SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.1.1.MF0489_3. Capítulo 1
Parte 1
Criptografía

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Criptografía:

“arte de escribir con clave secreta o de un modo enigmático”

2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Desde la Antigüedad hasta nuestros días, la criptografía ha sufrido una extraordinaria evolución.

2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Escítala

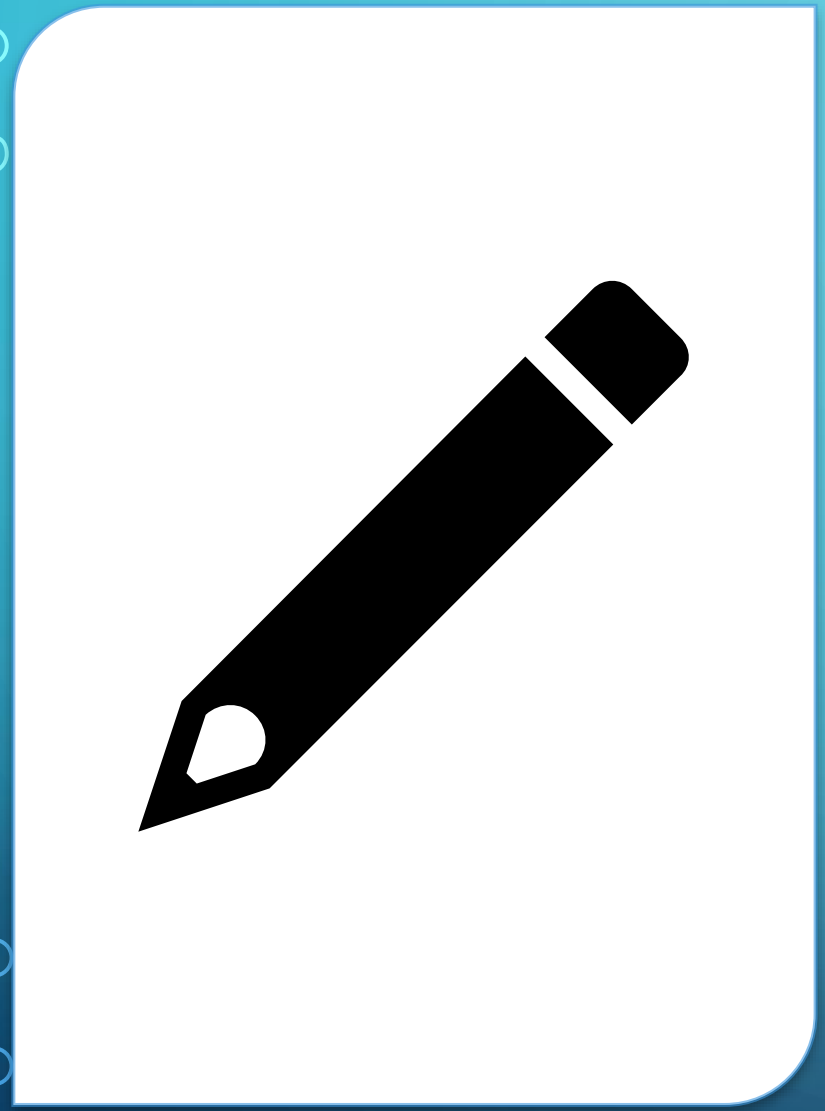
2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Cifrado del César

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p

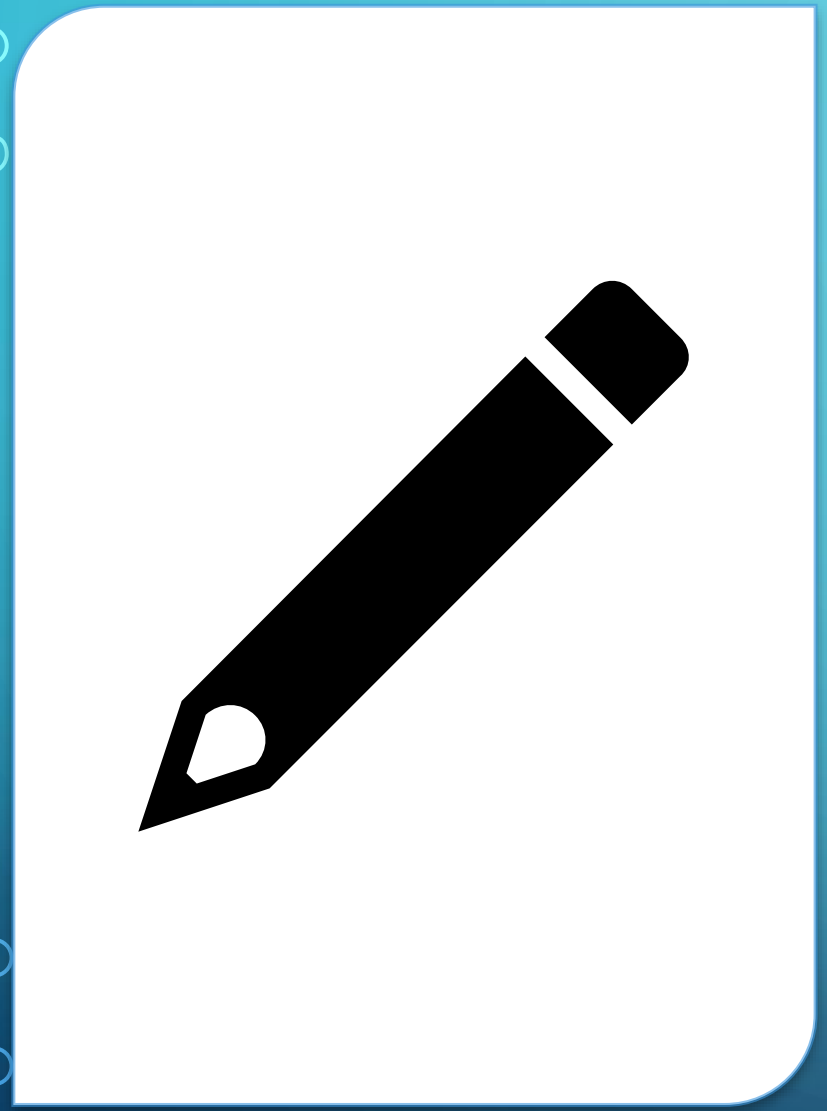
Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

Ejemplo



CIFRE EL TEXTO ‘INNOVACION Y CUALIFICACION’ UTILIZANDO EL CIFRADOR DE CÉSAR.

Ejemplo. Solución



SEGÚN HTTPS://ES.PLANETCALC.COM/1434/?LICENSE=1

LPPRYDFLRP B FXDÑLILFDFLRP

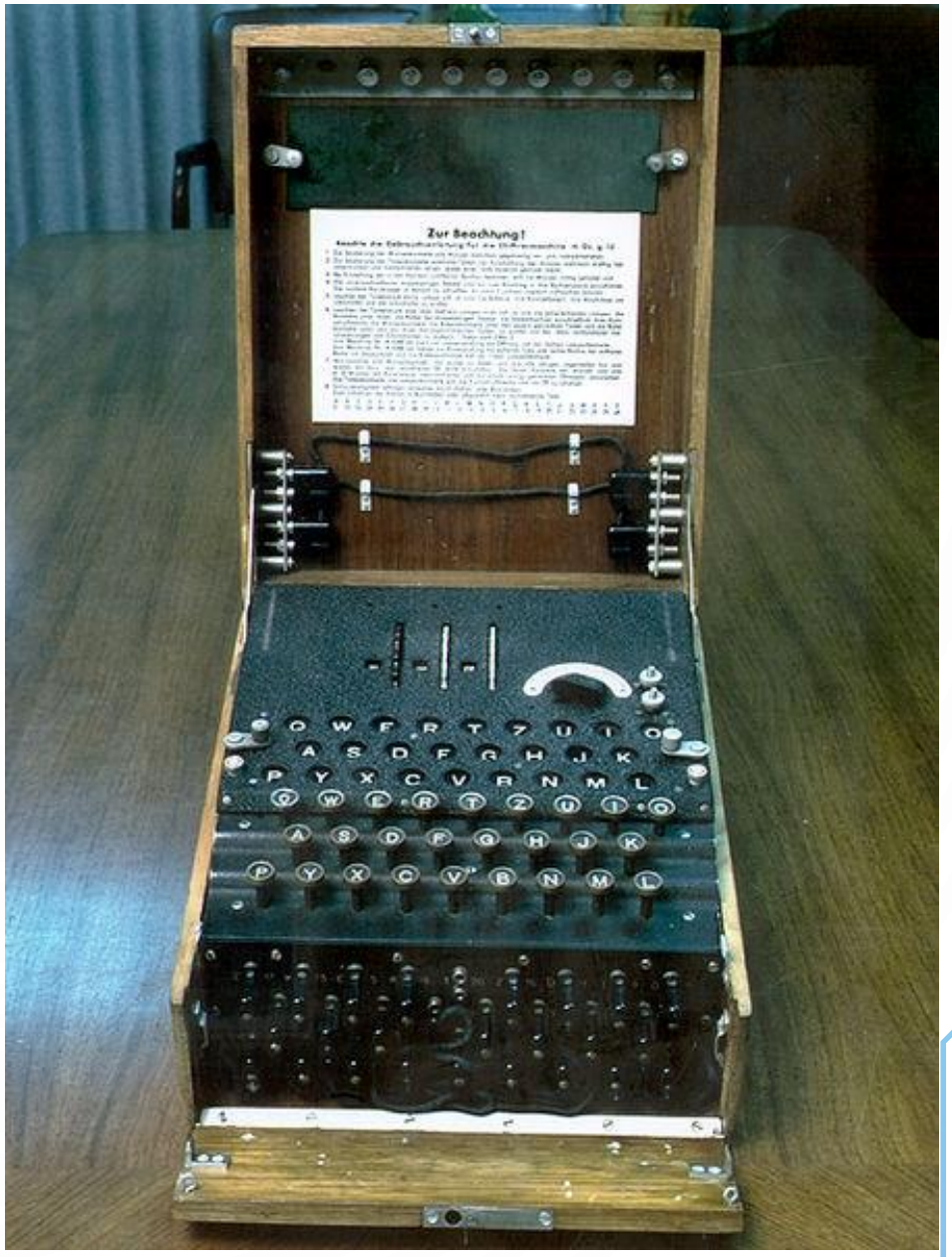
2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Cifrado de Vigenère

g	r	a	n	f	i	s	i	c	o		Mensaje
M	A	X	W	E	L	L	M	A	X		Clave
S	R	X	J	J	T	D	U	C	L		Cifrado

2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Máquina Enigma



2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Criptografía de clave privada

Criptografía de clave pública

Criptografía de curvas elípticas

Criptografía cuántica

2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

Esteganografía

2.1. FUNDAMENTOS DE CRIPTOANÁLISIS

Criptoanálisis

“arte de descifrar criptogramas”

3.1. CANTIDAD DE INFORMACIÓN. CONCEPTO DE ENTROPÍA

La entropía es una magnitud que permite medir la incertidumbre (o aleatoriedad) y, con ello, la cantidad de información de un determinado mensaje.

3.2. ESTABLECIENDO LA SEGURIDAD DE UN SISTEMA

En el marco de la Teoría de la información, Shannon determinó que un sistema se considera incondicionalmente seguro si no se obtiene ninguna información sobre la entrada obtenida a partir de la salida.

3.3. REDUNDANCIA Y COMPRESIÓN ÓPTIMA DE DATOS

En lo referente a la redundancia, lo deseable sería eliminarla antes de la transmisión para que esta fuese más corta.

Sin embargo, algunos canales de comunicación no están libres de errores y, por tanto, pueden producirse pérdidas o alteraciones de la información enviada.

Con este fin se desarrollaron los Códigos de Redundancia Cíclica (CRC).

4. PROPIEDADES DE LA SEGURIDAD QUE SE PUEDEN CONTROLAR MEDIANTE LA APLICACIÓN DE LA CRIPTOGRAFÍA

La seguridad de la información tiene como objetivo el establecimiento de medidas que controlen, mitiguen o prevengan distintos problemas de seguridad a los que un sistema puede enfrentarse, como pueden ser el acceso a datos no autorizados o la recepción de datos maliciosamente modificados.

4.1. CONFIDENCIALIDAD

La información ha de permanecer secreta desde el origen hasta ser recibida por destinarios autorizados.

4.2. INTEGRIDAD

La información ha de permanecer inalterable desde el origen al destino, donde inalterable significa exacta y completa.

4.3. AUTENTICIDAD

Esta propiedad afecta tanto al mensaje como a las entidades participantes:

- **Autenticidad del mensaje** se corresponde con recibir exactamente la misma información que fue enviada.
- **La autenticación de una entidad** se corresponde con determinar que una entidad es quien dice ser.

4.3. AUTENTICIDAD

Una de las técnicas utilizadas para satisfacer la autenticidad de los mensajes es la utilización de cifrado, códigos de autenticación de mensaje o funciones resumen.

Por otro lado, una técnica muy utilizada para autenticar a las entidades es la firma.

4.3. AUTENTICIDAD

La autenticación de entidades puede basarse en distintos factores:

- **Algo que se conoce,** como son las contraseñas
- **Algo que se tiene,** como son las tarjetas electrónicas o los USB
- **Algo que se es,** rasgos biométricos como la huella dactilar o el iris de los ojos
- **Una combinación de cualquiera de las anteriores.**

4.3. AUTENTICIDAD

Según los estándares ITU-T X.509 e ISO/IEC 9594-8:

- **Autenticación simple**
- **Autenticación fuerte unidireccional**
- **Autenticación fuerte bidireccional**
- **Autenticación fuerte de 3 sentidos**

4.4. NO REPUDIO

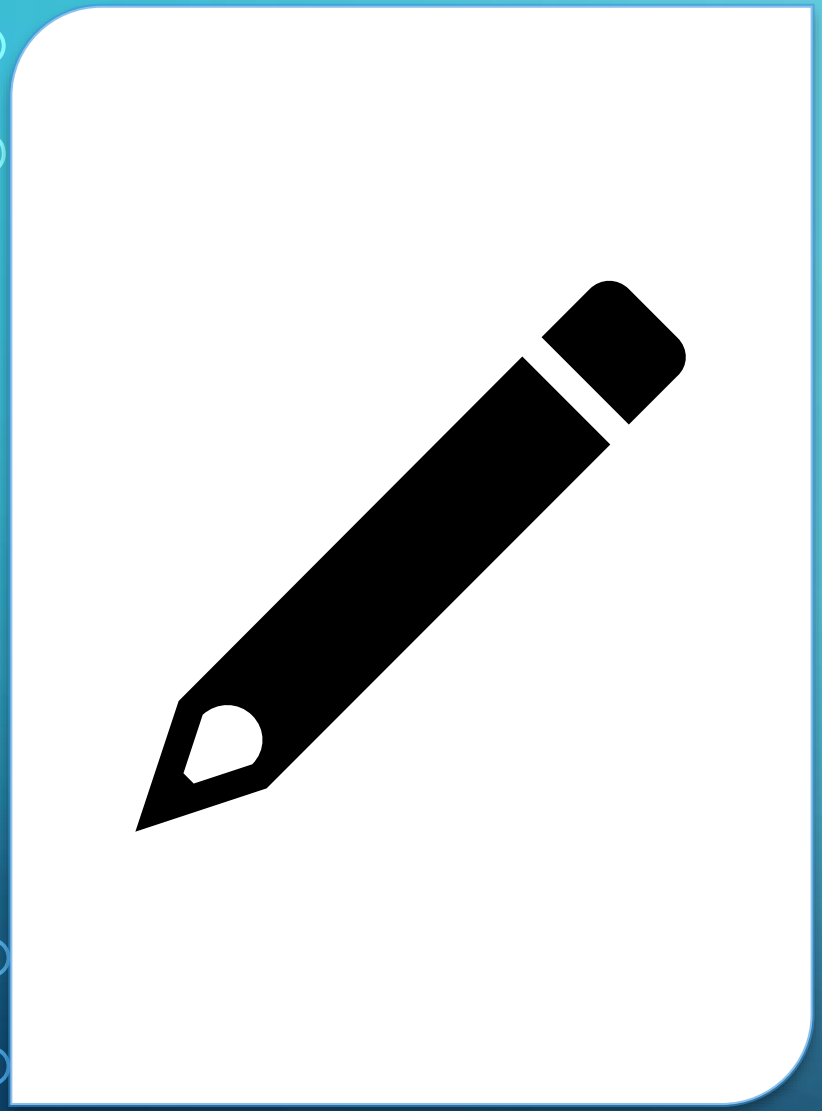
Se asegura que una determinada entidad no puede alegar que no ha realizado una acción.

4.5. IMPUTABILIDAD

Se realiza un seguimiento de todas las acciones de los usuarios del sistema, de modo que todos ellos sean responsables de sus acciones.

4.5. IMPUTABILIDAD

Se asegura que la información existió en un momento concreto y no ha sido modificada desde entonces.



Ejemplo.

COMO RESPONSABLE DE LA GESTIÓN DE UN PORTAL WEB PARA UN PROVEEDOR DE SERVICIOS DE LUZ Y GAS, SE ENCARGA DE DEFINIR QUÉ SERVICIOS DE SEGURIDAD ES NECESARIO PROPORCIONAR EN CADA UNA DE LAS FUNCIONALIDADES SIGUIENTES: (1) ACCESO DEL CLIENTE A SU ZONA PERSONAL; (2) CONSULTA DE FACTURAS; (3) BUZÓN DE RECLAMACIONES.

Ejemplo. Solución.

LOS SERVICIOS DE SEGURIDAD SON: INTEGRIDAD, CONFIDENCIALIDAD, AUTENTICACIÓN, NO-REPUDIO Y SELLADO DE TIEMPO.

EN LAS TRES ZONAS ES NECESARIO PROPORCIONAR:

INTEGRIDAD, PARA QUE LA INFORMACIÓN INTRODUCIDA NO SE ALTERE DE FORMA INADVERTIDA.
CONFIDENCIALIDAD, PUES SE UTILIZARÁN CREDENCIALES CONFIDENCIALES.
AUTENTICACIÓN, TANTO DEL CLIENTE COMO DEL SERVIDOR, PARA QUE AMBOS ESTÉN SEGUROS DE QUE EL INTERLOCUTOR ES QUIEN DICE SER.
ADEMÁS DE LO ANTERIOR, EN LA ZONA DE CONSULTA DE FACTURAS SE NECESITA NO REPUDIO EN EMISIÓN, PARA GARANTIZAR QUE LA FACTURA MOSTRADA ES EMITIDA POR EL PROVEEDOR. POR SU PARTE, EL BUZÓN DE RECLAMACIONES AÑADE A LO ANTERIOR LA NECESIDAD DE NO REPUDIO EN RECEPCIÓN (PARA QUE EL PROVEEDOR NO PUEDA NEGAR QUE LA RECIBIÓ) Y EL SELLADO DE TIEMPO (PARA PODER DEMOSTRAR CUÁNDO SE PUSO LA RECLAMACIÓN Y/O CUÁNDO SE RECIBIÓ).