Univerza v Ljubljani, Fakulteta za elektrotehniko
Podiplomski magistrski študijski program 2. stopnje Elektrotehnika
Biomedicinska tehnika - Biomedicinska informatika

NAVODILA

Vaja 4: Šifriranje podatkov

Pripravila: Žiga Bizjak & Tomaž Vrtovec

Navodila

Šifriranje podatkov ali kriptografija je področje skrivnega pisanja sporočil in njihovega razkrivanja, omogoča pa mehanizme za zaščito, zasebnost in zaupnost podatkov. Na podlagi preprostega algoritma šifrirajte oz. dešifrirajte dano besedilo z izbranim ključem, pri čemer ga v uporabno obliko pretvorite s kodiranjem oz. dekodiranjem po shemi Base64.

1. Napišite funkcijo za šifriranje besedila oz. čistopisa:

```
def encryptText(iText, iKey):
    # ...
    # your code goes here
    # ...
return oText
```

kjer vhodni argument `iText` predstavlja čistopis in `iKey` šifrirni ključ, izhodni argument `oText` pa predstavlja šifropis. Šifriranje opravite tako, da številčne vrednosti čistopisa prištejete številčnim vrednostim ključa (ključ po potrebi ponavljate do dolžine čistopisa).

Šifropis na koncu kodirajte po shemi Base64, v ta namen pa napišite funkcijo:

```
def encodeBase64(iText):
    # ...
    # your code goes here
    # ...
return oText
```

kjer vhodni argument `iText` predstavlja besedilo, izhodni argument `oText` pa besedilo, kodirano po shemi Base64.

Za pretvorbo med številčnimi vrednostmi in znaki besedila uporabite Python funkciji `ord` in `chr()`, za pretvorbo med desetiškim in dvojiškim sistemom pa Python funkcijo `binary_repr()`. Številčne vrednosti in znake besedila za kodiranje po shemi Base64 pridobite iz datoteke tableBASE64and58.csv.

2. Napišite funkcijo za dešifriranje besedila oz. šifropisa:

```
def decryptText(iText, iKey):
    # ...
    # your code goes here
    # ...
return oText
```

kjer vhodni argument `iText` predstavlja šifropis in `iKey` dešifrirni ključ, izhodni argument `oText` pa predstavlja čistopis. Dešifriranje opravite tako, da številčne vrednosti ključa odštejete od številčnih vrednosti šifropisa (ključ po potrebi ponavljate do dolžine šifropisa).

Šifropis najprej dekodirajte po shemi Base64, v ta namen pa napišite funkcijo:

```
def decodeBase64(iText):
    # ...
    # your code goes here
    # ...
return oText
```

kjer vhodni argument `iText` predstavlja besedilo, izhodni argument `oText` pa besedilo, dekodirano po shemi Base64.

Postopek je obraten šifriranju besedila, pomagajte pa si z enakimi Matlabovimi funkcijami kot pod točko 1.

Vprašanja

Odgovore na sledeča vprašanja zapišite v poročilo, v katerega vstavite zahtevane izrise in programske kode.

1. Čistopis `'Biomedicinska informatika'` šifrirajte z opisanim algoritmom, pri čemer za šifrirni ključ uporabite `'enkripcija'` in rezultat kodirate po shemi Base64. Zapišite dobljeni šifropis (tj. šifrirani in kodirani čistopis).

2. Šifropis `'uNSL3M6Q2crUwoT/36CJpIPjis/F2Nfh39/QifTKytfU5Mrezc6K0dPJzObU39mJ2tPNhdvkztTQzt7WhN+L29bV0djXgabO2t/O1MzM08/X0MyS0t7J2NzOxdnU3cqe'` dešifrirajte z opisanim algoritmom, pri čemer ga dekodirate po shemi Base64 in rezultat dešifrirate s ključem `'dekripcija'`. Zapišite dobljeni čistopis.

3. Glede na podatke iz vprašanj 1. in 2., zapišite dolžino (v bajtih), in sicer (a) čistopisa, (b) šifriranega in kodiranega čistopisa, (c) šifropisa in (d) dekodiranega in dešifriranega šifropisa. Odgovore ustrezno obrazložite v povezavi z dolžino začetnega besedila (čistopisa oz. šifropisa).

4. Zakaj je uporabno kodiranje po shemi Base64? Obrazložite odgovor.

5. Niz `'q9rOgtbXgt3by9bWx9iJxNzVONbUw6eJrM7Xx+eJsNzfw9ikgrHK1uLWgt/YzODd2M6jgp6bkKSXk6aflC'` predstavlja besedilo, ki je bilo šifrirano in kodirano s pomočjo opisanih algoritmov, pri čemer je šifrirni ključ neznan. Na osnovi izčrpnega iskanja (preverjanja vseh mogočih kombinacij) dešifrirajte besedilo ter poiščite šifrirni ključ, pri čemer upoštevate informacije, da besedilo vsebuje besedo `'Janez'` ter da ključ sestavljajo natančno tri male črke angleške abecede (`znaki = ['a':'z']`). Za iskanje prisotnosti niza znakov v danem besedilu si lahko pomagate s Python funkcijo `if part in text`

   Priložite programsko kodo ter zapišite dobljeni šifrirni ključ ter dešifrirano besedilo.

Dodatek

Odgovore na sledeče probleme ni potrebno prilagati k poročilu, prispevajo pa naj k boljšemu razumevanju vsebine.

Kodiranje po shemi Base58 je v primerjavi s shemo Base64 prilagojeno za izogibanje nealfanumeričnim znakom kot tudi alfanumeričnim znakom, ki so lahko zaznani dvoumno. V shemi Base58 tako ne nastopajo znaki + (plus), / (poševnica), 0 (številka nič), O (velika črka o),

I (velika črka i) ter l (mala črka L). Tako kodiranje se uporablja npr. za naslove valute BitCoin ter za ustvarjanje kratkih spletnih naslovov na portalu Flickr.

Napišite funkciji za kodiranje in dekodiranje po shemi Base58, ki je shranjena v datoteki table-BASE64and58.csv. Upoštevajte, da je shema Base58 namenjena kodiranju celih števil v besedila oz. dekodiranju besedil v cela števila, temelji pa na iskanju ostanka deljenja z 58.