***UNIVERSITETI I PRISHTINËS***

## FAKULTETI I INXHINIERISE ELEKTRIKE DHE KOMPJUTERIKE

**Inxhinieri Kompjuterike BACHELOR**



**- FAZA E TRETE E**

**-PROJEKTIT - LËNDA:**

**SIGURIA E TE DHENAVE**

**GRUPI:25**

Mentor: Kandidat:

Prof.Ass.Arbnor Halili Tahir Temaj,

Teuta Ukshini

Prishtinë,Qershor 2020

Permbajtja

Abstrakt....................................................................................................................................3

Hyrje…………………………………………………………………..…………………………..…………………………………..4

Pershkrimi i komandave te dhena……………………………………………………………………….………………5

Komanda create-user……………..........................................................................................6

Komanda delete-user….....................................................................................................9

Komanda login................................................................................................................10

Komanda status..............................................................................................................11

Komanda write-message................................................................................................12

Komanda read-message.................................................................................................13

Referencat…………………………………………………………………………………………………………………… 14

Abstrakt

Ky raport ka të bëjë me fazen e trete të projektit në lënden Siguria e të Dhënave ku si qëllim e kemi vazhdimin dhe zgjerimin e fazës së dyte. Komandat të cilat bazohen në teknika modern të enkriptimit simetrik dhe asimetrik. Në fazën e tretë të projektit do ta zgjerojme programin tuaj me menaxhim të fjalëkalimeve dhe vërtetim të autenticitetit përmes nënshkrimeve digjitale.

Këto komanda janë:

Komanda create-user

Komanda delete-user

Komanda login

Komanda status

Komanda write-message

Komanda read-message

HYRJE

Para se të tregojmë komandat dhe funksioni i tyre, së pari duhet të kemi njohuri mbi disa koncepte të tjera në mënyrë që ta kemi të qartë se për çfarë bëhet fjalë. Ky raport eshte ne lenden Siguri, perkatesisht Faza e trete e projektit,ku kem pas per te zgjeruar programin ekzistues ne github me komanda te cilat bazohen ne teknikat modern te enkriptimit simetrik dhe asimetrik.Gjate implementimit te ketyre kerkesave kem be perpunimin e te dhenave binare dhe enkodimeve te tyre. Projekti gjendet ne repository-n ***TahirT/DS\_1920\_Gr25***, si vazhdim I projektit te dyte,me gjuhe programuese ***Python***, I cili eshte implementuar me programin ***Pycharm 2020.1*.** Kemi lidhur *pythonin* me *Mysql*,pasi qe kemi bere ruajtje ne Database.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 Komandave te dhena

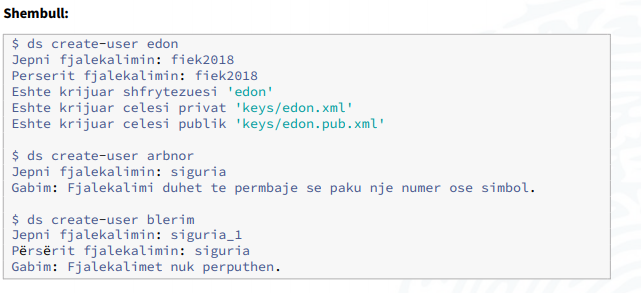
Ketu bejme pershkrimin per secilen metode te dhene si dhe ekzekutimi I tyre. Si fillim e krijojme nje folder me emrin **Keys** , I cili permban nje file te zbrazet,te cilin e kem emeruar **test.txt** ku realisht mbahen çelësat publik dhe privat.Dhe ktu behet ruajtje e tyre dhe manipulimi me to.Si dhe ruajtjen e tyre ne Database ne baze te kerkesave te projektit te trete me ane te fjalekalimit ne **Project.sql.** Kur krijohet shfrytëzuesi ju do ta ruani në bazë të shënimeve. Shënimet mund t’i ruani sipas dëshirës, psh. nëpër fajlla ose në ndonjë DBMS. Fjalëkalimin e shfrytëzuesit do ta ruani në formë të sigurt përmes hash algoritmeve dhe salting. Detajet e mënyrës së gjenerimit dhe ruajtjes janë sipas dëshirës. Rregullat për përpunimin e argumenteve janë të njëjta me fazat e kaluara: Në rast se argumentet mungojnë ose janë të jo-valide, atëherë do ta shfaqni një tekstme udhëzime rreth përdorimit dhe do ta mbyllni programin me kod dalës (exit code) 1. Poashtu, nëse gjatë ekzekutimit ka ndonjë dështim për shkak të hyrjeve jo-valide ose ndonjë gabimi gjatë shkrim-leximit në fajlla, programi duhet ta trajtojë gabimin dhe ta shfaqë në ekran një mesazh përshkrues. Në vazhdim e gjeni specifikimin e komandave, ku përfshihen edhe shembuj të përdorimit të tyre.

Komanda Create-user

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, si dhe behet ruajtja ne database ku gjatë krijimit të shfrytëzuesit të kërkohet edhe fjalëkalimi. Fjalëkalimi duhet të kërkohet përmes inputit, pasi që nuk preferohet të figurojë në histori. Fjalëkalimi duhet të ketë gjatësinë së paku 6 karaktere dhe duhet të përmbajë së paku një numër ose simbol.

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

**Kerkesat per komanden *Create-user***

****

***Ketu kemi bere krijimin e qelsave si dhe ruajtjen e tyre.***

## Screenshot_22.png

## Ketu kemi krijuar dy qelsat publik dhe privat,ku i kemi bere ruajtjen ne file ne folderin Keys.

## Screenshot_23.png

## Ketu kemi bere ruajtjen ne database:

## Screenshot_20.png

## Screenshot_4.png

## Po te duam te krijojme prape te njejtin qeles, atehere kemi bere gjenerimin e qelsave ashtu qe te mos lejoj te ruaj user te njejte.

## Screenshot_15.png

## Gjenerimi i qelsave behet me ane te passwordit:

## Screenshot_5.png

## Fjalëkalimi duhet të ketë gjatësinë së paku 6 karaktere dhe duhet të përmbajë së paku një numër ose simbol.

## Screenshot_18.png

## Kemi bere dhe validim te passwordit ne rast se kemi ndonje mos perputhje,pasi qe kerkohet te perseritet.

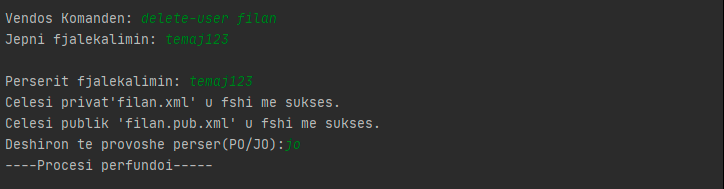
## Screenshot_17.png

Komanda Delete-user

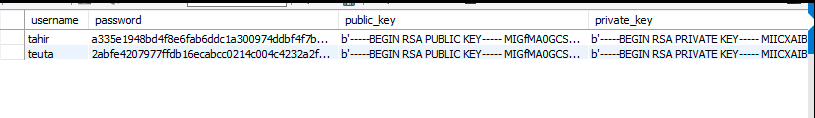
Gjate metodes **create-user** thame qe behet krijimi I nje useri me cift qelsat rsa publik dhe privat,ndersa ne baze te metodes **delete-user** behet implementimi I kodit per fshirjen e qelsave ekzistues te shfrytezuesit.Ku behet fshirja e qelsave ne fajll dhe ne database. Kur të thirret kjo komandë do të fshihen edhe të gjitha të dhënat e shfrytëzuesit nga baza e shënimeve.

**Kerkesa per komanden *Delete-user***

***Ketu eshte bere fshirja e qelsave***

****

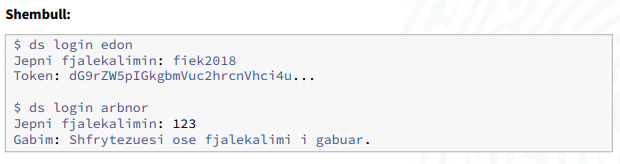
***Me ane te metodes Delete-user behet fshirja edhe ne baze te te dhenave (database) te qelsit ekzistues.***



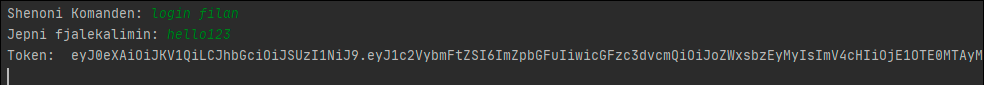
## Kemi bere fshirjen e qelsit ‘filan’

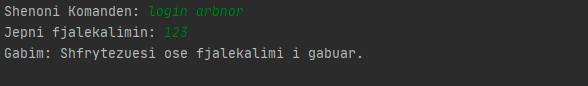
Komanda Login

Me ane te metodes **Login** teston çiftin shfrytëzues/fjalëkalim. Në rast suksesi lëshohet një token i nënshkruar i cili mund të përdoret për autentikim të shfrytëzuesit. Mënyra e ruajtjes së tokenit është sipas dëshirës, psh. ju mund ta lëshoni një JWT, një XML të nënshkruar, ose ndonjë format të vet-definuar. Me rëndësi është që për nënshkrim të tokenit të përdoret çelësi privat i shfrytëzuesit, ndërsa për vërtetim të nënshkrimit të përdoret çelësi publik i shfrytëzuesit. Tokeni skadon pas 20 minutave. Tokeni mund të përdoret vetëm për shfrytëzuesin për të cilin është lëshuar



Keto jane screenshots gjate ekzekutimit te komandes **Login**



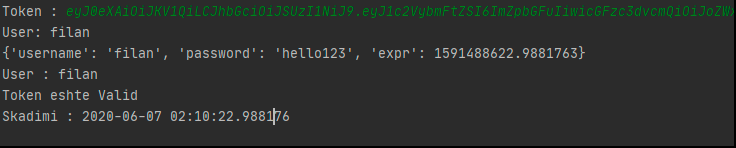


Komanda Status

Komanda Status eshte vazhdimi komandes Login,ku behet validimi I saj ne baze te tokenit. Si dhe I kemi dhene nje kohe skadimi. Nëse tokeni ka skaduar, nuk ka nënshkrim valid, ose nuk ekziston shfrytëzuesi, atëherë tokeni nuk konsiderohet valid.

**Shembull**

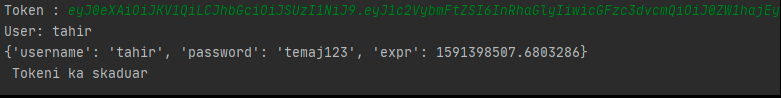




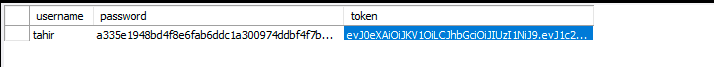
Ndersa nese tokeni ka skaduar, nuk ka nënshkrim valid, ose nuk ekziston shfrytëzuesi, atëherë tokeni nuk konsiderohet valid.



Si ne figuren e dhene:



Tokeni I krijuar ne Database



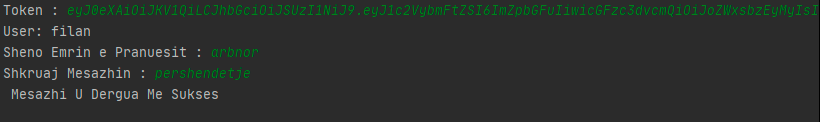
Komanda write-message

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. Kjo komandë zgjerohet ashtu që mund ta pranojë edhe opsionin --sender . Vlera sender është emri i shfrytëzuesit që i korrespondon tokenit token. Komanda dështon nëse tokeni nuk është valid ose ka skaduar. Nëse validohet tokeni me sukses, atëherë nënshkrimi bëhet me çelësin privat të dërguesit sender.

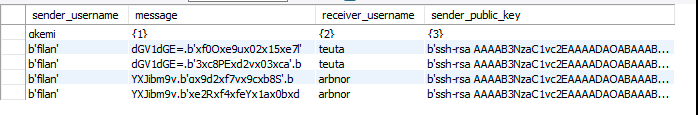
**Shembull**

****

Keto jane screenshots gjate ekzekutimit te komandes ***write-message***

****

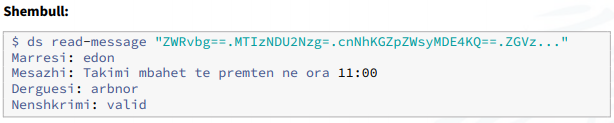
Ku ruajtja behet ne database

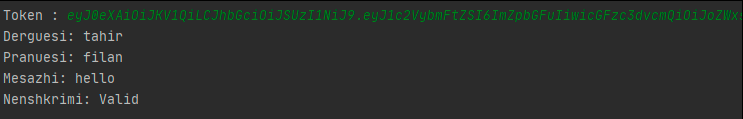


Ketu kemi sender dhe receiver

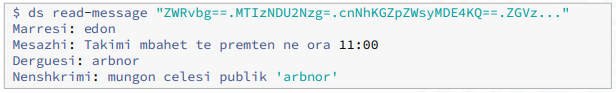
Komanda read-message

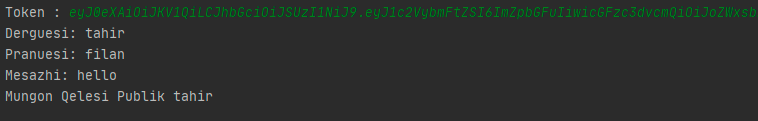
Kjo komande e dekripton dhe e shfaq ne console mesazhin e enkriptuar.Argumenti <encrypted-message> paraqet mesazhin e enkriptuar sipas skemës së komandës write -message. Nëse ky argument nuk përputhet me skemën e enkriptimit atëherë të provohet të lexohet argumenti si shteg i fajllit në të cilin gjendet 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. Komanda read-message zgjerohet ashtu që nëse figuron pjesa e dërguesit/nënshkrimit në mesazh, atëherë do të tentohet verifikimi i atij nënshkrimi duke përdorur çelësin publik të dërguesit. Nëse mungon pjesa e dërguesit/nënshkrimit, atëherë komanda e injoron dhe vepron sikur në fazën e dyte.



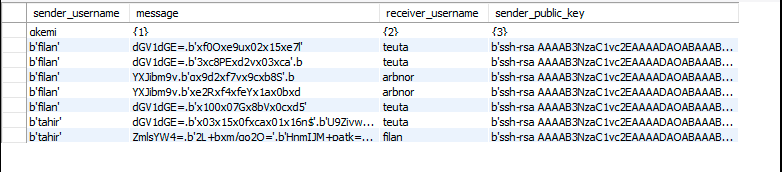
Screenshots nga komanda read message

Ndersa nese mungon qelsi publik





Te dhenat e derguara ne Database.



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)

**Perfundim**: Te gjitha komandat jane perfunduar me sukses.