Pràctica 2 - Criptografia

Presentació

En aquesta pràctica treballarem els diferents modes d'operació de les xifres de bloc i veurem les conseqüències d'utilitzar cadascun d'aquests modes. En primer lloc, implementarem el DES amb els modes d'operació ECB, CBC i CFB. Després, utilitzarem aquestes funcions per analitzar els resultats de xifrar imatges amb els diferents modes d'operació. D'aquesta manera podrem veure, de manera visual, quins efectes tenen els diferents modes de xifratge sobre el contingut xifrat que s'obté.

Competències

Competències transversals:

- Us i aplicació de les TIC en l'àmbit acadèmic i professional.
- 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'ús del criptosistema DES.
- Comprendre com funcionen els diferents modes de xifrat en bloc.
- Veure com afecten els diferents modes de xifrat al missatge xifrat.

Descripció de la Pràctica a realitzar

Exercici 1 (5 punts)

En aquest primer exercici implementarem una variant del criptosistema DES, que anomenarem UOC-DES.

La variant UOC-DES implementarà el DES tal i com està descrit en el mòdul didàctic de "xifres de clau compartida: xifres de bloc", però modificant el funcionament de les taules S de la següent manera:

> Cada caixa, S_j , rebrà el seu bloc corresponent de 6 bits $B_j = b_1b_2b_3b_4b_5b_6$, i en retornarà un de 4 bits de llargada, d'acord amb la taula inclosa a les pàgines 16 i

17 dels materials i el criteri per mitjà del qual s'assignarà una fila i una columna d'una caixa a B_j és el següent: l'índex j fixarà la caixa S_j, l'enter corresponent a b_1b_2 seleccionarà la fila i l'enter que correspon a $b_3b_4b_5b_6$ determinarà la columna.

Per a desenvolupar el UOC-DES cal que implementeu les següents funcions que us permetran validar la correcció de la vostra implementació amb el joc de proves que us proporcionem:

1. Implementeu una funció que permeti xifrar un bloc de 64 bits fent servir el UOC-DES. **(1 punt)**

   La funció prendrà com a arguments el bloc de bits a xifrar i una clau.

   a) `clar`: el primer argument contindrà el bloc de 64 bits a xifrar.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   La funció retornarà el bloc de bits xifrat fent servir UOC-DES.

2. Implementeu una funció que permeti desxifrar un bloc de 64 bits fent servir UOC-DES. **(1 punt)**

   La funció prendrà com a arguments el bloc xifrat i la clau.

   a) `xifrat`: el primer argument contindrà el bloc de 64 bits amb el contingut xifrat.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   La funció retornarà el bloc desxifrat.

3. Implementeu una funció que permeti xifrar una cadena de bits amb UOC-DES fent servir el mode d'operació ECB. **(0,5 punts)**

   La funció prendrà com a arguments una cadena de bits a xifrar i una clau.

   a) `clar`: el primer argument contindrà una cadena de bits amb el contingut a xifrar.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   La funció retornarà la cadena de bits xifrada fent servir UOC-DES en mode ECB. Per tal de simplificar la funció, assumirem que les cadenes rebudes sempre tenen una mida múltiple de 64 bits.

4. Implementeu una funció que permeti desxifrar cadenes de bits fent servir UOC-DES en mode ECB. **(0,5 punts)**

La funció prendrà com a arguments el contingut xifrat i la clau. De la mateixa manera que amb la funció de xifratge, assumirem que les cadenes de bits a desxifrar sempre tenen una mida múltiple de 64 bits.

a) `xifrat`: el primer argument contindrà una cadena de bits amb el contingut xifrat.

b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

La funció retornarà el contingut desxifrat.

5. Implementeu una funció que permeti xifrar una cadena de bits amb UOC-DES fent servir el mode d'operació CBC. **(0,5 punts)**

   La funció prendrà com a arguments una cadena de bits a xifrar, una clau i el vector inicial.

   a) `clar`: el primer argument contindrà una cadena de bits amb el contingut a xifrar.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   c) `vector_inicial`: el tercer argument contindrà una cadena de bits amb el vector inicial.

   La funció retornarà la cadena de bits xifrada fent servir UOC-DES en mode CBC. Per tal de simplificar la funció, assumirem que les cadenes rebudes sempre tenen una mida múltiple de 64 bits.

6. Implementeu una funció que permeti desxifrar cadenes de bits fent servir UOC-DES en mode CBC. **(0,5 punts)**

   La funció prendrà com a arguments el contingut xifrat, la clau i el vector d'inicialització fet servir. De la mateixa manera que amb la funció de xifratge, assumirem que les cadenes de bits a desxifrar sempre tenen una mida múltiple de 64 bits.

   a) `xifrat`: el primer argument contindrà una cadena de bits amb el contingut xifrat.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   c) `vector_inicial`: el tercer argument contindrà una cadena de bits amb el vector inicial.

   La funció retornarà el contingut desxifrat.

7. Implementeu una funció que permeti xifrar una cadena de bits amb UOC-DES fent servir el mode d'operació CFB. **(0,5 punts)**

   La funció prendrà com a arguments una cadena de bits a xifrar, una clau i el vector inicial.

   a) `clar`: el primer argument contindrà una cadena de bits amb el contingut a xifrar.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   c) `vector_inicial`: el tercer argument contindrà una cadena de bits amb el vector inicial.

   La funció retornarà la cadena de bits xifrada fent servir UOC-DES en mode CFB. Per tal de simplificar la funció, assumirem que les cadenes rebudes sempre tenen una mida múltiple de 64 bits. El mode CFB permet que la mida dels blocs a xifrar sigui diferent de la mida de bloc de l'algorisme de xifra que es fa servir. Tot i així, **assumirem que la mida dels blocs a xifrar és sempre la mida del bloc de l'algorisme de xifra**, en el nostre cas, els 64 bits de el UOC-DES.

8. Implementeu una funció que permeti desxifrar cadenes de bits fent servir UOC-DES en mode CFB. **(0,5 punts)**

   La funció prendrà com a arguments el contingut xifrat, la clau i el vector d'inicialització fet servir. De la mateixa manera que amb la funció de xifratge, assumirem que les cadenes de bits a desxifrar sempre tenen una mida múltiple de 64 bits.

   a) `xifrat`: el primer argument contindrà una cadena de bits amb el contingut xifrat.

   b) `clau`: el segon argument contindrà una cadena de bits que representa la clau de xifratge.

   c) `vector_inicial`: el tercer argument contindrà una cadena de bits amb el vector inicial.

   La funció retornarà el contingut desxifrat.

Exercici 2 (5 punts)

En aquesta segona part farem servir les funcions implementades a la primera part de la pràctica per analitzar el comportament dels diferents modes de xifrat, tot observant els efectes de xifrar imatges.

Atès que l'objectiu d'aquesta pràctica és estudiar els modes de xifra de bloc i no pas el tractament d'imatges amb SAGE, us proporcionem un petit tutorial que cobreix els aspectes no-criptogràfics de la implementació. El trobareu al fitxer Pràctica 2 – Intro.sws

En la resposta a cada pregunta, copieu la imatge resultant de cada procés.

1. Fent servir les funcions que us detallem al tutorial, carregueu i dibuixeu la imatge continguda en el fitxer image_64.bmp. Després, fent servir tant les funcions desenvolupades a la primera part de la pràctica com les funcions de tractament d'imatges que us donem al tutorial, xifreu la imatge fent servir el mode ECB i mostreu la imatge resultant. És a dir,

   1.- Carregueu la imatge i convertiu-la a una cadena de bits.

   2.- Xifreu la cadena de bits amb ECB fent servir una clau aleatòria.

   3.- Convertiu la cadena de bits resultant (el contingut xifrat) a un array tridimensional i mostreu la imatge que representa.

   En la imatge xifrada que obteniu, es protegeix totalment la informació que es mostra en la imatge original? Es pot dir alguna cosa de la imatge original si només es té la corresponent imatge xifrada? Per què es produeix aquest fenomen? **(1 punt)**

2. Repetiu el procediment fent servir una clau de xifratge diferent. Què observeu en aquest cas? Per què es produeix aquest fenomen? **(1 punt)**
3. Realitzeu el mateix procediment fent servir el mode CBC en comptes d'ECB. Quin n'és el resultat? Què podeu observar en aquest cas? A que es deu la diferència entre aquest resultat i l'obtingut a la pregunta 1? **(1 punt)**
4. Una vegada observats els efectes d'alguns modes sobre el contingut xifrat, passem a analitzar les conseqüències d'alguns processos sobre el text en clar obtingut després de desxifrar un missatge. En primer lloc, veiem la influència del vector inicial. Per fer-ho,

   1.- Carregueu la imatge (imatge_64.bmp) i convertiu-la a una cadena de bits.

   2.- Xifreu la cadena de bits amb CBC fent servir la clau "WWWWWWWW" i el vector d'inicialització "EBEBEBEB".

   3.- Desxifreu el contingut xifrat amb la clau correcta però fent servir un vector d'inicialització incorrecte ("00000000").

   4.- Convertiu la cadena de bits resultant (el contingut desxifrat) en un array tridimensional i mostreu la imatge que representa.

   Quina imatge s'obté? Per què s'obté aquesta imatge tot i fer servir un vector d'inicialització incorrecte? **(1 punt)**

5. Per veure la influència de la clau,

   1.- Carregueu la imatge i convertiu-la a una cadena de bits.

   2.- Xifreu la cadena de bits amb CBC fent servir la clau "XXXXXXX "

   i un vector d'inicialització aleatori.

   3.- Desxifreu el contingut xifrat amb la clau "XXXXXXX@" (fixeu-vos que només difereix en un sol bit de la clau de xifrat) i fent servir el mateix vector d'inicialització utilitzat en el pas 2.

   4.- Convertiu la cadena de bits resultant (el contingut desxifrat) en un array tridimensional i mostreu la imatge que representa.

   Quina imatge s'obté? Què en podem dir de la importància de la clau respecte a la importància del vector d'inicialització? **(1 punt)**

Format i data de lliurament

La data màxima de lliurament de la pràctica és el **27/04/2015** (a les 24 hores).

Juntament amb l'enunciat de la pràctica trobareu l'esquelet de la mateixa en format SAGE notebook worksheet (extensió .sws). També trobareu el fitxer Pràctica 2 – Intro (.sws) que conté les funcions que necessiteu per a treballar amb imatges juntament amb una petita explicació de com utilitzar-les. Finament, trobareu també la imatge que necessitareu per realitzar la pràctica.

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 d'un únic fitxer que lliurareu al registre d'avaluació continuada. Aquest serà un fitxer .zip que contingui el fitxer de SAGE worksheet (extensió sws)[1] on heu inclòs la vostra implementació i un pdf amb les respostes a les preguntes de la segona part de la pràctica.

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