbedne komunikacije i razmene podataka. Bilo da se radi o individualnim, privatnim razmenama informacija između ljudi ili rada nekih od najvećih državnih institucija, bezbedna i neometana interakcija i komunikacija među korisnicima na internetu je od presudnog značaja. Glavni problem nastaje kada spoljni korisnik koji nije predviđen kao deo veze pokuša da je prekine i dođe do određenih informacija koje su originalno bile namenjene jednom od povezanih korisnika. Upravo rešavanjem ovakvih problema bavi se **kriptografija**.

Kriptografija je oblast koja razvija tehnike koje omogućavaju zaštićenu i efikasnu digitalnu komunikaciju. Bez nje, komunikacija nebezbednim i nepoverljivim kanalima, što uključuje sve vrste mreža, a pogotovo internet, ne bi bila moguća. U ovom radu bavićemo se jednom od tehnika kriptografije koja se naziva **Diffie-Hellman algoritam** tj. **Diffie-Hellman protokol** i predstavićemo način rada algoritma, njegova osnovna svojstva, primene, prednosti i mane.

2 Asimetrična kriptografija i osnove Diffie-Hellman algoritma

Glavna klasifikacija kriptografskih algoritama deli ih na simetričnu kriptografiju, asimetričnu kriptografiju i heš funkcije; kako je Diffie-Hellman protokol predstavnik asimetrične kriptografije, nju ćemo posebno izdvojiti i definisati.

Asimetrična kriptografija ili tzv. tehnika javnog ključa podrazumeva korišćenje dva ključa – jednog za šivrovanje i drugog za dešifrovanje koda. „Tvorcima“ tj. pokretačima asimetrične kriptografije smatraju se **Whitfield Diffie** (Vitfild Difi) i Martin Hellman (Martin Helman), dok je **Ralph Merkle** (Ralf Merkl) takođe dao svoj doprinos ovoj oblasti radom na distribuciji javnog ključa. Njihova saradnja rezultirala je objavom zajedničkog rada pod nazivom "New Directions in Cryptography"("Novi pravci u kriptografiji"), novembra 1976. godine. U njemu su opisane osnove Diffie-Hellman algoritma, koji je upravo otud i dobio naziv. Diffie i Hellman su 2015. godine dobili Tjuringovu nagradu za svoja dostignuća u oblasti kriptografije.

U spomenutom radu, Diffie-Hellman algoritam opisan je kao algoritam koji koristi dva ključa i tako omogućava korisnicima bezbednu komunikaciju bez potrebe za deljenjem privatnog ključa. Osnovni princip na kome funkcioniše jeste korišćenje tzv. jednosmernih matematičkih funkcija, koje se lako izračunavaju u jednom smeru, dok isto ne važi i za njihove inverzne funkcije. Na ovaj način omogućeno je postojanje javnog ključa, bez rizika da ga treći korisnik koji nije predviđen kao deo mreže može zloupotrebiti

3 Engleski termini i citiranje

Na svakom mestu u tekstu naglasiti odakle tačno potiču informacije. Uz sve novouvedene termine u zagradi naglasiti od koje engleske reči termin potiče.

Naredni primeri ilustruju način uvođenja enlegskih termina kao i citiranje.

Primer 3.0.1 *Problem zaustavljanja (eng.* halting problem*) je neodlučiv [3].*

Primer 3.0.2 *Za prevođenje programa napisanih u programskom jeziku C može se koristiti GCC kompajler [?].*

Primer 3.0.3 *Da bi se ispitivala ispravost softvera, najpre je potrebno precizno definisati njegovo ponašanje [?].*

Ukoliko za unos referenci koriste datoteku *seminarski.bib*, prevođenje u pdf format u Linux okruženju može se uraditi na sledeći način:

```
pdflatex TemaImePrezime.tex
bibtex TemaImePrezime.aux
pdflatex TemaImePrezime.tex
pdflatex TemaImePrezime.tex
```

Prvo latexovanje je neophodno da bi se generisao *.aux* fajl. *bibtex* proizvodi odgovarajući *.bbl* fajl koji se koristi za generisanje literature. Potrebna su dva prolaza (dva puta pdflatex) da bi se reference ubacile u tekst (tj da ne bi ostali znakovi pitanja umesto referenci). Dodavanjem novih referenci potrebno je ponoviti ceo postupak.

Broj naslova i podnaslova je proizvoljan. Neophodni su samo Uvod i Zaključak. Na poglavlja unutar teksta referisati se po potrebi.

Primer 3.0.4 *U odeljku* **??** *precizirani su osnovni pojmovi, dok su zaključci dati u odeljku 9.*

4 Slike i tabele

Slike i tabele treba da budu u svom okruženju, sa odgovarajućim naslovima, obeležene labelom da koje omogućava referenciranje.

Primer 4.0.1 *Ovako se ubacuje slika. Obratiti pažnju da je dodato i*

```
\usepackage{graphicx}
```

Slika 1: Pande

Na svaku sliku neophodno je referisati se negde u tekstu. Na primer, na slici 1 prikazane su pande.

Primer 4.0.2 *I tabele treba da budu u svom okruženju, i na njih je neophodno referisati se u tekstu. Na primer, u tabeli 1 su prikazana različita poravnanja u tabelama.*

Tabela 1: Razlčita poravnanja u okviru iste tabele ne treba koristiti jer su nepregledna.

centralno poravnanje	levo poravnanje	desno poravnanje
a	b	c
d	e	f

5 Algoritam

Pre početka razmene ključeva, uspostavljaju se 2 javno poznata broja: p i g.

- p - bezbedan prost broj i modulo po kom radimo, preporuka je da to bude broj dužine 2048 bita (broj reda 10^{616}) [4]
- g - generator, mora da bude primitivni koren od p

Bezbedan prost broj: p je bezbedno prost ako može da se izrazi kao $p = 2q + 1$ gde je q takođe prost broj. q je Sofija Žermen prost (eng. *Sophie Germain prime*). Ovo je bitno kako bi se izbegao specifičan napad na Diffie-Hellman — Silver-Polig-Hellman algoritam (eng. *Silver-Pohlig-Hellman algorithm*) [5]

Primitivni koren: g je primitivni koren po modulu p ako za svaki celi broj a koji je uzajamno prost sa p postoji celi broj k tako da je

$$g^k \equiv a \mod p$$

Takvo k se naziva indeks ili diskretni logaritam od a sa odnovom $g \mod p$.

5.1 Koraci algoritma

Recimo da Anastasija i Boban žele da razmene ključeve.

- Pretpostavljamo da su se Anastasija i Boban već dogovorili oko brojeva g i p
- Anastasija nasumično bira neki tajni broj $x \in \mathbb{N}$ i izračuna njegov *najmanji pozitivni ostatak* (objašnjeno kasnije), čime dobija a, ovo je njen privatni ključ
- Zatim kalkuliše njen javni ključ koji je jednak $A = g^a \mod p$
- Boban će uraditi isto, nakon čega poseduje privatni ključ b i javni ključ $B = g^b \mod p$
- Anastasija i Boban sada razmene njihove javne ključeve (privatni ključevi ostaju tajni)
- Anastasija sada poseduje svoje ključeve, kao i Bobanov javni ključ
- Ona će izračunati tajni broj $K = B^a \mod p$. Ako zamenimo B, videćemo da je

$$\begin{aligned} K = (g^b \mod p)^a \mod p = \\ (g^b)^a \mod p = \\ g^{ab} \mod p \end{aligned}$$

- Boban poseduje svoje ključeve i Anastasijin javni ključ

- On će istim postupkom kao i Anastasija pronaći K

$$\begin{aligned} K = A^b \mod p = \\ (g^a \mod p)^b \mod p = \\ (g^a)^b \mod p = \\ g^{ab} \mod p \end{aligned}$$

Definicija 5.1.1 *Najmanji pozitivni ostatak nekog x po modulu p je najmanji pozitivni celi broj a tako da je*

$$x \equiv a \mod n$$

Primetimo da će i Anastasija i Boban izračunati isti broj K. K predstavlja ključ za enkripciju ključeva (engl. *Key-Encryption Key (KEK)*). Pomoću tog ključa mogu sinhrono da razmene novi ključ za enkripciju sadržaja (engl. *Content-Encryption Key (CEK)*) i da nastave komunikaciju pomoću njega. [6]

Neko ko je prisluškivao ovoj razmeni zna p, g, g^a i g^b. Da bi od ovih brojeva pronašao K, on mora da izračuna vrednost a ili b, problem koji se zove *komputacioni Diffie-Hellman problem* (engl. *computational Diffie-Hellman problem (CDH)*).

5.2 Problemi oslonci

Neka G bude ciklična grupa reda q, sa generatorom g. Drugačije rečeno, svaki broj x iz G je kongruentan sa nekim g^k, gde je k neki celi broj tako da je $0 \leq k \leq q-1$.

$$x = g^k$$

Ako znamo g i k, lako možemo izračunati x. Međutim, ako znamo x i g, pronalaženje k je veoma teško, i to je zapravo problem diskretnog logaritma.

Definicija 5.2.1 *Problem diskretnog logaritma u cikličnoj grupi G reda q je pronalaženje broja k, $0 \leq k \leq q-1$ tako da $x = g^a$, za neko g i x.*

Ako možemo da rešimo problem diskretnog logaritma, možemo da nađemo i tajni broj K iz Diffie-Hellman ako znamo oba javna ključa. Obrnuto nije dokazano: ako možemo da pronađemo tajni broj K, ne mora da znači da možemo rešiti bilo koji problem diskretnog logaritma.

Ne treba da pretpostavimo da je diskretni logaritam jedini način da se razbije Diffie-Hellman. Dovoljna je bilo koja metoda koja može da pronađe g^{ab} iz g^a i g^b, i otud uvođenje sledećeg problema:

Definicija 5.2.2 *Neka $a, b \in \mathbb{Z} \setminus q\mathbb{Z}$ (a i b su u nekoj cikličnoj grupi reda q **nek neko proveri ovo!**), i neka $A = g^a$ i $B = g^b$ **Komputacioni Diffie-Hellman problem** (CDH) je problem nalaženja g^{ab} ako znamo A i B u cikličnoj grupi $G = \langle g \rangle$ reda q.*

Na težini ovog problema se oslanja bezbednost Diffie-Hellman šeme. Komputacioni Diffie-Hellman je u srodstvu sa problemom Diskretog Logaritma, i najefikasnije rešenje za koje znamo je da rešimo problem Diskretnog Logaritma ali još uvek nije dokazana ekvivalencija između njih. [7] Takođe slična je i ElGamal enkripcija o kojoj će biti reči kasnije. Ona se oslanja na sledeći problem:

Definicija 5.2.3 *Neka $a, b, c \in \mathbb{Z}\backslash q\mathbb{Z}$ i $A = g^a$, $B = g^b$. Sa verovatnoćom $\frac{1}{2}$ postavimo $C = g^c$, a inače $C = g^{ab}$. Odlučujući Diffie-Hellman problem (engl.* Decisional Diffie-Hellman problem (DDH)*) je problem odlučivanja da li je $C = g^{ab}$, ako znamo $\langle g \rangle$ i A, B, C.*

Ako znamo da rešimo komputacioni Diffie-Hellman problem, lako je rešiti odlučujući Diffie-Hellman problem. Obrnuto ne važi. [citation needed]

6 Drugi naslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

6.1 ... podnaslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

7 n-ti naslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

7.1 ... podnaslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

7.2 ... podnaslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

8 Poslednji naslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

9 Zaključak

Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak.

Literatura

[1] Gary C. Kessler. *An Overview of Cryptography*, 2015.

[2] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb Omotunde. *Diffie-Hellman and Its Application in Security Protocols*, International Journal of Engineering Science and Innovative Technology (IJESIT), 2012.

[3] A. M. Turing. *On Computable Numbers, with an application to the Entscheidungsproblem.* Proceedings of the London Mathematical Society, 2(42):230–265, 1936.

[4] Adrian, David; et al. (October 2015). *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*

[5] Mollin, Richard (2006-09-18). *An Introduction To Cryptography* (2nd ed.). Chapman and Hall/CRC. p. 344

[6] E. Rescorla (June 1999). *Diffie-Hellman Key Agreement Method*

[7] Kevin S. McCurley (1990). *The Discrete Logarithm Problem*

A Dodatak

Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe. Ovde pišem dodatne stvari, ukoliko za time ima potrebe.