Universidad Pontificia Bolivariana SECCIONAL BUCARAMANGA	**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA** **ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA** **Asignatura: CRIPTOGRAFÍA – NRC: 47016** Facilitador: Julián Darío Miranda (julian.miranda@upb.edu.co) Semestre: 2019 - II

TALLER 1
MÉTODOS CRIPTOGRÁFICOS DE SUSTITUCIÓN

OBJETIVO

Identificar y comprender los procedimientos de cifrado por sustitución que están enmarcados dentro de los métodos criptográficos clásicos, mediante la práctica de ejercicios manuales y algorítmicos, con el fin de sentar una base teórico-práctica para los protocolos de cifrado modernos.

INSTRUCCIONES

- El taller se debe realizar en parejas. Se trabajará la aplicación de las técnicas de cifrado por sustitución de forma escrita-manual y se comprobarán los resultados haciendo uso de los algoritmos diseñados para este fin.
- Se trabajará sobre una máquina Linux Ubuntu 16.04.05 Desktop de 32 o 64 bits virtualizada con el entorno de Oracle VM VirtualBox. En caso de no tener esta versión, puede descargase de forma libre de: http://releases.ubuntu.com/16.04/. El archivo descargado se recomienda que esté en el formato de imagen *.iso* para poder montarlo fácilmente a la máquina virtual.
- La solución debe hacerse usando la ventana de comandos de la máquina virtual de Ubuntu instalada. Se evaluará el trabajo en clase y el informe entregado en la fecha estipulada en formato PDF con el nombre: InformeTaller1_*nombre&apellido*.pdf. **Fecha de entrega del informe: 06 de octubre de 2019 antes de las 23:59.**
- Se recomienda mantener una copia de fábrica de la máquina virtual en caso de eliminar cualquier archivo de sistema o ejecutar un proceso que colapse la instancia del Sistema Operativo virtualizado.
- El usuario sin privilegios de la máquina virtual es genérico con el nombre: *informatica* y la contraseña: *sistemas*.
- A continuación, se presenta la sección de procedimiento, a la que debe hacerse un seguimiento secuencial con el fin de mantener el orden y la cohesión del laboratorio. Los comandos por ejecutar se encontrarán en otro tipo de letra y en un color gris oscuro.

PROCEDIMIENTO

Cifrado Afín

Desarrollar los siguiente numerales teniendo en cuenta el alfabeto definido por el intervalo [0, 26], en el que la A corresponde al índice 0 y la Z al índice 26. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

1. Cifrar mediante el Cifrado Afín el siguiente texto: "ATACAR PEARL HARBOR AHORA", teniendo en cuenta:
   a) Una llave $(a, b) = (0, 126)$
   b) Una llave $(a, b) = (6, 0)$
   c) Una llave $(a, b) = (3, 92)$

2. Descifrar mediante el Cifrado Afín el siguiente texto: "WXAWVWRFWFJEPEZC", teniendo en cuenta la llave $(a, b) = (11, 56)$.

Comprobar las respuestas mediante la ejecución del algoritmo desarrollado en Python3 incluido en el archivo *01-AffineCypher.py* y *01-AffineDecrypt.py*, con los comandos en la consola de Ubuntu:

```
$ python3 01-AffineCypher.py
$ python3 01-AffineDecrypt.py
```

Haga uso del algoritmo desarrollado en Python3 incluido en el archivo *01-AffineDecrypt.py* para responder a los siguientes 2 numerales.

3. Descifrar mediante el Cifrado Afín el siguiente texto: "QTQEQFSWKMNKC", teniendo en cuenta la llave $(a, b) = (59, x)$ y mencionar el conjunto de valores de x que genera el mismo mensaje a partir del criptograma entregado.

4. Descifrar mediante el Cifrado Afín el siguiente texto: "HWKHSKEUISDSASV", teniendo en cuenta la llave $(a, b) = (x, 18)$ y mencionar el conjunto de valores de x que genera el mismo mensaje a partir del criptograma entregado.

Cifrado de Playfair

Desarrollar los siguiente numerales teniendo en cuenta el alfabeto definido por el intervalo [0, 26] y la matriz base como la que se muestra a la derecha. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

5. Cifrar mediante el Cifrado de Playfair el siguiente texto: "LAAUREIN FUE ARRESTADO", teniendo en cuenta:

   a) Una llave *k:* "CRIPTOGRAFIA"
   b) Una llave *k:* "JACOME"

6. Descifrar mediante el Cifrado de Playfair el siguiente texto: "GWLBSOLC FOBCRBOL NE", teniendo en cuenta la llave *k:* "CURRICULO".

7. Mencione al menos 10 claves con las cuales se puede generar el mismo criptograma del numeral anterior.

8. Se ha logrado recuperar una comunicación cifrada en la que se presenta el siguiente fragmento de interés: "NYOZSPSU RFMFRENK ZSPOTGXM XUXUSISF NYZKPYMI", cifrado a partir del método de Playfair. Aunque no se tiene la clave para descifrarlo, se ha logrado recuperar la matriz de Playfair, que luce como se muestra a la derecha. Con base en esta información, responder:

			I/J	A
B	C	D	E	F
G	H		M	N
O	P	Q	R	S
	V	W		Z

   a) ¿Cuántas (cantidad) posibles claves deben ser tenidas en cuenta para descifrar el criptograma?
   b) Descifrar el criptograma, entregando como resultado el mensaje en claro y la clave usada para descifrarlo.

Comprobar las respuestas mediante la ejecución del algoritmo desarrollado en Python3 incluido en el archivo *02-PlayfairCypher.py* y *02-PlayfairDecrypt.py*.

Cifrado de Vigenère

Desarrollar los siguiente numerales teniendo en cuenta el alfabeto definido por el intervalo [0, 26]. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

9. Cifrar mediante el Cifrado de Vigenère el siguiente texto: "WE ARE THE CHAMPIONS", teniendo en cuenta:
   a) Una llave *k:* "SEDENTARIO"
   b) Una llave *k:* "ARCHIVO"
   c) Una llave *k:* "ARAR"

10. Descifrar mediante el Cifrado de Vigenère el siguiente criptograma: "ACEBAIARSALRMLRPHLPL", teniendo en cuenta la llave k "LLAMARADA".

11. ¿Qué diferencia existe entre cifrar con la clave "ARAR" y cifrar con el patrón de claves "$(AR)^n$" donde n es un número natural que representa la cantidad de repeticiones de la cadena? Justificar la respuesta.

12. Cifrar el texto "PRUEBA DE COMPARACION" con el cifrado de Cesar y una llave k de desplazamiento de 19. Compare los resultados al cifrar el mismo texto con el cifrado de Vigenère y la llave k "T".

13. Analizar el patrón de cifrado afín por desplazamiento puro y el patrón de cifrado de Vigenère. ¿Qué similitudes y diferencias se encuentran? ¿Existe alguna relación entre estos dos métodos criptográficos? Justificar con argumentos la respuesta.

Comprobar las respuestas mediante la ejecución del algoritmo desarrollado en Python3 incluido en el archivo *03-VigenereCypher.py* y *03-VigenereDecrypt.py.*

Cifrado de Vernam

Desarrollar los siguiente numerales teniendo en cuenta el alfabeto definido por el intervalo: [A, Z]U[0, 9] y su equivalente decimal y hexadecimal de la codificación ASCII. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

14. Cifrar mediante el Cifrado de Vernam el siguiente texto: "SOMOS LOS REYES DE PERSIA", teniendo en cuenta:

a) Una llave *k:* "ESTA ES LA PRIMERA LLAVE1"
b) Una llave *k:* "LA SEGUNDA LLAVE2 ES ESTA"

Expresar el criptograma resultante como cuartetos en base hexadecimal.

15. Descifrar mediante el Cifrado de Vernam el siguiente criptograma: "171D1702041E1708061D0A0A09001F0817061A13040800", teniendo en cuenta la llave *k* "VIVA EL REINO DE ARISTOTELA" (sin espacios).

16. De acuerdo con el criptograma: "6171B19131200040D101A1C020C1E0C0E01" que se ha generado a partir del mensaje "RETIRADA A CONFIRMAR" (sin espacios), ¿cuál es la clave de generación del criptograma?

17. Se ha logrado recuperar una comunicación cifrada en la que se presenta el siguiente fragmento de interés: "30E0514130C190E05100E0D00021D1A0005141279637179", cifrado a partir del método de Vernam. Aunque no se tiene la clave para descifrarlo, se ha identificado que al momento de cifrar el mensaje en claro se ha repetido la clave sucesivamente, esta es de longitud 3 y se compone de solo vocales que no se repiten. Con base en esta información, responder:

    a) ¿Cuántas (cantidad) posibles claves deben ser tenidas en cuenta para descifrar el criptograma?
    b) Descifrar el criptograma, entregando como resultado el mensaje en claro y la clave usada para descifrarlo.

Comprobar las respuestas mediante la ejecución del algoritmo desarrollado en Python3 incluido en el archivo *04-VernamCypher.py* y *04-VernamDecrypt.py.*