



VÍDEO intypedia001es

LECCIÓN 1: HISTORIA DE LA CRIPTOGRAFÍA Y SU DESARROLLO EN EUROPA

EJERCICIOS

AUTOR: Arturo Ribagorda Garnacho

Universidad Carlos III de Madrid, España

EJERCICIO 1

El descubrimiento de que cada lengua tenía una frecuencia característica de aparición de sus letras, permitió la ruptura de los textos cifrados tipo César y, más general aún, los monoalfabéticos.

Por ello, los criptógrafos se afanaron desde el Renacimiento en encontrar nuevos métodos de cifrado, hallando entre otros los denominados polialfabeto. En éstos, se usan varios alfabetos cifrados, de modo que la letra cifrada de una dada depende de la posición de ésta en el texto en claro. De todos ellos el más sencillo es aquel que usa dos alfabetos de cifrado, uno para las letras que ocupan posiciones pares en el texto en claro y otro para las que se ubican en posiciones impares.

Así, un ejemplo podría ser:

Alfabeto para posiciones impares

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	e	i	m	p	t	x	b	f	j	n	q	u	Y	c	g	k	ñ	r	v	z	d	h	l	o	s	w

Alfabeto para posiciones pares

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	r	w	b	g	l	p	u	z	e	j	ñ	s	X	c	h	m	q	v	a	f	k	o	t	y	d	i

Suponiendo este método polialfabético cifre el texto en claro:

“SUSTITUCIÓN POLIALFABÉTICA”

SOLUCIÓN

Procediendo como se ha indicado resulta:

S	U	S	T	I	T	U	C	I	O	N	P	O	L	I	A	L	F	A	B	E	T	I	C	A
V	k	v	f	f	f	d	w	f	h	y	m	g	ñ	f	n	q	l	a	r	p	f	f	w	a

Así pues el resultado será:

v k v f f f d w f h y m g ñ f n q l a r p f j w a

EJERCICIO 2

1.- Un método de transposición muy empleado antiguamente es el conocido como TRANSPOSICIÓN COLUMNAR. Para empezar, se escribe el texto en claro (de izquierda a derecha y de arriba abajo), en una tabla de un número determinado de columnas (cada letra en una celda de la tabla) y usando tantas filas como sea necesario. Finalmente, el texto cifrado se obtiene escribiendo primeramente las letras que han quedado en la primera columna, a continuación las que están en la segunda columna y sucesivamente hasta terminar con todas las letras de la tabla.

Mediante el método de transposición columnar con cinco columnas cifre el texto en claro:

“EJEMPLO DE TRANSPOSICIÓN COLUMNAR”

2.- El procedimiento se puede complicar empleando una clave consistente en una palabra sin letras repetidas y con tantas de ellas como columnas se desea que tenga la tabla. Escribiendo la clave encima de la tabla (la primera letra de la clave encima de la primera columna, la segunda letra sobre la segunda columna, etc.), el texto cifrado resulta de escribir primeramente la columna cuya letra de comienzo (la letra de la clave) sea la primera en el alfabeto, después la columna cuya letra de la clave sea la siguiente en el alfabeto, y así sucesivamente.

Mediante el método de transposición columnar con la clave “EMISOR” cifre el texto en claro: “TENGO EXAMEN COMPLETO CON SOLUCIÓN”

SOLUCIÓN

1.- Se dispone el texto en claro en una tabla de cinco columnas:

E J E M P

L	O	D	E	T
R	A	N	S	P
O	S	I	C	I
O	N	C	O	L
U	M	N	A	R

Extrayendo las letras en el orden que marcan las columnas (primero las de la primera columna, después las de la segunda, luego las de la tercera y sucesivamente) queda el texto cifrado:

“e l r o o u j o a s n m e d n i c n m e s c o a p t p i l r”

2.- Como la clave tiene seis letras, las columnas serán igualmente seis. Por tanto, escribiendo el texto en claro en ese número de columnas, resultará:

T	E	N	G	O	E
X	A	M	E	N	C
O	M	P	L	E	T
O	C	O	N	S	O
L	U	C	I	O	N

Situando la clave encima:

E	M	I	S	O	R
T	E	N	G	O	E
X	A	M	E	N	C
O	M	P	L	E	T
O	C	O	N	S	O
L	U	C	I	O	N

Y escribiendo las letras de las columnas según el orden de las letras de la clave en el alfabeto (primero la E, luego la I, después la M y sucesivamente), el texto cifrado queda:

“t x o o l n m p o c e a m c u o n e s o e c t o n g e l n i

EJERCICIO 3

Rotos los métodos de sustitución monoalfabeto por el descubrimiento del criptoanálisis por los árabes, desde los años finales de la Baja Edad Media (más concretamente desde el Renacimiento) comenzaron a desarrollarse otros métodos de cifrado, entre los cuales se

hallaban los polialfabéticos y los nomenclátors. Estos últimos consistían en un catálogo de nombres que se deseaban ocultar, en el que cada uno aparecía asociado a una palabra, número o grupo de símbolos que lo sustituían en un texto cifrado.

A menudo, métodos polialfabéticos y nomenclátors se combinaban como ocurría en el disco de Alberti.

Considerando el disco de Alberti siguiente:

y el nomenclátor:

Felipe II	123
Rey	124
Walshingan	122



Descifre el texto:

“b a a & h p m i y v s v o i y l r l x c k n g k l”

NOTA 1: Cada diez letras descifradas, se ha de girar el disco externo (de las mayúsculas) dos posiciones en el sentido de las agujas del reloj.

NOTA 2: En el disco de Alberti, la u se identifica con la v al cifrar. Al descifrar, por el sentido de la frase, se puede conocer si se ha de escribir una u otra letra.

SOLUCIÓN:

Con los discos en la posición inicial:

b	a	a	&	H	p	m	i	Y	V
1	2	2	M	V	E	R	T	O	I

Con el disco externo girado 2 posiciones en el sentido de las agujas del reloj:

s	v	o	l	Y	l	r	l	X	C
N	F	O	R	M	A	D	A	L	1

Con el disco externo girado otras 2 posiciones en el sentido de las agujas del reloj:

k	n	g	k	L
2	4	1	2	3

Así pues el texto en claro (sin considerar el nomenclator) resulta:

“ 1 2 2 M V E R T O I N F O R M A D A L 1 2 4 1 2 3 ”

Es decir, tomando en consideración el nomenclátor (y añadiendo espacios entre las palabras para su mejor lectura) el texto completamente descifrado resulta:

“W a l s h i n g a m m u e r t o I n f o r m a d a l R e y F e l i p e I I ”

EJERCICIO 4

Los métodos de sustitución tipo César cambian cada letra del texto en claro por aquella otra situada un número fijo de posiciones tras ella en el alfabeto (en el caso César este número es tres).

Sabiendo que el siguiente texto cifrado:

“ i w x s i w y q i n i p t o h i g m j v h s p s q s e o j e f i x s x m t s g i w e v ”

se ha obtenido por un método tipo César, descífralo teniendo en cuenta la siguiente tabla de frecuencias característica del español:

e	a	O	L	s	n
15%	13%	9%	7%	8%	7%

SOLUCIÓN

Basta con hallar la letra cifrada que corresponde a la “e”, pues con ello tendremos el número que indica el desplazamiento de todas las letras cifradas respecto de las letras en claro y el descifrado será inmediato.

Si contamos cuantas veces aparecen las letras en el texto cifrado tenemos:

i	e	x	W	...
8	4	3	3	...

De modo que la letra cifrada “i” (la letra que más veces aparece) debe corresponder a la “e”. Así, el alfabeto usado debe ser:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

lo se corrobora porque la siguiente letra más frecuente en el cifrado, la “e” se corresponde con la “a”. Nótese que dada la escasa extensión del texto cifrado, el resto de letras no sigue la frecuencia típica. Cuanto más extenso sea un texto más se aproxima el número porcentual de aparición de las letras al predicho.

Considerando el texto en claro:

l w x s i w y q i n i p t o h i g m j v h s p s q s e o j e f i x s x m t s g i w e v

y usando el alfabeto obtenido:

i	W	x	S	i	w	y	q	l	N	i	p	t	o	H	i	g	m	j	v	h	s	P
E	S	T	O	E	S	U	N	E	J	E	M	P	L	O	D	E	C	I	F	R	A	D

s	Q	s	E	o	j	e	f	l	X	s	x	m	t	S	g	i	w	e	v		
O	M	O	N	O	A	L	F	A	B	E	T	O	T	I	P	O	C	E	S	A	R

resulta el texto en claro

buscado:

“Esto es un ejemplo de cifrado monoalfabeto tipo César”

EJERCICIO 5

A la hora de criptoanalizar un texto cifrado, un primer problema consiste en saber si se ha obtenido por un método de transposición o de sustitución. Como en el primer caso las letras no han cambiado de significado, si no sólo de posición, contando el número de veces que aparece cada una es aproximadamente igual al que corresponde según su frecuencia característica en el correspondiente idioma, el cifrado será de transposición.

Con ello, y sabiendo que la distribución de letras en castellano es aproximadamente:

E	a	o	L	s	n
15	13	9	8	8	7

Razone brevemente si el siguiente texto cifrado se ha obtenido mediante un método de sustitución monoalfabeto o uno de permutación:

“Is modí es unovedad porquean te slos hombrñe spodan divid irs es encillamf, igu rac i nhum an asi nparentoda l ahist, oriaele. Sp ecial ist ano ssi rveheaquunpór ecioso eje mpl ar dees te extraoho. Mb renuevoquehe int entad ente ensabiose igénorantesen ms omenoss a biosymso men osig no rantesoporu na yo tradesu. Svrti entes yha cesdefi nirñhe dichoquee, raunaconparac, on cretar e nrgicament, el aée s pecie yhacer n oás v ertod oelradical”.

SOLUCIÓN

Aproximadamente hay el siguiente número de letras:

e = 49

a = 44

o = 32

l = 9

s = 29

n = 28

Total letras = 368

Lo que hace: e= 13%; a=12%; O=9%; l=2%; s= 8%; n = 8%, que coincide bastante con la frecuencia natural de las letras en castellano por lo que nos hallamos ante un cifrado de transposición.

Madrid, España, septiembre de 2010

<http://www.intypedia.com>

<http://twitter.com/intypedia>

