Pràctica 1 - Criptografia

Presentació

En aquesta pràctica ens familiaritzarem amb el paquet matemàtic SAGE tot implementant un criptosistema històric, concretament la xifra nihilista. Aquest criptosistema va ser utilitzat pel moviment nihilista rus de la dècada del 1880 per organitzar actes de terrorisme contra el tsar, actes que van acabar amb la pròpia vida del tsar Alexandre II. En aquesta pàgina web[1] podeu trobar l'explicitació del criptosistema amb algun exemple.

Descripció de la PAC/pràctica a realitzar

La xifra nihilista es construeix a partir d'un quadrat de Polibi (veure Annex 1). En la nostra implementació, en comptes d'utilitzar un únic quadrat de Polibi fixat, farem que la clau per a xifrat/desxifrar la formin dues components, la primera permetrà obtenir el quadrat de Polibi i la segona component serà la clau pròpiament dita del xifrat nihilista.

Per implementar el criptosistema nihilista el dividirem en tres funcions: la generació de la clau, el xifrat d'un text en clar i el desxifrat d'un text xifrat. A continuació es proporcionen els detalls de les tres funcions:

1. Programeu una funció que implementi la generació de la clau de la xifra nihilista. **(2 punts)**

   La funció prendrà com a argument dues paraules i retornarà, d'una banda la matriu 5x5 que forma el quadrat de Polibi generat a partir de la primera paraula (veure l'Annex 1 d'aquest enunciat) i d'altra banda, la segona paraula exactament igual que en l'entrada. En cas que la funció no rebi alguna de les paraules com a argument, la funció generarà la clau amb dues paraules generades de forma aleatòria.

   Exemple:

   ```
   input: ['HELLO','FRIEND']
   sortida: ([['H', 'E', 'L', 'O', 'A'], ['B', 'C', 'D', 'F', 'G'], ['I', 'K', 'M','N', 'P'], ['Q', 'R', 'S', 'T', 'U'], ['V', 'W', 'X', 'Y', 'Z']], 'FRIEND')
   ```

1 http://goo.gl/TUDknD

2. Programeu una funció que implementi el procés de xifrat nihilista. **(4 punts)**

   La funció prendrà com a arguments a) el missatge i b) la clau.

   a) `missatge`: el primer argument contindrà el missatge de text en clar que volem xifrar.

   b) `clau`: el segon argument contindrà la clau, tal i com s'obté de la funció de generació de la clau.

   La funció retornarà el missatge xifrat, com un vector de nombres.

   Exemple:

   ```
   missatge: 'MYFIRSTCIPHER'
   clau: ([['H', 'E', 'L', 'O', 'A'], ['B', 'C', 'D', 'F', 'G'], ['I', 'K', 'M','N', 'P'], ['Q', 'R', 'S', 'T', 'U'], ['V', 'W', 'X', 'Y', 'Z']], 'FRIEND')
   sortida:
   [57, 96, 55, 43, 76, 66, 68, 64, 62, 47, 45, 35, 66]
   ```

3. Programeu una funció que implementi el procés de desxifrat de la xifra nihilista. **(4 punts)**

   La funció prendrà com a arguments a) el missatge i b) la clau.

   a) `missatge`: el primer argument contindrà el missatge xifrat que volem desxifrar, codificat com un vector de nombres.

   b) `clau`: el segon argument contindrà la clau, tal i com s'obté de la funció de generació de claus.

   La funció retornarà el missatge en clar.

   Exemple:

   ```
   missatge: [36, 95, 46, 45, 69, 36, 36]
   clau: ([['H', 'E', 'L', 'O', 'A'], ['B', 'C', 'D', 'F', 'G'], ['I', 'K', 'M','N', 'P'], ['Q', 'R', 'S', 'T', 'U'], ['V', 'W', 'X', 'Y', 'Z']], 'FRIEND')
   sortida: 'EXAMPLE'
   ```

Format i data de lliurament

La data màxima de lliurament de la pràctica és el 24/03/2014 (a les 24 hores).

Juntament amb l'enunciat de la pràctica trobareu l'esquelet de la mateixa en format SAGE notebook worksheet (extensió .sws). Aquest mateix fitxer és el que heu de lliurar un cop hi codifiqueu totes les funcions.

En aquest esquelet també hi trobareu inclosos els jocs de proves dels diferents apartats. Tal i com s'esmenta en el fitxer sws, **no es pot modificar cap part del fitxer corresponent al joc de proves**. Això vol dir que heu de respectar el nom de les funcions i variables que s'han definit en aquest esquelet.

El lliurament de la pràctica constarà de d'**un únic fitxer** SAGE worksheet (extensió sws) on heu inclòs la vostra implementació.

Annex 1

Existeixen diferents criptosistemes històrics que utilitzen com a clau (o com a part d'ella) una matriu on s'hi inclouen les lletres de l'abecedari. Aquestes matrius es denominen quadrats de Polibi ja que va ser aquest historiador grec (que visqué al voltant dels anys 205 a 120 aC) qui en va proposar el seu ús.

Un sistema molt simple per poder compartir quadrats de Polibi entre emissor i receptor sense haver de recordar tota la matriu és generar-la a partir d'una paraula clau que és més fàcilment memoritzable. Per a generar el quadrat de Polibi, es parteix de la paraula clau i es va omplint la matriu primer posant les lletres de la clau, sense repetir-les, i, un cop acabades, completant la matriu amb les lletres de l'abecedari que falten, en ordre alfabètic.

Per exemple, si la paraula clau és “CRYPTOGRAPHY” la matriu resultant seria:

$$\begin{pmatrix} C & R & Y & P & T \\ O & G & A & H & B \\ D & E & F & I/J & K \\ L & M & N & Q & S \\ U & V & W & X & Z \end{pmatrix}$$