***UNIVERSITETI I PRISHTINËS***

## FAKULTETI I INXHINIERISE ELEKTRIKE DHE KOMPJUTERIKE

**Inxhinieri Kompjuterike BACHELOR**



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

**SIGURIA E TE DHENAVE**

**GRUPI:25**

Mentor: Kandidat:

Prof.Ass.Arbnor Halili Tahir Temaj,

Teuta Ukshini

Prishtinë, Mars 2020

**Hyrje**

Siguria e të dhënave i referohet procesit të mbrojtjes së të dhënave nga aksesi i paautorizuar dhe korrupsioni i të dhënave gjatë gjithë ciklit të jetës së tij. Siguria e të dhënave përfshin kriptimin e të dhënave, shenjëzimin dhe praktikat kryesore të menaxhimit që mbrojnë të dhënat në të gjitha aplikacionet dhe platformat.

Kriptografia përdoret për të siguruar dhe mbrojtur të dhënat gjatë komunikimit. Kriptimi është një proces që shndërron informacionin origjinal në një formë të panjohshme. Decryption është një proces i konvertimit të të dhënave të koduara / enkriptuara në një formë që mund të lexohet dhe kuptohet nga një njeri ose një kompjuter

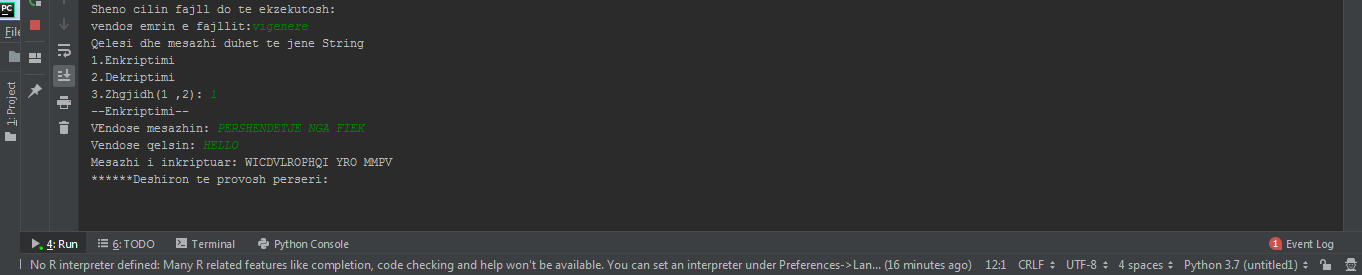
Ky projekt eshte nga lenda siguri dhe ka per qellim aftesimin dhe marrjen e njohurive rreth Kriptografise,me saktesisht metodave te ndryshme ,si dhe nenkomandat Enkriptimin dhe Dekriptimin.

Per realizimin e ketij projekti eshte perdorur gjuha programuese PYTHON dhe editori Visual Studio 2019.

Detyre e ketij projekti eshte krijimi dhe testimi I tij, i cili ka disa kerkesa qe duhet t’I permbushim.

Ne fazen e pare te projekti te te lendes Siguria e te Dhenave kemi pasur 3 komanda kryesore te cilat jane :**CASE, VIGENERE** dhe **FOUR SQUARE CIPHER**

-Keto komanda mund te ekzekutohen duke ndjekur udhezimet e programit permes fajllit kryesor **DS.py**



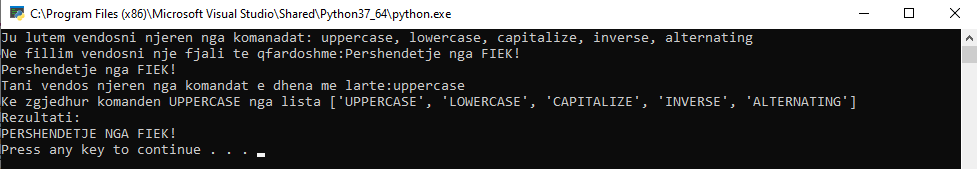
*Figura.1 Programi Kryesor DS.py*

-Me komanden **Case** mund te behet konvertimi i nje teksti ne 6 formate: **UPPERCASE, LOWERCASE, CAPITALIZE,INVERSE, ALTERNATING** dhe **SENTENCE**

**UpperCase->** Bene konvertimin e qfardo teksti ne shkronja te medha

**EXAMPLE**: **Pershendetje nga Fiek!**

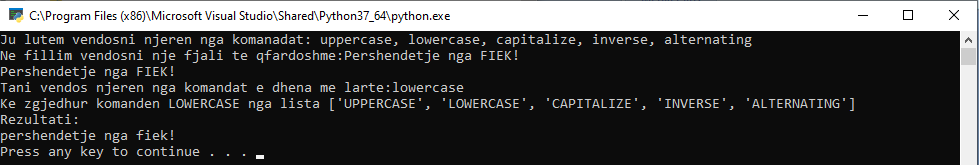
**REZULTATI**: **PERSHENDETJE NGA FIEK!**

****

**LowerCase->**Bene konvertimin e tekstit ne shkronja te vogla

**EXAMPLE**: **Pershendetje Nga Fiek!**

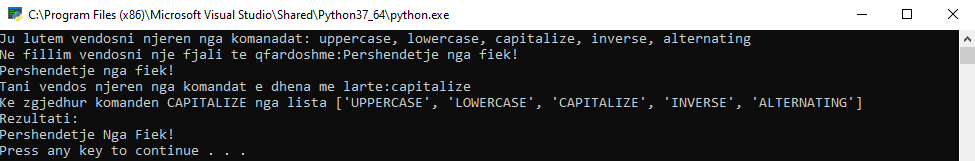
**EXAMPLE**: **pershendetje nga fiek!**

****

**Capitalize->**Konverton shkronjen e pare te fjaleve te tekstit ne shkronje te madhe

**EXAMPLE**: **pershendetje nga fiek!**

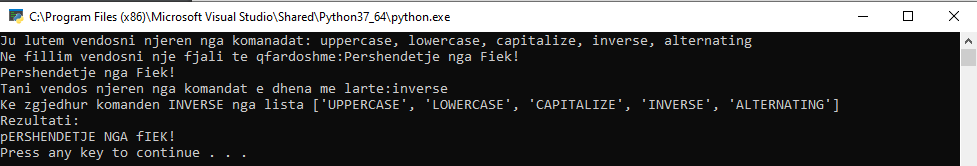
**EXAMPLE**: **Pershendetje Nga Fiek!**



**Inverse->**Konverton tekstin e dhene krejtesisht ne format te kundert.

**EXAMPLE**: **Pershendetje Nga Fiek!**

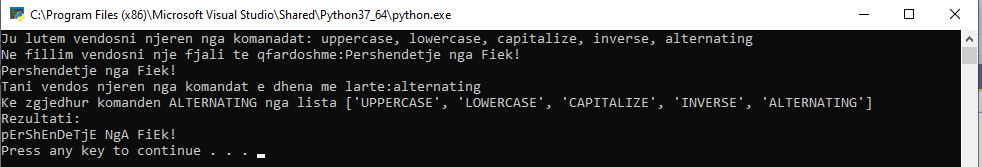
**EXAMPLE**: **pERSHENDETJE nGA fIEK!**



**Alternating->**Bene konvertimin e qdo 2 shkronjave ne shkronja te medha

**EXAMPLE**: **pershendetje nga fiek!**

**EXAMPLE**: **pErShEnDeTjE NgA FiEk!**



**Pike shtese:**

**Sentence->**Konverton tekstin e dhene ne perpikmeri me shenjat e piksimit dhe rregullat sintaksore.NOTE:Nuk e kemi be.

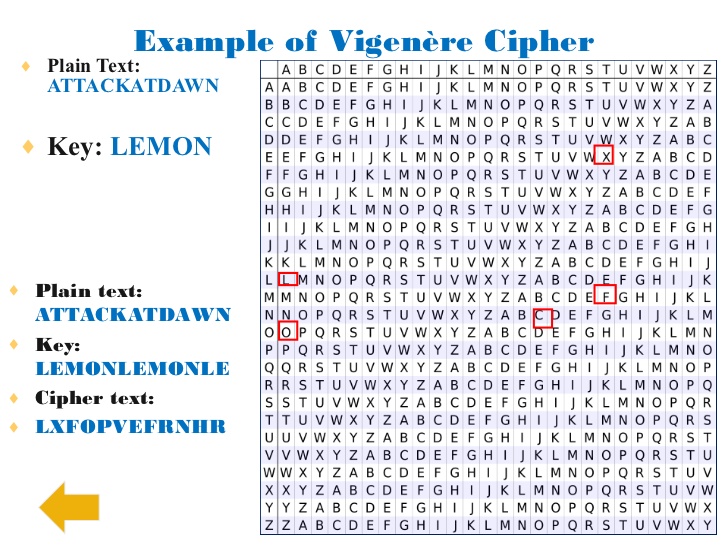
**EXAMPLE**: **pershendetje nga Fiek!mirupafshim.kaloni Mire!**

**EXAMPLE**: **Pershendetje nga fiek!Mirupafshim.Kaloni mire!**

**Vigenere**

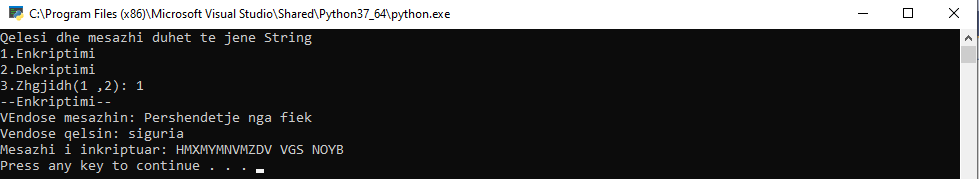
-Me komande **Vigenere** kemi enkriptimin dhe dekriptimin e nje teksti bazuar ne metoden Vigenere e cila eshte e ngjashme me metoden e Cezarit por perderisa metoda e Cezarit perdor nje qeles te vetem per te zhvendosur te gjitha shkronjat , metoda Vigenere perdor qeles qe zhvendos shkronjat per hapsira te ndryshme.

Enkriptimi kryhet permes tabeles Vigenere ku varesisht prej mesazhit dhe qelesit mirret shkronja e pare e mesazhit dhe shkronja e pare e qelsit dhe formojne si lloj koordinate e cila me ane te tabeles Vigenere lokalizon shkronjen e enkriptuar, e keshtu me radhe mirren edhe shkronjat tjera per te enkriptuar te gjithe mesazhin.

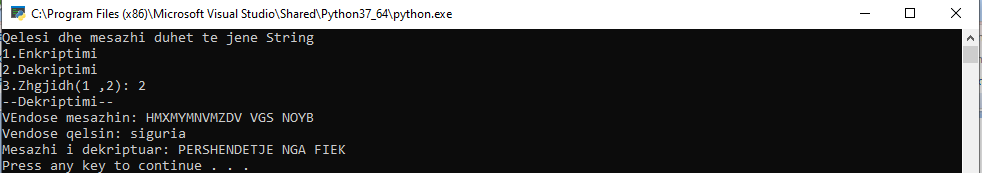


**Testimi I Vigenere**

***Enkriptimi:***



***Dekriptimi:***



**Metoda Four Square Chiper**

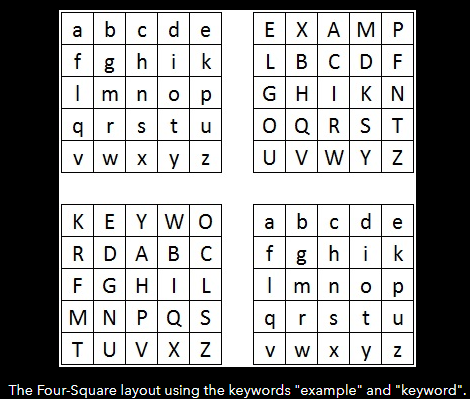
Four Square Chiper përdor katër matrica 5 në 5 **(5x5)** të rregulluar në një katror. Secila nga matricat 5 nga 5 përmban shkronjat e alfabetit (zakonisht duke lënë mënjanë "Q" ose duke vendosur të dy "I" dhe "J" në të njëjtin vend për të zvogëluar alfabetin që të përshtatet). Në përgjithësi, matricat e sipërm dhe të djathtë të djathtë janë "sheshet e thjeshtë" dhe secila përmban një alfabet standard. Sheshet e sipërm të djathtë dhe të majtë të poshtëm janë "sheshet e shifrës" dhe përmbajnë një sekuencë alfabetike të përzier

***Enkriptimi:***

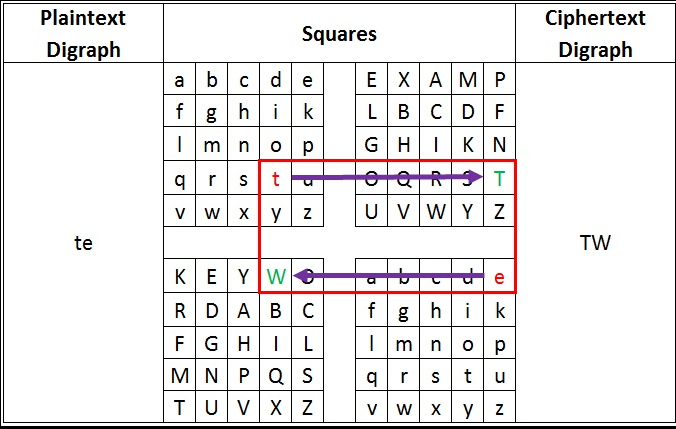
Per te enkriptuar duke perdorur Four Square Chiper se pari duhet te ndajme shifren (chipertext)ne diagrafe dhe duhet me ja shut nje “**X**” ne fund nese shkronja e fundit eshte tek.Pershembull –“Test plaintext

Screenshot_1.png

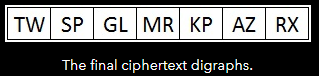
Tani mundemi me gjeneru Four Square per perdorim ne enkriptim.Nese marrim dy qelsa njeri example dhe tjetri keyword atehere kemi:



Për secilin shkrim të rrafshit, ju e vendosni shkronjën e parë në sheshin e sipërm të majtë, dhe shkronjën e dytë në sheshin e djathtë të poshtëm. Pastaj formoni drejtkëndëshin që ka këto dy pika si qoshe të kundërta. Dy qoshet e tjera formojnë digrafin e përpiktë, dhe ju merrni qoshen në sheshin e djathtë të sipërm si shkronjën e parë, dhe këndin në sheshin e poshtëm të majtë si shkronjën e dytë.



Dhe fitojme:

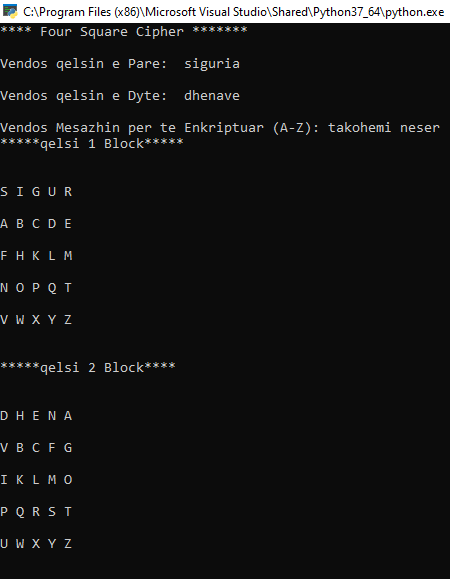


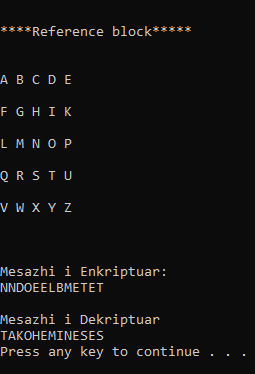
***Dekriptimi:***

Dekriptimi është shumë i njëjtë me kriptimin, por ndërsa fillojmë me tekstin e shifrës, ne i gjejmë në sheshet e shifrës cipertext dhe lexojmë nga sheshet e thjeshtë.

**Testimi I Four Square Chiper**

***Enkriptimi dhe Dekriptimi***





**Referencat**

1. <https://crypto.interactive-maths.com/four-square-cipher.html?fbclid=IwAR3483a9Eh4QAqTXvhc6ejfOT33suLfzX7QwyqbeDVeWQcpbk9sbjb2Z7ow>
2. <https://www.youtube.com/watch?v=SkJcmCaHqS0&fbclid=IwAR1ld5Uwc0XkKHnnez20zQgwy60c0CwNQcaWiStMqioyxrtrqDrJPT-n-XI>
3. <https://www.geeksforgeeks.org/vigenere-cipher/?fbclid=IwAR3ZDMsS73tzYN-BGSUWRN8LYkVkC7YmJcIXWoq_vvSHyObS7OFXtsaMCt>
4. <https://www.youtube.com/watch?v=rWyxZjjOGjY&fbclid=IwAR1cYE9sph28MWSGVoqk0471GdCrn9v-VAmf3tydT4KxqMSeg5Ey8nuTPq0>
5. <https://en.wikipedia.org/wiki/Four-square_cipher>
6. <https://docs.microsoft.com/en-us/windows/win32/seccrypto/data-encryption-and-decryption>
7. <https://docs.python.org/2/library/string.html>