UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"
FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE

Tema:Algoritmi PlayFair Ciper

Lënda:Siguria e te dhenave

Grupi 8:
Florian Shabani
Jon Sadiku
Syard Dauti

Profesor:
Besnik Duriqi

Permbajtja:

1.Pershkrimi i algoritmit Playfire cipher

Ne kuader te shkences kompjuterike,konkretisht te Kriptologjise qe eshte shkence qe merret me komunikimin dhe ruajtjen e të dhënave në formë të sigurt dhe zakonisht sekrete,eshte i definuar termi i Kriptografise qe është studimi i teknikave të komunikimit të sigurt që lejojnë vetëm dërguesin dhe marrësin e synuar të një mesazhi të shikojë përmbajtjen e tij[1].

Komunikin e sigurt te cilin e ofron kriptografia eshte i bere permes procesit te enkriptimit dhe dekriptimit,kriptimi.është një proces kompjuterik që kodon tekstin e thjeshtë/tekstin e qartë (të lexueshme nga njeriu) në tekst të koduar (të dhëna të palexuara) që është i aksesueshëm vetëm nga përdoruesit e autorizuar me çelësin e duhur kriptografik.Ndersa dekriptimi eshte proces i kudert enkriptues,pra, ka te beje me kalimin e te dhenave te koduara ne formen e tyre origjinale[2].

Ne kuader te shume teknikve kriptografike te cilat kane egzistuar,permes se cilave eshte ruajtur integriteti i te dhenave,njihet edhe teknika Playfire cipher.

Teknika e enkriptimit Playfair cipher mund të përdoret për të enkriptuar ose koduar mesazhe. Ajo funksionon saktësisht si kriptimi tipik.I vetmi ndryshim është se ai kodon një digraf, ose një palë dy shkronja, në krahasim me një shkronjë të vetme[3].

2.Historiku i zhvillimit te algoritmit.

Shifra Playfair u shpik në 1854 nga Sir Charles Wheatstone, një shkencëtar dhe shpikës britanik. Megjithatë, ai e emërtoi sipas mikut dhe shpikësit të tij, Baron Lyon Playfair, i cili ndihmoi në popullarizimin e shifrës.[4]

Fillimisht, shifra Playfair u përdor kryesisht nga organizatat ushtarake dhe qeveritare për të mbrojtur informacionin e ndjeshëm. Megjithatë, ajo shpejt fitoi popullaritet në mesin e grupeve të tjera, duke përfshirë gazetarët, diplomatët dhe madje edhe kriminelët.[5]

Gjatë viteve, disa modifikime dhe përmirësime janë bërë në shifrën Playfair, por parimet bazë mbeten të njëjta. Sot, ajo konsiderohet të jetë një metodë relativisht e dobët e kriptimit në krahasim me algoritmet më moderne të ditëve te sotme, por ende mban një vend të veçantë në historinë e kriptografisë.[6]

3.Implementimi i algorimit PlayFire Cipher

3.1.Enkritimi permes algoritmit PlayFire Cipher

Enkriptimi ne menyre manuale duke ndjekur algoritmin PlayFire Cipher,behet ashtu qe fillimisht krijohet nje matrice e rendit 5 x 5.Ne enkriptimin duke perdorur PayFire Ciper perdoret qelsi i cili paraqet tekst.Pas krijimit te matrices teksti i perdorur si qeles ndahet karakter per karakter dhe cdo karakter unik,vendoset radhazi ne matrice duke filluar me mbushjen e rreshit te pare,pas vendosjes ne matrice te karaktereve unike te cilat e perbejne qelsin,ne kolonat tjera te kolonat matrices vendosen shkronjat tjera te cilat nuk jane te perfshira ne qeles duke filluar nga shkronja “A”.
Meqense matrica 5 x 5,permbane gjithsej 25 kolona numri maksimal i shkronja te mundeshme qe te vendosen ne kolona eshte 25,meqense alfabeti anglez permbane 26 shkronja per ti ikur keti konfrontimi shkronja i dhe j ndaje nje kolone te perbashket.Figura 3.1, paraqet mbushjen e matrices ku si fjale kyqe eshte perdorur fjala “MONARCY”[5].

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

Fig3.1-Plotesimi i Matrices.

Pas plotesimit te matrices fjala e cila do te enkriptohet ndahet ne karaktere cifte(nga 2).Egzistojne disa kushte te cilat ciftet e karakterve i plotesjne.:
1.Karakteret e dhena te cilat ndahen duhet te jene cifte.Ne rast se jo,atehere nje “x” shtohet tek karakteri i fundit p.sh:
PRISHTINA—————”PR” “IS” “HT” “IN” “A**X”**

2.Brenda cdo cifti te karaktereve shkronjat duhet te jene unike,ne rast te mos arritjes se unicitet nje x shtohet tek karkteri i dyte brenda ciftit.P.sh:
“BALLOON”—————”BA” “L**X**” “LO” “ON”

Pas caktimit te karaktereve,ato krahasohen me pozicionet ne matrice.Duke pas parasyshe qe dy shkronja te vendosura ne matrice mund te jene ne te njejten kolone,rresht ose nuk mund te priten fare,egzistojne disa teknika te kodimit te cifteve:
1.Nese karakteret ndodhen te njejtin rresht atehere enkriptimi i atyre behet duke zevendesuar ciftin e shkronjave me shkronjat ne te djathten e tyre P.sh:
Cifti i shkronjave “ON”,zevendesohet me ciftin e shkronjave “NA”
2..Nese karakteret ndodhen te njejten kolone atehere enkriptimi i atyre behet duke zevendesuar ciftin e shkronjave me shkronjat poshte tyre P.sh:
Cifti i shkronjave “ME”, zevendesohet me ciftin e shkronjave “CL”
3.Nese shkronjat nuk pritnen ne rresht,kolone atehre krijohet nje drjetkendesh nga i cili ne kulmet e diagonales mbyllet me karakteret e ciftit,enkriptimi i karaktereve behet duke zevendesuar ato me karakteret te cilat ndodhen ne kulmet e kunderta te rreshtave perkates p.sh
Cifti i shkronjave “AT”, zevendesohet me ciftin e shkronjave “RS”[6].

A	R
B	D
I/J	K
S	T

Fig 3.2.Zv. ne kolona/rreshta te ndryshem

Enkriptimi i fjales “ATTACK” duke perdorur algoritmin PlayFire Cipher behet si ne figuren 3.3.

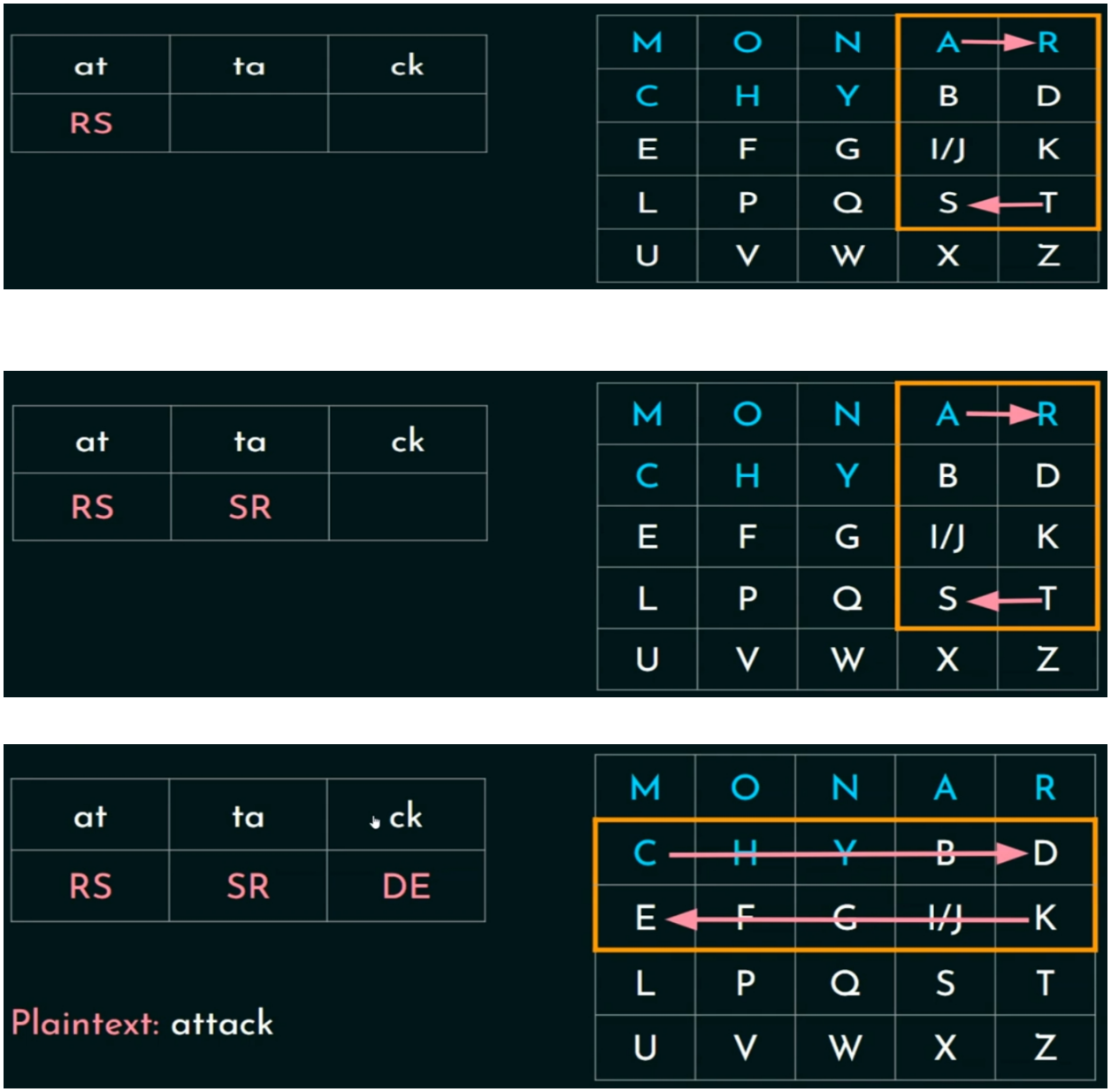

Figura 3.3:Enkriptimi i tekstit “ATTACK”

3.2. Dekriptimi permes algoritmit PlayFire Cipher

Dekriptimi duke perdorur algoritmin PlayFire Cipher,behet duke u mbeshtetur ne matricen qe eshte perdorur per enkriptim.Pas kesaj fjala e koduar ndahet ne karaktere,karakteret ne cife zevendesohen duke perdorur rregullat e kunderta te enkriptimit,keshtu qe nese:

1.shkronjat ndodhen ne te njejtin rresht te matrices atehere ato zevendesohen me shkronjat ne te majten e tyre

2.shkronjat ndodhen ne te njejten kolone te matrices atehere ato zevendesohen me shkronjat qe ndodhen lart tyre.

3.shkronjat nuk ndajne rresht/kolone te perbashket atehere krijohet drejtkendeshi i cili ne kulmet e kunderta permbane karakteret,dekriptimi behet duke zevendesuar karakteret perkatese me karakteret te cilat ndodhen ne kulmet e kunderta te rreshtave perkates.

Figura 3.4 paraqet dekriptimin e fjales koduese “GATLMZCLRQTX”me qe ratst fitohet fjala insruementsz.Enkodimi karakter pas karakteri jepet si[7]:

```
ga -> in
tl -> st
mz -> ru
cl -> me
rq -> nt
tx -> sz
```

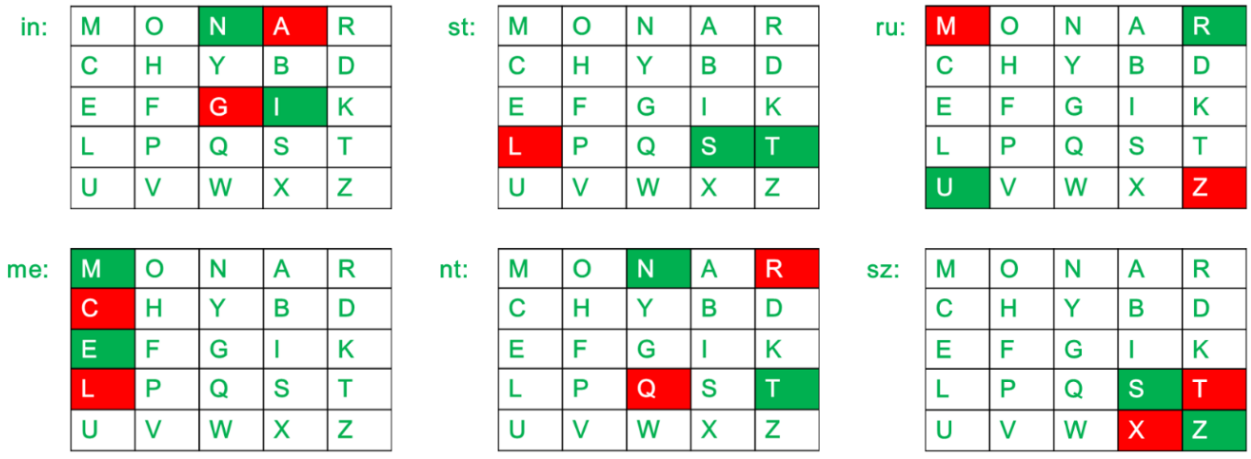

Fig.3.4 Procesi i dekriptimit te fjales GATLMZCLRQTX

5.Sulmimi i Algoritmit

Kodimi permes algoritmit playfire cipher është më i ndërlikuar se një kodim zëvendësuese, por i lehtë për t'u thyer duke përdorur qasje të automatizuara.Njera nga qasjet me te njohura e cila perdoret per ta thyer kete algoritem eshte duke u bazuar ne ate se cilat cifte te karaktereve perdoren zakzonisht me se afermi e njohur si frekuenca e qifteve te karaktereve.Meqense ne kete alogritem evendesimi bazohet ne ciftet e karaktereve kjo metode fshine statistikat e shkronjave te vetme,por me gjithe ate frekuencat e çifteve të shkronjave mbeten te pandryshuara,dhe ne baze te statistikave çiftet e shkronjave kanë një shpërndarje shumë 'më të sheshtë' sesa frekuencat e një shkronje të vetme,andaj kjo bene qe metoda e frekuences se shkronjave te jete me e suksesehme ne thyerjen e ketij algoritmi[8].Ne baze te statistikave ciftet e shkronjave te cilat me se shpeshti perdoren jane :TH, IN, ER, RE, AN, HE, AR, EN, TI, TE, AT, ON, HA, OU, IT[9]

5.Konkluzion

Si përfundim, shifra Playfair është një algoritëm interesant kriptimi me një histori të pasur. Ndonëse mund të mos jetë aq e sigurt sa metodat moderne të kriptimit, ajo ende ka vendin e saj në fushën e kriptografisë.

Duke eksploruar Algoritmin e shifrës Playfair, ne kemi fituar një kuptim më të mirë se si funksionon dhe si është përdorur gjatë historisë. Ne kemi mësuar gjithashtu për zhvillimin e tij dhe modifikimet dhe përmirësimet e ndryshme që janë bërë gjatë viteve.

Në përgjithësi, shifra Playfair është një pjesë e rëndësishme e historisë së kriptografisë dhe ia vlen të studiohet për këdo që është i interesuar në këtë fushë magjepsëse.

6.Referencat

[1].Cryptology | Definition, Examples, History, & Facts | Britannica
[2].What is Cryptography? Definition, Importance, Types | Fortinet
[3].What is Playfair Cipher? Example and Rules (intellipaat.com)
[4].Singh, S. (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor.
[5].Kahn, D. (1967). The Codebreakers: The Story of Secret Writing. Macmillan.
[6].Knight, C. (2011). Mathematical Recreations: A Collection in Honor of Martin Gardner. Dover Publications.
[7].Playfair Cipher with Examples - GeeksforGeeks
[8].Playfair Cipher - Crypto Corner (interactive-maths.com)
[9].Playfair Cipher Decryption | by Ruthu S Sanketh | Towards Data Science
[10].Practical Cryptography
[11].Cryptanalysis - The Playfair Cipher 101 (weebly.com)