ENCRIPTACIÓN Y CRIPTOGRAFÍA

Instructor: Leonardo…

Introducción

La **encriptación** es el proceso para volver ilegible información considerada importante refiriéndose al proceso de convertir información a una forma oculta o enmascarada para poder enviarla a través de canales potencialmente inseguros.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.

Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

La **criptografía** es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

ALGORITMOS CRIPTOGRÁFICOS CLASICOS
(Transposición)

La transposición consiste en crear el texto cifrado simplemente desordenando las unidades que forman el texto original. A diferencia de algoritmos de sustitución, los algoritmos de transposición, reordenan las letras pero no las disfrazan.

Alteran el orden de los caracteres dentro del mensaje a cifrar. El algoritmo de transposición más común consiste en colocar el texto en una tabla de **n** columnas. El texto cifrado serán los caracteres dados por columna (de arriba hacia abajo) con una clave **K** consistente en el orden en que se leen las columnas.

Ejemplo: Si **n = 3 columnas**, la clave **K es (3,1,2)**

Mensaje a cifrar **"SEGURIDAD INFORMATICA".**

El mensaje cifrado será: **" GIDNRTASUD FMIERAIOAC "**

Actividad: Si la clave **K es (2,3,1)** como seria el mensaje Cifrado?

n

1	2	3
S	E	G
U	R	I
D	A	D
	I	N
F	O	R
M	A	T
I	C	A

ALGORITMOS CRIPTOGRÁFICOS CLÁSICOS
(La cifra ADFGVX)

En la cifra **ADFGVX** hay sustitución y transposición. La codificación comienza dibujando una cuadrícula de **6x6**, y llenando los **36 cuadrados** con una disposición aleatoria de las **26 letras y los 10 dígitos.**

Cada línea y cada columna de la cuadrícula se identifica con una de las seis letra **A, D, F , G, V o X.** La disposición de los elementos de la cuadrícula funciona como parte de la clave, de modo que el receptor necesita conocer los detalles de la cuadrícula para poder descifrar los mensajes.

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	y
X	9	e	y	0	f	q

Mensaje: attack at 10 pm

Texto Plano	**a**	**t**	**t**	**a**	**c**	**k**	**a**	**t**	**1**	**0**	**p**	**m**
Criptograma	DV	DD	DD	DV	FG	FD	DV	DD	AV	XG	AD	GX

ALGORITMOS CRIPTOGRÁFICOS CLÁSICOS
(Polibio)

Polibio aparece en los libros de Criptografía como el inventor de un procedimiento para escribir las letras como pares de números. Mediante una tabla se hace corresponder a cada carácter de un alfabeto de **25** letras un par de números. La tabla de Polibio tiene la forma siguiente:

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

Ejemplo, la palabra ***Polibio*** se escribiría?

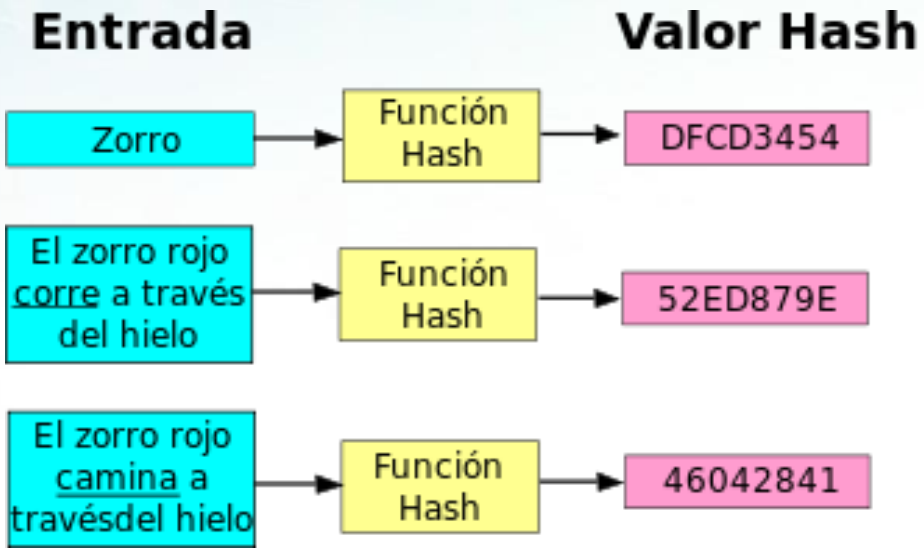
35 34 31 24 12 24 34

ALGUNOS CRIPTOSISTEMAS (ALGORITMOS)

HASH O FUNCIONES DE RESUMEN

Una función hash es método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital (o valor Hash), de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible.

La idea básica de un valor hash es que sirva como una representación compacta de la cadena de entrada. Por esta razón decimos que estas funciones resumen datos del conjunto dominio.



Ejemplos: Oracle

En el siguiente ejemplo se puede observar la actualización de caracteres por medio de la Función **Replace** tomando como referencia las vocales y cambiándolas por caracteres especiales.

ENCRIPTAR:

```
UPDATE persona
 SET apell_pers =
          REPLACE (REPLACE (REPLACE (REPLACE (REPLACE(apell_pers, 'E', '3'), 'A', '@'),
'O', '0'), 'I', '/'), 'U', '#')
```

DESENCRIPTAR:

```
SELECT ID_PERS, NOM_PERS, APELL_PERS APELL_ENCRIPTADO,
     REPLACE (REPLACE (REPLACE (REPLACE (REPLACE(apell_pers, '3', 'E'), '@', 'A'), '0',
'O'), '/', 'I'), '#', 'U') APELL_DESENCRIPTADO
FROM persona;
```

Gracias…

Instructor: Leonardo…