UF1.NF1.Criptografia

1.- Crea una clau simètrica DES i mostra el valor de la clau en Base64.

2.- Crea un hash amb l'algorisme SHA-512 del teu nom i i cognoms.

3.- Crea una clau simètrica AES a partir d'un text codificat (hash) amb SHA-256. Mostra el valor de la clau en Hexadecimal.

4.- Modifica l'exercici 2 per aplicar un salt abans de fer la codificació. Busca com generar el salt utilitzant la classe SecureRandom. Per a què serveix? És diferent al hash resultant?

5.- Crea una base de dades que es digui UF1Cripto<nom><cognoms> (pots utilitzar el SGBD que vulguis), que contingui, per cada usuari, el hash de la seva contrasenya i el salt aplicat.

6.- Crea un mètode que, a partir d'un usuari i contrasenya, guardi a la base de dades de l'exercici anterior, el salt i el seu hash. (Per fer el salt, genera un enter aleatori i passa'l a Hexadecimal).

7.- Crea un mètode que, a partir d'un usuari i contrasenya, verifiqui aplicant el hash i el salt corresponent, si coincideix amb el de la base de dades.

8.- Crea un mètode que retorni un parell de claus asimètriques.

9.- Crea un mètode encripti una contrasenya a partir d'una clau privada.

10.- Modifica l'exercici anterior perquè encripti el hash de la contrasenya.

11.- Crea un mètode que desencripti la informació encriptada de l'exercici anterior a partir d'una clau pública.

12.- Utilitzant el keytool, crea una clau simètrica i mostra-la pel cmd.

13.- Crea un mètode que mostri la clau creada a l'exercici anterior

14.- Crea un mètode que crei una clau simètrica al keytool i la mostri per pantalla.