Pràctica 3 - Criptografia

Presentació

En aquesta pràctica treballarem, d'una banda, el criptosistema RSA, i comprovarem que efectivament té propietats homomòrfiques, concretament, que l'operació de xifrar i desxifrar conserva el producte. També veurem com aquesta propietat es pot utilitzar en aplicacions com les votacions electròniques. D'altra banda, també veurem com s'implementa un sistema de compartició de secrets.

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

- Comprendre com funciona l'algorisme RSA.
- Familiaritzar-se amb les propietats homomòrfiques de l'RSA.
- Entendre el funcionament dels sistemes de compartició de secrets.
- Saber treballar amb certificats digitals i entendre'n les possibles febleses.

Descripció de la Pràctica a realitzar

Exercici 1 (3 punts)

En aquest exercici implementarem l'RSA i comprovarem les propietats homomòrfiques que té.

1. Programeu una funció que generi un parell de claus RSA[1].**(0,5 punts)**

   La funció rebrà com a argument la mida de la clau.

   a) `mida_clau`: la mida del valor *n* (en bits)

   La funció retornarà una llista amb el parell de claus generat, en el format [clau_pública, clau_privada]=[[e,n], [d,n]].

   Exemple:

   ```
   mida_clau: 32
   sortida: [[2373182305, 3805851499], [2613273097, 3805851499]]
   ```

2. Programeu una funció que implementi el xifratge amb RSA.**(0,5 punts)**

   La funció rebrà com a arguments una clau pública i el valor numèric representant el missatge.

   a) `clau_publica`: una llista amb els valors públics *n* i *e*.

   b) `missatge`: el valor numèric representant el missatge en clar.

   La funció retornarà el valor del missatge xifrat amb la clau pública.

   Exemple:

   ```
   clau_publica: [2373182305, 3805851499]
   missatge: 3141592
   sortida: 3600087771
   ```

3. Programeu una funció que implementi el desxifratge amb RSA. La funció rebrà com a arguments una clau privada i el missatge xifrat.**(0,5 punts)**

   a) `clau_privada`: una llista amb els valors *d* i *n*.

   b) `xifrat`: valor xifrat

   La funció retornarà el valor del missatge desxifrat fent servir la clau privada.

---

1 Si voleu, opcionalment, podeu utilitzar les condicions sobre els primers p i q que s'indiquen en el mòdul 5 dels materials de l'assignatura.

Exemple:

```
clau_privada: [2613273097, 3805851499]
xifrat: 3600087771
sortida: 3141592
```

4. L'RSA és un criptosistema homomòrfic respecte la multiplicació. Això vol dir que és el mateix multiplicar dos valors i desxifrar-ne el resultat que multiplicar els dos valors en clar. Veiem com podem aprofitar aquesta propietat per dissenyar un sistema de votació electrònica **(0,5 punts)**:

   Els vilatans d'un poble molt petit han decidit fer una votació per elegir-ne l'alcalde. Com que són molt moderns, faran la votació electrònicament, xifrant el seus vots amb el criptosistema RSA. Per fer-ho, la mesa electoral contacta amb una entitat independent i de confiança perquè emeti una parella de claus RSA. La clau pública es dóna a conèixer a tots els ciutadans; la clau privada només la coneix l'entitat independent.

   Per tal de votar, cada vilatà elegeix a un dels candidats a alcalde i envia la seva elecció xifrada amb la clau pública que la mesa electoral ha publicat. El valor corresponent a cada candidat que els ciutadans han de xifrar ve donat per la següent taula:

Candidat	Valor
A	3
B	7
C	11
D	13

   Una vegada rebuts tots els vots xifrats, la mesa electoral els multiplica i obté el valor del resultat de l'elecció xifrat. Aquest resultat xifrat s'envia a l'entitat independent per tal que, utilitzant la clau privada de la votació, pugui fer el recompte de vots. Noteu que en aquest procés no es vulnera la privacitat dels vilatans que han votat, ja que d'una banda, la mesa electoral no desxifra els vots individuals i, d'altra banda, l'entitat independent no té cap informació sobre quins vilatans han participat ni quin vot ha enviat cadascun.

   Donat que sou els experts en criptografia del poble, la mesa electoral us demana que els ajudeu a implementar el sistema de votacions i programeu una funció que donat el resultat de l'elecció de xifrat i la clau privada associada a una mesa electoral, retorni els resultats de l'elecció. La funció rebrà com a paràmetres:

   a) `resultat_multiplicació`: el resultat de multiplicar tots els vots xifrats.

b) `clau_privada`: clau privada corresponent a la clau pública amb la que s'han xifrat els vots.

La funció retornarà una llista de 4 elements amb el número de vots de cada un dels candidats ([votsA, votsB, votsC, votsD]). Si es detecta que el resultat de la multiplicació és erroni (per exemple, si es troben vots a un presumpte candidat E amb valor de votació 2) aleshores retornarà un missatge d'error indicant-ho.

Exemple:

```
resultat_multiplicació: 2552240738913504118
clau_privada: [2110852667915760397, 11223528526523661079]
sortida: [1, 2, 1, 3]
```

5. Tenint en compte la informació que es vol xifrar, indiqueu quines són les restriccions que s'haurien de posar sobre la mida *n* de les claus a generar per cada mesa electoral, per tal que el sistema funcionés correctament. **(0,5 punts)**

6. Fent servir la funció que heu desenvolupat en l'apartat 4 i, donat els valors següents, responeu a les següents preguntes **(0,5 punts)**:

```
resultat_multiplicació: 625038406528158349623372276428445087 60
clau_privada:[430834626564949809317586870725581135 9,
241105554432731134882248281879817445397]
```

a) Quants vots ha rebut cada candidat?

b) Descriviu quin problema de seguretat té aquest sistema que, amb la implementació que n'hem fet nosaltres, fa que no es pugui utilitzar. (Indicació: analitzeu si, malgrat es pugui comprovar que cada vilatà enviï un sol missatge, també es pot assegurar que només haurà votat a un candidat)

Exercici 2 (3 punts)

En aquest segon exercici implementarem un esquema de compartició de secrets polinomial de Shamir.

1. Programeu una funció que implementi la generació dels fragments que cada usuari reb en l'esquema de compartició de secrets. **(1,5 punts)**

   La funció prendrà com a arguments el secret, el nombre d'usuaris, el llindar i el nombre primer.

a) `secret`: el primer argument contindrà el valor del secret que volem compartir. Aquest serà un valor numèric.

b) `usuaris`: el segon argument contindrà el nombre d'usuaris que té els sistema, és a dir, el nombre total de fragments a generar.

c) `llindar`: el llindar fixarà el nombre mínim d'usuaris necessari per recuperar el secret a partir dels fragments. Si el valor del llindar és superior al nombre d'usuaris la funció retornarà un error indicant-ho.

d) `primer`: Aquesta variable inclourà un nombre primer que determinarà el cos sobre el que es construirà el sistema. La funció comprovarà que el valor sigui un primer, que aquest sigui més gran que el secret a compartir i que el nombre d'usuaris. En cas contrari, retornarà un error.

La funció retornarà en una llista tots els fragments dels usuaris generats.

Exemple 1:

```
secret: 22
usuaris: 10
llindar: 4
primer: 43
sortida: [[26, 22], [37, 30], [14, 15], [20, 17], [31, 41], [42, 7], [29, 31], [33, 37], [20, 17], [14, 15]]
```

Exemple 2:

```
secret: 22
usuaris: 10
llindar: 4
primer: 42
sortida: 'ERROR: Prime parameter is not a prime number.'
```

2. Programeu una funció que recuperi el secret a partir dels fragments de diferents usuaris. **(1,5 punts)**

   La funció rebrà com a arguments els fragments, el llindar i el primer:

   a) `fragments`: llista amb els fragments dels usuaris.

   b) `llindar`: el llindar fixa el nombre mínim d'usuaris necessari per recuperar el secret a partir dels fragments. Si el nombre de fragments és menor que el valor del llindar la funció retornarà un error indicant-ho.

   c) `primer`: Aquesta variable inclourà el nombre primer que determinarà el cos sobre el que està construït el sistema.

   La funció haurà de retornar el valor del secret.

Exemple:

```
fragments: [[26, 22], [14, 15], [31, 41], [29, 31]]
llindar: 4
primer: 43
sortida: 22
```

Exercici 3 (4 punts)

Fa un temps que sou usuaris d'un sistema que utilitza una infraestructura de clau pública per a garantir la seva seguretat. Cada usuari del sistema té un parell de claus (privada i pública) i aquesta última està certificada per una autoritat de certificació a través d'un certificat estàndard X.509.

Últimament no heu fet servir gaire els serveis que precisen de la infraestructura de clau pública i ara que els necessiteu us heu adonat que no sabeu on teniu el fitxer amb la clau privada. De fet, us sembla recordar que el vau esborrar amb la última actualització del sistema operatiu que vau fer.

Com sempre, ara que us cal utilitzar la clau privada no teniu temps de revocar el certificat, generar unes noves claus i demanar el nou certificat digital, ja que això suposaria anar personalment a una agència de registre per tal que puguin tornar a validar la vostra identitat.

El que si que recordeu és que hi ha un directori públic de certificats que l'autoritat de certificació té penjat. D'altra banda, també recordeu que la mida de la clau del criptosistema que s'utilitzava no era gaire llarga i que, per tant, potser vosaltres mateixos, amb el que heu après a l'assignatura de criptografia i alguns programes de factorització que podeu trobar a la xarxa, sou capaços d'obtenir la vostra clau privada a partir de la pública.

Juntament amb l'enunciat d'aquesta Pràctica trobareu un fitxer comprimit amb els certificats que una autoritat de certificació ha generat. Obtingueu el vostre certificat digital[2] i responeu a les següents preguntes:

a) Indiqueu qui és l'autoritat de certificació que ha emès el vostre certificat i expliqueu com podeu identificar que no és un certificat autosignat. (**0,5 punts**)
b) Determineu a quin criptosistema correspon la clau certificada i quin és el període de validesa del certificat. (**0,5 punts**)
c) Detalleu tots els passos a realitzar per aconseguir la vostra clau privada a partir de la clau pública. (**0,5 punts**)

2 Fixeu-vos que cada estudiant té el seu certificat digital, que és el que ha d'utilitzar per fer l'exercici.

d) Utilitzant les eines adequades que podeu trobar a la Xarxa, trobeu la vostra clau privada. Doneu el detall de tots els passos que heu realitzat, les eines que heu utilitzat i ostreu el valor de la vostra clau privada en format hexadecimal. (**2 punts**)
e) Justifiqueu perquè el procés que he fet servir en aquest exercici no es pot utilitzar, per exemple, amb el certificat digital del DNIe. Indiqueu les característiques dels certificats que conté el DNIe que fan que no sigui possible. (**0,5 punts**)

Format i data de lliurament

La data màxima de lliurament de la pràctica és el **11/06/2015** (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 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 en format zip que lliurareu al registre d'avaluació continuada. Aquest fitxer inclourà, d'una banda, el fitxer SAGE worksheet (extensió sws)[3] on heu inclòs la vostra implementació i, per altra banda, un fitxer en format pdf que contingui les respostes a les preguntes 5 i 6 del primer exercici així com la resposta del tercer exercici.

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