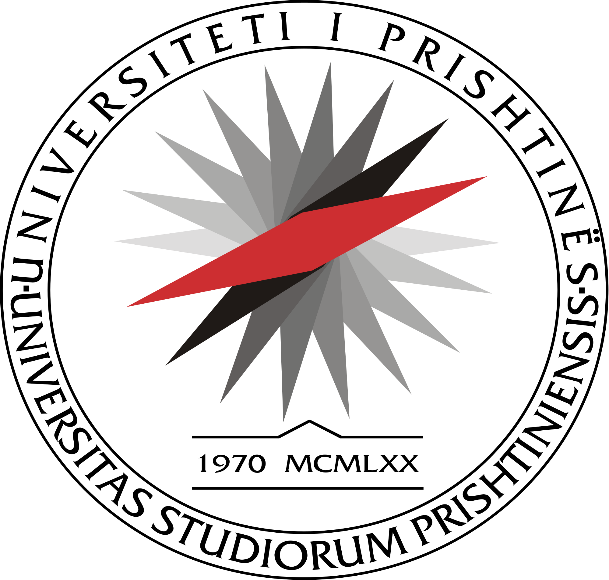
**UNIVERSITETI I PRISHTIN****ËS­**

Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike

Departamenti i Inxhinierisë Kompjuterike

­

**SIGURIA E TË DHËNAVE**

Raporti i fazës së tretë

Studentë: Natyra Vitija Profesori i lëndës: Blerim Rexha

Toni Krasniqi Asistenti i lëndës: Arbnor Halili

Zahir Maliqi

Prishtinë,Qershorë 2020

**Përmbajtja**

1. Hyrje..................................................................................................................................3

2. Komanda create-user……………..........................................................................................4

3. Komanda delete-user….....................................................................................................5

4.Komanda login...................................................................................................................5

5.Komanda status……............................................................................................................6

6.Komanda write-message...................................................................................................6

7.Komanda read-message....................................................................................................7

8.Piket shtese…………………………………………………………………………………………………………………..8

9. Udhëzimet rreth ekzekutimit te komandave…………………………………………………………….…8

# **Abstrakti**

Ky raport ka të bëjë me fazen e tretë të projektit në lënden Siguria e të Dhënave ku si qëllim e kemi vazhdimin dhe zgjerimin e fazës së dytë. Komandat të cilat bazohen në teknika për menaxhimin e fjalëkalimeve dhe vërtetimit të autenticitetit përmes nënshkrimeve digjitale.

Këto komanda janë:

Komanda create-user

Komanda delete-user

Komanda login

Komanda status

Komanda write-message

Komanda read-messag

# **Hyrja**

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.

Hashing është një funksion i njëanshëm ku të dhënat regjistrohen në një vlerë me gjatësi fikse. Hashing është përdorur kryesisht për vërtetim. Salting është një hap shtesë gjatë hashit, që zakonisht shihet në shoqërim me fjalëkalimet hash, që shton një vlerë shtesë në fund të fjalëkalimit që ndryshon vlerën e hash të prodhuar.

Një token sigurie është një pajisje periferike që përdoret për të fituar qasjen në një burim të kufizuar elektronikisht. Tokeni përdoret përveç ose në vend të një fjalëkalimi. Ajo vepron si një çelës elektronik për të pasur akses apo casje në diçka.

Një nënshkrim dixhital është një skemë matematikore për verifikimin e origjinalitetit të mesazheve ose dokumenteve dixhitale. Një nënshkrim i vlefshëm dixhital, ku plotësohen parakushtet, i jep një marrësi një arsye shumë të fortë për të besuar se mesazhi është krijuar nga një dërgues i njohur (autentifikimi), dhe se mesazhi nuk është ndryshuar në tranzit (integritet).

# **Komanda create-user**

Kjo komande ka per detyre qe te krijon një çift publik/privat të RSA .Në fazen e tret tani për të krijuar ciftin e celesave te shfrytezuesit do te të kërkohet edhe fjalëkalimi. Fjalëkalimi duhet të kërkohet përmes inputit.

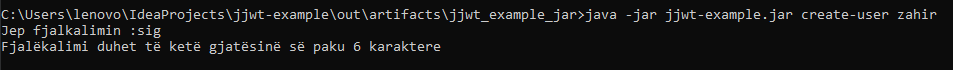
Ekzekutimi I komandes:

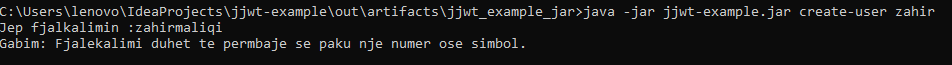
create-user <name>

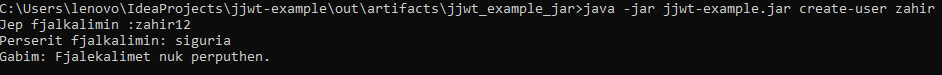
Per shembull:

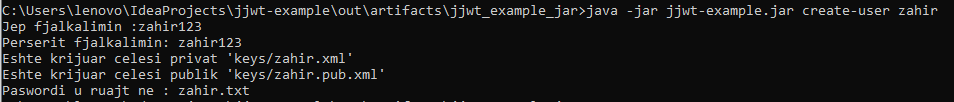
create-user zahir

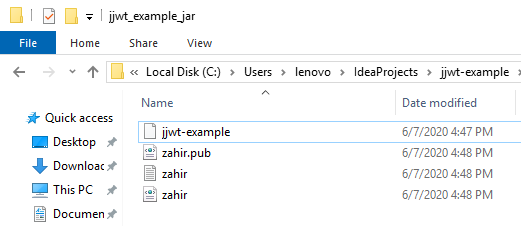
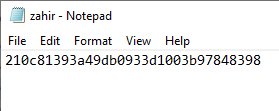
Fjalëkalimi duhet të ketë gjatësinë së paku 6 karaktere.



Fjalëkalimi duhet të ketë gjatësinë së paku 6 karaktere por duhet të përmbajë së paku një numër ose simbol:

Në rastin kur fjalëkalimi ka 6 karaktere (ku perfshihet nje numer ose simbol) atëhere duhet te perseritet:

Nese shkon gjithqka në rregullë atehere do të na krijohen celsat publike dhe private te shfrytezuesit .Dhe fjalëkalimi do te na ruhet ne një txt file me emër si te shfrytezuesit.Ne txt file do ta ruajm paswordin në formë të sigurt përmes hash algoritmeve dhe salting.



# **Komanda delete-user**

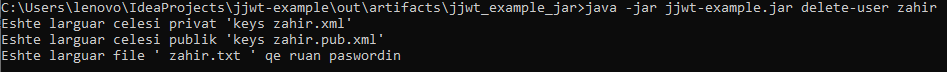
I largon të gjithë çelësat ekzistues të shfrytëzuesit dhe të gjitha të dhënat e shfrytëzuesit nga txt file .Pra e fshinë file txt (që permbane hash-in e paswordit ) me atë emer.

Ekzekutimi I komandes:

delete-user <name>

Per shembull:

delete-user zahir



# **Komanda login**

Teston çiftin shfrytëzues/fjalëkalim. Në rast suksesi lëshohet një token i nënshkruar i cili mund të përdoret për autentikim të shfrytëzuesit.Tokeni e kemi ruajtur ne JWR (JSON Web Tokens).Tokeni ka pjesen e tret te nenshkrimit e tokenit , që përdoret çelësi privat i shfrytëzuesit . Tokeni skadon pas 20 minutave.

Ekzekutimi I komandes:

login <name>

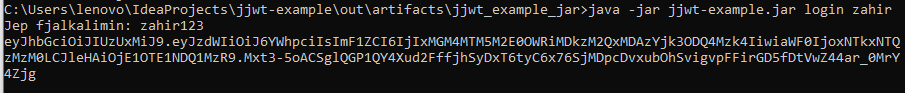
Per shembull:

login zahir

Kemi raste kur nje shfrytëzuesit nuk ia dime fjalëkalimi :



Ose kemi bëre login një shfrytëzues qe fare nuk eshte ekziston ne path-in tone :

Ne rastin kur kemi fjalëkalimi e shfrytëzues mire lëshohet një token i nënshkruar i cili përdoret për autentikim të shfrytëzuesit.

# **Komanda status**

Jep informata rreth tokenit.

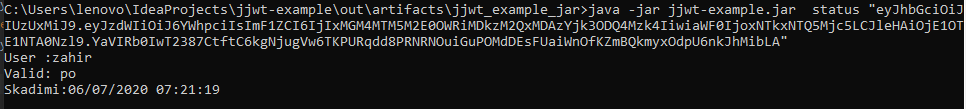
Ekzekutimi I komandes:

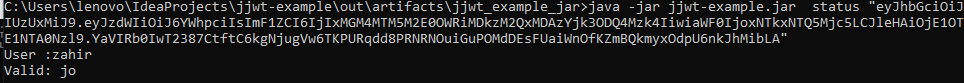
status <token>

Per shembull:

status …

Jep informata rreth tokenit :



Nëse tokeni ka skaduar ose nuk ekziston shfrytëzuesi, atëherë tokeni nuk konsiderohet valid:

Ndersa nese kemi nenshkrime valid , vete jwt refuzon qe te lexoje te dhena:

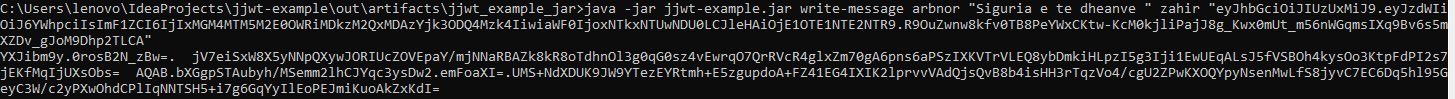
# **Komanda write-message**

Kjo komandë qe e kemi ndertuar ne fazen e dyte zgjerohet ashtu që mund ta pranojë edhe opsionin sender <token>.

Ekzekutimi I komandes:

write-message <name> <message> sender <token>

Per shembull :



Kjo komand zgjerohet ashtu qe :

ciphertext = base64(utf8(<name>)) .

base64(<iv>) .

base64(rsa(<key>)).

base64(des(<message>)) .

base64(utf8(<sender>)) . base64(signature(des(<message>)))

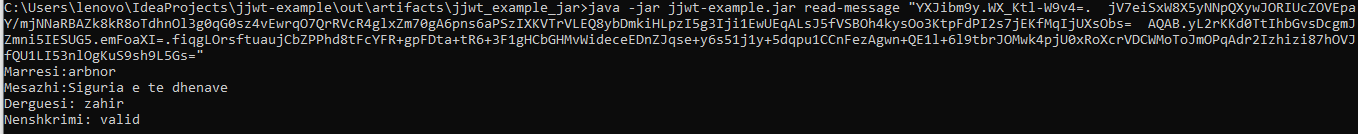
Merret sender nga tokeni dhe behet ne base64 dhe mesazhi i enkriptuar me DES nenshkruhet me celesin private te “sender”.

# **Komanda read-message**

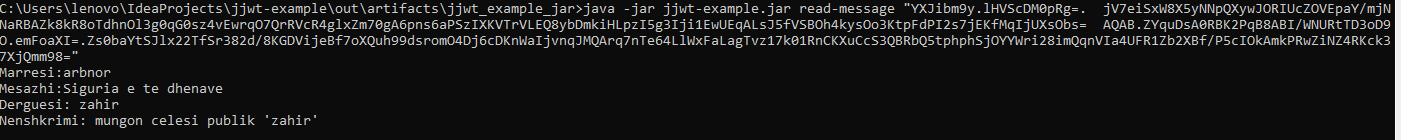
Komanda read-message zgjerohet ashtu që nëse figuron pjesa e dërguesit/nënshkrimit në mesazh, atëherë do të tentohet verifikimi i atij nënshkrimi duke përdorur çelësin publik të dërguesit.

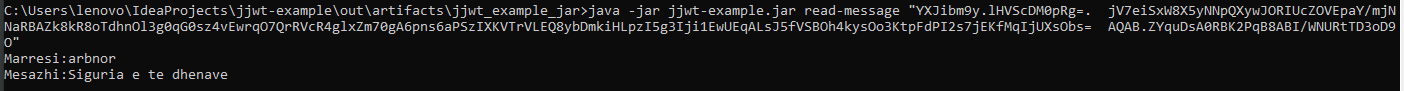
Ekzekutimi I komandes:

read-message <pjesa e fituar nga write-message>

Per shembull :

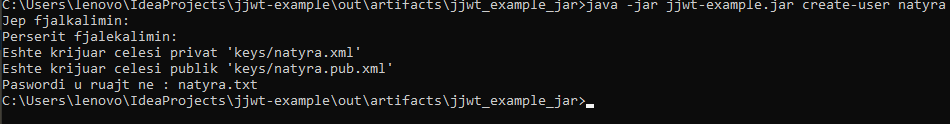
Ekziston mundësia që marrësi nuk e ka çelësin publik të dërguesit:



Nëse mungon pjesa e dërguesit/nënshkrimit, atëherë komanda e injoron dhe vepron sikur në fazën e dytë:

# **Piket shtese**

Lexohet fjalëkalimi pa echo të simboleve në ekran (sikur read -s).



# **Udhezimet rreth ekzektumit te komandave**

# **Komanda create-user:** **create-user <name>**

# **Komanda delete-user: delete-user <name>**

# **Komanda login : login <name>**

# **Komanda status : status <token>**

# **Komanda write-message: write-message <name> <message> sender <token>**

# **Komanda read-message: read-message <pjesa e fituar nga write-message>**