#### Evaluación de Aprendizaje

Pág. 1 de 3



# Evaluación de Aprendizaje 2

#### **Temas**

Criptografía.

# Fechas limites de entregas

ENTREGA	Lunes 2/11/2020	Fecha de Entrega
DEVOLUCION RDOS	Lunes 9/11/2020	Fecha Máxima de Devolución de Resultados
REENTREGA	Lunes 16/11/2020	Fecha de Reentrega

# Consigna

Realice los ejercicios planteados a continuación:

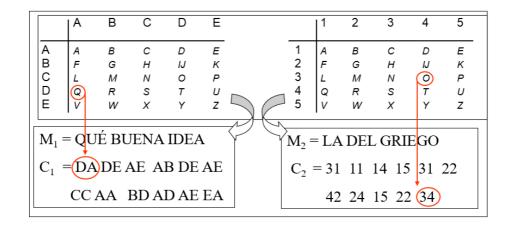
# 1. Cifrador Polybios:

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.c.).

El mismo trabaja con una matriz, por lo general cuadrada (en este caso de 5x5), en la cual se colocan los caracteres del alfabeto original.

Para obtener el mensaje cifrado, se busca el par fila/columna y se lo coloca como cifrado. Como puede verse en el gráfico, la letra Q deriva en DA.

Nota: Los espacios en blanco no son tomados en cuenta.



Se pide:

### Evaluación de Aprendizaje





- Cifrar el mensaje "Seguridad y Calidad en Aplicaciones Web"
- Responder: ¿Qué característica tiene el presente cifrador que lo hace poco interesante para su uso? (sin importar la época histórica)

#### 2. Cifrador Vernam:

En 1917 Gilbert Vernam (MIT) propone un cifrador por sustitución binaria con clave de un único uso, basado en el código Baudot de 5 bits:

La operación de cifrado es la función XOR.

El algoritmo de descifrado es igual al de cifrado por la involución de la función XOR.

La clave será tan larga o más que el mensaje y se usará una sola vez.

# Código BAUDOT

bits	letra	figs	hexa	bits	letra	figs	hexa
00011	Α	-	03	01100	Ν	,	0C
11001	В	?	19	11000	0	9	18
01110	С	:	0E	10110	Р	0	16
01001	D	\$	09	10111	Q	1	17
00001	Ε	3	01	01010	R	4	0A
01101	F	!	0D	00101	S	BEL	L 05
11010	G	&	1A	10000	Т	5	10
10100	Н	STO	OP 14	00111	U	7	07
00110	- 1	8	06	11110	V	;	1E
01011	J	•	0B	10011	W	2	13
01111	K	(	0F	11101	Χ	/	1D
10010	L	)	12	10101	Υ	6	15
11100	M		1C	10001	Z	"	11

Se cifra tomando un carácter del mensaje original y un carácter de la clave y se realiza un XOR. Ejemplo:

$$B \oplus V = 11001 \oplus 11110 = 00111 = U$$

Se pide:

Cifrar el mensaje "clasesremotas" con la clave "segaridrdycclidad "

## 3. Criptoanálisis

Descifrar el siguiente texto: "LZAHL ZBTHW YBLIH XBLKL ILYOH ZLYCH ROKH" por medio de un ataque por características/estadísticas del lenguaje, en nuestro

# Evaluación de Aprendizaje

Pág. 3 de 3



caso el castellano, y teniendo en cuenta el uso intensivo de las vocales "A","E", y "O" del mismo.

Mencionar método de cifrado utilizado y su clave

# 4. Responda las siguientes preguntas de concepto:

- a) ¿Cuál de los métodos analizados/utilizados anteriormente le parece más seguro?
- b) ¿En qué situaciones podrían utilizarse cada uno de estos métodos? (si no fuera conveniente, mencionarlo. No tomar en cuenta la época histórica)
- c) ¿Cómo serían clasificados cada uno de estos métodos analizados/utilizados en los puntos 1, 2 y 3?
- d) ¿Qué clase de algoritmo es AES?