INFORME DE TALLER 2

Métodos criptográficos de transposición

García Grimaldos, Alberto Manuel; Álvarez Caballero, Hernán David
alberto.garcia.2016@upb.edu.co; hernan.alvarez.2014@upb.edu.co
Universidad Pontificia Bolivariana
Seccional Bucaramanga
Octubre 6 de 2019

I. *OBJETIVOS DE DESARROLLO*

Objetivo General

- *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.*

II. INTRODUCCIÓN

El cifrado de transposición es un método de cifrado en el cual las posiciones de los caracteres de texto sin formato se desplazan de acuerdo con un sistema, en este laboratorio se evidencia el funcionamiento del cifrado por Escítala, ADFGVX y de transposición por series. Se puede decir que se utiliza una función biyectiva (función entre los elementos de dos conjuntos , donde cada elemento de un conjunto se combina con exactamente un elemento del otro conjunto) en las posiciones de los caracteres para cifrar y una función inversa para descifrar, de modo que el texto cifrado se puede ver como una permutación del texto en claro.

El cifrado Escítala se usaba en la antigüedad griega para encriptar mensajes. El dispositivo utilizado para hacer estos cifrados era una varilla con una base poligonal, que estaba envuelta en papel. La gente podía escribir en el papel horizontalmente. Cuando se retiraba el papel del dispositivo, se formaba una tira de letras que parecían aleatorizadas. La única forma de leer el mensaje sería tener una máquina Escítala propia.

El cifrado ADFGVX, fue utilizado en la primera guerra mundial, las letras de su nombre se eligieron porque son muy diferentes entre sí en el código Morse, lo que reduce el riesgo de errores de operador de telegrafía. La 'clave' para un cifrado ADFGVX es un 'cuadrado clave', el cual es de 6 por 6 que contiene todas las letras y los números del 0 al 9, y una palabra clave.

El cifrado basado en transposición por series reordena los caracteres del mensaje a cifrar como una serie de submensajes, donde cada uno de los submensajes sigue una función determinada, del total de caracteres que conforman el texto a cifrar con base en la posición que ocupa cada uno en el mensaje.

III. *PROCEDIMIENTO*

Para cifrar por escítala, se necesita crear una matriz de k columnas y m/k (aproximando ascendentemente) filas, en las cuales se ubicarán los caracteres del mensaje en claro, en el orden original, pasando a la siguiente fila de ser necesario. La lectura del criptograma se realizará leyendo los caracteres por columnas (caracteres columna0+caracteres columna1+…+caracteres columna(k-1))

En el procedimiento para descifrar escítala se necesita calcular el pad (cantidad de espacios restantes en la matriz de caracteres) $pad = (-LM) \; mod(k) = (-longitudMensaje)\%(clave)$. Se debe escribir en cada columna los caracteres del criptograma ordenados, tener en cuenta el pad para no escribir en los espacios sobrantes de

la última fila. El mensaje en claro será la sucesión de caracteres ordenados por filas.

Para cifrar por el método ADFGVX se debe crear una matriz con los 26 caracteres del alfabeto y los 10 dígitos numéricos de forma aleatoria. Posteriormente se deben seleccionar las coordenadas de cada carácter así (fila)(columna), lo que generará el primer criptograma.

Definiremos una segunda clave de seis caracteres, que ubicamos en una nueva matriz en la primera fila. Posteriormente se debe llenar la nueva matriz con los caracteres del criptograma en orden (un carácter por casilla). Finalmente ordenaremos la matriz en orden lexicográfico con respecto a la segunda clave. El texto cifrado resultante serán los caracteres ordenados por columnas sin incluir la clave.

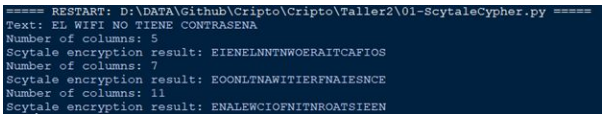
Finalmente se analizó el cifrado de transposición por series, se divide el texto en claro de acuerdo con el orden de los elementos del mismo, y dependiendo de ese orden los elementos son agrupados, de forma que el mensaje original se transmite como: $M' = M_{S1}M_{S2}M_{S3}...M_{SN}$ donde para cada M_{Si} se sigue una serie.

Para obtener C o texto cifrado mediante la transposición por series es requerido conocer cada M_{Si} o serie, como por ejemplo M_{S1} son la relación de números impares o de la sucesión de Fibonacci visto en los numerales 10.a y 10.b, y según el orden de estas obtendremos el orden de caracteres para C, variando el orden de cada M_{Si} obtendremos C diferentes de forma que tendremos *n!* variaciones.

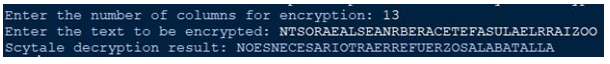
En el proceso de descifrado, al igual que en el de cifrado, es necesario conocer las series y su orden para posteriormente asignarle un número a cada carácter de C y ordenarlos por orden creciente para tener como resultado el texto en claro M.

IV. *ANÁLISIS DE RESULTADOS*

1. El cifrado por método de escítala con claves 5, 6 y 11 del mensaje “EL WIFI NO TIENE CONTRASENA” arroja los siguientes resultados.



2. El descifrado por el método de escítala del criptograma “NTSORAEALSEANRBERACETEFASUL AELRRAIZOO” con la clave **k=13** da el siguiente resultado.



3. El criptograma queda exactamente igual al mensaje en claro, pues la cantidad de columnas a ordenar es mayor o igual que la cantidad de caracteres del mensaje en claro; solo hay un caracter por columna ordenada. En caso de ser k=1, también queda exactamente igual, pues solo hay una fila por caracter.

4. Para que que al menos una fracción de cinco caracteres del mensaje se vean en el criptograma, el menor número posible de k es uno, tal que si k=1, todo el criptograma se leerá igual que el mensaje en claro.

5. El descifrado del subcriptograma “CEAILLFAAREASDCOIDT” por fuerza bruta desde 2 hasta longitud de la cadena, da como resultado los siguientes posibles submensajes en claro.

```
Columns: 2
Scytale decryption result: CEEAASIDLCLOFIADATR
Columns: 3
Scytale decryption result: CADEACAROIEILADLSTF
Columns: 4
Scytale decryption result: CLEOEFAIAASDIADTLRC
Columns: 5
Scytale decryption result: CLASIELRDDAFECTIAAO
Columns: 6
Scytale decryption result: CLAEDIELAACDAFRSOTI
Columns: 7
Scytale decryption result: CIFRSODELAEDITALAAC
Columns: 8
Scytale decryption result: CIFRADODELAESCITALA
Columns: 9
Scytale decryption result: CILARADODELFAESCITA
Columns: 10
Scytale decryption result: CALFAESCITEILARADOD
Columns: 11
Scytale decryption result: CALFAESCIDTEILARADO
Columns: 12
Scytale decryption result: CALFAESCOIDTEILARAD
Columns: 13
Scytale decryption result: CALFAESDCOIDTEILARA
Columns: 14
Scytale decryption result: CALFAEASDCOIDTEILAR
Columns: 15
Scytale decryption result: CALFAREASDCOIDTEILA
Columns: 16
Scytale decryption result: CALFAAREASDCOIDTEIL
Columns: 17
Scytale decryption result: CALLFAAREASDCOIDTEI
Columns: 18
Scytale decryption result: CAILLFAAREASDCOIDTE
```

Por inferencia, podemos deducir que la clave correcta y el mensaje en claro son 8 y "CIFRADODELAESCITALA" respectivamente.

Para el cifrado ADFGVX se utilizó la siguiente matriz de cifrado.

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

6. El cifrado del mensaje "DIME CON QUIEN ANDAS Y TE DIRE" con las claves "GALPON", "ORQUESTA" y "ALGORITMICOS" da como resultado los siguientes criptogramas.

```
Enter the text to be encrypted: DIME CON QUIEN ANDAS Y TE DIRE
Enter the key: GALPON

ADFGVX encryption result: XXVVFFFVXAFGFFDGGVDAFXAGVFGVXDXXVAGFXAXAVFAXVAXD
Enter the key: ORQUESTA

ADFGVX encryption result: XXVVFFFVXAFGFFDGGVDAFXAGVFGVXDXXVAGFXAXAVFAXVAXDXAVFXXV
FAXDGXVGFXXGAGFAGXFGFAXVVXXFDADFFAAVFVVDV
Enter the key: ALGORITMICOS

ADFGVX encryption result: XXVVFFFVXAFGFFDGGVDAFXAGVFGVXDXXVAGFXAXAVFAXVAXDXAVFXXV
FAXDGXVGFXXGAGFAGXFGFAXVVXXFDADFFAAVFVVDVXFFDFXADGDFAVGXXVAXGXVFFXVFVVAVXAFAAVGXX
FVDXAGFG
```

7. Descifrar el criptograma "AXAA AAFA VXXV XAGG FDDA GFXG XXVD FGAX FFFX AXAX AD" con la clave "ACOPIAR" da el siguiente resultado.

Teniendo la matriz de cifrado:

	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

Y la matriz del criptograma (la cantidad de columnas se halló con el tamaño de la clave).

A	A	C	I	O	P	R
A	F	X	D	X	A	A
X	A	A	A	X	X	X
A	V	G	G	V	F	A
A	X	G	F	D	F	X
A	X	F	X	F	F	A
A	V	D	G	G	X	D

Organizándola nos da:

A	C	O	P	I	A	R
A	X	X	A	D	F	A
X	A	X	X	A	A	X
A	G	V	F	G	V	A
A	G	D	F	F	X	X
A	F	F	F	X	X	A
A	D	G	X	G	V	D

Nos da el siguiente resultado:

AX XA DF AX AX XA AX AG VF GV AA GD FF XX AF FF XX AA DG XG VD

Utilizando la tabla de cifrado, nos queda: "ESTEESELCIFRADFGVX" como mensaje en claro

8. Siendo “LE GUSTABA CENAR UN EXQUISITO SANDWICH DE POLLO CON JUGO DE ZUMO DE PINA Y VODKA FRIO MIENTRAS CONTABA 0123456789” el mensaje en claro, “ABELISCO” la clave y "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" el criptograma,

Se tiene la siguiente tabla criptograma

A	B	C	E	I	L	O	S
X	X	V	F	V	V	G	V
F	X	F	V	A	D	F	D
A	D	G	V	F	A	F	V
A	D	G	V	V	F	F	G
F	X	X	A	X	V	G	F
D	X	V	F	D	X	D	X
X	G	G	F	A	X	F	D
F	A	V	X	D	V	A	X
A	A	D	F	F	A	A	V
X	G	X	X	X	X	G	X
V	A	G	X	G	G	X	F
V	G	F	V	X	V	A	G
F	V	A	G	V	A	F	G
X	G	D	F	F	A	A	V
D	X	G	G	A	F	D	D
G	G	D	X	F	G	V	A
A	D	D	A	V	X	X	F
X	G	F	A	D	F	V	X
G	F	A	V	V	D	D	F
F	X	G	V	X	A	F	G
V	D	A	A	F	D	D	F

Que organizada queda de la siguiente manera:

A	B	E	L	I	S	C	O
X	X	F	V	V	V	V	G
F	X	V	D	A	D	F	F
A	D	V	A	F	V	G	F
A	D	V	F	V	G	G	F
F	X	A	V	X	F	X	G
D	X	F	X	D	X	V	D
X	G	F	X	A	D	G	F
F	A	X	V	D	X	V	A
A	A	F	A	F	V	D	A
X	G	X	X	X	X	X	G
V	A	X	G	G	F	G	X
V	G	V	V	X	G	F	A
F	V	G	A	V	G	A	F
X	G	F	A	F	V	D	A
D	X	G	F	A	D	G	D
G	G	X	G	F	A	D	V
A	D	A	X	V	F	D	X
X	G	A	F	D	X	F	V
G	F	V	D	V	F	A	D
F	X	V	A	X	G	G	F
V	D	A	D	F	F	A	D

El resultado sería: “XX FV VV VG FX VD AD FF AD VA FV GF AD VF VG GF FX AV XF XG DX FX DX VD XG FX AD GF FA XV DX VA AA FA FV DA XG XX XX XG VA XG GF GX VG VV XG FA FV GA VG AF XG FA FV DA DX GF AD GD GG XG FA DV AD AX VF DX XG AF DX FV GF VD VF AD FX VA XG GF VD AD FF AD”.

Convirtiendo cada tupla de caracteres en un caracter del mensaje en claro -como si de un diccionario se tratase-, tenemos la siguiente matriz de cifrado:

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

No se pudo establecer la posición de los dígitos numéricos, pues estos no se encontraban en el criptograma dado.

9. Siendo la clave compuesta por los caracteres {L, A, N, U} y mencionando que antes y después de cada consonante hay una vocal, las únicas posibilidades son {LUNA, LANU, ALUN, ULAN}. Siendo "LUNA" la única palabra dentro del diccionaro castellano, se toma esta como clave para comenzar a descifrar el criptograma.

Se toma la siguiente matriz de criptograma.

A	L	N	U
V	F	F	F
V	D	G	G
G	A	D	F
F	G	F	D
V	A	G	A
A	F	X	F

Ordenada queda:

L	U	N	A
F	F	F	V
D	G	G	V
A	F	D	G
G	D	F	F
A	A	G	V
F	F	X	A

Siendo "FF FV DG GV AF DG GD FF AA GV FF XA" el resultado, lo convertimos al texto en claro "ANGIOGRAFIAS".

Las angiografías son un tipo de examen por imágen para el estudio de vasos sanguíneos que no son visibles por otros estudios radiológicos.

10.a. Del mensaje "M E N S A J E E S C O N D I D O E N T E X T P L A N O", el cual tiene una longitud de 27 caracteres, y las series: M_{S1} = {1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27}, M_{S2} = {10, 20} , M_{S3} = {2} y M_{S4} = {4, 6, 8, 12, 14, 16, 18, 22, 24, 26} genera un $M' = M_{S1}, M_{S2}, M_{S3}, M_{S4}$ = {1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 10, 20, 24, 6, 8, 12, 14, 16, 18, 22, 24, 26} y un *C = "M N A E S O D D E T X P A O C E E S J E N I O N T L N".*

m	M	E	N	S	A	J	E	E	S	C	O	N	D	I	D	O	E	N	T	E	X	T	P	L	A	N	O
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
M'	1	3	5	7	9	11	13	15	17	19	21	23	25	27	10	20	2	4	6	8	12	14	16	18	22	24	26
C	M	N	A	E	S	O	D	D	E	T	X	P	A	O	C	E	E	S	J	E	N	I	O	N	T	L	N
MS1	1	3	5	7	9	11	13	15	17	19	21	23	25	27													
MS2	10	20																									
MS3	2																										
MS4	4	6	8	12	14	16	18	22	24	26																	

10.b. Al mismo mensaje anterior se aplicó las series M_{S1} = {1, 2, 3, 5, 8, 13, 21}, M_{S2} = {7, 11, 12, 14, 16, 20, 23, 25} , M_{S3} = {9, 10, 18, 27} y M_{S4} = {4, 6, 15, 17, 19, 22, 24, 26} generando un *M' = {1, 2, 3, 5, 8, 13, 21, 7, 11, 12, 14, 16, 20, 23, 25, 9, 10, 18, 27, 4, 6, 15, 17, 19, 22, 24, 26}* y un *C* = "M E N A E D X E O N I O E P A S C N O S J D E T T L N"

m	M	E	N	S	A	J	E	E	S	C	O	N	D	I	D	O	E	N	T	E	X	T	P	L	A	N	O
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
M'	1	2	3	5	8	13	21	7	11	12	14	16	20	23	25	9	10	18	27	4	6	15	17	19	22	24	26
C	M	E	N	A	E	D	X	E	O	N	I	O	E	P	A	S	C	N	O	S	J	D	E	T	T	L	N
MS1	1	2	3	5	8	13	21																				
MS2	7	11	12	14	16	20	23	25																			
MS3	9	10	18	27																							
MS4	4	6	15	17	19	22	24	26																			

11. Con el mensaje "M U R C I E L A G O E N E L C O B E R T I Z O" y 3 series: M_{S1} = {1, 3, 5, 7, 9, 11, 13, 15, 17, 19}, M_{S2} = {2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22} y M_{S3} = {21, 23} se pueden obtener *3! = 6* combinaciones:

- $M' = M_{S1}, M_{S2}, M_{S3}$ = MRILGEECBRUCEAONLOETZIO
- $M' = M_{S1}, M_{S3}, M_{S2}$ = MRILGEECBRIOUCEAONLOETZ
- $M' = M_{S2}, M_{S1}, M_{S3}$ = UCEAONLOETZMRILGEECBRIO
- $M' = M_{S2}, M_{S3}, M_{S1}$ = UCEAONLOETZIOMRILGEECBR
- $M' = M_{S3}, M_{S1}, M_{S2}$ = IOMRILGEECBRUCEAONLOETZ

- $M' = M_{S3}, M_{S2}, M_{S1}$ = IOUCEAONLOETZMRILGEECBR

12. Considerando el criptograma "EEJAODINEUASOUEASLCIDADLIRTN DTSLAUO" y las claves: M_{S1} = {1, 5, 12, 22, 35}, M_{S2} = {10, 15, 20, 25, 30}, M_{S3} = {3, 6, 9, 13, 16, 19, 23, 26, 29, 31, 32, 33, 34}, M_{S4} = {2}, M_{S5} = {7, 11, 17}, M_{S6} = {8, 21}, M_{S7} = {27} y M_{S8} = {4, 14, 18, 24, 28} se obtuvo el mensaje en claro: "E L A S E S I N O D R J U L I E T A A N D A S U E L T O C U I D A D O".

V. *CONCLUSIONES*

Respecto al laboratorio anterior se resalta que los algoritmos de transposición son más tediosos de descifrar a mano que los métodos de sustitución.

Para utilizar los metodos clasicos de criptografía sería adecuado implementar aquellos que empleen la sustitución y transposición conjuntamente, esto con el fin de garantizar uno de los pilares básicos de la seguridad informática: la confidencialidad.

Aunque sea transparente para el usuario final las matemáticas están siempre presente tanto en los métodos de sustituciones como en los de transposición al igual que en la criptografía moderna.

VI. *REFERENCIAS BIBLIOGRÁFICAS*

[1] García, R. D. M. Criptografía clásica y moderna, 2009. Recuperado de https://ebookcentral.proquest.com

[2] Rodriguez, C. D. ADFGVX CIPHER. Recuperado de https://crypto.interactive-maths.com/adfgvx-cipher.html