Pràctica 2b: Encriptació de clau pública

1- Objectius de la pràctica

Aquesta activitat té com objectius adquirir els següents resultats d'aprenentatge i continguts marcats al currículum de la UF a DOGC:

- RA1 i C1 →
  - RA1.7 --> Aplica tècniques criptogràfiques en l'emmagatzematge i la transmissió de la informació.
  - C1.6 → Seguretat Lògica

Un altre objectiu de l'activitat és avaluar si s'han assolit correctament aquests coneixements per mitjà d'una pràctica.

Per desenvolupar aquests objectius:

- L'alumne haurà de llegir i entendre la documentació. Per resoldre qualsevol dubte sobre la documentació, es durà a terme una sessió a classe per explicar els conceptes més importants i resoldre els dubtes que hagin aparegut durant la lectura de la documentació.
- L'alumne haurà de lliurar una pràctica funcionant d'acord a allò que es demani a l'enunciat.

2- Documentació: Encriptació de clau pública (o asimètrica)

1. A la criptografia de clau secreta (o simètrica), cada usuari sap la clau secreta necessària per encriptar (que significa el mateix que xifrar) i desencriptar (que significa el mateix que desxifrar) les dades enviades per la xarxa local o internet i mantenir les comunicacions segures. La clau secreta només l'han de coneixer els que volen comunicar-se.

2. A la criptografia de clau pública (o simètrica), cada usuari té un parell de claus una clau pública i una clau privada. La clau privada es manté secreta, mentre que la clau pública es pot dir a tothom.

3. La clau pública s'ha de publicar i tothom ha de saber-la. Per un atacant la clau pública no serveix per atacar al propietari de la clau. La clau privada sí que és secreta.

4. Si un usuari (al qual anomenarem **usr1**) vol enviar un missatge encriptat i secret a un altre usuari (al qual anomenarem **usr2**), llavors:
   - L'usuari **usr1** encriptarà (o xifrarà) el missatge amb la **clau pública** de l'usuari **usr2** i ho enviarà per la xarxa local o internet.
   - L'usuari **usr2** desencriptarà (o desxifrarà) el missatge amb la seva **clau privada**.

5. Si l'usuari **usr1** vol signar un document i enviar-lo a **usr2**, llavors:
   - L'usuari **usr1** encriptarà el seu missatge amb la seva pròpia **clau privada** i enviarà el missatge encriptat a l'usuari **usr2**.
   - L'usuari **usr2** desencriptarà el missatge amb la **clau pública** de l'usuari **usr1**. Si es pot desencriptar el missatge, **usr2** tindrà una confirmació de que realment va ser creat per **usr1**.

6. Si l'usuari **usr1** vol enviar una **clau simètrica** a **usr2**,
   - L'usuari **usr1** encriptarà la **clau simètrica** amb la **clau pública** de l'usuari **usr2** i l'enviarà per la xarxa local o internet
   - L'usuari **usr2** desencriptarà el missatge amb la seva **clau privada** i aconseguirà la **clau simètrica**.

7. La criptografia de clau pública (o asimètrica) normalment s'utilitza per:
   - Encriptar i desencriptar quan el volum de dades és petit.
   - Signar documents
   - Interncanviar claus simètriques.

8. La criptografia de clau secreta (o simètrica) és més ràpida que la pública (o asimètrica) i requereix menys recursos (CPU, RAM..). Per aquest motiu, s'utilitza per encriptar i desencriptar quan el volum de dades és molt gran.

9. Algorismes més utilitzats de clau pública:
   - RSA
   - DSA
   - ECC
   - ECDSA

10. Un paràmetre important de les claus és la seva mida, que es mesura en bits:
    - Com més gran sigui el número de bits més segures són les claus. Avui dia es considera segura una clau RSA o DSA a partir de 2048 bits (RSA-2048 o DSA-2048) tot i que cada cop s'utilitza més 4096 (RSA-2048 o DSA-2048).
    - Com més gran sigui el número de bits cal més potència de CPU, més espai de disc i més utilització de memòria. No sempre el el maquinari que tenim pot treballar amb la quantitat de bits que volem.

11. Les claus secretes (o simètriques):
    - També tenen una mida en bits però amb molts menys bits que les asimètriques són molt més segures. Un clau simètrica AES de 128 bits simètrica pot ser tant segura com una de 3072 de tipus RSA. Un AES de 256 bits pot ser tan segur com un RSA de 15360 bits.
    - Un algorisme simètric típic és l'AES que avui dia s'utilitza normalment amb 256 bits (AES-256).
    - Desencriptar una clau AES-128 amb la capacitat actual dels ordinadors requeriria aproximadament el mateix temps que l'edat estimada de l'univers (uns 13800 milions d'anys)

12. Les comunicacions comercials avui dia utilizen normalment RSA-2048 combinada amb AES-128 o AES-256. RSA-1024 es considera obsolet i RSA-4096 a vegades pot donar algún problema en funció dels programes i maquinari utilitzats.

3- Generació i publicací d'una clau pública (o asimètrica) de RSA-4096 bits amb AES-256

a) Comprova que el paquet **openssl** que permet generar parelles de **claus privada** i **pública** Executa:

```
aptitude search ^openssl$
```

i el resultat ha de ser:

```
i A openssl          - Secure Socket Layer toolkit - cryptographic utility
```

b) Com usuari del sistema crea una carpeta de nom **claus**. Accedeix a la carpeta **claus**.

c) **Genera** un fitxer amb una parella de **clau privada i pública**, de nom **claus.pem**, que utiltizi **l'agorisme RSA** per generar claus de longitud igual a **4096 bits**, que treballarà conjuntament amb una clau d'encriptació simètrica **AES** de **256 bits**. Dins de la carpeta **claus**, executa:

```
dacomo@inf1-dacomo:~$ openssl genpkey -algorithm RSA -out claus.pem -pkeyopt rsa_keygen_bits:4096 -aes256
```

Si et demana entrar una contransenya per la clau (PEM pass phrase), escriu: **clotfje**. A continuació comprova que s'ha creat **claus.pem** dins del directori **claus** amb la parella de clau pública i privada.

d) Extreu la **clau pública** de **claus.pem** i desa-la dins d'un fitxer de nom **claupub.pem**. Dins de la carpeta **claus**, executa:

```
dacomo@inf1-dacomo:~/claus$ openssl rsa -in claus.pem -out pubclau.pem -outform PEM -pubout
```

e) Converteix el fitxer **pubclau.pem** a un fitxer de format **html**. Dins de la carpeta **claus**, executa:
- Instal·la **txt2html**:
  `sudo aptitude install txt2html`
- Converteix **pubclau.pem** a html afegint el teu correu al títol:
  `txt2html pubclau.pem --title xxxxxx.clot@fje.edu > pubclau.html`
  NOTA: Canvia xxxxxx pel teu codi de correu de l'escola

f) Publica la teva clau pública amb el teu servidor web. Dins de la carpeta **claus**, executa:
- **`sudo cp pubclau.html /var/www/html`**
- **`sudo systemctl start apache2`**

g) Obre el teu navegador, estableix una connexió a **http://localhost/pubclau.html** i comprova que tens la teva **clau publica** publicada via web i al títol es veu la teva adreça de correu de l'escola.

4- Desencriptació amb la clau privada d'un fitxer previament encriptat amb la clau pública publicada via web

a) Obre un terminal i executa l'ordre: **`ip -4 -br add show dev enp0s3`** . Comprova amb el navegador pots accedir a la web **pubclau.html** utilitzant l'adreça IP de la teva màquina virtual.

b) Demana al teu company de grup que es connecti a la teva pàgina **pubclau.html** per copiar la teva clau pública. El teu company haura de copiar la clau i desar-la dins d'un fitxer de nom **pubclau_company.pem** dins de la seva carpeta **claus** i utilitzant **nano**. El teu company pot copiar la teva **clau pública** i enganxar-la dins del fitxer amb l'ajuda de **nano**.

c) Demana al teu company que crei un fitxer de nom **missatge.txt** dins de la carpeta **claus** i a dins escrigui alguna cosa. A continuació, demana al teu company que encripti el missatge amb la teva **clau pública** executant:

```
daniel@sh3:~/tmp/claus$ openssl rsautl -encrypt -inkey pubclau_company.pem -pubin -in missatge.txt -out missatge.txt.ssl
```

d) Demana al teu company que enviï el fitxer **missatge.txt.ssl** adjunt a un correu a la teva adreça de l'escola que s'ha de veure en el títol de la teva pàgina **pubclau.html**. L'assumpte del correu serà "missatge encriptat". No s'ha d'escriure res dins del correu, només adjuntar el fitxer.

e) Si en la teva carpeta claus hi ha un **missatge.txt** i **missatge.txt.ssl**, esborra'ls per poder desar ara el fitxer que t'ha enviat el teu company.

f) Recull el correu enviat pel teu company. Descarrega el fitxer **missatge.txt.ssl** enviat que segurament anirà a parar a la carpeta **Downloads** i copia'l dins de la carpeta **claus.** Des de dins de la carpeta **claus** executa l'ordre: **`cat missatge.txt.ssl`** i comprova que el seu contingut no es pot llegir.

g) Desencripta el fitxer amb la teva clau privada executant des de dins de a carpeta **claus**:

```
dacomo@inf1-dacomo:~/claus$ openssl rsautl -decrypt -inkey claus.pem -in missatge.txt.ssl -out missatge.txt
Enter pass phrase for claus.pem:
```

h) Ara comprova que dins de **claus** s'ha creat el fitxer **missatge.txt**. Des de dins de la carpeta **claus** i amb l'ordre **`cat missatge.txt.ssl`** comprova quin es el contingut del fixer **missatge.txt**.

Forma de lliurament de la pràctica

1- Activitat en grups de 2 persones o individual.

2- Demostració:

a) Indica'm l'adrreça IP de la teva màquina virtual. Comprovaré que puc veure la teva clau pública i la teva adreça de correu dins de la pàgina **pubclau.html**.

b) Encriptaré un fitxer amb la teva clau pública i t'ho enviaré encriptat a la teva adreça de l'escola. M'hauràs de mostrar el contingut del missatge.

3- Dates de lliurament: Setmana del **21-11-21 al 26-11-21** dins de l'horari escolar per aconseguir el **100%** de la nota. La setmana del **29-11-21 al 3-12-21** per aconseguir el **70%** de la nota. Després d'aquesta setmana, no s'acceptarà aquesta pràctica.