GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

Unidad 4.2
Criptografía
Ejercicio evaluable 5

Licencia

1 Criptografía asimétrica – Verificar una signatura

Crear en python el programa que verifica una firma. Usa este ejemplo de la librería pycriptodom como ayuda:

- https://www.pycryptodome.org/src/signature/pkcs1_v15

En el ejemplo del enlace usan el algoritmo de firma:

- pkcs1_15.new(key).sign(codigoHash)

Tú usa:

- PKCS1_PSS.new(key).verify(codigoHash,firma)

¿Qué fichero tengo que verificar?

- Te adjunto un código Python y un fichero.
- Ejecuta el código Python para crear la signatura. Tendrás el archivo:
  - “SignaturaFichero.txt”

¿Qué tiene que hacer tu código?

- Primero, pedir al usuario el fichero. En este caso “AudreyTang.txt”
- Segundo, pide al usuario que indique la firma del documento. En este caso (“SignaturaFichero.txt”)
- Tercero, dar un mensaje de respuesta al usuario:
  - **Si la verificación ha ido bien**: La signatura es correcta, el fichero es auténtico y no ha sido modificado
  - **Si la verificación ha ido mal:** La signatura es incorrecta. No se puede autenticar el fichero.

2 Estructura de tu código - Firma digital – Verificar una firma:

Cuando recibes un documento firmado, debes verificar el documento con su firma. El documento nos lo ha enviado firmado la persona A.

Pasos a seguir:

1. Quiero verificar la firma del documento firmado por la persona A.
2. Abro la **clave pública** RSA de la persona A.
3. Abro el fichero que me ha enviado la persona A y creo el Hash del fichero usando el algoritmo SHA256. Uso SHA256 porque es el mismo algoritmo Hash que ha usado la persona A y que recomienda la librería pycryptodom.(Le diré H**ash comprobación**)
4. Abro el fichero que contiene la firma, en este caso: SignaturaFichero.txt.
5. Uso el mismo algoritmo de encriptación-desencriptación que la persona A.
   - En este caso la librería pycryptodom había recomendado usar el algoritmo PKCS1_PSS
   - Al algoritmo PKCS1_PSS le paso los siguientes parámetros:
     - La clave pública RSA de la persona A
     - El código Hash que he calculado yo (Hash comprobación)
     - La firma que me ha enviado la persona A (es el Hash del mismo fichero pero encriptado con la clave privada de la persona A)
6. El algoritmo PKCS1_PSS me dirá:
   - Si todos los datos son correctos (autentifica el documento y la persona)
   - Generará una excepción si algo falla.
7. Si todo es correcto podemos usar el documento, teniendo la tranquilidad que es de la persona A y que nadie lo ha manipulado.