CRIPTOGRAFÍA

LECCIÓN 0:

OBJETIVOS

- EXPLICAR EL USO DE LA CRIPTOGRAFÍA
- DESCRIBIR LOS DIVERSOS MECANISMOS DE CIFRADO

CONTENIDO

- ALFABETOS MEZCLADOS

METODO AUTOCLAVE

Constituido por un elemento cifrante (regleta), que utiliza un indicativo (letra, palabra o frase clave) para comenzar el cifrado y luego se "toma" el mismo texto claro o cripto (autoclave) para cifrar las siguientes letras.

CIFRADO

- La letra, palabra o frase clave (indicativo), se escribe en la parte superior del texto claro.
- Hacer coincidir la letra o cada una de las letras del indicativo con la posición inicial de la regleta y sustituir la letra del texto claro por su representación en el alfabeto secundario, repitiéndose hasta terminar de cifrar con el indicativo disponible.
- Para continuar el cifrado se utilizará el mismo texto claro o cripto como clave (según convenio).

	ABCDEFGHIJKLMNOPQRSTUVWXYZ	
WMHBRYSDJ	AZTFKNPXQICUVLGOEWMHBRYSDJ	AZTFKNPXQICUVLGOE

CIFRADO UTILIZANDO CRIPTO COMO AUTOCLAVE

Indicativo	: AVIONAPTKYQNTBG
Texto Claro	: AUTORIZARSALIDA
Texto Cripto	: APTKYQNTBGQECSG

CIFRADO UTILIZANDO CLARO COMO AUTOCLAVE

Indicativo : A V I O N A U T O R I Z A R S
Texto Claro : A U T O R I Z A R S A L I D A
Texto Cripto : A P T K Y Q C T P L I V Q D S

DESCIFRADO

- La letra, palabra o frase clave (indicativo), se escribe en la parte superior del texto cripto.
- Hacer coincidir la letra o cada una de las letras del indicativo con la posición inicial de la regleta y sustituir la letra del texto cripto (secundario) por su representación en el alfabeto primario, repitiéndose hasta terminar de descifrar con el indicativo disponible.
- Para continuar el descifrado se utilizará el mismo texto claro o cripto como clave (según convenio).

DESCIFRADO UTILIZANDO CRIPTO COMO AUTOCLAVE

Indicativo : A V I O N A P T K Y Q N T B G
Texto Cripto : A P T K Y Q N T B G Q E C S G
Texto Claro : A U T O R I Z A R S A L I D A

DESCIFRADO UTILIZANDO CLARO COMO AUTOCLAVE

Indicativo : A V I O N A U T O R I Z A R S
Texto Cripto : A P T K Y Q C T P L I V Q D S
Texto Claro : A U T O R I Z A R S A L I D A

MÉTODO DELASTELLE

Procedimiento que utiliza cuadros cerrados, donde se inscribe el alfabeto primario y el secundario está constituido por los índices de línea y columna (bibase o tribase).

Corresponde al tipo de claves por fraccionamiento, debido que en el cifrado emplea simultáneamente:

SUSTITUCION + TRANSPOSICION + SUSTITUCION

49

CIFRADO

- Las letras del texto claro se toman del cuadro (bibase o tribase) y su representación está dada por números del índice de línea y columna.
- Los números cifrantes se colocan en forma vertical debajo de las letras del texto claro.
- Seguidamente los valores numéricos son tomados en forma HORIZONTAL de dos en dos o tres en tres (según cuadro utilizado).
- Luego son recifrados en el mismo cuadro a fin de obtener un valor literal, siempre guiándose por la dirección del índice. Al finalizar la primera línea numérica, se continuará con la segunda o tercera línea hasta terminar la serie numérica.

CIFRADO CON CUADRO BIBASE

BIBASE

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

Texto claro : E J E R C I T O P E R U A N O
(Sustitución) : 5 5 5 3 3 4 5 5 1 5 3 1 1 4 5
1 2 1 4 1 2 4 3 4 1 4 5 1 3 3

(Transposición)

55 53 34 55 15 31 14 51 21 41 24 34 14 51 33

(Sustitución)

Z O R Z U C P E B D Q R P E M

Texto cripto : ZORZU CPEBD QRPEM

CIFRADO CON CUADRO TRIBASE

TRIBASE

	1	2	3
1 1	C	D	E
1 2	H	I	J
1 3	M	N	O
2 1	R	S	T
2 2	X	Y	Z
2 3	A	F	P
3 1	U	B	G
3 2	L	Q	V
3 3	W	K	Ñ

Texto claro : R E P U B L IC A D E P E R U
(Sustitución) : 1 3 3 1 2 1 2 1 1 2 3 3 3 1 1

1 1 3 1 1 2 2 1 3 1 1 3 1 1 1

2 1 2 3 3 3 1 1 2 1 1 2 1 2 3

(Transposición)

133 121 211 233 311 113 112 213 113 111 212 333 112 112 123
W H D K E U R B U C S Ñ R R L

(Sustitución)

Texto cripto : WHDKE URBUC SÑRRL

DESCIFRADO

- Se cuenta la cantidad total de letras del cripto.
  Texto cripto : WHDKE URBUC SÑRRL = 15

- En base a la cantidad obtenida, se coloca HORIZONTALMENTE los dígitos que resultan de descifrar cada una de las letras del cripto en el cuadro empleado (bibase o tribase). Si la cantidad es 30 la primera línea será de 30 dígitos, continuándose con la segunda o tercera línea según sea el caso.

  1 3 3 1 2 1 2 1 1 2 3 3 3 1 1
  1 1 3 1 1 2 2 1 3 1 1 3 1 1 1 = 15
  2 1 2 3 3 3 1 1 2 1 1 2 1 2 3

- Los dígitos obtenidos se toman en forma VERTICAL y se sustituyen por las letras ubicadas en el cuadro.

  1 3 3 1 2 1 2 1 1 2 3 3 3 1 1
  1 1 3 1 1 2 2 1 3 1 1 3 1 1 1
  2 1 2 3 3 3 1 1 2 1 1 2 1 2 3

Texto Claro : R E P U B L I C A D E P E R U

METODO LORD BACON

Conformado por un alfabeto primario ordenado en donde cada letra está representada por un grupo de cinco letras (secundario) en el que participan solamente la "A" y la "B".
El secundario a su vez es sustituido por un texto de apariencia normal, en el que las letras que representan a la "A" van en minúsculas y las que representan a la "B" en mayúsculas. Tal sustitución es convencional y puede hacerse a la inversa. Finalmente cada letra del texto claro, estará representada por cinco letras.
Corresponde al tipo de claves por fraccionamiento, debido que en el cifrado emplea:

SUSTITUCIÓN + SUSTITUCIÓN

TABLA ORIGINAL

A aaaaa	F abaab	K aabbb	P bbaaa	U bbaba
B aaaab	G ababa	L aaabb	Q bbbaa	V bbbbb
C aaaba	H abbaa	M aabaa	R babaa	X bbbba
D aabab	I abbab	N abbba	S babab	Y baaab
E aabba	J abbbb	O baaaa	T bbaab	Z bbabb

(Se excluye la W y la Ñ)

CIFRADO

- Las letras del texto claro se sustituyen por su representación en grupos de cinco letras (secundario).
- Se toma un texto de apariencia normal cualquiera y se coloca debajo de los grupos, separados ambos de cinco en cinco.
- El texto de apariencia normal, será el cripto y respetará las mayúsculas ("B") y minúsculas ("A")
- La transmisión del texto cripto será como palabras normales.

Texto Claro	:	S	I	R	V	A	S	E
Sust. Original	:	babab	abbab	babaa	bbbbb	aaaaa	babab	aabba
Texto cripto	:	LaCoR	rIEnT	EdEln	IÑOPE	rjudi	CaLaP	esCAx
Texto a trasmitir	:	La CoRrIEnTE dEl nIÑO PErjudiCa La PesCA						

DESCIFRADO

- Se separa el texto recibido de cinco en cinco.
- Se otorgan los valores de "B" a cada una de las letras mayúsculas y "A" a las minúsculas.
- Los grupos obtenidos (de cinco letras) son ubicados en la tabla original y se obtiene el claro.

Texto recibido	:	La CoRrIEnTE dEl nIÑO PErjudiCa La PesCA						
Texto cripto	:	LaCoR	rIEnT	EdEln	IÑOPE	rjudi	CaLaP	esCAx
Sust. Original	:	babab	abbab	babaa	bbbbb	aaaaa	babab	aabba
Texto Claro	:	S	I	R	V	A	S	E