Pràctica 2c: Signatura digital de codi

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- Signatura digital

1. La creació d'un codi hash d'un fitxer com van veure a la pràctica m11uf1pr2a només ens assegura la **integritat** de les dades rebudes però no ens proporciona un mecanisme per d'**autenticació**.

2. Si volem **integritat** i **autenticació** llavors hem de crear una **signatura digital** de les dades. La **signatura digital** no és res més que el **hash de les dades** que ha estat **encriptat** amb una **clau privada**.

3. La signatura digital no té com objectiu encriptar les dades, només assegurar que les dades rebudes són les originals, sense modificació i assegurar l'autenticitat de la persona que les signa, o sigui, confirmar la identitat del creador de les dades.

4. La signatura digital de documents és avui dia un més dels diversos passos que s'han de seguir per dur a terme molts tràmits administratius habituals i serveix com alternativa al sistema tradicional de signar manualment un document físic.

5. Per crear una signatura digital, el signat de les dades (que serà l'emissor) ha de:
   - 1r pas) Generar un hash de les dades del fitxer.
   - 2n pas) Encriptar el hash de les dades amb una clau privada creant així una fitxer que serà signatura digital de les dades a enviar.
   - 3r pas) Distribuir les dades i la seva signatura digital (via web, correu electrònic, etc...) i publicar la nostra clau pública.

6. Per verificar una signatura digital, el receptor de les dades ha de:
   - 1r pas) Generar un hash del fitxer de dades rebudes.
   - 2n pas) Utilitzar la clau pública del signant (l'emissor) per desencriptar el fitxer amb la signatura digital. D'aquesta manera obtindrà el codi hash del fitxer de dades.
   - 3r pas) Comprovar que el hash generat a l'apartat 1 i el desencriptat a l'apartat 2 són iguals.

7. El programa **openssl** pot fàcilment, amb només una instrucció, els 2 primers passos del procés de creació de la signatura digital de les dades d'un fitxer.

8. El programa **openssl** pot fer fàcilment amb només una instrucció els 3 passos del procés de verificació de la signatura digital de les dades d'un fitxer.

3- Verificant el codi font d'un programa publicat a internet

a) Crea dins del teu directori personal, un directori de nom **nota2**.

b) Descarrega dins del directori **nota2**:
- El codi font **nota2.c** que trobaràs a:
  http://www.collados.org/asix1/m11/uf1/m11uf1pr2c/nota2.c
- La signatura digital **nota2.c.sign** del fitxer **nota2.c** que trobaràs aquí:
  http://www.collados.org/asix1/m11/uf1/m11uf1pr2c/nota2.c.sign
- La meva clau pública **pubclau.pem** que trobaràs aquí:
  http://www.collados.org/asix1/m11/uf1/m11uf1pr2c/pubclau.pem

c) **Verifica** que la signatura digital (integritat + autenticació) del codi distribuït. Executa:

```
dacomo@inf1-dacomo:~/nota2$ openssl dgst -sha256 -verify pubclau.pem -signature nota2.c.sign nota2.c
Verified OK
```

Comprova que el resultat és **`Verified OK`**.

4- Signat i distrubuint codi font d'un programa

a) Crea un directori de nom **nota3** dins del teu directori personal. Fes una còpia de **nota2.c** dins del directori **nota3** amb el nom **nota3.c**. Fes aquests canvis dins de **nota3.c** i salva el fitxer :
- Modifica la **línia 2** del fitxer **nota3.c** i canvia **Versió 0.2** per **Versió 0.3**
- Modifca la **línia 3** del fitxer **nota3.c** i canvia el nom de l'autor pel teu nom real i el teu correu.
- Modifca la **línia 4** del fitxer **nota3.c** i canvia la data.
- Modifca la **línia 5** del fitxer **nota3.c** i canvia la instrucció de compilació del programa.
- Modifca la **línia 6** del fitxer **nota3.c** i canvia la instrucció d'execució del programa.
- Modifica la **línia 13** del fitxer **nota3.c** i canvia **0.205** per **0.25.**
- Modifica la **línia 14** del fitxer **nota3.c** i canvia 0.41 per **0.4**.
- Modifica la **línia 15** del fitxer **nota3.c** i canvia 0.205 per **0.25**.
- Modifica la **línia 16** del fitxer **nota3.c** i canvia 0.18 per **0.1**.

b) **Crea** una **signatura digital** de **nota3.c** amb el nom **nota3.c.sign** utilitzant la clau privada que vas crear a la pràctica **m11uf1pr2b**, que s'hauria de dir **clau.pem** i trobar-se al directori **claus**. Executa la següent ordre:

```
dacomo@inf1-dacomo:~/nota2$ openssl dgst -sha256 -sign ~/claus/claus.pem -out nota3.c.sign nota3.c
Enter pass phrase for /home/dacomo/claus/claus.pem:
```

MOLT IMPORTANT: Aquesta ordre funciona si **claus.pem** està a la carpeta **claus** del teu directori personal tal i com es va indicar que s'havia de fer a la pràctica anterior (m11uf1pr2b)!!!!!!!!!!!!!!!!!!!!!!!!!!

c) Crea un fitxer de nom **nota3.html** amb aquest codi HTML:

```
<html>
  <head>
    <title>m11uf1pr2c</title>
  </head>
  <body>
    <p>Autor: xxxx yyyy zzzz</p>
      <p><a href="nota3.c">nota3.c</a></p>
      <p><a href="nota3.c.sign">nota3.c.sign</a></p>
      <p><a href="pubclau.pem">pubclau.pem</a></p>
  </body>
</html>
```

i canvia **xxxx yyyy zzzz** amb els teus noms i cognoms reals.

d) Copia el **nota3.c**, **nota3.c.sign** i **nota3.html** fitxer dins de **/var/www/html**. Copia també dins de **/var/www/html** el fitxer amb la teva clau pública **pubclau.pem** que vas crear a la pràctica anterior i que hauria d'estar a la carpeta **claus**.

e) Executa l'ordre: **`ip -4 -br add show dev enp0s3`** . Comprova amb el navegador pots accedir a **nota3.html** utilitzant l'adreça IP de la teva màquina virtual.

5- Verifica el codi de programa publicat pel company de grup

a) Des del terminal, crea dins del teu directori personal un nou directori de nom **nota3.d**.

b) Demana al teu company que et doni la seva adreça IP. Connecta't a la seva pagina web **nota3.html** des del navegador.

c) Descarrega dins del directori **nota3.d** els fitxer **nota3.c**, **nota3.c.sign** del teu company i la seva clau pública **pubclau.pem**.

d) Verifica la signatura digital del seu codi. Executa:

```
daniel@sh3:~/nota3.d$ openssl dgst -sha256 -verify pubclau.pem -signature nota3.c.sign nota3.c
Verified OK
```

Comprova que el resultat és **`Verified OK`**.

e) Si tot ha funcionat, esborra el contingut del directori **nota3.d** abans de cridar-me per corregir aquesta pràctica.

Forma de lliurament de la pràctica

1- Activitat en grups de 2 persones o individual.

2- Demostració:
a) Demanaré a un membre del grup que em demostri que pot verificar la signatura digital del meu codi que ha descarregat des de la meva web.
b) Demanaré a l'altre membre del grup que descarregui els fitxers **nota3.c**, **nota3.c.sign** i **pubclau.pem** de la web de seu company dins de **nota3.d** i comprovi la seva signatura digital.

3- Dates de lliurament:
* Setmana del **13-12-21 al 17-12-21** dins de l'horari escolar per aconseguir el **100%** de la nota.
* Setmana del **20-12-21 al 22-12-21** dins de l'horari escolar per aconseguir el **100%** de la nota.
* Setmana del **10-01-22** al **14-01-22** dins de l'horari escolar per aconseguir el **70%** de la nota.
* Després del **14-01-22** no s'accepta la pràctica