CIFRADOS POLIGRÁFICOS (POR BLOQUES).

Profesores del curso:

Ronald Mass [1]

Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

3 de septiembre de 2020

Tabla de contenidos

Cifrados por bloques

Definición 1

Un **cifrado por bloques** *o también llamado* **cifrado poligráfico** *es un criptosistema the separa el texto plano en cadenas, llamadas* **bloques**, *todas de longitud fija* $k \in \mathbb{N}$, *llamado* **longitud del bloque** *y cifra un bloque a la vez.*

Tabla de contenidos

Cifrado de Vigenere

Sea $n \in \mathbb{N}$ y sean $k_1 k_2 \dots k_r$ para $1 \leq r \leq n$ una **clave primaria**. Entonces, dado un mensaje en texto plano $m = (m_1, m_2, \dots, m_s)$ donde $s > r$, entonces se generan las siguientes cadenas:

$$k = k_1 k_2 \dots k_r m_1 m_2 \dots m_{s-r}.$$

Luego, el cifrado se realiza considerando:

$$E_{k_j}(m_j) = (m_j + k_j)\,(mod\ n) = c_j \quad \text{para} \quad j = 1, 2, \dots, r$$

y

$$E_{k_j}(m_j) = (m_j + m_{j-r})\,(mod\ n) = c_j \quad \text{para} \quad j > r.$$

Desciframiento de Vigenere

El proceso de descifrado se realiza usando:

$$D_{k_j}(c_j) = (c_j - k_j)\,(mod\ n) = m_j \quad \text{para} \quad j = 1, 2, \ldots, r$$

y

$$D_{k_j}(c_j) = (c_j - m_{j-r})\,(mod\ n) = m_j \quad \text{para} \quad j > r.$$

Considere la tabla:

Texto	a	b	c	d	e	f	g	h	i	j	k	l
plano	0	1	2	3	4	5	6	7	8	9	10	11
Texto	m	n	o	p	q	r	s	t	u	v	w	x
plano	12	13	14	15	16	17	18	19	20	21	22	23
Texto	y	z										
plano	24	25										

Ejemplo:

Considere el texto plano $m =$ *" study right now "* y la clave $k = 372m_1m_2 \ldots m_{10}$. Es decir:

$$r = 3,\ s = 10,\ k_1 = 3, k_2 = 7, k_3 = 2, m_1 = s, \ldots, m_{10} = t.$$

Luego, el proceso de ciframiento inicia:

s	t	u	d	y	r	i	g	h	t	n	o	w
18	19	20	3	24	17	8	6	7	19	13	14	22
3	7	2	s	t	u	d	y	r	i	g	h	t
			18	19	20	3	24	17	8	6	7	19
21	26	22	21	43	37	11	30	24	27	19	21	41

Tomando residuo módulo 26:

21	26	22	21	43	37	11	30	24	27	19	21	41
21	0	22	21	17	11	11	4	24	1	19	21	15
v	a	w	v	r	l	l	e	y	b	t	v	p

por tanto, el texto cifrado es:

$$c = vawvrlleybtvp$$

Para descifrar el mensaje, procedemos de la forma siguiente:

$$\begin{aligned} m_1 &= c_1 - k_1 = 21 - 3 = 18\,(mod\,26) \\ m_2 &= c_2 - k_2 = 0 - 7 = -7\,(mod\,26) = 19\,(mod\,26) \\ m_3 &= c_3 - k_3 = 22 - 2 = 20\,(mod\,26) \end{aligned}$$

Continuamos con el descifrado:

$$
\begin{array}{lcl}
m_4 & = & c_4 - m_{4-3} = 21 - m_1 = 21 - 18 = 3\,(mod\,26) \\
m_5 & = & c_5 - m_{5-3} = 17 - m_2 = 17 - 19 = -2 \equiv 24\,(mod\,26) \\
m_6 & = & c_6 - m_{6-3} = 11 - m_3 = 11 - 20 = -9 \equiv 17\,(mod\,26) \\
\hline
m_7 & = & c_7 - m_{7-3} = 11 - m_4 = 11 - 3 = 8 \\
m_8 & = & c_8 - m_{8-3} = 4 - m_5 = 4 - 24 = -20 \equiv 6\,(mod\,26) \\
m_9 & = & c_9 - m_{9-3} = 24 - m_6 = 24 - 17 = 7\,(mod\,26) \\
\hline
m_{10} & = & c_{10} - m_{10-3} = 1 - m_7 = 1 - 8 = -7 \equiv 19\,(mod\,26) \\
m_{11} & = & c_{11} - m_{11-3} = 19 - m_8 = 19 - 6 = 13 \\
m_{12} & = & c_{12} - m_{12-3} = 21 - m_9 = 21 - 7 = 14 \\
\hline
m_{13} & = & c_{13} - m_{13-3} = 15 - m_{10} = 15 - 19 = -4 \equiv 22\,(mod\,26) \\
\hline
\end{array}
$$

Los valores obtenidos para m_i $(i = 1, 2, \ldots, 13)$ se resumen en la siguiente tabla

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}
18	**19**	**20**	**3**	**24**	**17**	**8**	**6**	**7**	**19**	**13**	**14**	**22**
s	**t**	**u**	**d**	**y**	**r**	**i**	**g**	**h**	**t**	**n**	**o**	**w**

observando así que recuperamos le mensaje original.

Segundo método de Vigenere

Para este método de cifrado se usa una clave primaria $k = k_1 k_2 \ldots k_r$ y una tabla de 26 x 26 casilleros, que van de la "A" a la "Z" tanto en filas como en columnas (ver figura en la siguiente página). Esta tabla recibe el nombre de "cuadro de Vigenère".

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

Proceso de ciframiento

Veamos con un ejemplo:
Considere la clave primaria $k = morsa$ y el texto plano: m =*bienvenido*. Luego, considere la siguiente tabla:

b	i	e	n	v	e	n	i	d	o	s
m	o	r	s	a	m	o	r	s	a	m

Considerando este particular ejemplo, se toma la primera letra del texto a cifrar, así como la primera letra de la clave primaria. Esto nos da la coordenada de la columna y fila respectivamente. Así encontramos la letra cifrada. Por ejemplo, de acuerdo a la tabla, si la primera letra es la "B" (de BIENVENIDO) –la columna, la letra de la clave primaria correspondiente es la "M" (de MORSA), que es la fila. Así en la posición **(M,B)** se obtiene la letra cifrada correspondiente que es "N".

Este proceso lo realizamos para todas las letras y así generamos el texto cifrado. ¨Podemos ver que si aplicamos este algoritmo, resulta la siguiente tabla y el texto cifrado.

b	i	e	n	v	e	n	i	d	o	s
m	o	r	s	a	m	o	r	s	a	m
N	W	V	F	V	Q	B	Z	V	O	E

Proceso de desciframiento

El descifrado de un mensaje del código Vigenère se hace de la siguiente manera: se va a la fila de la tabla en donde está la letra correspondiente a la llave. Se encuentra entonces la letra a la cual se cifró y entonces, se busca la columna correspondiente, que viene ser la letra sin cifrar. Por ejemplo, si la primera letra del mensaje cifrado es "N" y la primera letra de la llave es "M" (de MORSA), hallamos que la "N" aparece en la columna "B", que es la primera letra del texto sin cifrar. Tomamos la segunda letra de la llave, la "O" y nos posicionamos en esa fila en la tabla de Vigenère. Vemos en qué columna está la "W" (la letra cifrada) y veremos que se encuentra en la columna "I", que es la segunda letra del texto original.

Cifrado de Hill

Considere:

$$\begin{aligned} \mathcal{K} &= \{e \in \mathbb{M}_{r\times r}(\mathbb{Z}_n) \,/\, e \quad \text{es invertible}\}, \\ \mathcal{M} &= \mathcal{C} = (\mathbb{Z}_n)^r. \end{aligned}$$

Luego, para $m \in \mathcal{M}$ y $e \in \mathcal{K}$ se define:

$$E_e(m) = me \quad \text{y} \quad D_d(c) = ce^{-1}.$$

Ejemplo:

Considere el texto plano $m = MISSISSIPPI$ y la clave $e = \begin{pmatrix} 3 & 25 \\ 24 & 17 \end{pmatrix}$.

Para el proceso de ciframiento, se obtiene la siguiente tabla:

m	i	s	s	i	s	s	i	p	p	i
12	8	18	18	8	18	18	8	15	15	8

formamos la matriz:

$$M = \begin{pmatrix} 12 & 8 \\ 18 & 18 \\ 8 & 18 \\ 18 & 8 \\ 15 & 15 \\ 8 & 8 \end{pmatrix} \Rightarrow C = Me = \begin{pmatrix} 12 & 8 \\ 18 & 18 \\ 8 & 18 \\ 18 & 8 \\ 15 & 15 \\ 8 & 8 \end{pmatrix} \begin{pmatrix} 3 & 25 \\ 24 & 17 \end{pmatrix}$$

multiplicando y tomando módulo 26 resulta:

$$C = \begin{pmatrix} 228 & 436 \\ 486 & 756 \\ 456 & 506 \\ 246 & 586 \\ 405 & 630 \\ 216 & 336 \end{pmatrix} \equiv \begin{pmatrix} 20 & 20 \\ 18 & 2 \\ 14 & 12 \\ 12 & 14 \\ 15 & 6 \\ 8 & 24 \end{pmatrix} (mod\, 26)$$

obteniendo la siguiente tabla:

20	20	18	2	14	12	12	14	15	6	8	24
u	u	s	c	o	m	m	o	p	g	i	y

y el mensaje cifrado es:

$$c = "u\ u\ s\ c\ o\ m\ m\ o\ p\ g\ i\ y"$$

Desciframiento del método de Hill

Para esto recuerde que:

$$e^{-1} = [det(e)]^{-1} adj(e)$$

donde $[det(e)]^{-1}$ es el inverso de $det(e)$ módulo n. Luego:

$$M = D_d(C) = Ce^{-1}.$$

Calculemos e^{-1}: $det(e) = -549$ y por el algoritmo de Euclides:

$$\begin{array}{rcl} 549 &=& 26(21)+3 \\ 26 &=& 3(8)+2 \\ 3 &=& 2(1)+1 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 &=& 3-2(1) \\ 1 &=& 3-[26-3(8)](1) \\ &=& 9(3)-26 \\ 1 &=& 9[549-26(21)]-26 \\ &=& 9(549)-190(26). \end{array}$$

Por tanto: $[det(e)]^{-1} = 549^{-1} \equiv 9\,(mod\,26)$. Luego:

$$e^{-1} = 9\begin{pmatrix} -17 & 25 \\ 24 & -3 \end{pmatrix} = \begin{pmatrix} -153 & 225 \\ 216 & -27 \end{pmatrix}$$

tomando módulo 26:

$$e^{-1} = \begin{pmatrix} 3 & 17 \\ 8 & 25 \end{pmatrix}$$

Por tanto:

$$M = \begin{pmatrix} 20 & 20 \\ 18 & 2 \\ 14 & 12 \\ 12 & 14 \\ 15 & 6 \\ 8 & 24 \end{pmatrix}\begin{pmatrix} 3 & 17 \\ 8 & 25 \end{pmatrix} = \begin{pmatrix} 220 & 840 \\ 70 & 356 \\ 138 & 538 \\ 148 & 554 \\ 93 & 405 \\ 216 & 736 \end{pmatrix}$$

Tomando módulo 26 resulta:

$$M = \begin{pmatrix} 12 & 8 \\ 18 & 18 \\ 8 & 18 \\ 18 & 8 \\ 15 & 15 \\ 8 & 8 \end{pmatrix}$$

y así tenemos la siguiente tabla:

12	8	18	18	8	18	18	8	15	15	8	8
m	i	s	s	i	s	s	i	p	p	i	i

es decir, hemos recuperado el mensaje original:

$$m\ i\ s\ s\ i\ s\ s\ i\ p\ p\ i$$