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 3
CRIPTOANÁLISIS DE MÉTODOS DE CIFRADO CLÁSICOS

OBJETIVO

Identificar y comprender los procedimientos de criptoanálisis a métodos criptográficos por sustitución y transposición, mediante la práctica de ejercicios manuales y algorítmicos, con el fin de sentar una base teórico-práctica para los protocolos de criptoanálisis de cifrado moderno.

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: InformeTaller3_ *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

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. Se ha logrado recuperar una comunicación en castellano cifrada en la que se presenta el siguiente fragmento de interés cifrado usando el Cifrado de Afín de desplazamiento puro, con una clave b desconocida.

   LEUZRCRRSLVCRUVTRGVILTZKRHLVMZMZRVEVCSFJHLVVEWVIDFPCRDRUIVUV
   TRGVILTZKRCVGZUZFHLVCVCCVMRIRLERTVJKRTFELERKFIKRPLEKRIIFUVDREK
   VHLZCCRTRGVILTZKRRTVGKFVETREKRUR

   Descifrar el criptograma, escribir el mensaje en texto claro original y la clave usada para descifrarlo. Puede hacer uso de los algoritmos de cifrado y descifrado Afín, ejecutando los comandos:

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

2. Se ha logrado recuperar una comunicación en castellano cifrada en la que se presenta el siguiente fragmento de interés cifrado usando el Cifrado de Afín de desplazamiento puro, con una clave b desconocida.

   GKUHYTQXYBTUDEIQRUISKQDJECUQFUJUSULEBLUHQSQIQUDBYBBUIQDTSQ
   BSKBEGKUQJUHHYPQHUUDAZULYAJUCFHQDEBQDESXUTUIQDZKQDCUXKRY
   UHQWKIJQTELEBLUHFQHQJKSKCFBUQEIFUHEUIJEORQZEEHTUDUICYBYJQHUI
   QSQCRYEFKUTEFHECUJUHJUGKUUIJEOFEDYUDTEJETECYUCFUEUDKDWHQD
   HUWQBEGKUHUSYRYHQIUBTYQTUJKSKCFBUQEIKDSQHYEIEIQBKTETUQBWKY
   UDGKUIYUCFHUFYUDIQUDUBVKJKHETUIKXYZQUDLYEKDQSEFYQTUUIJQFEIJQ
   BQQBWKYUDGKUBEITEISEDESUCEIOQBESECFHUDTUHQIXYBTUSYJQFEHQXE
   HQUIJEOIYUDTECKOCYIJUHYEIEFUHEOQBEUDJUDTUHQIIEVYQSEWYEBQIYWK
   YUDJUFEIJQBGKUHYTQXYBTUQGKYQRQZEIULYLUIEBEUBCECUDJEIYTUQBWE
   CUQSEHTQHUTUUIJEICUIUIUDUBBYRQDEIUHQTUUIJQUJUHDQUIFUHQFUHEX
   QWEBEGKUFKUTEFQHQGKUJUDWQIUBCUZEHHUWQBEFEIYRBUUDJKTUSYCE
   GKYDJESKCFBUQEIDEFKUTETUSYHCQIFEHQXEHQCUYCFEDWEQCYCYICEKDQI
   ULUHQSUDIKHQQRHQPEIFQFQ

Descifrar el criptograma, escribir el mensaje en texto claro original y la clave usada para descifrarlo. Puede hacer uso de los algoritmos de cifrado y descifrado Afín, ejecutando los comandos:

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

3. Se ha encontrado un texto cifrado con el Cifrado de Vigenère en el que se conoce que el mensaje en claro está en idioma inglés y que trata de algoritmos criptográficos. Se descubre que la cadena TVAIVCXIERAA aparece dos veces en el criptograma en las posiciones 4 y 235 y se sospecha que puede corresponder con la palabra *cryptography*. Si todo lo anterior fuera acertado, seleccionar de la siguiente tabla todas las posibles claves usadas para cifrar el mensaje en claro y justificar el porqué de la selección de cada una de ellas.

society	marry	property	ceiling
behavior	rare	book	guide
hesitant	council	hand	provide
plaster	stew	correct	beautiful
network	tacit	box	crevice

4. Sea C un criptograma correspondiente al cifrado de un texto en castellano mediante el Cifrado de Vigenère. En la siguiente tabla se expresan los n-gramas que aparecen repetidos a lo largo de C y la distancia a la que se encuentran las repeticiones.

n-grama	Distancias
PQMI	28, 329
QAWA	42
ASJU	98
BLVE	112
QOSO	154

Calcular la longitud más probable que tiene la clave usada para cifrar el mensaje en claro y obtener el criptograma analizado.

5. Un texto cifrado mediante el Cifrado de Vigenère contiene tres apariciones de la secuencia de letras CGDRTHGH en las posiciones 37, 1283, 2291. Calcular la longitud más probable que tiene la clave usada para cifrar el mensaje en claro y obtener el criptograma analizado.

6. Se ha logrado recuperar una comunicación en castellano cifrada en la que se presenta el siguiente fragmento de interés cifrado usando el Cifrado de Vigenère, con una clave desconocida.

   GBCTWCPRGEFSSHKQHRAEDWRNRXSETHQOMXRCRFNRFWRXPXSETHQOMXR
   CRFJYKNFBVUSUXPCQZNHCRTHQQSITXCBROIPOUHINJVGEFCVKECZVKKKQFT
   PCOMXRCRVOIPOUHCGBSHKQHRLSNCGHHKOMXVNOCNDFSCWMCQFFSCJV
   GEFSMXRCRFXPCJVGEFCMXRCRF

   Con base en este criptograma:

   a) Marcar las secuencias repetidas de 3 o más caracteres.
   b) Hallar la longitud más probable de llave utilizada (la llave tiene una longitud mayor a 2 caracteres).
   c) Extraer las letras más probables para las subclaves utilizadas.
   d) Expresar las combinaciones de clave que pueden obtenerse con las subclaves del punto anterior.
   e) Descifrar el criptograma con las combinaciones de clave y escribir el mensaje en texto claro original.

   Puede hacer uso de los algoritmos de búsqueda de n-gramas, ejecutando el comando:

```
$ python3 02-Find_n-gramspy.py
```

7. A continuación, se presenta un mensaje intervenido en una comunicación entre la Embajada de España en Marruecos a sus colegas en el Congreso Español en Madrid. El mensaje se encuentra cifrado con el cifrado de Vigenère. Descifre el mensaje por sus propios medios y escriba el mensaje en texto claro obtenido, explicando los procedimientos ejecutados.

   YWTXZEYPVBXIAALLPWPNZEMOIDODBCFGFMPCXPVWAGZZFRMIPYTPQRSCLX
   JHFQFPXVIUAYLTBEIMLOIQEIABFMQYVDLYTJFVRLCVPWUEPDBBTIIDTWOIELLB
   CFRFSETMOIECLFBJZFSWLKMEMEOPMOXIAOLIMEJEOPLFPJUWEIOEKOPDMM
   WZGFTMOXVCZYRVRKOOPVPZVNELGESJLPEZBWTIQCIEEJCZYMMGZFCLLPHV
   CPDISHVLBFMOSJENZVPGVLLNTBZVOMZBYICNPXBHAOFEVSOBMHWIMGXBKS
   UVCXVTFESUPEGSQCLBZHVUVYBVLYPUUKKWSWFLXCNTVPJFOMEVJIMYKWM
   FGMBXPDXFVRMZDXVIUAYCMTGRTLCVPWGRZYBPECEYEZBVRLNLAUMCLZNW

KEEEWACOXFDPLKDIJOLWIEIIENSIFWFLZDTMIMACLIMETAGPZOEFPFPAUERDZ
YLFLRYFYOSYGOOPOVEIDTLADYRNOZMTXVNPYTBGRVPCVBKVNPCMOYEAOT
AUVRCNTWOIJOSLZBULEWZAHYRROTITZRYLYPBGZAFDBFHVSXTMOXIADDME
MIIRPVIETILPTDYRREZLFPCAGPADSAAYWITPCAGPACEAEYOWTTZSZDXPVVLNL
TMIAOYOMMEDAYNPBVFJLJDFVRNWLADICDLDLFTIIDTWOIIODPAUEDODLXSIJ
AOZAFRCAOPKJQRCPWLBQLCSLAVIITP

Puede hacer uso de los algoritmos de búsqueda de n-gramas, ejecutando el comando:

```
$ python3 02-Find_n-gramspy.py
```