Pràctica 1 - Criptografia

Presentació

En aquesta pràctica ens familiaritzarem amb el paquet matemàtic SAGE tot implementant un criptosistema històric, concretament la xifra dels Quatre-Quadrats. Aquest criptosistema va ser proposat pel criptògraf francès Félix-Marie Delastelle (1840-1902).

Competències

Competències transversals:

- Us i aplicació de les TIC en l'àmbit acadèmic i professional.
- Capacitat de comunicació en llengua estrangera.
- Capacitat per adaptar-se a les tecnologies i als futurs entorns actualitzant les competències professionals.

Competències específiques:

- Capacitat de fer servir fonaments matemàtics, estadístics i físics per a entendre els sistemes TIC.
- Capacitat d'analitzar un problema en el nivell d'abstracció adequat a cada situació i aplicar les habilitats i coneixements adquirits per resoldre'l.

Objectius

- Familiaritzar-se amb l'entorn de treball SAGE.
- Implementar un criptosistema històric.

Descripció de la PAC/pràctica a realitzar

La xifra dels Quatre-Quadrats va ser proposat pel criptògraf francès Félix-Marie Delastelle (1840-1902) i es tracta d'un criptosistema de substitució poligràfica, en el qual la mida dels blocs de lletres a xifrar és de dos caràcters. A la pàgina anglesa de la wikipèdia[1] podeu trobar l'explicitació detallada del criptosistema, incloent-hi també algun exemple.

Per implementar la xifra dels Quatre-Quadrats dividirem la feina 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 dels *Quatre-Quadrats*. **(2 punts)**

   La funció prendrà com a arguments les dues paraules que generen cada una de les matrius i retornarà les quatre matrius que formen la clau. L'ordre amb que la funció retornarà les quatre matrius serà: superior-esquerra, inferior-esquerra , superior-dreta, inferior-dreta.

   Exemple:

   `keyword1: 'HELLO'`

   `keyword2: 'WORLD'`

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

2. Programeu una funció que implementi el procés de xifrat de la xifra dels *Quatre-Quadrats*. **(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 una cadena de caràcters amb la clau, tal i com s'obté de la funció de generació de la clau.

   La funció retornarà el missatge xifrat.

   Exemple:

   `missatge: 'FIRSTEXERCISE'`

1 http://goo.gl/u5KC0

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

sortida: 'FASNURZLSODRLZ'
```

3. Programeu una funció que implementi el procés de desxifrat de la xifra dels *Quatre-Quadrats*. **(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.

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

   La funció retornarà el missatge en clar.

   Exemple:

```
missatge: 'RISJJEWZLUYARI'

clau: '([['A', 'B', 'C', 'D', 'E'], ['F', 'G', 'H', 'I', 'J'],
['K', 'L', 'M', 'N', 'O'], ['P', 'R', 'S', 'T', 'U'], ['V', 'W', 'X',
'Y', 'Z']], [['F', 'R', 'I', 'E', 'N'], ['D', 'S', 'A', 'B', 'C'], ['G',
'H', 'J', 'K', 'L'], ['M', 'O', 'P', 'T', 'U'], ['V', 'W', 'X', 'Y',
'Z']], [['A', 'L', 'W', 'Y', 'S'], ['B', 'C', 'D', 'E', 'F'], ['G', 'H',
'I', 'J', 'K'], ['M', 'N', 'O', 'P', 'R'], ['T', 'U', 'V', 'X', 'Z']],
[['A', 'B', 'C', 'D', 'E'], ['F', 'G', 'H', 'I', 'J'], ['K', 'L', 'M',
'N', 'O'], ['P', 'R', 'S', 'T', 'U'], ['V', 'W', 'X', 'Y', 'Z']])'

sortida: 'SECONDEXERCISE'
```

Recursos

Bàsics

- Four Square Cipher (**http://en.wikipedia.org/wiki/Four-square_cipher**)
- Mòdul 1: Introducció a la criptografia.
- Mòdul 2: Fonaments de criptografia.

Criteris de valoració

En cada apartat trobareu la puntuació que se li assigna.

Format i data de lliurament

La data màxima de lliurament de la pràctica és el 23/03/2015 (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 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[2]) on heu inclòs la vostra implementació.

2 No s'acceptaran lliuraments que estiguin en altres formats: zip, rar, sagews, ...