***UNIVERSITETI I PRISHTINËS***

## FAKULTETI I INXHINIERISE ELEKTRIKE DHE KOMPJUTERIKE

**Inxhinieri Kompjuterike BACHELOR**



**- FAZA E PARE E -PROJEKTIT - LËNDA:**

**SIGURIA E TE DHENAVE**

**GRUPI:7**

Mentor: Kandidat:

Prof.Ass.Arbnor Halili Natyra Vitija,

Toni Krasniqi

Zahir Maliqi

Prishtinë, Mars 2020

Hyrje

**Siguria e të dhënave** është një shkence e cila studion metodat e mbrojtes së të dhënave kompjuterike. Pra, siguri e të dhënave do të thotë ruajtja e të dhenave nga keqpërdorimet, dhe qasja ne këto të dhëna të jet nën kontroll. Në këtë mënyrë, siguria ë të dhënave na ndihmon në ruajtjen e privatësisë. Kjo gjithashtu ndihmon në ruajtjen e të dhënave personale. Sistemet kompjuterike të lidhura në rrjetë, në ditët e sotme, shpesh janë të pambrojtura nga kode të krijuara nga burime pothuajse të panjohura. Kodi mund të jetë i bashkangjitur me email (ang.e-mail), mund të jetë i përmbajtur në dokumente apo mund të jetë i shkarkuar (ang.downloaded) nga Interneti. Fatkeqësisht, shumica e shfrytëzuesve të kompjuterëve janë të sprovuar drejtpërsëdrejti nga efektet e kodeve mobile keqdashëse sikurse janë viruset (ang.viruses) dhe krimbat (ang.worms) e të cilët i dëmtojnë apo edhe mund ti shkatërrojnë shënimet. E në të njëjtën kohë na sjellin dëme duke na kushtuar në kohë dhe para.

Ne lenden Siguria e te Dhenave, gjegjesisht ne fazen e pare te projektit nga kjo lende, ne kemi pasur per detyre te bejme kodin per enkriptimin dhe dekriptimin e algoritmeve ne vijim:

Frequency

Four-Square

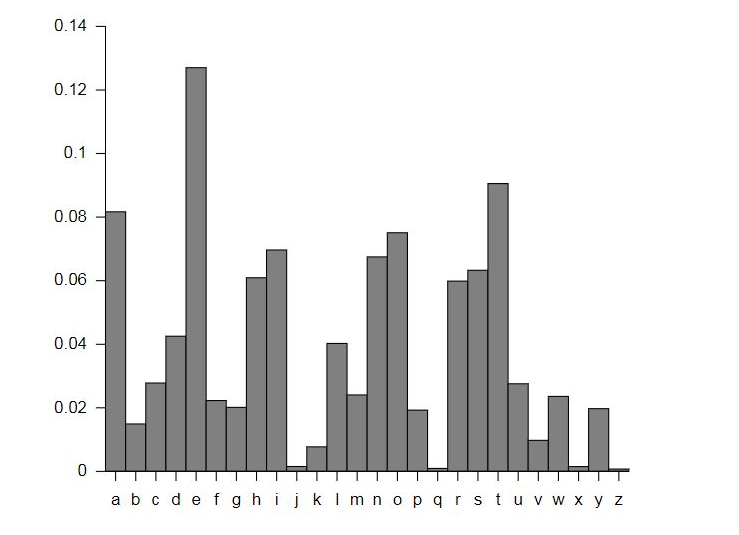
Vigenere

Te koduara ne gjuhen programuese Java.

**Komanda Frequency**

Analiza e frekuencës është studimi i shkronjave ose grupeve të shkronjave që përmbahen në një tekst të saktë në përpjekje për të zbuluar pjesërisht mesazhin. Gjuha angleze (si dhe shumica e gjuhëve të tjera) ka disa shkronja dhe grupe shkronjash shfaqen në frekuenca të ndryshme.

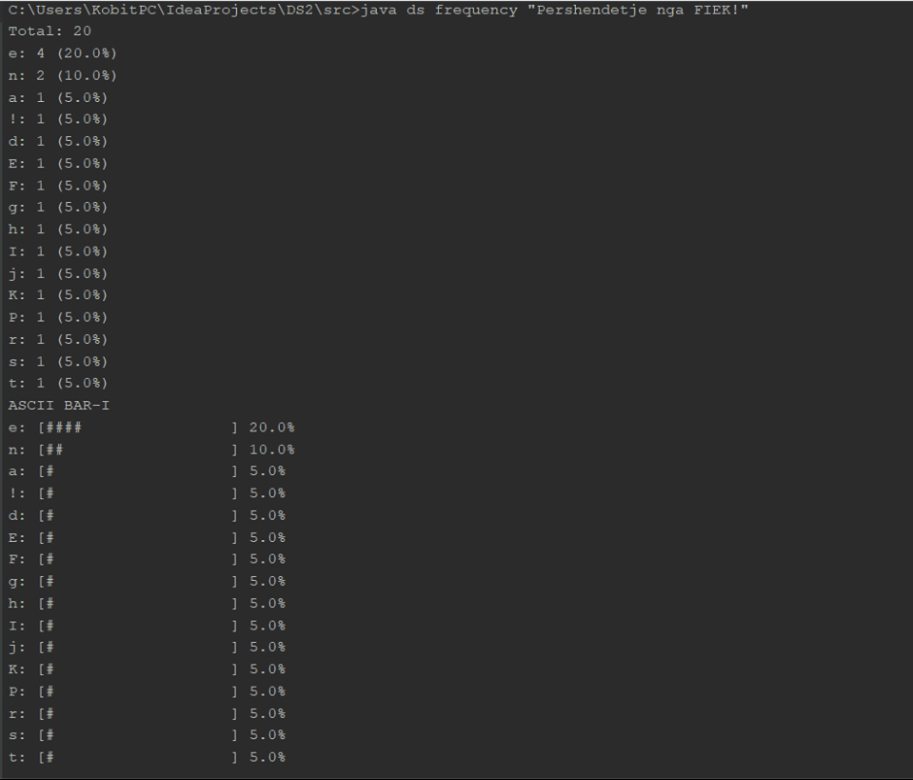
Kjo është një tabelë e shpërndarjes së frekuencës së shkronjave në alfabetin anglez. Siç mund ta shihni, shkronja ‘e’ është më e zakonshme, e ndjekur nga ‘t’ dhe ‘a’, me ‘j’, ‘q’, ‘x’ dhe ‘z’ duke qenë shumë e rrallë.



Duke ditur frekuencat e zakonshme të shkronjave në komunikimin anglez, nëse metoda e kriptimit nuk i maskon në mënyrë efektive këto frekuenca, është e mundur që në mënyrë statistikore të përcaktohen pjesë të plaintext nga shikimi vetëm i shifrës. Le të shohim një shembull të bazuar në një tekst të thjeshtë të koduar me Ciparin Cezar - një shifër që nuk siguron mbrojtje nga analiza e frekuencës.

Ne kemi parë që ka shumë çelësa të mundshëm për të provuar në një sulm brutal të forcës në shifrën e alfabetit të miksuar, dhe duke pasur parasysh që ne mund të përdorim gjithashtu simbole në zëvendësimin tonë, ekzistojnë pafundësisht shumë çelësa të ndryshëm për një shifër zëvendësimi Monoalphabetic. Pavarësisht kësaj, sidoqoftë, çdo shembull i vetëm i këtij lloji të shifrave është thyer me lehtësi, duke përdorur një metodë të vetme që funksionon mbi të gjitha:   
Frekuenca.

Shembulli konkret



**Metoda Four-Square**

Algoritmi Four-Square përdor katër matrica 5 në 5 (5x5) të rregulluar në një katror. Secila nga matricat 5 nga 5 përmban shkronjat e alfabetit (zakonisht duke lënë mënjanë "Q" ose duke vendosur të dy "I" dhe "J" në të njëjtin vend për të zvogëluar alfabetin që të përshtatet).

Këtu janë matricat për fjalët kyçe "shembull" dhe "fjalen kyçe". Matricat e plaintext janë me shkronja të vogla dhe matricat e ciphertext janë me shkronja te medha për ta bërë këtë shembull vizualisht më të thjeshtë.

a b c d e E X A M P

f g h i j L B C D F

k l m n o G H I J K

p r s t u N O R S T

v w x y z U V W Y Z

K E Y W O a b c d e

R D A B C f g h i j

F G H I J k l m n o

L M N P S p r s t u

T U V X Z v w x y z

Per ta bere enkriptimin duhet ta ndajme mesazhin ne shkronja dy nga dy. Psh. HELLO WORLD behet HE LL OW OR LD.

Duhet gjetur shkronjen e pare ne dyshkronjesh ne matricen e majt e siperme te plaintext- it.

Duhet gjetur shkronjen e dyte ne dyshkronjesh ne matricen e djatht e poshtme te plaintext-it.

Shkronja e pare e dyshkronjeshit te enkriptuar eshte ne te njejtin rresht me shkronjen e pare te plaintext-it dhe ne te njejten kolone me shkronjen e dyte te plaintext-it. Andaj eshte ne matricen e siperme te djathte te ciphertext-it.

Shkronja e dyte e dyshkronjeshit te enkriptuar eshte ne te njejtin rresht me shkronjen e dyte te plaintext-it dhe ne te njejten kolone me shkronjen e pare te plaintext-it. Andaj eshte ne matricen e poshtme te majt te ciphertext-it.

a b c d e E X A M P

f g **h** i j L B C D ***F***

k l m n o G H I J K

p r s t u N O R S T

v w x y z U V W Y Z

K E Y W O a b c d **e**

R D A B C f g h i j

F G H I J k l m n o

L M N P S p r s t u

T U V X Z v w x y z

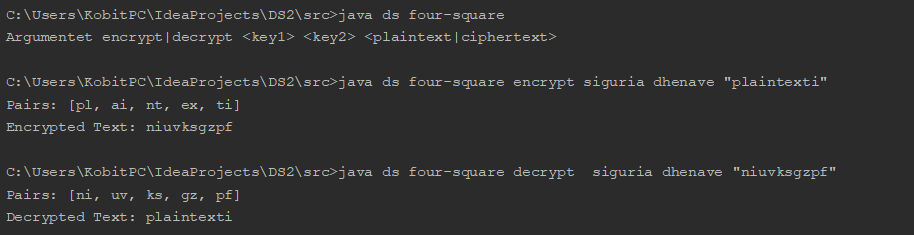
Nga shembulli I mesiperm ne do ta enkriptonim plaintextin si ne vijim:

Plaintext: he lp me ob iw an ke no bi

Ciphertext: FY GM KY HO BX MF KK KI MD

Testimi I algoritmit Four- Square

Enkriptimi dhe dekriptimi



**Metoda Vigenère**

Vigenere Cipher është një metodë e kriptimit të tekstit alfabetik. Përdor një formë të thjeshtë të zëvëndësimit polialfabetik. Një shifër polifafetike është çdo shifër e bazuar në zëvendësim, duke përdorur alfabete të shumta zëvendësimi. Kriptimi i tekstit origjinal bëhet duke përdorur tabelën Vigenère ose tabelën Vigenère.

Tabela përbëhet nga alfabete të shkruara 26 herë në rreshta të ndryshëm, secila alfabet zhvendoset në mënyrë ciklike në të majtë, krahasuar me alfabetin e mëparshëm, që korrespondon me 26 shifrat e mundshme të Cezarit.

Në pika të ndryshme në procesin e kriptimit, shifri përdor një alfabet të ndryshëm nga një prej rreshtave.

Alfabeti i përdorur në secilën pikë varet nga një fjalë kyçe që përsëritet.

A picture containing text, newspaper

Description automatically generated

Tabela Vigenère ose tabela Vigenère, e njohur gjithashtu si tabula recta, mund të përdoret për enkriptim dhe dekriptim.

• **Enkriptimi (agl. Encryption)** – është procesi përmes të cilit plaintexti konvertohet në ciphertext. Pra enkriptimi është procesi me të cilin tentohet që nga plaintexti të fitojmë një strukturë të të dhënave inkoherente (ciphertext).

• **Dekriptimi (angl. Decryption)** – është pocesi i kundërt i kriptimit. Ai kthenë ciphertextin në plaintext përseri.

Shembuj:

