Criptografía

Profesor: Melvin Fernández Ch.

Video 4

fidélitas

Virtual

fidélitas Virtual

Criptografía clásica y cifra moderna

Módulo: 2

Principios de Kerckoffs

fidélitas Virtual

- Auguste Kerckhoffs fue un lingüista y criptógrafo holandés nacido en 1835. En 1883 publicó un ensayo en el diario de las ciencias militares titulado “La criptografía militar”. En ese trabajo quedaron expuestos los siete principios de Kerckhoffs, que buscan evaluar un método criptográfico.

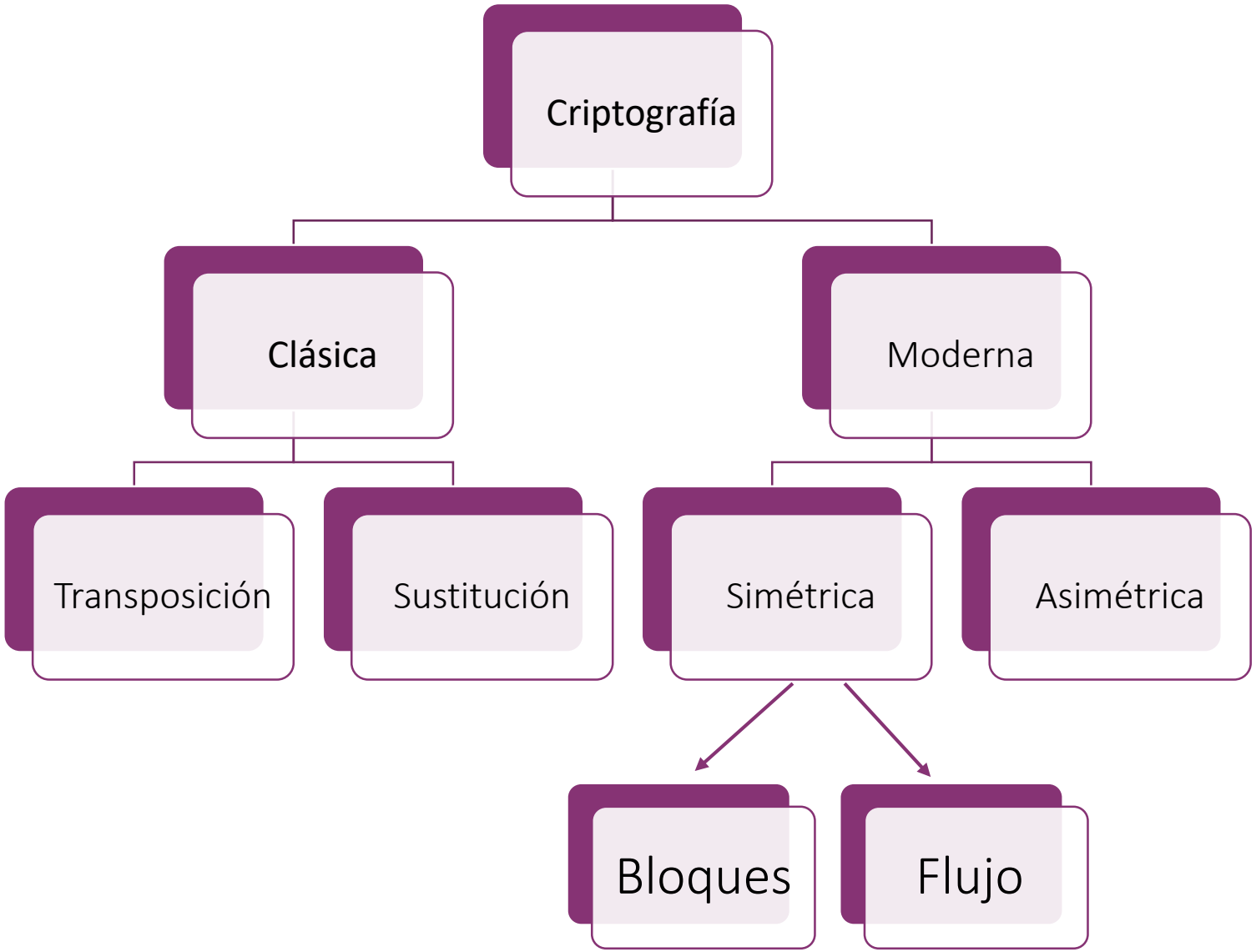
- La mayoría de estos principios siguen siendo válidos hoy en día.

Principios de Kerckoffs

- El principio más importante es el segundo que dice: “El sistema no debe ser secreto y no debe ser un problema que caiga en manos del enemigo”.

- Este principio tiene una aplicación directa en nuestros días, ya que a partir de él se concluye que: “La seguridad de un sistema criptográfico se basa totalmente en el secreto de la clave”.

Criptografía clásica y moderna



Sistemas de cifra clásica

La criptografía clásica fue de gran importancia durante la primera y segunda guerra mundial.

Se le denomina clásica debido a las técnicas que se utilizaron en ese entonces, las cuales realizaban operaciones de sustitución y de transposición.

La seguridad de ambos sistemas dependía de los algoritmos de cifrado (que no eran de dominio público) y el uso de la clave secreta.

Cifrado por sustitución

- Los algoritmos que se basan en la sustitución de partes del texto original por otros textos del mismo o de otros alfabetos, tienen como objetivo básico aumentar la confusión. Se pueden dividir en dos tipos según la complejidad del algoritmo:

  - Monoalfabéticos.

  - Polialfabéticos.

Criptografía: Monoalfabéticos

Cambian cada carácter por otro carácter o símbolo. Son muy sencillos y se conocen desde la antigüedad.

Uno de los algoritmos más conocidos es el de Julio Cesar, que tiene un desplazamiento de tres y consiste en sumar 3 al número de orden de cada letra, de esta forma a la A le corresponde la D, a la B la E y así sucesivamente.

Sustituir	A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z
Por	D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z C B A
Texto:	MENSAJE DE PRUEBA
Cifrado:	OHPVDM GH SUXHED

Criptografía: Polialfabéticos

- Cambian grupos de caracteres por otros caracteres o símbolos dependiendo de la frecuencia de su distribución en el texto original.

Ejemplo: Con una clave 2-3-1
Sustituir A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z
Por :

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

Texto: Es otra prueba
Cifrado: vv dtmf dvovñf

Cifrado por transposición

- Los algoritmos de transposición reordenan la estructura interna del objeto original para obtener un objeto cifrado cuya estructura no es aparente. Los algoritmos más populares de este tipo son los de transposición por columnas, que reordenan el objeto en columnas de forma que un cierto número de elementos (número de columnas) se agrupan y luego se reordenan aplicando el algoritmo de cifrado.

Cifrado por transposición

Texto claro:
AQUÍ SE ROMPIO UNA TAZA Y CADA QUIEN A SU CASA

Llave: CIFRADO

Cifrado:
SOAUCDAOAANAEUYIAEUPAASBQMTDAARNCESFIIZQUC

C	I	F	R	A	D	O
2	5	4	7	1	3	6
A	Q	U	I	S	E	R
O	M	P	I	O	U	N
A	T	A	Z	A	Y	C
A	D	A	Q	U	I	E
N	A	S	U	C	A	S
A	A	B	C	D	E	F

Gracias

fidélitas Virtual