Universiteti i Prishtinës
Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike

Projekti në lëndën Siguria e të Dhënave

Faza e dytë

Blerim Rexha, Arbnor Halili, Edon Gashi

Prill 2020

Abstrakt: Në fazën e dytë të projektit ju do ta zgjeroni programin tuaj me komanda të cilat bazohen në teknikat moderne të enkriptimit simetrik dhe asimetrik. Gjatë implementimit të këtyre kërkesave ju do të shkathtësoheni në përpunimin e të dhënave binare dhe enkodimet e tyre. Ju lusim ta lexoni me kujdes këtë dokument dhe të veproni sipas udhëzimeve.

Përmbajtja

Kërkesat

Detyra juaj është ta zgjeroni programin ekzistues të fazës së parë me komanda të reja. Komandat që duhet t'i shtoni janë të specifikuara në këtë dokument.

Pasi që do ta zgjeroni programin ekzistues, ju duhet ta vazhdoni punën në të njëjtin repository dhe me të njëjtën gjuhë programuese. Pra, duhet ta keni parasysh që:

- Duhet të vazhdohet programi ekzistues, e jo të krijohet i ri.
- Kërkesat të plotësohen ashtu siç janë specifikuar.
- Të gjitha veprimet të kryhen nga programi i njëjtë, pra jo nga një program për secilën komandë.
- Kodet që i merrni të gatshme nga interneti duhet të referencohen në `README`.

Në rast se vendosni ta ndryshoni platformën ose gjuhën programuese, ju duhet t'i ri-implementoni të gjitha kërkesat e fazës së parë në gjuhën e re, përndryshe konsiderohet faza e parë e paplotësuar dhe ju anulohen pikët e arritura.

Rregullat për përpunimin e argumenteve janë të njëjta me të fazës së parë: Në rast se argumentet mungojnë ose janë të jo-valide, atëherë do ta shfaqni një tekst me 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

Sintaksa: `ds create-user <name>`

Krijon një çift të publik/privat të RSA me emrat `<name>.xml` dhe `<name>.pub.xml` brenda direktoriumit të çelësave `keys`.

Direktoriumi i çelësave `keys` është folder që i mban çelësat publik dhe privat. Ky direktorium ruhet diku sipas dëshirës. Mund të jetë relativ ndaj fajllit ekzekutiv, ose mund të jetë në home apo kudo që ju përshtatet juve.

Pra fajllat e krijuar do të jenë `keys/<name>.xml` dhe `keys/<name>.pub.xml`.

Nuk jeni të obliguar t'i ruani çelësat në formatin `xml`. Çelësat mund të ruhen edhe si `pem` fajlla. Madhësia e çelësit është sipas dëshirës. Emrat duhet të përmbajnë vetëm simbolet `A-Z`, `a-z`, `0-9`, dhe `_`. Emrat nuk guxojnë të përmbajnë hapësira.

Shembull:

```
$ ds create-user edon
Eshte krijuar celesi privat 'keys/edon.xml'
Eshte krijuar celesi publik 'keys/edon.pub.xml'

$ ds create-user arbnor
Eshte krijuar celesi privat 'keys/arbnor.xml'
Eshte krijuar celesi publik 'keys/arbnor.pub.xml'

$ ds create-user edon
Gabim: Celesi 'edon' ekziston paraprakisht.
```

Komanda delete-user

I largon të gjithë çelësat ekzistues të shfrytëzuesit.

Sintaksa: `ds delete-user <name>`

Shembull

```
$ ds delete-user edon
Eshte larguar celesi privat 'keys/edon.xml'
Eshte larguar celesi publik 'keys/edon.pub.xml'

$ ds delete-user edon
Gabim: Celesi 'edon' nuk ekziston.

$ ds delete-user blerim
Eshte larguar celesi publik 'keys/blerim.pub.xml'
```

Komanda export-key

Eksporton çelësin publik ose privat të shfrytëzuesit nga direktoriumi i çelësave.

Sintaksa: `ds export-key <public|private> <name> [file]`

Argumenti `<public|private>` e përcakton llojin e çelësit që eksportohet.

Argumenti `<name>` e përcakton çelësin e cilit shfrytëzues të eksportohet.

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.

Shembull:

```
$ ds export-key public edon
<RSAKeyValue>
  <Modulus>xkNfR4...</Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>

$ ds export-key private edon
<RSAKeyValue>
  <Modulus>xkNfR4...</Modulus>
  <Exponent>AQAB</Exponent>
  <P>+EZth9...</P>
  <Q>zG6WRR...</Q>
  <DP>khmvvu...</DP>
  <DQ>IjdMLW...</DQ>
  <InverseQ>kX+viS...</InverseQ>
  <D>IOrUqe...</D>
</RSAKeyValue>

$ ds export-key public arbnor celesi.xml
Celesi publik u ruajt ne fajllin 'celesi.xml'.

$ ds export-key public filan
Gabim: Celesi publik 'filan' nuk ekziston.
```

Shembull:

Ndonjëherë mund ta kemi vetëm çelësin publik të një shfrytëzuesi, prandaj nëse e kërkojmë çelësin privat do të shfaqet një mesazh gabimi.

```
$ ds export-key public blerim
<RSAKeyValue><Modulus>t6oKpf...</RSAKeyValue>

$ ds export-key private blerim
Gabim: Celesi privat 'blerim' nuk ekziston.
```

Komanda import-key

Importon çelësin publik ose privat të shfrytëzuesit nga shtegu i dhënë dhe e vendos në direktoriumin e çelësave.

Sintaksa: `ds import-key <name> <path>`

Argumenti `<name>` e përcakton emrin e çelësit që do të ruhet në direktoriumin `keys`.

Argumenti `<path>` e përcakton shtegun e çelësit që do të importohet.

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.

Shembull:

```
$ ds import-key edon some_public_key.xml
Celesi publik u ruajt ne fajllin 'keys/edon.pub.xml'.

$ ds import-key arbnor some_private_key.xml
Celesi privat u ruajt ne fajllin 'keys/arbnor.xml'.
Celesi publik u ruajt ne fajllin 'keys/arbnor.pub.xml'.

$ ds import-key edon other_key.xml
Gabim: Celesi 'edon' ekziston paraprakisht.

$ ds import-key blerim foto.png
Gabim: Fajlli i dhene nuk eshte celes valid.
```

Nëse shtegu `<path>` fillon me `http://` ose `https://`, atëherë do të dërgohet një GET request në URL `<path>` dhe do të merret trupi i përgjigjes si vlera e çelësit.

Shembull:

```
$ ds import-key blerim https://pastebin.com/raw/568vxV7i
Celesi publik u ruajt ne fajllin 'keys/blerim.pub.xml'.
```

Komanda write-message

E shkruan një mesazh të enkriptuar të dedikuar për një shfrytëzues.

Sintaksa: `ds write-message <name> <message> [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.

Enkriptimi bëhet sipas skemës në vijim:

```
ciphertext = base64(utf8(<name>)) . base64(<iv>)
  . base64(rsa(<key>)) . base64(des(<message>))
```

Në skemën e mësipërme termet paraqesin:

- `<name>` dhe `<message>` janë argumentet e komandës.
- `base64` paraqet procesin e enkodimit të bajtave përmes Base64.
- `utf8` paraqet procesin e enkodimit të tekstit në bajta sipas UTF8.
- `rsa` paraqet enkriptimin përmes RSA me çelësin publik `keys/<name>.pub.xml`.
- `<iv>` dhe `<key>` janë vlera 8 bajtëshe të gjeneruara rastësisht.
- `des` paraqet enkriptimin përmes DES me çelësin `<key>`.
- Karakteri `.` paraqet ndarësin ndërmjet komponenteve në ciphertext.

Shembull:

```
$ ds write-message blerim "Takimi mbahet te premten ne ora 11:00"
Ymxlcmlt.MTIzNDU2Nzg=.cnNhKGZpZWsyMDE4KQ==.
ZGVzKFRha2ltaSBtYmFoZXQgdGUgcHJlbXRlbiBuZSBvcmEgMTE6MDAp

$ ds write-message arbnor "Pershendetje" ciphertext.txt
Mesazhi i enkriptuar u ruajt ne fajllin 'ciphertext.txt'.

$ ds write-message filan "Pershendetje"
Gabim: Celesi publik 'filan' nuk ekziston.
```

Komanda read-message

E dekripton dhe e shfaq në console mesazhin e enkriptuar.

Sintaksa: `ds read-message <encrypted-message>`

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.

Shembull:

```
$ ds read-message "ZWRvbg==.MTIzNDU2Nzg=.cnNhKGZpZWsyMDE4KQ==.ZGVz..."
Marresi: edon
Mesazhi: Takimi mbahet te premten ne ora 11:00

$ ds read-message "Ymxlcmlt.MTIzNDU2Nzg=.cnNhKGZpZWsyMDE4KQ==.ZGVz..."
Gabim: Celesi privat 'keys/blerim.xml' nuk ekziston

$ ds read-message ciphertext.txt
Marresi: arbnor
Mesazhi: Pershendetje
```

Vlerësimi

Kjo fazë vlerësohet me maksimalisht 10 pikë.

Ju do të gjykoheni në bazë të:

- Kërkesave të plotësuara.
- Cilësisë së kodit.
- Korrektësisë në menaxhimin e repository.
- Njohurive teorike.
- Njohurive teknike.

Dorëzimi

Repository ekzistues mund ta përditësoni deri më datën **30.04.2020 23:59**.

Në `README` duhet të figurojnë këto informata:

1. Udhëzimet për kompajllimin dhe ekzekutimin e programit.
2. Udhëzimet se çfarë bëjnë dhe si duhet të ekzekutohen komandat.

Gjithashtu kujdesuni ta keni ose ta përditësoni `.gitignore` adekuate ashtu që mos të ngarkohen fajlla të padobishëm në repository.

Kujdes: Cilido lloj i plagjiaturës, qoftë në kod apo në përshkrim, do të ndëshkohet me **0 pikë për të gjitha grupet ku gjendet materiali i kopjuar**, pavarësisht se cili grup e ka punuar i pari.