CS

AES Lab

En aquesta pràctica farem el xifrat d'AES pas a pas de forma manual (o relativament manual). L'objectiu es entendre com funciona cada etapa de xifrat i com es fa cadascuna de les operacions. Per aixo es demana implementar les principals funcions de xifrat d'AES i xifrar un text curt d'exemple.

1 Text a xifrar

El text a xifrar ha de ser un string amb els vostres noms (y algun caràcter addicional si cal fer padding). L'string ha de tenir 16 caràcters, ja que cada caràcter es representarà amb un byte. Per això farem servir el codi UTF-8 (o ASCII) del caràcter. P.e. si volem xifrar el nom "Ennio Morricone" el codificarem com:

E	n	n	i	o		M	o	r	r	i	c	o	n	e	
45	6e	6e	69	6f	20	4d	6f	72	72	69	63	6f	6e	65	20

es a dir com a la cadena de bits que en hexadecimal representem com `45 6e 6e 69 6f 20 4d 6f 72 72 69 63 6f 6e 65 20`.

Una de les moltes maneres en les que podeu convertir un string a una llista amb el codi corresponent és mitjançant la funció `ord`:

```
>>> [hex(ord(c)) for c in "Ennio Morricone "]
['0x45', '0x6e', '0x6e', '0x69', '0x6f', '0x20', '0x4d', '0x6f', '0x72',
 '0x72', '0x69', '0x63', '0x6f', '0x6e', '0x65', '0x20']
```

2 Clau

Podeu triar la clau que vulgueu. Per simplificació es recomana fer servir una clau de 128 bits (16 caràcters). Per exemple, una possible clau, en hexadecimal podria ser: `00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff`.

3 Xifrat amb AES

Cal que xifreu el text en clar amb la clau fent servir AES. Per això caldrà que feu totes les operacions amb les iteracions corresponents (veure Figura 1). El mode d'operació de xifrat ha sigut ECB. Noteu que només xifrem un sol bloc.

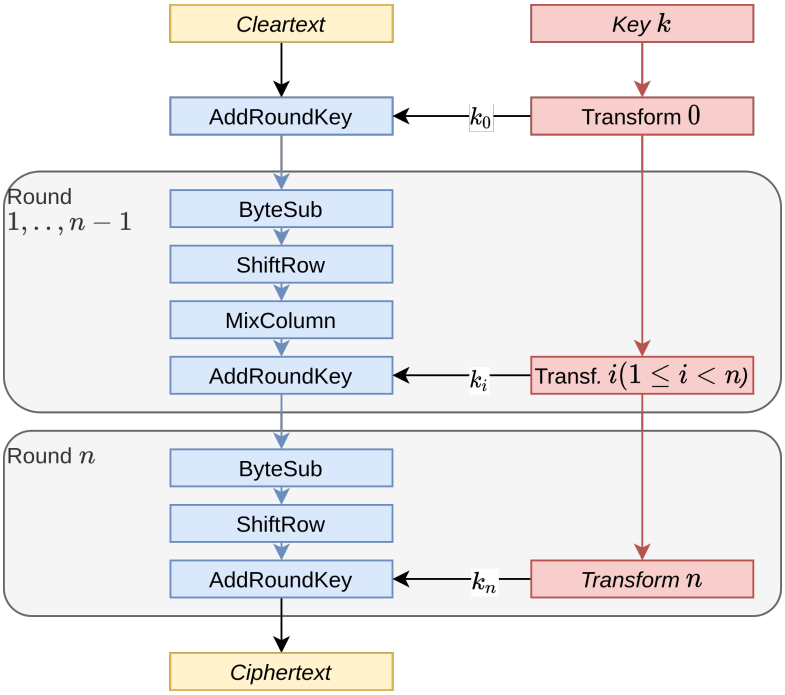

Figure 1: Operacions de xifrat de l'AES.

- Ho podeu implementar com més us convingui. Podeu fer una implementació en Python o en qualsevol altre llenguatge, fer les funcions manualment, ...En qualsevol cas cal de especifiqueu com s'ha fet (si es la funció, cal que doneu la funció i si ho heu fet manualment, cal que indiqueu les operacions que heu fet). Noteu que el fet de fer-ho d'una o altra manera no tindrà repercussió en la nota. Es valorarà que sigui correcte, no que s'hagi fet d'una o altra manera.
- Podeu fer servir material que trobeu per Internet però sempre cal que citeu la font i expliqueu perque i com ho feu servir. P.e. si trobeu una funció que fa la operació X i la feu servir cal que expliqueu com és aquella operació.

4 Lliurament

Cal que lliureu dos fitxers:

- Un informe en un fitxer comprimit que ha de contenir el codi del vostre programa
- Un PDF amb la memòria amb la informació que es detalla a continuació.

1. La pràctica es farà en grups de dues persones.
2. Dades personal: nom i cognoms dels integrants del grup. Només es lliurarà un informe per grup.
3. Estructura general de l'operació de xifrat. Cal indicar el nom de les operacions, l'ordre i el nombre d'interacions. Podeu indicar-ho de forma esquemàtica.

4. Primer resultat de cada operació. El primer cop que es faci una operació concreta: *AddRoundKey*, *ByteSub*, *ShiftRow*, ... Cal que doneu la següent informació:
   - Matriu d'estat d'entrada i de sortida.
   - Descripció de l'operació i indicació dels càlculs
   - Com s'ha fet el càlcul?: ho heu implementat vosaltres, heu fet el càlcul manualment, heu fet servir alguna llibreria?
5. Resultat de xifrat final.
6. Cal que verifiqueu el resultat. Per això heu de desxifrar el ciphertext amb la mateixa clau i veure que obteniu el resultat esperat. Cal que expliqueu com heu fet aquesta verificació. Podeu fer servir alguna implementació existent de AES o fer-la vosaltres.

5 Alguns enllaços d'interès

- AES animation `https://formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng-html5.html`
- Cryptography (pyca). `https://github.com/pyca/cryptography`
- PyCryptodome. `https://github.com/Legrandin/pycryptodome`
- AES (step-by-step) CrypTool Online. `https://www.cryptool.org/en/cto/aes-step-by-step`
- M2Crypto. `https://gitlab.com/m2crypto/m2crypto` (OpenSSL wrapper)