***UNIVERSITETI I PRISHTINËS***

## FAKULTETI I INXHINIERISE ELEKTRIKE DHE KOMPJUTERIKE

**Inxhinieri Kompjuterike BACHELOR**



**- FAZA E DYTE E**

**-PROJEKTIT - LËNDA:**

**SIGURIA E TE DHENAVE**

**GRUPI:25**

Mentor: Kandidat:

Prof.Ass.Arbnor Halili Tahir Temaj,

Teuta Ukshini

Prishtinë, Maj 2020

**Hyrje**

Ky raport eshte ne lenden Siguri, perkatesisht Faza e dyte e projektit,ku kem pas per te zgjeruar programin ekzistues ne github me komanda te cilat bazohen ne teknikat modern te enkriptimit simetrik she asimetrik.Gjate implementimit te ketyre kerkesave kem be perpunimin e te dhenave binare dhe enkodimeve te tyre.Eshte dhene kerkesa per komandat:**create-user,delete-user,export-key,import-key,write-massage,read-message.** Projekti gjendet ne repository-n TahirT/DS\_1920\_Gr25, si vazhdim I projektit te pare,me gjuhe programuese **Python**, I cili eshte implementuar me programin **Pycharm 2020.1.** Ne qofte se kemi ndonje deshtim gjate ekzekutimit per shkak te hyrjeve jo-valide ose ndonje gabimi gjate shkrim-leximit ne fajlla,kem bere pershkrim per trajtim te gabimeve dhe shfaqjen e nje mesazhi pershkrues ne ekran.

**Pershkrimi I metodave dhe implementimi I tyre**

Ketu bejme pershkrimin per secilen metode te dhene si dhe ekzekutimi I tyre.

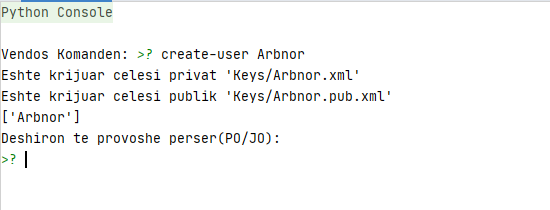
Thirrjen e ketyre metodave e kemi ba me ane te programit **DS.py** qe I bashkon programet edhe I thirr nje nga nje per cdo metode, eshte bere update nga faza e pare e projektit.

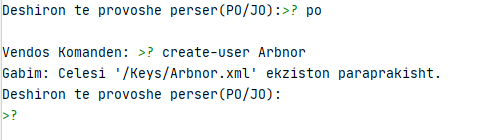
Si fillim e krijojme nje folder me emrin **Keys** , I cili permban nje file te zbrazet,te cilin e kem emeruar **test.txt** ku realisht mbahen çelësat publik dhe privat.Dhe ktu behet ruajtje e tyre dhe manipulimi me to.

**Create-user <*name*>**

Metoda **Create-user** ka per qellim krijimin e nje useri I cili permban dy çelsa publik dhe privat ose me mire te themi një çift të publik/privat të RSA me emrat <name> .xml dhe <name>.pub.xml brenda direktoriumit të çelësave keys.Fajllat qe krijohen mund te krijohen si .xml ose si .pem. Fajllat qe jane krijuar shfaqen si Keys/<name>.xml dhe Keys/<name>.pub.xml.

Kto jane screenshots te bera gjate ekzekutimit te komandes **Create-user**

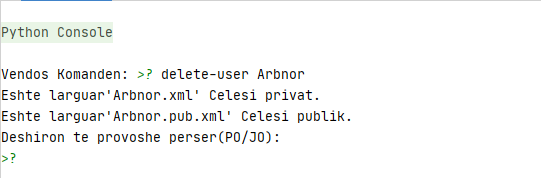


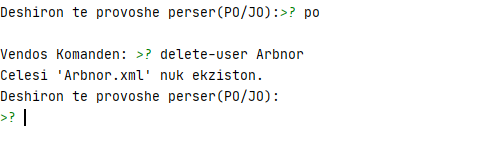


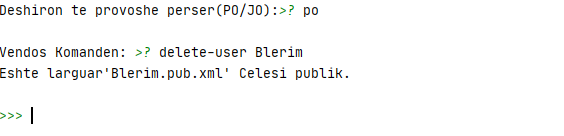
**Delete-user <*name*>**

Gjate metodes **create-user** thame qe behet krijimi I nje useri me cift qelsat rsa publik dhe privat,ndersa ne baze te metodes **delete-user** behet implementimi I kodit per fshirjen e qelsave ekzistues te shfrytezuesit.

Keto jane screenshots gjate ekzekutimit te komandes **Delete-user**

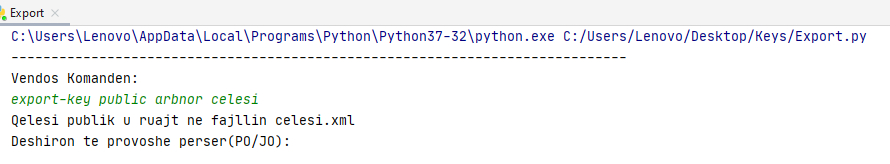


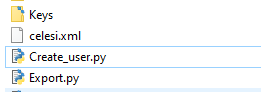




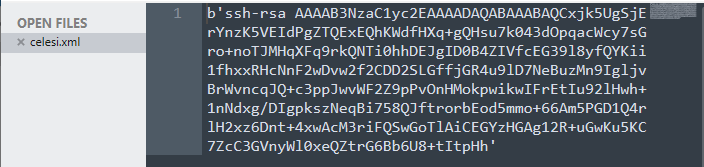
**Export-Key *<public|private><name>[file]***

Kjo metode ka te beh me eksportimin e celsit public ose privat te shfrytezuesit nga direktoriumi I celesave. Po ashtu bejme edhe trajtimin e gabimeve, argumenti opsional [file] e përcakton shtegun e fajllit se ku do të ruhet çelësi i eksportuar. Nëse mungon argumenti atëherë çelësi do të shfaqet në console.

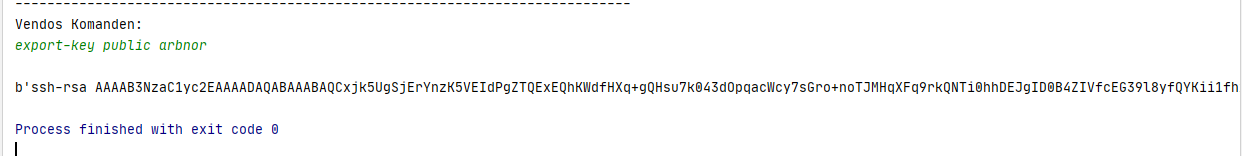




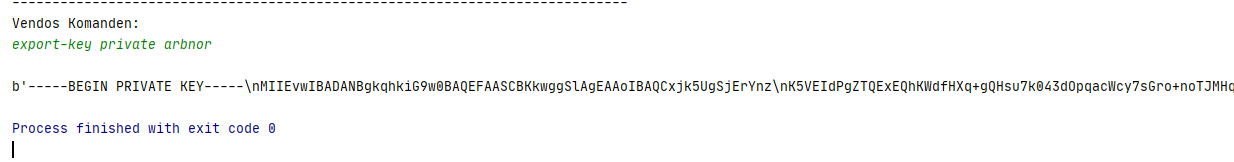
Qelsi I eksportuar



Pamja e qelsit publik te eksportuar.

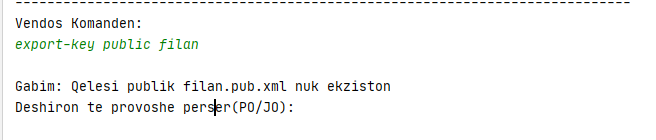


Eksportimi I qelsit publik ne console



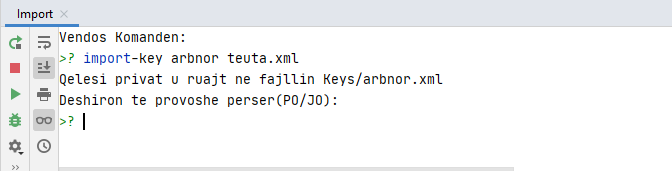
Eksportimi I qelsit privat ne console

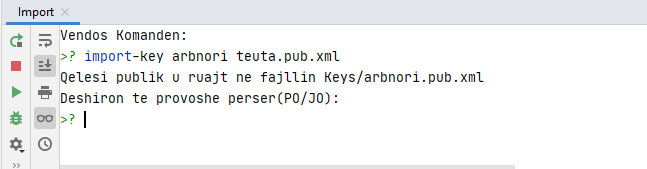
Po ashtu nese ekziston qe gjate shenimit te behet ndonje gabim atehere kemi bere eedhe trajtimit te gabimit.

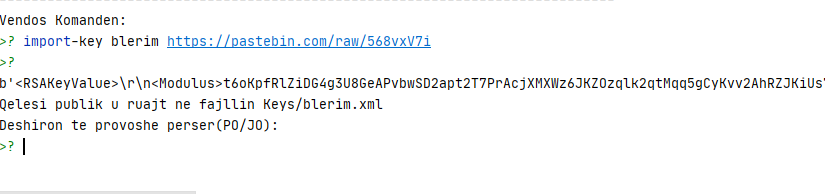


**Import-key *<name> <path>***

Kjo komande ka per qellim me importu çelësin publik ose privat të shfrytëzuesit nga shtegu i dhënë dhe e vendos në direktoriumin e çelësave. Çelësi i importuar mund të jetë publik ose privat. Programi juaj automatikisht e kupton se çfarë lloj çelësi është duke e shikuar përmbajtjen e fajllit të importuar. Nëse çelësi që po importohet është privat, atëherë ju automatikisht do ta gjeneroni edhe pjesën publike që t’i ruani të dyjat në direktoriumin e çelësave.

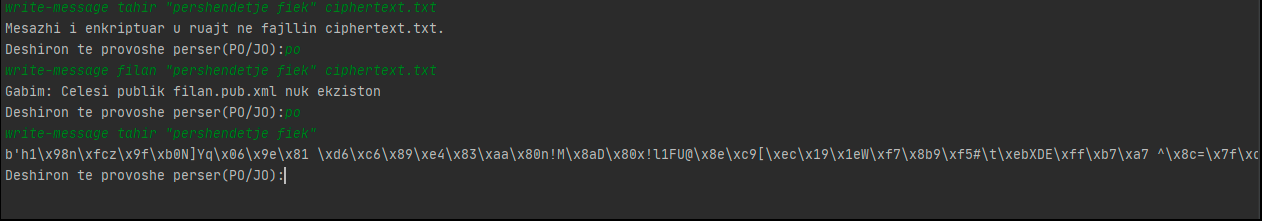






**Write-message*<name><message><file>***

Kjo komande e shkruan nje mesazh te enkriptuar te dedikuar per nje shfrytezues.Perbehet nga argumentet <name> , <message> dhe <file>.Argumenti <name> e paraqet marrësin e mesazhit (çelësin publik). Argumenti<message> e paraqet mesazhin që do të enkriptohet. Argumenti opsional [file] e përcakton shtegun e fajllit se ku do të ruhet mesazhi i enkriptuar. Nëse mungon argumenti, atëherë mesazhi i enkriptuar do të shfaqet në console.



**Read-message** ***<encrypted-message>***

Kjo komande e dekripton dhe e shfaq ne console mesazhin e enkriptuar.Argumenti <encrypted-message> paraqetmesazhin e enkriptuar sipas skemës së komandës write -message. Nëse ky argument nuk përputhet me skemën e enkriptimit atëherë të provohet të lexohet argumenti si shteg i fajllit në të cilin gjendet mesazhi. Emri i shfrytëzuesit/çelësit dekodohet nga mesazhi. Kuptohet që për ta dekriptuar mesazhin nevojitet çelësi privat i shfrytëzuesit. Nëse mungon ky çelës do të shfaqet një mesazh gabimi

***REFERENCAT***

* <https://www.youtube.com/watch?v=XiXe8rkA39g&t=39s>
* <https://www.namecheap.com/support/knowledgebase/article.aspx/798/67/what-is-an-rsa-key-used-for>
* <https://www.youtube.com/watch?v=8I7BNgD2Yag>
* <https://www.youtube.com/watch?v=seq8foEVQNA>
* [*https://www.youtube.com/watch?v=uF\_ewHntpeg*](https://www.youtube.com/watch?v=uF_ewHntpeg)