Kriptovana komunikacija primjenom modifikovane Plejfer šifre

Dušan Perišić, Andrija Karadžić, Ognjen Letić, Ivan Tot

***Apstrakt*— XXI vijek možemo slobodno nazvati vijek informacionih tehnologija obzirom da je razvoj tehnike i tehnologije donio i nove društvene promjene, kako na stil života tako i na druge društvene aspekte. Računarski sistemi, pored toga što su postali neizostavan dio svakodnevnice, postali su i kritični segment društva. Sve je veći broj napada na takve sisteme pa potreba za zaštitom sve veća. Sve više se govori o problemu privatnosti i krađi identiteta putem interneta.**

U radu je predstavljeno jedno od rješenja zaštite prenosa tekstualnih poruka primjenom modifikovane Plejfer šifre u ECB (Electronic CodeBook) modu, koja koristi dinamički generisane ključeve. Aplikacija koja prati ovaj rad pogramirana je u programskom jeziku C#.

***Ključne riječi*—kriptografija, bezbjedna komunikacija.**

I. UVOD

U tekstovima koji se bave predviđanjima budućnosti danas se veoma mnogo govori o nanotehnologiji i biotehnologiji kao naukama vremena koje je pred nama. Očekuje se da će one dati sasvim nove, sofisticirane projekte i omogućiti primjenu u elektronici, računarstvu, vojsci, medicini, proizvodnji hrane, energije, itd. Ova predviđanja i naznačeni okviri novih projekata navode nas na sve ozbiljnija razmišljanja i o promjenama danas poznatih granica između čovjeka i mašina. Između ostalog, projekti budućnosti, koji se usmjeravaju na period posle 2030; godine, sadrže i mogućnosti implantacije nanorobota ili ultramikročipova (ne većih od nekoliko nanometara) u ljudski organizam, čija bi uloga bila nadgradnja i poboljšanje intelektualnih sposobnosti čovjeka.[3]

O značaju i pravovremenosti informacija govori i podatak da je 1815. godine u okršaju kod Nju Orleansa između američkih i engleskih vojnika bilo oko 2000 žrtava iako je dvije nedelje prije toga potpisan mirovni sporazum u Briselu. Naime, ta informacija nije na vrijeme dospjela do njih.

Dušan Perišić – student, Vojnoelektronsko inžinjerstvo, Vojna akademija, Univerzitet odbrane Beograd, Pavla Jurišića Šturma 33, 11000 Beograd, Srbija (e-mail: kontakt@dusanperisic.com).

Andrija Karadžić – student, Vojnoelektronsko inžinjerstvo, Vojna akademija, Univerzitet odbrane Beograd, Pavla Jurišića Šturma 33, 11000 Beograd, Srbija (e-mail: andrija.karadzic@va.mod.gov.rs).

Ognjen Letić – student, Vojnoelektronsko inžinjerstvo, Vojna akademija, Univerzitet odbrane Beograd, Pavla Jurišića Šturma 33, 11000 Beograd, Srbija (e-mail: ognjen.letic@va.mod.gov.rs).

Ivan Tot – docent, Vojnoelektronsko inžinjerstvo, Vojna akademija, Univerzitet odbrane Beograd, Pavla Jurišića Šturma 33, 11000 Beograd, Srbija (e-mail: totivan@gmail.com).

II. OSNOVNI POJMOVI

Otvoreni tekst (engl. plaintext) predstavlja svaki sadržaj (govor, računarski podaci, itd) koji se sastoji od konačnog broja simbola određenog alfabeta (slova, brojevi, biti, bajti itd). Otvoreni tekst koji predstavlja određenu logičku cjelinu naziva se **poruka** (engl. message). Postupak transformacije otvorenog teksta u zaštićen oblik primjenom određenog kriptografskog postupka naziva se **šifrovanje** (engl. Encription, Encipherment). U savremenim sistemima zaštite šifrovanje poruke realizuje se primjenom odgovarajuće kriptografske transformacije (algoritma) i korišćenjem tajnog parametra – kriptografskog ključa. Sadržaj dobijen nakon realizacije procesa šifrovanja naziva se **šifrovani tekst** ili **šifrat** (engl. ciphertext). Inverzan postupak, transformacija šifrata u otvoreni tekst naziva se **dešifrovanje** (Decryption, Decipherment).

U savremenoj kriptografiji **kriptoanaliza** se može definisati kao nauka o mogućnosti otkrivanja otvorenog teksta poruke, na osnovu posjedovanja šifrata, bez poznavanja ključa. Uspješnom kriptoanalizom šifrovane poruke dolazi se do otvorenog teksta ili ključa.[2]

III. ISTORIJAT KRIPTOGRAFIJE

Kada je pismo postalo sredstvo komunikacije, pojavila se potreba da se neka pisma sačuvaju od tuđih pogleda. Tada je i kriptografija ugledala svjetlost dana. Od samog početka, enkripcija podataka koristila se prvenstveno u vojne svrhe. Jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke bio je Julije Cezar. Naime, kada je Cezar slao poruke svojim vojskovođama, on je te poruke šifrovao tako što su sva ili pojedina slova u tekstu bila pomjerana za tri, četri ili više mjesta u abecedi. Takvu poruku mogli su da dešifruju samo oni koji su poznavali pomeri za pravilo. Poznata Cezarova izjava prilikom prelaska Rubikona u šifriranom dopisivanju glasila bi: fqkf ofhzf kyz. Pomicanjem svakog slova za šest mjesta u abecedi lako se može pročitati pravi smisao poruke: Alea iacta est (kocka je bačena). [2]

Danas se primjenjuju različiti mnogo složeniji postupci koji se implementiraju na računarima velikih brzina.

IV. MODIFIKACIJA PLEJFER ŠIFRE

Postupak šifrovanja sa plejfer šifrom zasniva se na zamjeni blokova od dva slova ili simbola (bigrami). Ovaj postupak šifrovanja predložio je Čarls Vitson (Charles Wheatstone) 1854. godine. Plejfer šifru su koristili Britanci u vrijeme Prvog svjetskog rata. Ključ Plejfer šifre bila je matrica [5 x 5] sa 25 slova, karakter "J" se nije koristio ili je bio prisvojen

nekom drugom slovu (zamijenjen slovom "I"). Matrica se konstruiše na osnovu izabrane ključne riječi. Par slova (bigram) otvorenog teksta m1 i m2 šifruje se u skladu sa sledećim pravilima:

- Ako su m_1 i m_2 u istom redu, tada su c_1 i c_2 dva slova desno od m_1 i m_2, usvojeno je da je prva kolona susjedna kolona poslednjoj koloni;
- Ako su m_1 i m_2 u istoj koloni, tada su c_1 i c_2 dva slova ispod m_1 i m_2, usvojeno je da je prvi red susjedni donji poslednjem redu;
- Ako su m_1 i m_2 u različitim kolonama i redovima, tada su c_1 i c_2 ostale dvije ivice (tjemena) pravougaonika koji sadrži ivice m_1 i m_2, gdje je c_1 u istom redu kao i m_1 dok je c_2 u istom redu kao c_2;
- Ako je $m_1=m_2$, tada se vrši umetanjem neutralnog (null) karaktera (npr, Z) između m_1 i m_2;
- Ukoliko poruka otvorenog teksta ima neparan broj slova tada se na kraj poruke dodaje neutralni (null) karakter.[1]

TABELA 1
PRIMJER ŠIFROVANJA PLEJFER ŠIFROM

I	N	F	O	R
M	A	T	K	B
C	D	E	G	H
L	P	Q	S	U
V	W	X	Y	Z

U ovom primjeru korišten je ključ INFORMATIKA, stim što u ključu imamo po dva slova I i A, od kojih se koristi samo njihovo prvo pojavljivanje u ključu. Slovo "J" zamijenjeno je slovom "I", za null karakter odabran je "Z".

Enkripcija riječi KRIPTOGRAFIJA obavlja se na sledeći način:

KRIPTOGRAFIJA→KR IP TO GR AF IZ IA

KR→BO, IP→NL, TO→KF, GR→HO, AF→TN, IZ→RV, IA→NM

I dobija se šifrat: BONLK FHOTN RV

U ovom radu korištena je modifikovana Plejfer šifra, a modifikacija se ogleda u tome da je proširen skup karaktera koje koristi (dodati su brojevi, znaci interpukcije i dodatni specifični karakteri), ovim proširenjem povećan je broj mogućih ključeva koje je moguće iskoristiti za šifrovanje poruka koje se prenose.

Broj mogućih ključeva iznosi 64!, što daje cifru 126886932185884164103433389335161480802865516174545192198801894375214704230400000000000000000 ili približno $1{,}2689 \cdot 10^{90}$.

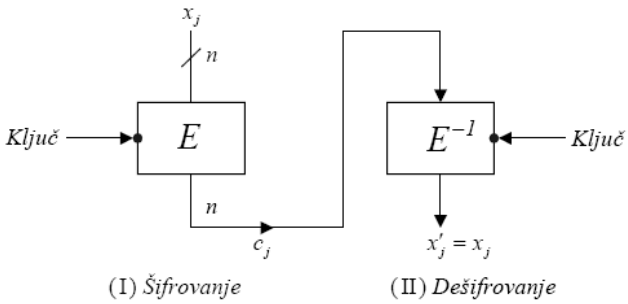
V. KRIPTOANALIZA PLEJFER ŠIFRE

Sigurnost ove šifre zavisi od veličine otvorenog teksta koji se šifruje. Ukoliko je šifrat dovoljno velik, moguće je primijeniti analizu frekvencija nad bigramima. Tačnije ukoliko je uzorak dovoljan, kriptološki metod na osnovu statistike će biti uspješniji. Poznato je da i kod ove šifre dio strukture jezika ostaje sačuvan. Slova u šifratu nisu uniformno raspoređena, tako da njihova raspodjela odgovara raspodjeli nekog slučajnog niza. Zapravo, razlika koja postoji između ovih raspodjela (raspodjela slova u šifratu i u slučajnom nizu) predstavlja taj dio strukture jezika koji će biti iskorišten za kriptoanalizu plejfer šifre, gdje se koristi statistika o frekvenciji slova i bigrama u datom jeziku. Ukoliko je dobijeni šifrat isuviše mali, analizom frekvencija nije moguće uraditi kriptoanalizu datog šifrata.[2]

VI. EBC KRIPTOGRAFSKI MOD

Kriptografski mod predstavlja način upotrebe bazičnog šifarskog algoritma i najčešće je kombinacija neke vrste povratne petlje i određenih jednostavnih operacija. Operacije koje se primjenjuju nad algoritmom su uglavnom jednostavne jer je bezbednost određena bazičnim šifarskim algoritmom a ne kriptografskim modom.

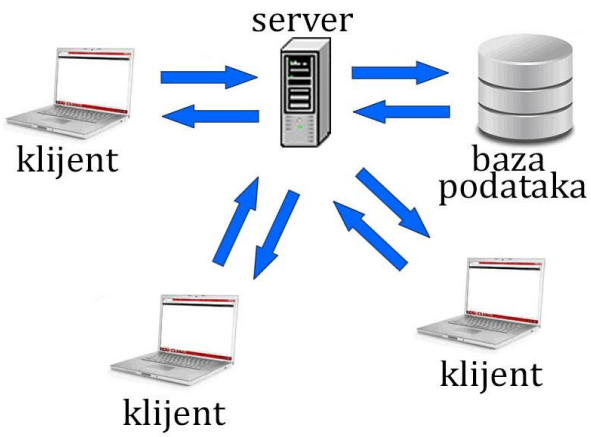
Mod elektronske kodne knjige (ECB – Electronic CodeBook mode) predstavlja najprirodniji i najlakši način primene blok šifarskih sistema - blok OT se šifruje u blok ST (Sl. 1.). Svaki OT blok šifruje se nezavisno.[2]



Sl. 1. Grafički prikaz operacija u ECB modu. Sa E je označena enkripcija ulaznog bloka podataka (u našem slučaju slova poruke), a sa E^{-1} dešifrovanje šifrata određenim ključem.

VII. SOFTVERSKA IMPLEMENTACIJA

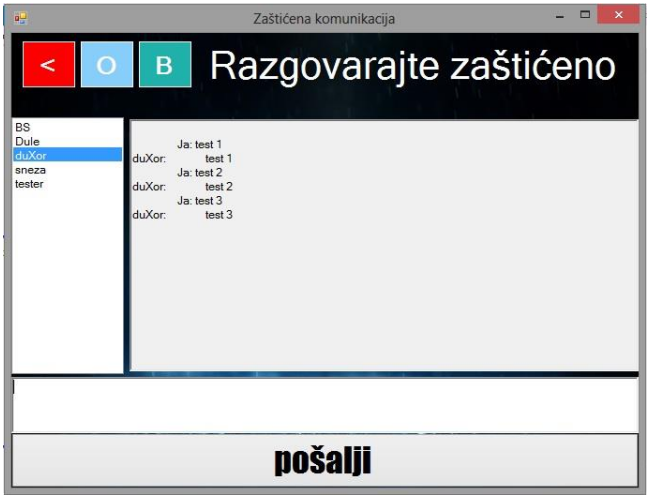
Rad je implementiran na principima klijent – server modela, gdje imamo server (Sl. 2.) koji u potpunosti kontroliše sve segmente komunikacije, od početka do kraja i nema direktnog povezivanja korisnika, već se povezuju posredstvom server.



Sl. 2. Klijent-server princip rada. Na slici je prikazana povezanost između klijenata (učesnika) posredstvom servera koji komunicira sa bazom podataka.

Projekat, na čiju temu govori ovaj rad, implementiran je u tri nivoa:

- aplikativni dio (korisnički interfejs (Sl. 3.) i programske klase koje upravljaju svim funkcionalnostima aplikacije);
- server posrednik (interfejs između korisnika i baze podataka);
- baza podataka



Sl. 3. Korisnički interfejs. Na slici je prikazan korisnički interfejs aplikacije realizovane ovim pri izradi ovog rada, ito dio u kome korisnici komuniciraju međusobno. Sa lijeve strane je potrebno izabrati korisnika kome je poruka namijenjena, poruka se piše u tekstualno polje iznad dugmeta "pošalji".

Aplikativni dio čini aplikacija implementirana u C# programskom jeziku koja korisniku omogućava jednostavnost korištenja, osmišljena je tako da je mogu koristiti i korisnici bez programerskog znanja.

Server posrednik je naziv za dio koga čine php i mysql skripte, koji korisničkoj aplikaciji omogućava komunikaciju sa bazom podataka.

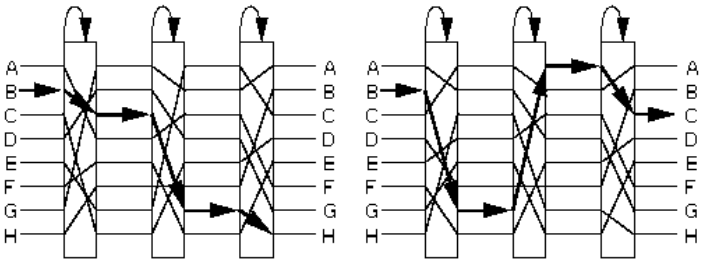
Iskorištena je mysql relaciona baza podataka u kojoj su smješteni korisnički nalozi, kao i poruke koje se prenose između korisnika.

VIII. PRINCIP RADA

Princip rada podijeljen je u dva nivoa ito identifikacija i komunikacija,

Identifikacija predstavlja dio u kome se vrši identifikacija korisnika, razmjena poruka između korisničke aplikacije i server posrednika vrši se u šifrovanom obliku gdje je korišten ENIGMA princip, zasnovan na tri rotora (Sl. 4.).

.



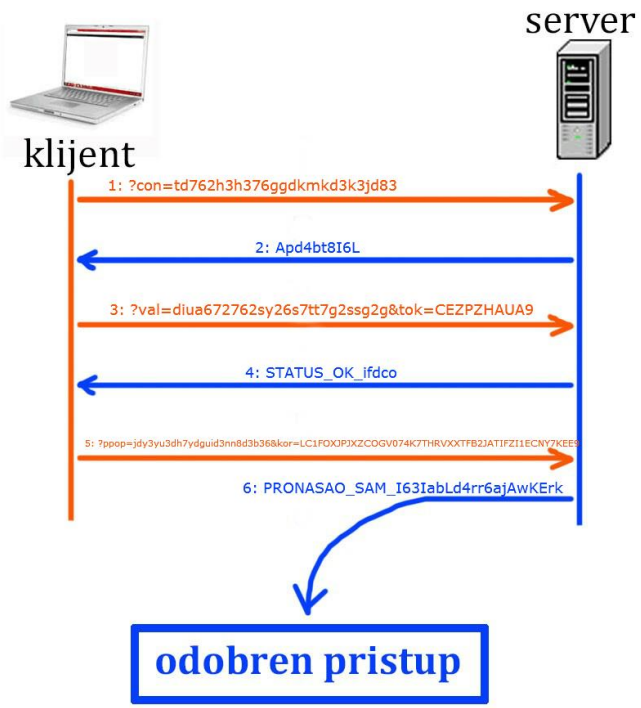
Sl. 4. ENIGMA kriptografski princip rada. Na slici je prikazan primjer dijela od sva tri rotora, gdje se za istu ulaznu vrijednost dobija različit izlaz, zavisno od pozicije svakog od tri rotora.

Za formiranje rotora korišteni su nizovi slova i brojeva, gdje je svaka pozicija rotora povezana sa tačno jednom pozicijom na narednom rotoru.

Prvo se izvrši postavljanje početne pozicije po definisanom ključu, pa se pri svakom sledećem unosu prvi rotor okrene za jedno mjesto (polje), kada prvi rotor napravi pun krug, drugi se okreće za jedno polje. Isto važi i za sledeći rotor, tako da će izlaz zavisiti ne samo od ulaznog karaktera već i od pozicije rotora.

Obzirom da aplikacija čiji je princip rada opisan u ovom radu koristi slučajne vrijednosti za prenos, to će smanjiti vjerovatnoću dešifrovanja prenosnog niza karaktera.

Identifikacija se realizuje kroz šest faza (Sl. 5.).



Sl. 5. Na slici su prikazane faze identifikacije korisnika i primjer poruka koje razmjenjuju klijent i server: 1. klijent šalje zahtjev za pristup (?con=td762h3h376ggdkmkd3k3jd83); 2. server odgovara nizom slučajnih karaktera a niz dobijen kao: enigma(enigma(niz slučajnih karaktera)) upisuje u bazu podataka (Apd4bt8I6L); 3. klijent odgovara serveru sa enigma(niz slučajnih karaktera koji je dobio od server u prethodnok koraku) (?val=diua672762sy26s7tt7g2ssg2g&tok=CEZPZHAUA9); 4. server šalje novi niz slučajnih karaktera koji klijent koristi kao dodatak ključu za šifrovanje pristupnog imena i pristupne šifre (STATUS_OK_ifdco); 5. klijent šalje ime i šifru u kriptovanom obliku (?ppop=jdy3yu3dh7ydguid3nn8d3b36&kor=LC1FOXJPJXZCOGV074K7THRVXXTFB2JATIFZI1ECNY7KEE9); 6. server u bazu podataka sa tabelom korisnika upisuje niz slučajnih karaktera koji će u budućem komuniciranju sa klijentom zahtijevati od klijenta, isti šalje klijentu sa odobrenjem pristupa (PRONASAO_SAM_I63IabLd4rr6ajAwKErk).

Osnovni cilj identifikacije je provjera korisnika i sticanje povjerenja između korisničke aplikacije i serverskog dijela, nakon čega server šalje odobrenje klijentu.

U svakoj od faza identifikacije provjerava se klijentova ip adresa, pa u slučaju promjene iste proces se vraća na početne parametre.

Komunikacija između članova slijedi nakon dobijanja serverskog odobrenja. U ovoj fazi se prelazi na šifrovanje Plejfer šifrom, gdje je server stekao povjerenje klijentske aplikacije i može da počne sa slanjem poruka. Server u ovoj fazi prelazi na posrednički režim rada, identifikaciju vrši na osnovu tokena (stringa) koji je dobio sa odobrenjem korisnika.

Šifrovanje svake poruke koja se šalje vrši se drugim ključem, koji se formira tako što se tajnom ključu sa lijeve strane dodaje slučajni niz karaktera koji se prenosi serveru, a on šalje korisniku koji čita poruku.

Server kao posrednik komunikacije nije u mogućnosti da dešifruje poruke koje se razmjenjuju izmedju korisnika i ne posjeduje mehanizam Plejfer šifre.

Nakon što klijent pročita poruku sa servera, koja je namijenjena za njega, sistem je briše iz baze podataka.

Za očuvanje integriteta poruke zadužena je md5 heš funkcija kojom korisnička aplikacija formira heš string i šalje poruku zajedno sa heš stringom koji se prenose pri svakom slanju i prijemu poruke. Prilikom prijema poruke, od strane klijentske aplikacije, poruka se dešifruje, a zatim se formira heš string md5 funkcijom čiji je ulazni parametar dešifrovana poruka i taj heš se upoređuje sa hešom dobijenim od strane servera. U slučaju ne poklapanja korisniku se prikazuje poruka uz napomenu da je došlo do njene promjene tokom prenosa.

IX. ZAKLJUČAK

Računar je postao neizostavna komonenta života, proizvodne i druge mašine upravljane od strane računara i aplikativnih prorama sve više zamjenjuju radna mjesta ljudi. Računarski sistemi su postali kritična infrastruktura današnjice, sve je veći broj napada i sve više se govori o zaštiti kritičnih informacionih infrastruktura ali i privatnosti korisnika na globalnoj mreži.

Čim se javila potreba za prenosom informacija, javila se i potreba za njenim skrivanjem od neželjenih pogleda, pa su tako nastale različite metode skrivanja otvorenog teksta i njegovo konvertovanje u šifrovan oblik.

Rad razmatra jedno od rješenja zaštite informacija i šifrovanu razmjenu informacija između učesnika. Modifikacijom Plejfer šifre dobijena je znatno složenija šifra zadržavajući isti šifarski princip i snagu.

Aplikacija, koja prati ovaj rad, programirana je na objektnoorjentisanom principu i pruža veliku skalabilnost i modularnost čija snaga leži u promjeni kriptografskih algoritama (Plejfer šifre i ENIGME) jednostavnim dodavanjem novih klasa i objekata.

Dodatna zaštita šifrata može se obezbijediti primjenom drugog kriptografskog moda.

LITERATURA

[1] Singidunum, Univerzitet. "KRIPTOLOGIJA I." *Acta facultatis medicae Naissensis* 27.4.
[2] B. Jovanović, "Bezbednost informacija", Zaštita računarskih sistema – skripta za kadete Vojne akademije, 2014 Beograd
[3] D. Koridić, "Sistem čovek – mašina", Vojna psihologija – skripta za kadete Vojne akademije, 2012 Beograd

ABSTRACT

The 21st century can be called the century of information technology, considering that the technology development has brought social changes affecting both lifestyle and other social aspects. Computer systems, besides being a crucial part of the every day life, have also become a critical element of society. The number of attacks on such systems is increasing and so is the need to protect them. The problem of privacy and identity theft on the internet is becoming obvious. This paper presents one of the solutions to protect textual data transfer using a modified Playfair code with the ECB (Electronic CodeBook)

mode, using dynamically generated keys. The application monitoring this process is coded using the C# progamming language.

Encrypted communication using a modified Playfair cipher

Dušan Perišić, Andrija Karadžić, Ognjen Letić, Ivan Tot