Criptografía y Cifrado por transposición

Ing. Max Alejandro Antonio Cerna Flores

Agenda

Criptografía

- Definición
- Historia
- Objetivos
- Proceso
- Tipos de Criptografía

Cifrado por Transposición

Criptografía

Definición

Es un método de protección de la información y las comunicaciones mediante el uso de códigos, de modo que sólo aquellos a quienes va dirigida la información puedan leerla y procesarla.

En ciencias de la computación, se refiere a las técnicas de información y comunicación derivadas de conceptos matemáticos y un conjunto de cálculos basados en reglas, para transformar mensajes en formas que son difíciles de descifrar convirtiéndolos en un mecanismo seguro.

Historia

La palabra "criptografía" se deriva del griego kryptos, que significa oculto.

El prefijo "cripto" significa "oculto", y el sufijo "-grafía" significa "escritura".

El origen de la criptografía se suele fechar alrededor del año 2000 a.C., con la práctica egipcia de los jeroglíficos.

Historia

El primer uso conocido de un cifrado moderno fue por Julio César (100 a. C. a 44 a. C.), quien no confiaba en sus mensajeros cuando se comunicaba con sus gobernadores y oficiales.

Por eso creó un sistema en el que cada carácter de sus mensajes era sustituido por un carácter tres posiciones delante de él en el alfabeto romano.

Objetivos

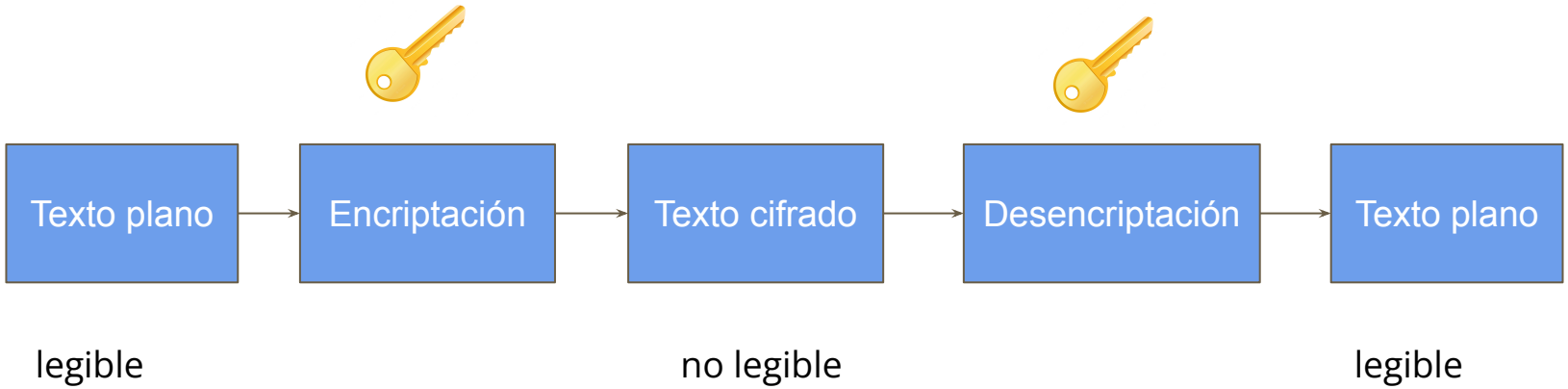
Confidencialidad: La información no puede ser entendida por nadie para quien no estaba destinada.

Integridad: La información no puede alterarse durante el almacenamiento o el tránsito entre el remitente y el destinatario previsto sin que se detecte la alteración.

No repudio: El creador/remitente de la información no puede negar en una etapa posterior sus intenciones en la creación o transmisión de la información.

Autenticación: El emisor y el receptor pueden confirmar la identidad del otro y el origen/destino de la información.

Proceso

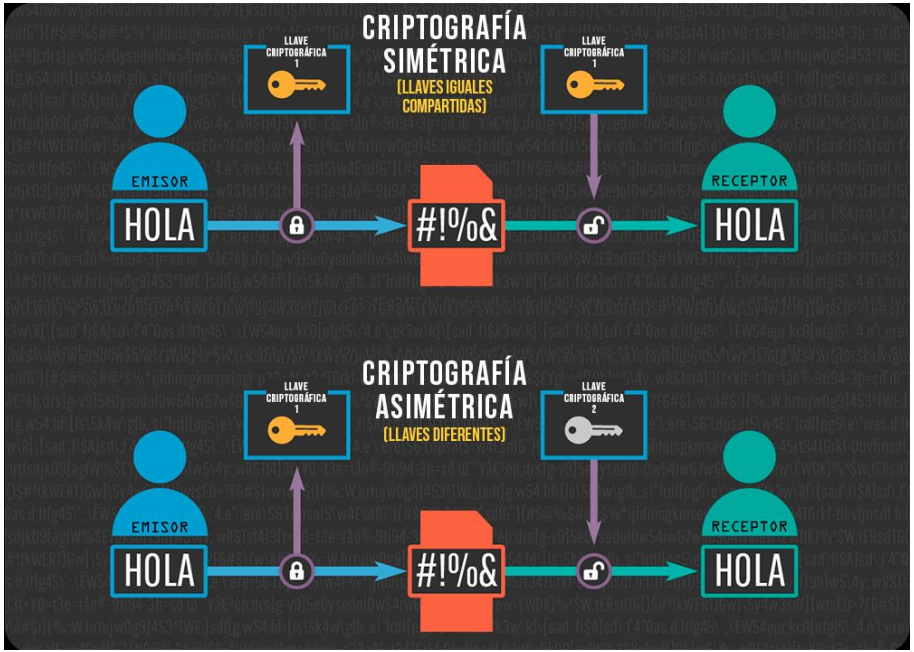

Texto plano
Encriptación
Texto cifrado
Desencriptación
Texto plano
legible
no legible
legible

Tipos de Criptografía

El cifrado se puede clasificar en los siguientes tipos:

- Cifrado Simétrico.
- Cifrado Asimétrico.

Tipos de Criptografía



Tipos de Criptografía

Característica	Simétrica	Asimétrica
Llave usada	la misma llave para ambos procesos	una llave usada para encriptar y una para desencriptar
Velocidad	muy rápida	más lenta
tamaño del resultado	usualmente el mismo o menos que el texto utilizado	más que el original
intercambio de llave	un gran problema	no hay problema en absoluto
número de llaves requeridas vs el número de participantes	igual al cuadrado del número de participantes	el mismo que el número de participantes.
Uso	principalmente usado en encriptación y desencriptación, no para firma digital (integridad y no repudio).	principalmente usado en encriptación y desencriptación,para firma digital (integridad y no repudio).

Tipos de Criptografía

Simétrica	Asimétrica
DES Triple DES AES Blowfish IDEA RC4 RC5 RC6	RSA DSA ECDSA Cifrado ElGamal.

Cifrado por Transposición

Definición

Consiste en intercambiar la posición de las letras de una palabra o frase siguiendo siempre un esquema bien definido, que puede ser sencillo o muy complejo.

La técnica más sencilla es invertir el texto por ejemplo:

input: primer cifrado

output: odarfic remirp

Definición

Consiste en intercambiar la posición de las letras de una palabra o frase siguiendo siempre un esquema bien definido, que puede ser sencillo o muy complejo.

La técnica más sencilla es invertir el texto por ejemplo:

input: primer cifrado

output: odarfic remirp

Escitala

La escítala espartana fue mencionada por primera vez por un poeta griego, Archilochus. El método consistía en escoger una vara o escítala, y se enrollaba una cinta a lo largo de la vara. El emisor escribía horizontalmente sobre la vara y al desenrollar la cinta se creaba un mensaje oculto.

La clave para descifrar el mensaje es escoger una vara con el mismo diámetro para que una vez enrollada la cinta por parte del emisor se pudiera leer el mensaje.

Escitala

Transposición por Columna Simple

Llave: MILLAVE

Mensaje: haremos el desembarco en Normandia

M	I	L	L	A	V	E
6	3	4	5	1	7	2

Se enumera en orden alfabético pero no se cambia el orden.

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrni

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_aemea

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_aemearlbnn

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_aemearlbnne_a_d

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_aemearlbnne_a_dh_e_m

Transposición por Columna Simple

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
	e	l		d	e	s
e	m	b	a	r	c	o
	e	n		n	o	r
m	a	n	d	i	a	

mdrnissor_aemearlbnne_a_dh_e_moecoa

Transposición por Columna Simple

original
haremos_el_desembarco_en_normandia

cifrado
mdrnissor_aemearlbnne_a_dh_e_moecoa

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

longitud del mensaje = 35

longitud llave = 7

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
				m		
				d		
				r		
				n		
				i		

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
				m		s
				d		s
				r		o
				n		r
				i		_

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
	a			m		s
	e			d		s
	m			r		o
	e			n		r
	a			i		_

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
	a	r		m		s
	e	l		d		s
	m	b		r		o
	e	n		n		r
	a	n		i		_

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
	a	r	e	m		s
	e	l	_	d		s
	m	b	a	r		o
	e	n	_	n		r
	a	n	d	i		_

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

35/7 = 5

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m		s
_	e	l	_	d		s
e	m	b	a	r		o
_	e	n	_	n		r
m	a	n	d	i		_

Descifrado

mdrnissor_aemearlbnne_a_dh_e_moecoa

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
_	e	l	_	d	e	s
e	m	b	a	r	c	o
_	e	n	_	n	o	r
m	a	n	d	i	a	_

Descifrado

haremos_el_desembarco_en_normandia

M	I	L	L	A	V	E
6	3	4	5	1	7	2
h	a	r	e	m	o	s
_	e	l	_	d	e	s
e	m	b	a	r	c	o
_	e	n	_	n	o	r
m	a	n	d	i	a	_