

Universiteti i Prishtinës
Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike



Projekti në lëndën Siguria e të Dhënave

Faza e parë, Grupi 11

Blerim Rexha, Arbnor Halili, Edon Gashi

Mars 2020

Abstrakt: Kjo fazë ka për qëllim familjarizimin tuaj me teknikat klasike të enkriptimit dhe përpunimin e të dhënave tekstuale. Këto teknika do t'i demonstroi duke e shkruar një program të thjeshtë i cili ofron disa shërbime përmes komandave. Ju lusim ta lexoni me kujdes këtë dokument dhe të veproni sipas udhëzimeve.

Përmbajtja

Kërkesat	3
Komanda vigenere	4
Nënkomanda encrypt	4
Nënkomanda decrypt	4
Komanda playfair	5
Nënkomanda encrypt	5
Nënkomanda decrypt	5
Komanda numerical	6
Nënkomanda encode	6
Nënkomanda decode	6
Vlerësimi	7
Dorëzimi	7

Kërkesat

Detyra juaj është ta shkruani një console program me emrin `ds` i cili pranon komanda përmes argumenteve. Programi juaj do t'i analizojë argumentet, dhe varësisht nga përmbajtja e tyre do ta ekzekutojë ndonjërin prej komandave të specifikuara.

Argumentet janë termet që vijnë pas programit. Shumica e ambienteve programuese mundësojnë leximin e tyre, psh. `String[] args` në Java, `process.argv` në Node, `sys.argv` në Python, etj.

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 fajllë, programi duhet ta trajtojë gabimin dhe ta shfaqë në ekran një mesazh përshkrues.

Nuk ka kufizim sa i përket gjuhës programuese, por duhet ta keni parasysh që:

- 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 komente.

Në vazhdim e gjeni specifikimin e komandave, ku përfshihen edhe shembuj të përdorimit të tyre.



Shënim: Edhe pse preferohet të implementohet programi në console, jeni të lirë ta zhvilloni në platformë tjetër sipas dëshirës (GUI, Web) me kushtin që të ofrohet funksionaliteti ekuivalent dhe të respektohen rregullat e mësipërme.

Komanda vigenere

Vigenère Cipher është version më i avancuar i Kodit të Cezarit pasi që përdor më shumë se një zhvendosje si çelës. Lexo më shumë *këtu*.

Nënkomanda encrypt

Sintaksa: `ds vigenere encrypt <key> <plaintext>`

Enkripton plaintextin <plaintext> me një çelës <key> përmes algoritmit të Vigenère dhe e shtyp ciphertextin në ekran.

Shembull:

```
$ ds vigenere encrypt siguria "Pershendetje nga FIEK!"  
Hmxmymnvmzdv vgs NOYB!
```

Nënkomanda decrypt

Sintaksa: `ds vigenere decrypt <key> <ciphertext>`

Dekripton ciphertextin <ciphertext> me një çelës <key> përmes algoritmit të Vigenère dhe e shtyp plaintextin në ekran.

Shembull:

```
$ ds vigenere decrypt siguria "Hmxmymnvmzdv vgs NOYB!"  
Pershendetje nga FIEK!
```

Komanda playfair

Cipher që transformon plaintextin përmes një table 5×5 dhe disa rregullave. Lexo më shumë **këtu**.

Nënkomanda encrypt

Sintaksa: `ds playfair encrypt <key> <plaintext>`

Enkripton plaintextin `<plaintext>` me një çelës `<key>` përmes Playfair Cipher dhe e shtyp ciphertextin në ekran.

Shembull:

```
$ ds playfair encrypt siguria "takohemi nesar"  
ne hp mb hr ta ra gz
```

Nënkomanda decrypt

Sintaksa: `ds playfair decrypt <key> <ciphertext>`

Dekripton ciphertextin `<ciphertext>` me një çelës `<key>` përmes Playfair Cipher dhe e shtyp plaintextin në ekran.

Shembull:

```
$ ds playfair decrypt siguria "ne hp mb hr ta ra gz"  
takohemineser
```



Pikë shtesë

Të shtohet opsioni `--table`, i cili nëse i shtohet komandës do të paraqitet në ekran tabela 5×5 e ndërtuar nga çelësi.

Komanda numerical

Me këtë enkodim secila shkronjë zëvendësohet me pozitën e saj në alfabet. Kështu shkronja “a” enkodohet në numrin 1, shkronja “b” në numrin 2, etj.

Nënkomanda encode

Sintaksa: `ds numerical encode <text>`

Enkodon tekstin `<text>` në pozitat alfabetike të shkronjave.

Shembull:

```
$ ds numerical encode "takohemi nesar"  
20 1 11 15 8 5 13 9 14 5 19 5 18
```

Nënkomanda decode

Sintaksa: `ds numerical decode <code>`

Dekodon vargun `<code>` nga shifrat në shkronjat përkatëse.

Shembull:

```
$ ds numerical decode "20 1 11 15 8 5 13 9 14 5 19 5 18"  
takohemineser
```



Pikë shtesë

Të shtohet opsioni `--separator <char>` i cili e specifikon karakterin ndarës.
Të ruhen hapësirat në tekstin origjinal duke i enkoduar në ndonjë karakter.

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.



Pikët shtesë: Në disa vende mund të jenë cekur kërkesa shtesë. Nuk jeni të obliguar t'i plotësoni këto kërkesa, por do të shpërbleheni me pikë shtesë nëse arrini t'i implementoni.

Dorëzimi

Kodi burimor i programit duhet të vendoset në GitHub para datës **20.03.2020 23:59**. Në rast se repository bëhet privat atëherë duhet të ofrohet qasje leximi në llogarinë edongashi (edon.gashi@uni-pr.edu).

Në [README](#) duhet ta bëni një përshkrim të shkurtër të projektit. Pikat që duhet t'i diskutoni janë:

1. Udhëzimet për ekzekutimin e programit.
2. Përshkrim i shkurtër për secilën komandë.
3. Rezultatet e ekzekutimit me nga një shembull për secilën komandë dhe nënkomandë.

Gjithashtu kujdesuni ta vendosni një `.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.