**Laboratorio 2**

**Criptografía y**

**Seguridad Informática**

Jorge Rodríguez Fraile, 100405951

# Bouncy Castle

## Crear archivo de texto

Permite crear un archivo de texto dentro de la carpeta files para poder usarlo posteriormente en las demás opciones de la demostración

## **Sección** **DES**

Cuestiones

1. Consulte la siguiente página web y evalúe con la información proporcionada si hubiese sido más adecuado utilizar la clase java.util.Random de Java. <https://wiki.sei.cmu.edu/confluence/display/java/MSC02-J.+Generate+strong+random+numbers>
2. Observe el método “generateKey” de la clase “DES.java”. ¿Por qué se multiplica la longitud preestablecida de una clave DES por 8? Cambie dicha longitud por otra, ¿qué ocurre durante la ejecución?

Cuestiones

1. Consulte la documentación de Bouncy Castle y cambie el modo de Bloque del cifrador al modo CFB y OFB. Genere un archivo cifrado para cada modo de bloque a partir de un mismo texto en claro. Si cambiamos algún byte del archivo cifrado (es decir, introducimos errores), ¿qué ocurre al intentar descifrarlo en cada uno de los modos?

## Sección AES

Cuestiones

1. Observe el método “generateKey” de la clase “AES.java”. ¿Por qué se añade blocksize a la longitud de la clave AES en la generación del número aleatorio? Cambie dicha longitud por otra, ¿qué ocurre durante la ejecución?
2. Observe los métodos encrypt y decrypt de la clase AES.java. ¿pueden unificarse ambos métodos en uno sin modificar el resultado de la ejecución?
3. En la librería BouncyCastle, el algoritmo Rijndael es un modo “rápido” de cifrado AES que permite distintos tamaños de clave mientras que ésta sea múltiplo de 32 bits. Modifique el Cifrado en Java Curso 2019/2020 - Página 5 de 6 - COSEC · Dpto. Informática método encrypt para que se cifre mediante el algoritmo Rijndael que sea compatible con la función decrypt ya existente. La implementación de Rijndael en BouncyCastle se realiza en la clase RijndaelEngine

## **Sección Funciones** **Resumen**

Cuestiones

1. MD5 y SHA1 son funciones hash rotas hoy en día, por lo que no deberían usarse. Consulte la documentación de BouncyCastle e implemente una nueva opción que genere resúmenes usando SHA512.

## Generación de par de claves RSA

Observe el método “generateKey” de la clase “RSA.java”. En este caso, y para que el alumno esté familiarizado con el formato, la información de las claves se almacena en archivos en Base64, no en Hexadecimal, usando la clase Base64Encoder

El formato Base64 es un formato de representación de bytes en forma de caracteres ASCII que permite intercambiar información entre distintos ordenadores, sistemas operativos sin que la representación de la información dependa del modo de almacenamiento de ésta entre origen destino (Big-Endian / Little-Endian, etc.). Este formato es especialmente útil cuando se desea transmitir información entre, por ejemplo, dispositivos móviles y servidores Unix en internet. Adicionalmente, esta forma de representación es la estándar para el intercambio de Certificados y Claves públicas y privadas en criptografía

## Cifrado/Descifrado RSA

Cuestiones

1. Realice el cifrado de dos ficheros de texto, uno de ellos con una longitud menor en bytes que la longitud de clave usada y otro mayor. ¿Qué ocurre cuando se intenta cifrar un texto mayor que la longitud de la clave?
2. Pruebe a generar, cifrar y descifrar texto con claves de distinto tamaño (por ejemplo, 256, 1024 y 2500) ¿qué ocurre?