2º SMR B - SEGURIDAD INFORMÁTICA

EXAMEN DEL TEMA 4: CRIPTOGRAFÍA - PRÁCTICO

(16-02-2024)

IES Camas - Antonio Brisquet.

Realiza el siguiente ejercicio práctico de criptografía:

1. Genera una pareja de claves asimétricas y llámalas *tunombre.priv* y *tunombre.pub* usando RSA con 2048 bits. NO cifres tu clave privada con cifrado simétrico.
2. Dispones en esta tarea del fichero *docexamen.pdf*.
3. Cifra el fichero *docexamen.pdf* con el algoritmo simétrico AES-256-CBC, usando PBKDF2 con 120.000 iteraciones y usando también "sal". Utiliza la contraseña EXA2023. El documento cifrado debe llamarse *docexamen.sim*
4. Calcula el hash SHA 512 del fichero *docexamen.sim*. El fichero resultante debe llamarse *docexamen.sha*.
5. Cifra el fichero *docexamen.sha* con tu clave pública. El documento cifrado debe llamarse *docexamen.lock*.
6. Emite un certificado digital autofirmado para el nombre de dominio www.examen.es. El emisor será el IES Camas y debe tener una caducidad de 10 años. Debes obtener una clave privada llamada *server.priv*, una clave pública llamada *server.pub* y un certificado llamado *server.crt*

Debes entregar los siguientes ficheros:

- *tunombre.priv*
- *tunombre.pub*
- *docexamen.sim*
- *docexamen.sha*
- *docexamen.lock*
- *server.priv*
- *server.pub*
- *server.crt*

Entrega también un documento pdf con todos los comandos que has ejecutado para hacer el ejercicio. Llámalo *exa_tunombre.pdf*.