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 Osnovna uputstva

Vaš seminarski rad mora da sadrži najmanje jednu sliku, najmanje jednu tabelu i najmanje tri reference u spisku literature. **Dužina seminarskog rada treba da bude:**

- Ukoliko tim ima dva člana, tada od 3 do 5 strana
- Ukoliko tim ima tri člana, tada od 4 do 6 strana

Ко жели, може да пише рад ћирилицом. У том случају, неопходно је да су инсталирани одговарајући пакети: texlive-fonts-extra, texlive-latex-extra, texlive-lang-cyrillic, texlive-lang-other.

Nemojte koristiti stari način pisanja slova, tj ovo:

```
\v{s} i \v{c} i \'c ...
```

Koristite direknto naša slova:

```
š i č i ć ...
```

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

Primer 3.2 *Za prevođenje programa napisanih u programskom jeziku C može se koristiti GCC kompajler [2].*

Primer 3.3 *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 3.4 *U odeljku 5 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 4.1 *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 4.2 *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, uspostavljaju se 2 javno poznata broja: n i g.

- n - opseg u kom računamo, preporuka je da to bude broj dužine 3072 bita (broj reda 10^{925})[ref needed]
- g - generator, mora da bude primitivni koren od n

Primitivni koren: g je primitivni koren po modulu n ako za svaki celi broj a koji je uzajamno prost sa n postoji celi broj k tako da je $g^k \equiv an$. Takvo k se naziva indeks ili diskretni logaritam od a sa odnovom gn.

5.1 Prvi podnaslov

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

5.2 Drugi podnaslov

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

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. Ovde pišem zaključak.

Literatura

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

[2] Free Software Foundation. GNU gcc, 2013. on-line at: http://gcc.gnu.org/.

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

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.