**Taller 8 – Cifrado Simétrico**

El propósito de este taller es estudiar algunos métodos de cifrado de información disponibles en librerías Java (javax.crypto.\*).

# Parte 1: Cifrar y descifrar con cifrado simétrico

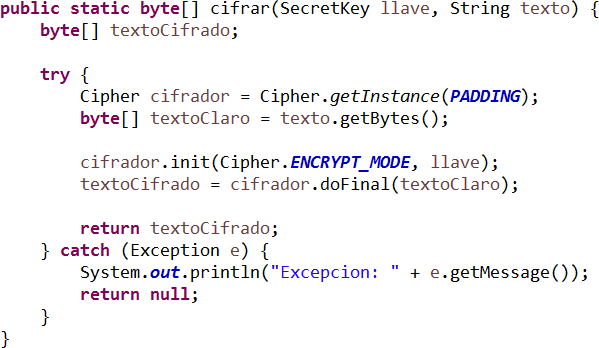
1. Escriba una clase llamada **Simetrico** en la cual vamos a incluir los métodos **cifrar()** y

**descifrar()**.

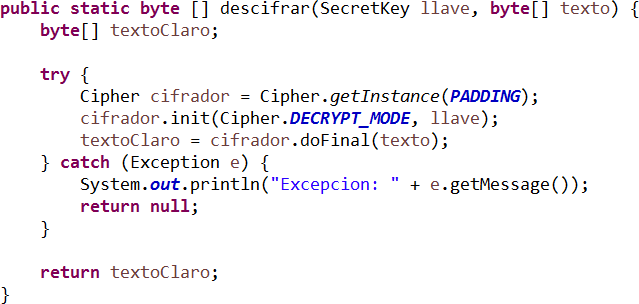
Puede utilizar la siguiente constante, la cual determina el mecanismo de ***padding*** a utilizar para cifrar y descifrar:



Cree el método **cifrar()** usando el siguiente código.



Cree el método **descifrar()** usando el siguiente código.



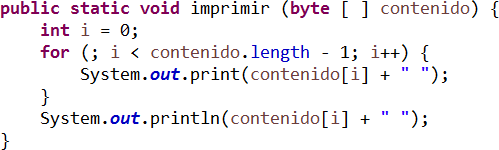
2. Escriba una clase **Main** para crear una instancia de la clase **Simetrico**.

En el método **main()**:

1. Utilice la siguiente constante para indicar que utilizará el algoritmo **AES** para cifrar y descifrar sus mensajes:



1. Reciba por teclado la entrada de un texto.
2. Imprima el texto recibido por el teclado.
3. Imprima texto claro en **byte []**. Utilice el método **getBytes()** de la clase **String** para convertir el mensaje a **byte[]**. Para imprimr el contenido del **byte[]** utilice el método **imprimir()**.



1. Genere la llave secreta, la cual será empleada para cifrar y descifrar. Utilice el siguiente fragmento de código:



1. Obtenga un **byte []** con el texto cifrado, invocando al método **cifrar()** de la clase

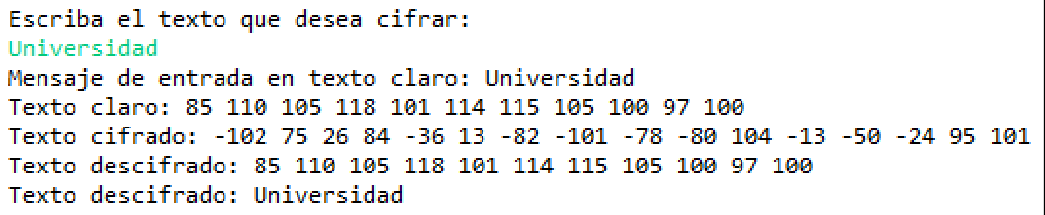
## Simetrico.

1. Imprima el texto cifrado en **byte []**. Utilice el método **imprimir()**.
2. Obtenga un **byte []** con el texto descifrado, invocando al método **descifrar()** de la clase

## Simetrico.

1. Imprima el texto descifrado en **byte []**. Utilice el método **imprimir()**.
2. Convierta el **byte[]** con el texto descifrado a **String**. Utilice el método constructor de la clase **String**.

Un ejemplo de la salida en consola de la ejecución del programa se puede ver a continuación:



1. Escriba el método **main()**.

**try**

{

System.***out***.println("Escriba el texto que desea cifrar:");

BufferedReader in = **new** BufferedReader(**new** InputStreamReader(System.***in***));

String texto = in.readLine();

System.***out***.println("El texto escrito es: " + texto);

System.***out***.print("Texto original: ");

*imprimir* (texto.getBytes());

KeyGenerator keygen = KeyGenerator.*getInstance*(***ALGORITMO***);

SecretKey llave = keygen.generateKey();

**byte**[] cifrado = *cifrar*(llave, texto);

System.***out***.print("Texto cifrado: ");

*imprimir* (cifrado);

**byte**[] descifrado = *descifrar* (llave, cifrado);

System.***out***.print("Texto descifrado: ");

*imprimir*(descifrado);

System.***out***.println("Texto original: " + **new** String(descifrado));

}

**catch** (Exception e)

{

System.***out***.println("Exception :" + e.getMessage());

e.printStackTrace();

}

3. Responda las siguientes preguntas:

* 1. ¿Qué significa ECB como modo de ejecución del algoritmo de cifrado?

Electronic Codebook, para cada bloque de texto que se desea cifrar igual siempre se producirá el mismo texto cifrado

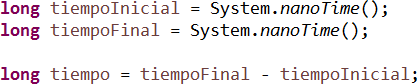
* 1. ¿Cuál es la ventaja de ECB comparado con CBC?

Es más rápido ya que no entrelaza distintos bloques.

* 1. ¿Qué es y para qué se necesita el padding?

Es añadir información en alguna parte del mensaje antes de encriptarlo, así se vuelve más difícil descifrar un mensaje ya que este tendrá información que parecería irrelevante o fuera de contexto

* 1. ¿Cuánto tiempo tarda cifrar y descifar el mensaje de entrada? Utilice el siguiente fragmento de código:



Cifrar: 12050769ns

Descifrar:124099ns

4. Cree una clase llamada **Main2** y en ella cree el método **main()** de acuerdo con las siguientes modificaciones al método **main()** inicial y responda:

* + 1. Genere dos llaves simétricas, **k1** y **k2**.
    2. Cifre un mensaje de entrada con la llave **k1** y obtenga un objeto de tipo **byte[]** llamado **tc1**

con el mensaje de entrada cifrado.

* + 1. Cifre un mensaje de entrada con la llave **k2** y obtenga un objeto de tipo **byte[]** llamado **tc2**

con el mensaje de entrada cifrado.

* + 1. Descifre **tc1** con **k1**. ¿Qué resultados obtiene?

El texto original

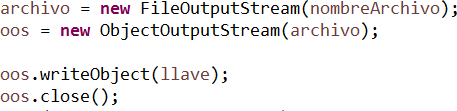
* + 1. Descifre **tc1** con **k2**. ¿Qué resultados obtiene?

Algo que no tiene mucho sentido

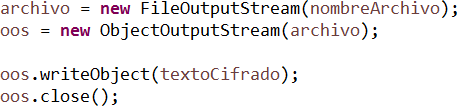
* + 1. Escriba el método **main()**.

5. Cree una clase llamada **Main3** en ella cree el método **main()** de acuerdo con las siguientes modificaciones al método **main()** inicial y responda:

1. Genere una llave secreta y guardela en un archivo. Utilice el siguiente fragmento de código:

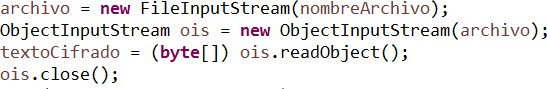


1. Cifre un mensaje de entrada. Almacene el texto cifrado en un archivo. Utilice el siguiente fragmento de código:

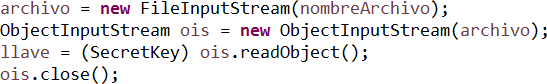


6. Cree una clase llamada **Main4** en ella cree el método **main()** de acuerdo con las siguientes modificaciones al método **main()** inicial y responda

1. Recupere la llave que está en el archivo. Utilice el siguiente fragmento de código:



1. Recupere el texto cifrado que está en el archivo. Utilice el siguiente fragmento de código:



# Parte 2: Criptoanálisis

1. Descifre el mensaje utilizando la técnica especificada.

1. En este caso utilice el **Caesar Shift Cipher** conocido como cifrado de César con un corrimiento del alfabeto de tres lugares. El mensaje original está en italiano (tomado de The Code Book).

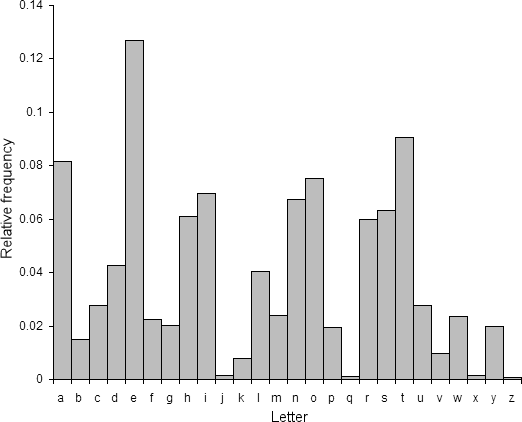
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Y** | **H** | **Q** | **L** |  | **Y** | **L** | **G** | **L** |  | **Y** | **L** | **F** | **L** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. En este ejercicio, el mensaje está cifrado con un algoritmo de sustitución de letras por corrimiento.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **r** | **h** | **v** | **o** | **r** | **t** | **x** | **h** | **x** | **v** | **w** | **h** | **g** | **v** | **d** | **e** | **h** | **h** | **v** | **o** | **r** | **t** | **x** | **h** | **x** | **v** | **w** | **h** | **g** | **h** | **v** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Descifre el siguiente mensaje usando análisis de frecuencias. El mensaje está en inglés y las frecuencias de uso de las letras fue tomada de Wikipedia.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **5** | **3** | **+** | **+** | **!** | **3** | **0** | **5** | **)** | **)** | **6** | **\*** | **;** | **4** | **8** | **2** | **6** | **)** | **4** | **+** | **.** | **)** | **4** | **+** | **)** | **;** | **8** | **0** | **6** | **\*** | **;** | **4** | **8** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **!** | **8** | **]** | **6** | **0** | **)** | **)** | **8** | **5** | **;** | **,** | **+** | **8** | **\*** | **;** | **:** | **+** | **\*** | **8** | **!** | **8** | **3** | **(** | **8** | **8** | **)** | **5** | **\*** | **!** | **;** | **4** | **6** | **(** | **;** | **8** | **8** | **\*** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **9** | **6** | **\*** | **?** | **;** | **8** | **)** | **\*** | **+** | **(** | **;** | **4** | **8** | **5** | **)** | **;** | **5** | **\*** | **!** | **2** | **:** | **\*** | **+** | **(** | **;** | **4** | **9** | **5** | **6** | **\*** | **2** | **(** | **5** | **\*** | **‐** | **4** |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **)** | **8** | **]** | **8** | **\*** | **;** | **4** | **0** | **6** | **9** | **2** | **8** | **5** | **)** | **;** | **)** | **6** | **!** | **8** | **)** | **4** | **+** | **+** | **;** | **1** | **(** | **+** | **9** | **;** | **4** | **8** | **0** | **8** | **1** | **;** | **8** | **:** | **8** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **+** | **1** | **;** | **4** | **8** | **!** | **8** | **5** | **;** | **4** | **)** | **4** | **8** | **5** | **!** | **5** | **2** | **8** | **8** | **0** | **6** | **\*** | **8** | **1** | **(** | **+** | **9** | **;** | **4** | **8** | **;** | **(** | **8** | **8** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **;** | **4** | **(** | **+** | **?** | **3** | **4** | **;** | **4** | **8** | **)** | **4** | **+** | **;** | **1** | **6** | **1** | **;** | **:** | **1** | **8** | **8** | **;** | **+** | **?** | **;** |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



1. Descifre el siguiente mensaje usando análisis de frecuencias. El mensaje está en español y las frecuencias de uso de las letras fue tomada de Wikipedia.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **h** | **j** | **l** | **n** |  | **j** | **z** | **d** | **r** |  | **n** | **u** |  | **q** | **r** | **m** | **j** | **u** | **p** | **x** |  | **o** | **d** | **n** | **a** | **c** | **n** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **z** | **d** | **n** |  | **j** |  | **c** | **j** | **u** |  | **n** | **g** | **c** | **a** | **n** | **v** | **x** |  | **u** | **u** | **n** | **p** | **x** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **m** | **n** |  | **e** | **j** | **u** | **r** | **n** | **w** | **c** | **n** |  | **z** | **d** | **n** |  | **b** | **n** |  | **j** | **m** | **e** | **r** | **n** | **a** | **c** | **n** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **z** | **d** | **n** |  | **u** | **j** |  | **v** | **d** | **n** | **a** | **c** | **n** |  | **w** | **x** |  | **c** | **a** | **r** | **d** | **w** | **o** | **x** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **m** | **n** |  | **b** | **d** |  | **e** | **r** | **m** | **j** |  | **l** | **x** | **w** |  | **b** | **d** |  | **v** | **d** | **n** | **a** | **c** | **n** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

