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 2
MÉTODOS CRIPTOGRÁFICOS DE TRANSPOSICIÓN

OBJETIVO

Identificar y comprender los procedimientos de cifrado por transposición 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 transposición 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: InformeTaller2_*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 por Escítala

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

1. Cifrar mediante el Cifrado de la Escítala el siguiente texto: "EL WIFI NO TIENE CONTRASENA", teniendo en cuenta:
   a) Una llave k de 5
   b) Una llave k de 7
   c) Una llave k de 11

2. Descifrar el siguiente texto "NTSORAEALSEANRBERACETEFASULAELRRAIZOO" mediante el Cifrado de la Escítala, teniendo en cuenta la llave k de 13.

3. ¿Qué sucede cuando la clave k es mayor a igual a la longitud del mensaje en texto en claro a cifrar? ¿Qué sucede cuando es igual a uno? Justificar las respuestas.

4. Si tiene el siguiente mensaje M: "ESTAMOS LISTOS PARA EL COMBATE", ¿Cuál es el menor valor de k tal que al menos una porción de 5 caracteres del mensaje siga apareciendo de forma idéntica en el criptograma? Justificar la respuesta.

5. Se ha logrado recuperar una comunicación cifrada en la que se presenta el siguiente fragmento de interés: "CEAILLFAAREASDCOIDT", cifrado usando una Escítala de clave desconocida. Con base en esta información, 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 *01-ScytaleCypher.py* y *01-ScytaleDecrypt.py*, con los comandos en la consola de Ubuntu:

```
$ python3 01-ScytaleCypher.py
$ python3 01-ScytaleDecrypt.py
```

Cifrado ADFGVX

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

6. Cifrar mediante el Cifrado ADFGVX el siguiente texto: "DIME CON QUIEN ANDAS Y TE DIRE", teniendo en cuenta las claves siguientes y la matriz aleatoria presentada:

   a) Una llave k "GALPON"
   b) Una llave k "ORQUESTA"
   c) Una llave k "ALGORITMICOS"

	A	D	F	G	V	X
A	F	Y	O	L	1	E
D	Q	K	T	G	W	Z
F	2	7	A	5	N	4
G	B	R	9	U	I	P
V	0	X	C	H	M	8
X	S	J	6	V	3	D

7. Descifrar el siguiente texto "AXAA AAFA VXXV XAGG FDDA GFXG XXVD FGAX FFFX AXAX AD" mediante el Cifrado ADFGVX, teniendo en cuenta la llave k "ACOPIAR" y la matriz aleatoria de generación del ejercicio anterior.

8. Reconstruir la matriz aleatoria de cifrado ADFGVX, teniendo en cuenta que se ha cifrado el mensaje en claro "LE GUSTABA CENAR UN EXQUISITO SANDWICH DE POLLO CON JUGO DE ZUMO DE PINA Y VODKA FRIO MIENTRAS CONTABA 0123456789" (sin espacios) con la clave "ABELISCO" y se ha obtenido el resultado: "XFAA FDXF AXVV FXDG AXGF VXXD DVXG AAGA GVGX GDGF XDVF GGVV GVDX GFAD GDDF AGAF VVVA FFXF XXVG FGXA AVVA VAFV XDAD FXGX VFAF VDVX FVDA FVXX VAXG VAAF GXFD ADGF FFGD FAAG XAFA DVXV DFDV DVGF XDXV XFGG VDAF XFGF".

9. Se ha logrado recuperar una comunicación cifrada en la que se presenta el siguiente fragmento de interés: "VVGF VAFD AGAF FGDF GXFG FDAF", cifrado usando el cifrado del ADFGVX y la matriz aleatoria del ejercicio 6. Pese a que la clave de cifrado es desconocida, se identifica que tiene las siguientes cuatro letras sin repetirse: 'L', 'N', 'A' y 'U', y que antes y después de cada consonante hay una vocal.

   Con base en esta información, escribir los diferentes posibles mensajes en claro que pueden obtenerse al hacer combinaciones con la información entregada de la clave y 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-ADFGVXCypher.py*.

Cifrado de Transposición por Series

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

10. Cifrar mediante el Cifrado por trasposición de series el siguiente texto: "MENSAJE ESCONDIDO EN TEXTO PLANO", teniendo en cuenta el siguiente grupo de series:

    a) Series:
        1) MS1: relación de números impares
        2) MS2: relación de números múltiplos de 5
        3) MS3: relación de números primos
        4) MS4: relación de números pares
    b) Series:
        1) MS1: relación de números de la sucesión de Fibonacci
        2) MS2: relación de números cuya suma de dígitos es prima
        3) MS3: relación de números cuya suma de dígitos es impar
        4) MS4: relación de números cuya suma de dígitos es par

11. Escribir todas las combinaciones distintas que pueden obtenerse al cifrar, mediante el Cifrado por trasposición de series, el siguiente texto: "MURCIELAGO EN EL COBERTIZO", teniendo en cuenta variaciones en el orden del siguiente grupo de series:

    1) MS1: relación de números impares cuya multiplicación de dígitos es impar
    2) MS2: relación de números pares
    3) MS3: relación de números impares cuya primera cifra sea el 2

12. Considerar el siguiente criptograma: "EEJAODINEUASOUEASLCIDADLIRTNDTSLAUO" que ha sido cifrado mediante el Cifrado por trasposición teniendo en cuenta las siguientes series:

    1) MS1: relación de números pentagonales
    2) MS2: relación de números múltiplos de 5
    3) MS3: relación de números cuyos dígitos multiplicados sean múltiplos de 3

4) MS4: relación de números que siguen la secuencia: $p(n) = 2(n^2 - 3)$ con $n \geq 2$
5) MS5: relación de números primos
6) MS6: relación de números de la sucesión de Fibonacci
7) MS7: relación de números impares
8) MS8: relación de números pares

Escriba los elementos que componen cada sucesión y descifre el mensaje entregado.