SHIFRIMI AFIN

Rreze Vrapçani[#1]
FSHMN - Shkencë Kompjuterike
Universiteti i Prishtinës
Prishtinë, Kosovë, 10000
1 rreze.vrapcani@student.uni-pr.edu

Erë Dedinca[#2]
FSHMN - Shkencë Kompjuterike
Universiteti i Prishtinës
Prishtinë, Kosovë, 10000
2 ere.dedinca@student.uni-pr.edu

Rubina Berisha[#3]
FSHMN - Shkencë Kompjuterike
Universiteti i Prishtinës
Pejë, Kosovë, 10000
3 rubina.berisha@student.uni-pr.edu

Abstrakt: **Në këtë punim do të përfshihen disa detaje në lidhje me shifrimin afin, do të spjegohet algoritmi përkatës, do ceken disa nga përparësitë e mangësitë e përdorimit të këtij algoritmi dhe më tutje përfshihet implementimi I këtij algoritmi duke përdorur gjuhën programuese Java. Gjithashtu paraqiten edhe shembuj me anë të të cilëve është ilustruar se si bëhet enkriptimi dhe dekriptimi I mesazheve.**

Fjalë kyçe: Kriptografia, Afin, algoritëm, enkriptim, dekriptim, siguri.

I. KRIPTOGRAFIA

Kriptografia (nga greq. κρυπτός, kriptos - i fshehtë, dhe γραφία, grafia - shkrim) është shkenca e kodimit dhe e përçimit të informacioneve dhe të dhënave të fshehta (sekrete). Qëllimi kryesor i kriptografisë është fshehja e kuptimit të mesazheve, por zakonisht jo ekzistencës së tyre. Kriptografia përkufizohet sipas kriptografit të njohur Ron Rivest si "komunikimi në prani të kundërshtarëve". Ajo është pjesë qëndrore e disa fushave: sigurimit të informacioneve dhe çështjeve përkatëse, veçanërisht identifikimit dhe kontrollit hyrës. Kriptografia luan një rol të rëndësishëm edhe në informatikë, veçanërisht në teknikat e përdorura në sigurinë kompjuterike dhe rrjetore, si p.sh. kontrolli hyrës apo të së drejtës së përdorimit të një aparati kompjuterik dhe besueshmërisë së informacioneve. Kriptografia përdoret gjithashtu në shumë zbatime që ndeshen në jetën e përditshme, si fjalëkalimet kompjuterike, kartat bankare dhe tregtinë elektronike. Kriptografia së bashku me kriptoanalizën formojnë kriptologjinë [1].

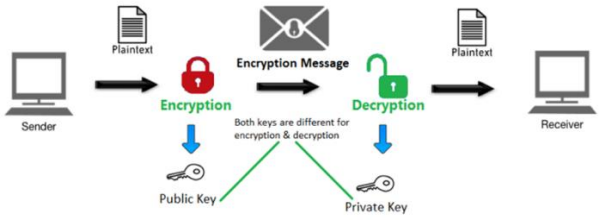

Figura 1. Ilustrim i përcjelljes së mesazhit

II. HISTORIA

Kriptografia thuhet të jetë një nga fushat më të vjetra të hulumtimeve teknike për të cilën mund të gjenden gjurmë nga historia njerëzore deri në 4000 vite më parë. Hieroglifët dekoronin varret e sundimtarëve dhe mbretërve. Këto shkrime me hieroglifë tregonin historitë jetësore të mbretërve duke shpalosur edhe veprimet fisnike të tyre. Kinezët e lashtë përdornin natyrën ideografike te gjuhës së tyre për të fshehur domethënien e fjalëve. Mesazhet zakonisht transformoheshin në ideografe për qëllime intimiteti. Për dallim nga Egjipti dhe Kina, në Indi shkrimet sekrete ishin dukshëm më të avancuara, përfshi këtu qeveritë e asokohshme, të cilat përdornin kodet e fshehura për të komunikuar me spiunët e shpërndarë nëpër gjithë vendin.

Historia e kriptografisë të Mesopotamisë ishte e ngjashme me atë të Egjiptit dhe shkrimi

kuneiform përdorej për të shifruar tekstin. Në dramën e famshme greke “Iliada”, kriptografia është përdorur në rastin kur Bellerophoni është dërguar te mbreti me një pllakë sekrete, e cila po i kërkonte mbretit ta dënonte atë me vdekje. Spartanët pardonin një sistem të përbërë nga një fletë e hollë e papirusit e mbështjellë rreth një shtize (sot quhet “shifrues prej shtize”). Një metodë tjetër e kriptografisë qe zhvilluar nga Polybius (tashmë quhet “katrori i Polybius”). Jul Cezari përdorte sistemin kriptografik (i quajtur “Shifruesi i Cezarit”), i cili zhvendos dy shkronja më tej nëpër tërë alfabetin. Arabët ishin të parët që bënë përparim të dallueshëm në fushën e kriptoanalizës. Një autor arab, Qalqashandi, zhvilloi një teknikë për zbulimin e shifrimit, e cila përdoret edhe në ditët e sotme [2].

III. LLOJET E KRIPTOGRAFISË

Si themeli i sistemeve moderne të sigurisë, kriptografia përdoret për të siguruar transaksione dhe komunikime, për të mbrojtur informacionin personal të identifikueshëm (PII) dhe të dhëna të tjera konfidenciale, për të vërtetuar identitetin, për të parandaluar ndërhyrjet e dokumenteve dhe për të vendosur besimin midis serverëve. Kriptografia është një nga mjetet më të rëndësishme që bizneset përdorin për të siguruar sistemet që mbajnë asetin e saj më të rëndësishëm – të dhënat – qofshin ato në pushim apo në lëvizje [3].

KRIPTOGRAFIA ME ÇELËS PRIVAT

Përdor vetëm një çelës. Me anë të këtij çelësi, mesazhi i dhënë në formë të lexueshme do të enkriptohet në mesazh të pakuptueshëm me gjatësi të përafërt sa edhe i lexueshmi. Në rastin e de-enkriptimit, përdoret i njëjti çelës që është përdorur për enkriptim. Nganjëherë, kriptografia me çelës të fshehur quhet edhe kriptografi tradicionale apo simetrike. Kodi Captain Midnight dhe MonoAlphabetic paraqesin dy lloje të algoritmeve të çelësit të fshehur, edhe pse tashmë për të dy ekzistojnë dëshmi se thyhen lehtë. Shembuj të kriptografisë me çelës të fshehur janë: DES, Triple DES apo 3DES, International Data Encryption Algorithm (IDEA) dhe AES.

KRIPTOGRAFIA ME ÇELËS PUBLIK

Kriptografia me çelës publik apo kriptografia asimetrike, është një disiplinë e re e shpikur më 1975. Për dallim nga kriptografia me çelës të fshehur, në kriptografinë me çelës publik çelësat nuk ndahen. Këtu, secili individ ka dy çelësa: çelësi privat, që nuk duhet t’i zbulohet askujt dhe çelësi publik, që preferohet të jetë i ditur për secilin [4]. Dallim tjetër i kriptografisë me çelës publik është edhe mundësia e gjenerimit të nënshkrimit dixhital në mesazh. Nënshkrimi dixhital është një numër i lidhur me mesazhin, që gjenerohet vetëm nga individi që ka çelësin privat. Shembuj të kriptografisë me çelës publik janë: RSA, DSS, ElGamal, Diffie-Hellman, Zero Knowledge Proof Systems, Pretty Good Privacy (PGP) dhe Elliptic Curve Cryptography (ECC).

ALGORITMET HASH

Algoritmet Hash ndryshe njihen edhe si përvetësuesit e mesazhit ose transformuesit me një drejtim. Funksioni kriptografik hash është një transformim matematik i mesazhit me gjatësi arbitrare në një gjatësi bitësh nga e cila do të njehsohet numri me gjatësi fikse. Algoritmet hash nuk përdorin çelësa për veprimet e tyre. Shembuj të algoritmeve hash janë: Secure Hash Algorithm – 1 (SHA – 1) dhe Message Digest (MD2, MD4 dhe MD5) [4].

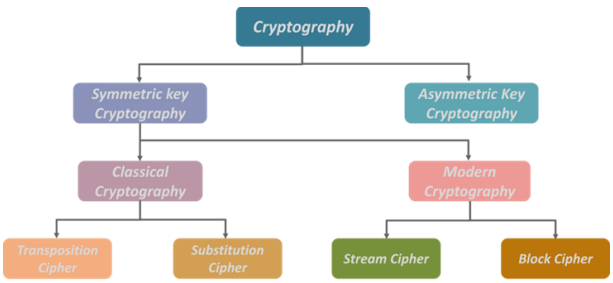

Figura 2. Llojet e Kriptografisë

IV. SHIFRIMI AFIN

Shifrimi Affin është një lloj shifrimi zëvendësues monoalfabetik, ku çdo shkronjë në një alfabet është hartuar me ekuivalentin e saj numerik, i koduar duke përdorur një funksion të thjeshtë matematikor dhe kthehet përsëri në një shkronjë. Formula e përdorur do të thotë që çdo shkronjë kodon në një shkronjë tjetër dhe përsëri, që do të thotë se shifra është në thelb një shifër zëvendësuese standarde me një rregull që rregullon se cila shkronjë shkon në cilën.

I gjithë procesi mbështetet në punën e modulit m (gjatësia e alfabetit të përdorur). Në shifrimin afin, shkronjat e një alfabeti me përmasa m fillimisht krahasohen me numrat e plotë në rangun 0 … m-1.

"Çelësi" për shifrën Affine përbëhet nga 2 numra, ne do t'i quajmë ata a dhe b. Diskutimi i mëposhtëm supozon përdorimin e një alfabeti me 26 karaktere (m = 26). a duhet të zgjidhet të jetë relativisht i thjeshtë me m (d.m.th. a nuk duhet të ketë faktorë të përbashkët me m).

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Figura 3. Indeksat e shkronjave

ENKRIPTIMI

Ai përdor aritmetikën modulare për të transformuar numrin e plotë që i korrespondon çdo shkronje e tekstit të thjeshtë (plaintext) në një numër tjetër të plotë që korrespondon me një shkronjë të tekstit shifror (ciphertext) [5]. Funksioni i enkriptimit për një shkronjë të vetme është:

$$E(x) = (a\,x + b) \bmod m$$

modulus m: size of the alphabet
a and b: key of the cipher.
a must be chosen such that a and m are coprime

DEKRIPTIMI

Në deshifrimin e tekstit të shifruar, ne duhet të kryejmë funksionet e kundërta (ose të anasjellta) në tekstin e shifruar për të marrë tekstin e thjeshtë. Edhe një herë, hapi i parë është konvertimi i secilës prej shkronjave të tekstit të koduar në vlerat e tyre të plota. Funksioni i deshifrimit është:

$$D(x) = a^{-1}(x - b) \bmod m$$

a^{-1}: modular multiplicative inverse of a modulo m. i.e., it satisfies the equation

$$1 = a\,a^{-1} \bmod m$$

GJETJA E INVERZIT

Duhet të gjejmë një numër x të tillë që:

Nëse e gjejmë numrin x të tillë që ekuacioni të jetë i vërtetë, atëherë x është e anasjellta e a-së dhe e quajmë a^{-1}. Mënyra më e lehtë për të zgjidhur këtë ekuacion është të kërkoni secilin nga numrat 1 deri në 25 dhe të shihni se cili e plotëson ekuacionin.

```
[g,x,d] = gcd(a,m);
x = mod(x,m);
```

Nëse tani shumëzoni x dhe a, dhe zvogëloni rezultatin (mod 26), do të merrni përgjigjen 1. Ky është vetëm përkufizimi i një inversi, d.m.th. nëse a*x = 1 (mod 26), atëherë x është një invers i a-së (dhe a është një invers i x-it) [3].

SHEMBULL

Encryption: Key Values a=17, b=20

Original Text	T	W	E	N	T	Y		F	I	F	T	E	E	N
x	19	22	4	13	19	24		5	8	5	19	4	4	13
ax+b % 26*	5	4	10	7	5	12		1	0	1	5	10	10	7
Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H

Decryption: a^-1 = 23

Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H
Encrypted Value	5	4	10	7	5	12		1	0	1	5	10	10	7
23 *(x-b) mod 26	19	22	4	13	19	24		5	8	5	19	4	4	13
Decrypted Text	T	W	E	N	T	Y		F	I	F	T	E	E	N

Figura 4. Shembull

IV. SHIFRIMI AFIN HAP PAS HAPI

Supozoni se duam të kodojmë mesazhin "beach" duke përdorur një shifër afinale me çelësin e enkriptimit (3, 1)

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 5. Indeksat

i. Duke përdorur tabelën, ne mund të paraqesim shkronjat në mesazhin tonë "plazh" me numrat e tyre përkatës: 1 4 0 2 7.

ii. Tani shumëzojmë secilin nga numrat nga hapi (i) me numrin e parë në çelësin e enkriptimit, (3 në këtë rast), për të marrë: 3 12 0 6 21.

iii. Më pas, shtoni numrin e dytë në çelësin e enkriptimit, (1 në këtë rast), në secilin prej numrave nga hapi (ii) për të marrë: 4 13 1 7 22.

iv. Tani përdorni tabelën për të zëvendësuar numrat nga hapi (iii) me shkronjat e tyre përkatëse për të marrë tekstin e koduar: ENBHW.

Ashtu si me shifrat e zhvendosjes, ka një ndërlikim të vogël kur aritmetika që bëjmë në hapat (ii) dhe (iii) më sipër prodhon një numër që është më i madh se 25. Për shembull, nëse marrim parasysh tekstin e ri të thjeshtë "surf" dhe përdorim çelësin e enkriptimit (3,1) përsëri, atëherë teksti shifror që rezulton është "NRLN". Kriptimi duket në këtë mënyrë:

$$\text{surf} \xrightarrow{i} 18,20,17,5 \xrightarrow{ii} 54,60,51,15 \xrightarrow{iii}$$

$$55,61,52,16 \xrightarrow{*} 3,9,0,16 \xrightarrow{iv} \text{DJAQ}$$

Çdo numër është zëvendësuar nga grupi i numrave {0,..., 25} që është në përputhje me të modulo 26. Si përmbledhje, enkriptimi afin në alfabetin anglez duke përdorur çelësin e enkriptimit (α, β) realizohet nëpërmjet formulës $y \equiv \alpha x + \beta \pmod{26}$.

Për një shembull tjetër, kriptimi i tekstit të thjeshtë "sail" duke përdorur një shifër afine me çelësin e enkriptimit (3,7) prodhon tekstin e koduar "JHFO" në këtë mënyrë:

$s \rightarrow 18 \rightarrow 3 \cdot 18 + 7 \equiv 9 \pmod{26} \rightarrow J$

$a \rightarrow 0 \rightarrow 3 \cdot 0 + 7 \equiv 7 \pmod{26} \rightarrow H$

$i \rightarrow 8 \rightarrow 3 \cdot 8 + 7 \equiv 5 \pmod{26} \rightarrow F$

$l \rightarrow 11 \rightarrow 3 \cdot 11 + 7 \equiv 14 \pmod{26} \rightarrow O$

Si rikuperohet mesazhi origjinal (plain text) nga teksti i enkoduar nëse dihet çelësi i enkriptimit? Teksti i mëposhtëm shifror u prodhua duke përdorur një shifër afine me çelësin e enkriptimit (3,7): QTORHG. Për ta deshifruar atë (d.m.th., për të rikuperuar mesazhin me tekst të thjeshtë), ne mund të kthejmë hapat në enkriptim: së pari shtojmë 19 (ose zbresim 7) në secilin prej numrave që përfaqësojnë tekstin e shifruar shkronjat, më pas shumëzojeni rezultatin me 9. Ajo që kemi bërë mund të përmblidhet me formulën $x \equiv 9(y + 19) \pmod{26}$, ose, më thjesht, me $x \equiv 9y + 15 \pmod{26}$, (shënim $9 \cdot 19 \equiv 15 \pmod{26}$). Këtu (9,15) është çelësi i deshifrimit për shifrën afinale me çelësin e enkriptimit (3,7).

$Q \rightarrow 16 \rightarrow 9 \cdot 16 + 15 \equiv 3 \pmod{26} \rightarrow d$

$T \rightarrow 19 \rightarrow 9 \cdot 19 + 15 \equiv 4 \pmod{26} \rightarrow e$

$O \rightarrow 14 \rightarrow 9 \cdot 14 + 15 \equiv 11 \pmod{26} \rightarrow l$

$R \rightarrow 17 \rightarrow 9 \cdot 17 + 15 \equiv 12 \pmod{26} \rightarrow m$

$H \rightarrow 7 \rightarrow 9 \cdot 7 + 15 \equiv 0 \pmod{26} \rightarrow a$

$G \rightarrow 6 \rightarrow 9 \cdot 6 + 15 \equiv 17 \pmod{26} \rightarrow r$

Tani le të shpjegojmë pse kemi shumëzuar me 9 në deshifrimin e mësipërm. Ne po përpiqeshim të zgjidhnim kongruencën e kriptimit

$y \equiv 3x + 7 \pmod{26}$

për ndryshoren x në terma y. Së pari, shtuam 19 në të dyja palët për të marrë

$$y + 19 \equiv 3x + 26 \pmod{26},$$

Meqenëse po punojmë modulin 26, kjo është e barabartë me

$$y + 19 \equiv 3x \pmod{26}.$$

Në këtë pikë, ne duam të izolojmë x. Nëse ky do të ishte një ekuacion në vend të një kongruence, ne mund ta bënim këtë duke shumëzuar të dyja anët me 1/3. Megjithatë, nuk është kurrë një ide e mirë që të futen thyesat në një kongruencë. Por ne mund t'i shumëzojmë të dyja anët me një numër të plotë. Numri i plotë që na nevojitet duhet të ketë efektin e zëvendësimit të 3 me një 1. Pra, ne duam të shumëzojmë me një numër të plotë a të tillë që $3a \equiv 1 \pmod{26}$. Nga inspektimi, zbulohet se $3 \cdot 9 = 27 \equiv 1 \pmod{26}$, pra 9 është shumëzuesi ynë i dëshiruar. Duke e përdorur atë, arrijmë në

$$9(y + 19) \equiv 9 \cdot 3x \equiv x \pmod{26}.$$

Në këtë pikë, ne mund të shpjegojmë plotësisht se çfarë përfshin një çelës kriptimi të vlefshëm (α, β). Në mënyrë që shifra të jetë e dobishme, procesi i enkriptimit duhet të jetë i kthyeshëm, d.m.th., (α, β) duhet të ketë një çelës deshifrimi të lidhur, le të themi (γ, δ). Në mënyrë që γ dhe δ të ekzistojnë, çfarë duhet të jetë e vërtetë për α dhe β? Duke parë shembullin e mësipërm, vëmë re se na duhej të zbritnim β nga të dyja anët e kongruencës së enkriptimit. Kjo është e mundur për çdo vlerë të β. Por më vonë, na duhej të shumëzonim të dyja anët e një kongruence me një numër të plotë a (a = 9 në shembull) në mënyrë që $\alpha a \equiv 1 \pmod{26}$. Kjo nuk është e mundur për çdo numër të plotë α në grupin $\{0, 1,.., 25\}$: qartë $\alpha = 0$ nuk funksionon, por ka elementë jozero të grupit që gjithashtu nuk funksionojnë. Për shembull, nëse do të kishim zgjedhur $\alpha = 2$, atëherë do të përpiqeshim të gjenim një numër të plotë të tillë që $2a \equiv 1 \pmod{26}$, që është ekuivalente me $2a - 1$ të ndahet me 26. Meqenëse $2a - 1$ është gjithmonë tek, nuk mund të pjesëtohet kurrë me numrin e plotë çift 26. Pra, nuk mund të përdorim $\alpha = 2$ në një çelës enkriptimi afin ku grupi i karaktereve ka 26 shkronja.

Cilat vlera tjera të α nuk mund të përdoren? Rezulton se nëse α ka një faktor tjetër përveç ± 1 të përbashkët me 26, atëherë nuk është një zgjedhje e vlefshme për një çelës enkriptimi. Çelësat e vlefshëm të enkriptimit (për një grup karakteresh me 26 shkronja) janë të formës (α, β), ku $\alpha, \beta \in \{0, 1, \dots, 25\}$ dhe $\gcd(\alpha, 26) = 1$.

Një vlerë e α që funksionon është $\alpha = 11$. Cili është numri i plotë a i tillë që $\alpha \cdot a \equiv 1 \pmod{26}$? Duke testuar mundësitë ndërmjet 0 dhe 25, shohim se $19 \cdot 11 = 209 \equiv 1 \pmod{26}$, pra a = 19 është numri i plotë i dëshiruar. Kështu, për shembull, nëse (11, 14) është çelësi ynë i enkriptimit, atëherë çelësi i deshifrimit është (19, 20) [6].

V. PËRFUNDIMI

Me aplikimin e kompjuterëve kuantik, kriptografia do të gjente akoma më shumë zbatim se ç'përdoret sot. Është interesant fakti që aplikacioni i parë i kompjuterit kuantik të ditëve të sotme i përket fushës së enkriptimit, ku një kod enkriptimi i rëndomtë (dhe me i mirë), i njohur si RSA, bazohet kryesisht ne vështirësitë e faktorizimit të numrave të mëdhenj të përbërë në primet e tyre. Kështu, po që se kompjuterët kuantik një ditë bëhen realitet, atëherë ekziston potencial i madh që një transformim radikal të ndodhë në fushën e kriptografisë. Kjo për faktin që natyra e kriptosistemeve ekzistuese tashmë të aplikuara në kompjuterët klasik do të duhej të modifikohej për të qenë të përshtatshëm për aplikim dhe përdorim në llojin e kompjuterëve kuantik.

Të gjithë jemi dëshmitarë që ditë e më shumë softuerët për enkriptimin e të dhënave personale dhe avancim të intimitetit po bëhen gjithnjë e më të rëndësishëm dhe me interes për përdoruesin e rëndomtë. Natyrisht, këto aplikacione po mundësojnë qasje, mbartje dhe ruajtje më të

sigurt të të dhënave. Me dashje ose pa dashje, realiteti aktual në internet dhe kudo në rrjete kompjuterike po ndikon që në nivelin e përdoruesve përdorimi i aplikacioneve të bazuar në kriptografi të bëhet standard.

REFERENCAT

[1] ""Kriptografia,"," [Online]. Available: https://sq.wikipedia.org/wiki/Kriptografia..

[2] "Historia e Kriptografise," https://pcworld.al/shkenca-e-kriptografise-te-gjitha-ne-nje-vend/.

[3] Y. Zafar, ""Affin Cipher,"," [Online]. Available: https://www.geeksforgeeks.org/implementation-affine-cipher/..

[4] "Types of Cryptography," [Online]. Available: https://www.naukri.com/learning/articles/types-of-cryptography/.

[5] "Uregina, Affine Ciphers," [Online]. Available: https://uregina.ca/~kozdron/Teaching/Cornell/135Summer06/Handouts/affine.pdf.

[6] ""Math and Cryptography,"," [Online]. Available: https://math.asu.edu/sites/default/files/affine.pdf..

[7] Y. Zafar, "Affin Cipher," https://www.geeksforgeeks.org/implementation-affine-cipher/.