TEMA: SHIFRA VIGENÈRE

LËNDA: SIGURIA E TË DHËNAVE

UNIVERSITETI I PRISHTINËS

PUNOI:
BLEON BALAJ
ELJON KASTRATI

2023

PËRMBAJTJA

ÇFARË ËSHTË KRIPTOGRAFIA KLASIKE?

Kriptografia është arti dhe shkenca e fshehjes dhe zbulimit të informacionit duke përdorur kode dhe shifra.

Është si një bravë dhe një çelës që mbron dhe lejon akses në sekretet e vlefshme apo edhe si një lojë fshehjeje ku dërguesi edhe marrësi kanë rënë dakord për një rrugë të fshehtë për ta gjetur njëri tjetrin në mes të një turme të madhe njerëzish. Kriptografia nuk është vetëm një mjet praktik për sigurinë dhe privatësinë, por edhe një temë magjepsëse për eksplorim dhe zbulim.

Kriptografia klasike është një degë e kriptografisë që merret me enkriptimin dhe deshifrimin e mesazheve duke përdorur teknika matematikore që mund të kryhen me dorë ose me makina të thjeshta. Kriptografia klasike u prezantua për herë të parë në kohët e lashta, kur njerëzit përdornin metoda të ndryshme për të fshehur mesazhet e tyre nga armiqtë ose spiunë. Pra është përdorur për komunikime sekrete.
Në kohët e sotme, kjo formë e kriptografisë nuk përdoret më, mirëpo është shumë më e advancuar me metoda kompjuterike.

FORMAT E PARA TË PËRDORIMIT TË KRIPTOGRAFISE

Kriptografia ka një histori të gjatë dhe magjepsëse që përfshin mijëra vjet dhe qytetërime të ndryshme.

Disa nga format më të hershme të kriptografisë u gjetën në Egjiptin e lashtë, Greqinë dhe Romën, ku skribët përdornin simbole, alfabete ose rregullime jo standarde për të fshehur kuptimin e mesazheve të tyre.

Egjiptianët përdorën hieroglife në mënyra të pazakonta rreth vitit 1900 p.e.s., dhe grekët përdorën një pajisje të quajtur scytale për të mbështjellë një rrip pergamenë rreth një shufre dhe për të shkruar përgjatë gjatësisë së saj.

Romakët përdorën zëvendësimin monoalfabetik me një zhvendosje të thjeshtë ciklike të alfabetit. Julius Caesar përdori një zhvendosje prej tre pozicionesh në mënyrë që teksti i thjeshtë A të kodohej si D, ndërsa August Cezari përdori një zhvendosje të një pozicioni në mënyrë që teksti i thjeshtë A të kodohej si B.

Përpos këtyre kishte edhe mënyra të tjera per fshehjen e informacioneve në kohërat e lashta.

KRIPTOGRAFIA NË KOHËN E MESJETËS DHE RILINDJES

Kriptografia vazhdoi të evoluonte dhe të zhvillohej gjatë Mesjetës dhe Rilindjes, me metoda të ndryshme zëvendësimi, transpozimi, teknika polialfabetike dhe steganografike të shpikur dhe përdorur nga kultura të ndryshme.

Për shembull, arabët prezantuan konceptin e analizës së frekuencës për të thyer shifrat monoalfabetike, dhe gjithashtu zhvilluan disqe shifrore që mund të rrotullonin alfabete të ndryshme.

Europianët përdorën shifra të bazuara në fjalë kyçe, poligrafe ose nule për të fshehur komunikimet e tyre diplomatike ose ushtarake. Një shembull i famshëm është shifra Vigenère, e cila u konsiderua e pathyeshme për shekuj derisa u thye nga Charles Babbage në 1854.

Blaise de Vigenère

TEKNIKAT E KRIPTOGRAFISË KLASIKE

Disa nga teknikat e zakonshme të kriptografisë klasike janë zëvendësimi dhe transpozimi. Zëvendësimi është një teknikë ku çdo element në tekstin e thjeshtë (si një shkronjë, shifër ose simbol) zëvendësohet nga një element tjetër sipas një rregulli ose çelësi të caktuar.

Për shembull, një nga shifrat më të thjeshta të zëvendësimit është shifra e Cezarit, ku çdo shkronjë në tekstin e thjeshtë zhvendoset nga një numër fiks pozicionesh në alfabet. Transpozimi është një teknikë ku elementët në tekstin e thjeshtë riorganizohen ose ndërrohen sipas një rregulli ose çelësi të caktuar.

Për shembull, një nga shifrat më të thjeshta të transpozimit është shifra e gardhit hekurudhor, ku çdo shkronjë në tekstin e thjeshtë shkruhet në një rresht të ndryshëm të një rrjeti dhe më pas lexohet sipas kolonave.

KRIPTOGRAFIA KLASIKE NË KOHËT MË TË VONA

Disa nga makinat që janë përdorur për kriptografinë klasike janë edhe makinat me rotorë dhe makinat Enigma.

Makinat e rotorit janë pajisje elektro-mekanike që përdorin disqe rrotulluese (të quajtura rotorë) me modele të ndryshme instalime elektrike për të enkriptuar dhe deshifruar mesazhet.

Makinat Enigma janë një lloj makinerie me rotorë që u përdorën nga Gjermania gjatë Luftës së Dytë Botërore për komunikim ushtarak. Ata kishin disa rotorë që mund të ndryshoheshin çdo ditë dhe një prizë që lejonte personalizimin e mëtejshëm të çelësit të enkriptimit.

SHIFRA VIGENÈRE

ALGORITMI

Siç e cekëm më herët, shifra Vigenère është një kriptografi klasike e ngjajshme me shifrën e Cezarit, por më e sigurtë. Shifra Vigenère përfshinë në vetëvete 26 shifra të Cezarit (shifër e zëvendësimit - polialfabetik) në një matricë 26 x 26. Shifra Vigenère është një metodë e enkriptimit të tekstit me shifrën e rreshtave bazuar në fjalë kyçe. Një metodë e përdorimit të shifrës Vigenère për enkriptim është duke përdorur tabelën katrore (ndryshe e quajtur tablea Vigenère) dhe për dekriptim në rast se dihet fjala kyçe.

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

Fig. 2 Tabela Vigenere

Përpos metodës së enkriptimit me tabelë, ekzistojnë dhe funksione matematikore të cilat lehtësojnë implementimin e shifrës Vigenère në kod kompjuterik. Në mënyrë algjebraike, procesi i enkriptimin mund të kryhet me anë të formulës:

$$C_i = E_K(M_I) = (M_I + K_I) mod 26$$

Ku M_i paraqet karakterin që gjindet në pozitën i tek mesazhi, dhe K_i karakterin që gjindet në pozitën i tek çelësi.

Njejtë ekziston edhe formula algjebraike për dekriptim:

$$M_i = D_K(C_I) = (C_I - K_I) mod 26$$

Me të vetmin ndryshim, C_i që paraqet shifrën e enkriptuar. Variablat M, K dhe C mund të kenë vlera nga 0 deri 25, ku A=0, B=1 ... Dhe Z=25.

PROCESI I ENKRIPTIMIT

Shembull për spjegimin e procesit të enkriptimit dhe dekriptimit, kemi marrur mesazhin "datasecurity", dhe çelësi "FSHMN".

1. Çelësi përsëritet n-herë deri sa gjatësia e tij të jetë e barabartë me atë të mesazhit.

   FSHMN → FSHMNFSHMNFS

2. Duke përdorur formulat algjebraike të mësipërme, kryejmë enkriptimin e mesazhit:

$$C_1 = E_K(M_1) = (3 + 6) mod 26 = 9$$
$$C_2 = E_K(M_2) = (0 + 19) mod 26 = 19$$
$$\dots$$
$$C_{12} = E_K(M_{12}) = (24 + 18) mod 26 = 16$$

Pasi përfundojmë në tërësi procesin e enkriptimit, fitojmë shifrën: **isamfjubdvyq**.

SIGURIA E SHIFRËS VIGENÈRE

PËRPARËSITË

E spjeguar për herë të parë nga Giovan Battista Bellaso në 1553, shifra është e lehtë për t'u kuptuar dhe zbatuar, por ai u rezistoi të gjitha përpjekjeve për ta thyer atë deri në 1863. Kjo i dha asaj përshkrimin le chiffrage indéchiffrable (frëngjisht për 'shifror i padeshifrueshëm).

MANGESITË

Dobësia kryesore e shifrës Vigenère është natyra përsëritëse e çelësit të tij. Nëse një kriptanalist e merr me mend saktë gjatësinë n të çelësit, teksti i shifrës mund të trajtohet si n shifra të ndërthurura të Cezarit, të cilat mund të thyhen lehtësisht individualisht. Gjatësia e çelësit mund të zbulohet duke testuar çdo vlerë të mundshme të n-së me forcë brutale.

IMPLEMENTIMI I ALGORITMIT NË GJUHËN JAVA

Për shkak se algoritmi për enkriptim është relativish i thjeshtë, duke përdorur funksionet algjebraike të mësipërme lehtësisht mund të implementojmë algoritmin në JAVA.

Duke përdorur metodat e listuara në tabelë, mund të kodojmë algoritmin për enkriptim dhe dekriptim:

Krijoçelësin(String, String):String	Gjeneron çelësin për enkriptim i cili ka gjatësinë e njejtë me atë të mesazhit.
Enkriptotekstin(String, String): String	Metoda për enkriptim. Enkripton tekstin bazuar në çelësin e dhënë.
Dekriptotekstin(String, String): String	Dekripton tekstin, në rast se dihet çelësi.

KOMPLEKSITETI I ALGORITMIT

Algoritmi ndryshon individualisht secilin karakter të stringut (mesazhit) të dhënë dhe për këtë arsye ka kompleksitetin e kohës: **O(n)**, ku n=gjatësia e stringut. Për të njejtë arsye, algoritmi ka kompleksitetin e hapësirës: **O(n)**, ku n=gjatësia e stringut.