Seguridad en Sistemas Informáticos

Módulo I: Preliminares y conceptos básicos

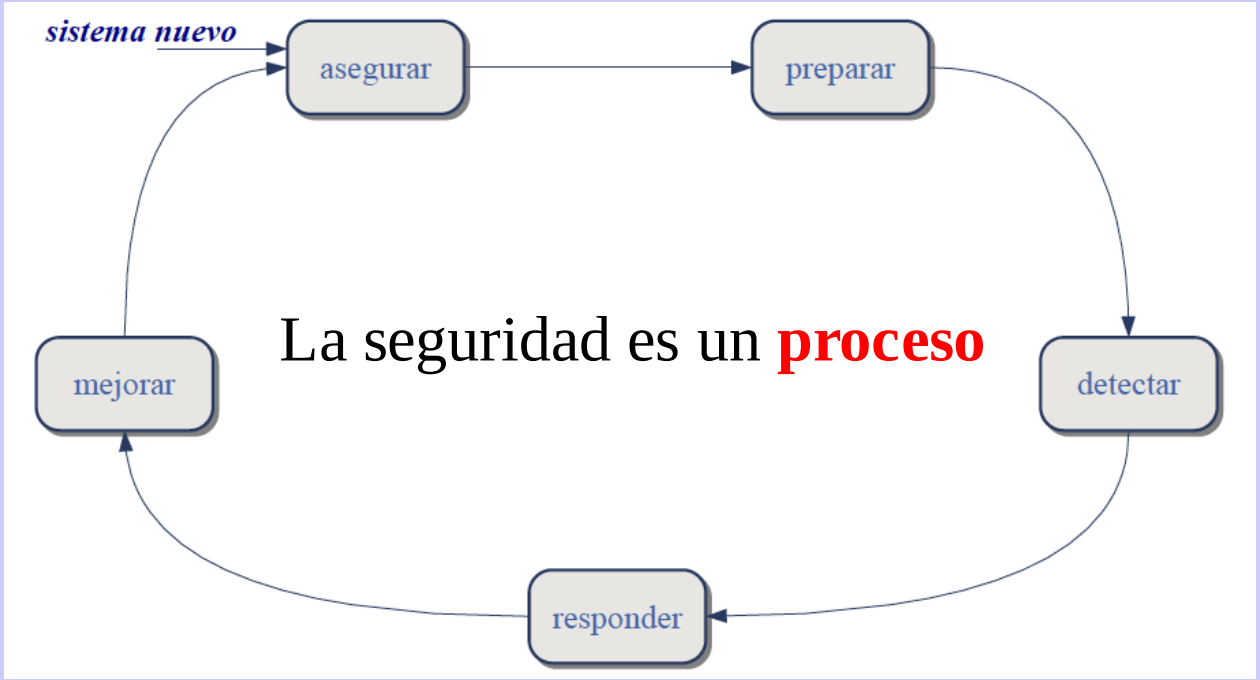
–Tema 1: Conceptos Básicos: Amenazas y vulnerabilidades

–Tema 2: Evolución histórica

Seguridad en Sistemas Informáticos

Es el área de la informática que se enfoca hacia la protección de la infraestructura computacional y todo lo relacionado con ella (incluyendo la **información** que contiene).

https://www.ccn-cert.cni.es/



CryptULL

Ciberseguridad

CryptULL

Protagonistas de la Seguridad en Sistemas Informáticos

- **Software:** Se protege con navegadores y SO seguros, y suites que incluyen cortafuegos y antivirus contra bombas lógicas, troyanos, gusanos, puertas falsas…

- **Hardware:** Hay riesgo si llega a manos ajenas.
- **Datos:** Se protegen con **Criptografía**, que utiliza técnicas de cifrado.

Protagonistas de la Seguridad en Sistemas Informáticos

- **La infraestructura computacional.** Hay que vigilar que los equipos funcionen adecuadamente y prever posibles casos de fallos, robos, desastres, etc.
- **La información.** Hay que evitar que usuarios externos no autorizados puedan acceder a ella, y garantizar el acceso legítimo a la información.
- **Los usuarios.** Son personas que usan la infraestructura computacional y gestionan la información, así que hay que establecer normas de uso para minimizar los riesgos para la infraestructura informática y/o la información.

Ejemplos de Amenazas

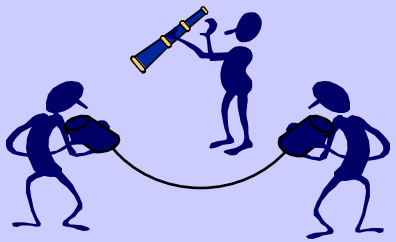
- **Usuarios**: causa del mayor problema de seguridad de S.I.
- **Intrusos**: personas que consiguen acceder a los datos o programas a los cuales no tienen acceso permitido.
- **Programas maliciosos o malware**: programas para perjudicar o hacer un uso ilícito de los recursos del sistema, como virus, gusanos, troyanos, bombas lógicas o programas espía o Spyware.
- **Phishing:** a través de emails falsos, de por ejemplo un banco, para robar datos, antes era la peor amenaza. Hoy gracias a los filtros antispam, son sobre todo las redes sociales, los acortadores de URLs y USB infectados lo que más se usa.
- **Siniestros físicos:** robos, incendios, inundaciones...

Tipos de Amenazas

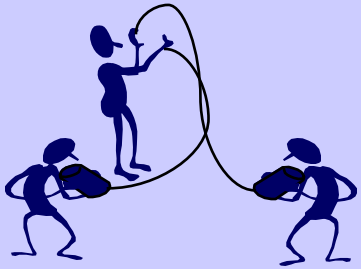
- **Amenazas internas**: Suelen ser peores que las externas porque:
  - –Los usuarios conocen los S.I. y su funcionamiento.
  - –Tienen algún nivel de acceso a la red.
  - –Los Sistemas de Prevención de Intrusos (o IPS) y cortafuegos (o firewalls) no son efectivos contra amenazas internas.
- **Amenazas externas**: Se originan fuera del S.I. así que al no tener toda la información sobre el S.I., el atacante primero tiene que dar pasos para conocerlo y buscar una manera de atacarlo. El administrador puede prevenir muchos ataques externos.

Amenazas Contra la Transmisión de Información

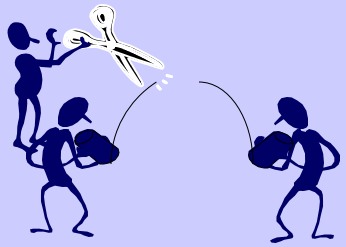
- **Intercepción:**



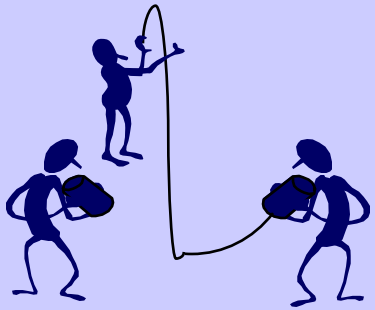
- **Modificación:**



- **Interrupción:**



- **Generación:**



CryptULL

Vulnerabilidades Principales

- **Confidencialidad:** Disponibilidad de la información sólo para usuarios autorizados.
- **Integridad:** Garantía de la imposibilidad de modificar la información.
- **Autenticidad:** Legitimidad del origen de la información.

Más Vulnerabilidades

- **Accesibilidad:** Posibilidad de acceso eficiente sólo para entidades autorizadas.
- **No repudio:** Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.
- **Anonimato**: Secreto de identidad del emisor de un mensaje o usuario de un sistema.

Nociones Básicas de Ciberseguridad

- **Cifrado**
- **Gestión de claves**
- **Autenticación**

Reglamento General de Protección de Datos (RGPD)

Reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, con **penalizaciones** severas de hasta el 4% de la facturación.

Obliga a **informar** en un plazo de 72 horas de que han sufrido un incidente de seguridad tanto a las autoridades competentes, como a todos los usuarios cuyos datos se hayan podido ver comprometidos. Es una manera de luchar contra los ciberataques.

Exige que la información personal de los ciudadanos de la UE solo puede recopilarse y guardarse para "fines específicos, explícitos y legítimos". Además debe contar con el **consentimiento** explícito y verificable del usuario, quien además debe ser capaz de retirarlo.

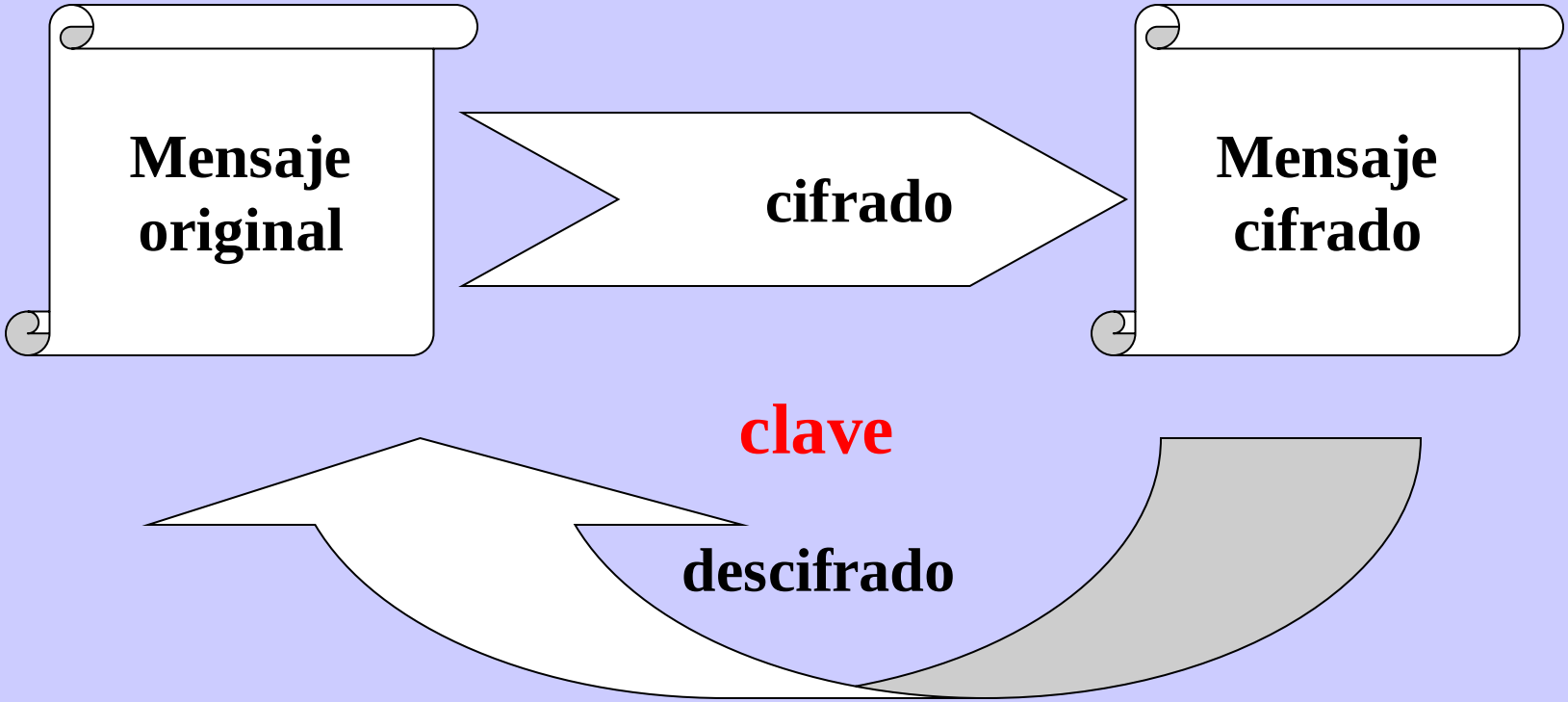
El **Delegado** de protección de datos debe poder aportar **pruebas** de la implementación de medidas.

El RGPD recomienda el **cifrado de los datos.**

CryptULL

Cifrado

Para proteger la confidencialidad



CryptULL

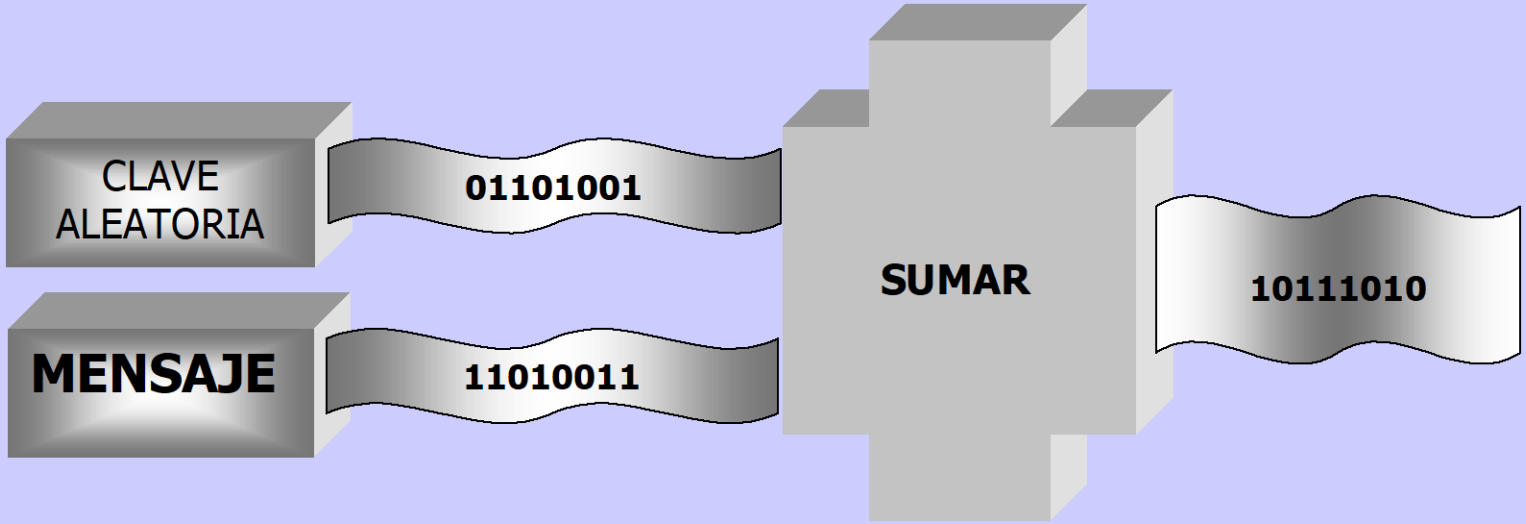
Reglas de Kerckhoffs (s.XIX)

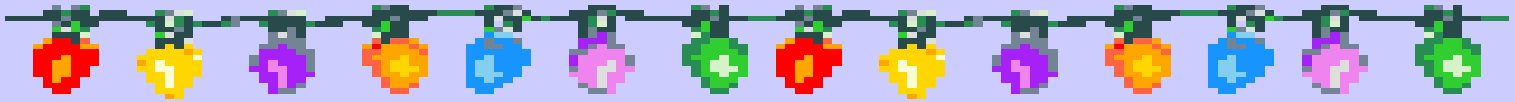
1. No debe existir ninguna forma de recuperar el texto en claro a partir del texto cifrado.
2. Todo sistema criptográfico debe estar compuesto por información pública (familia de algoritmos que lo definen) e información secreta (clave).
3. La elección de la clave debe ser fácil de recordar y de modificar.
4. El texto cifrado debe poderse enviar con los medios habituales de comunicación.
5. La complejidad del proceso de recuperación del texto original debe ser proporcional a la importancia de la información protegida.

Tipos de Secreto

1. **Secreto práctico o computacional**: Seguro frente a recursos acotados.
2. **Secreto perfecto, teórico o incondicional**: Seguro frente a recursos ilimitados.

Cifrado de Vernam (Bell Labs, 1917) One-Time Pad



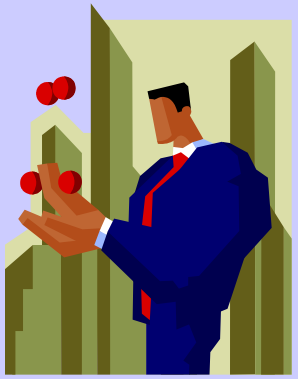


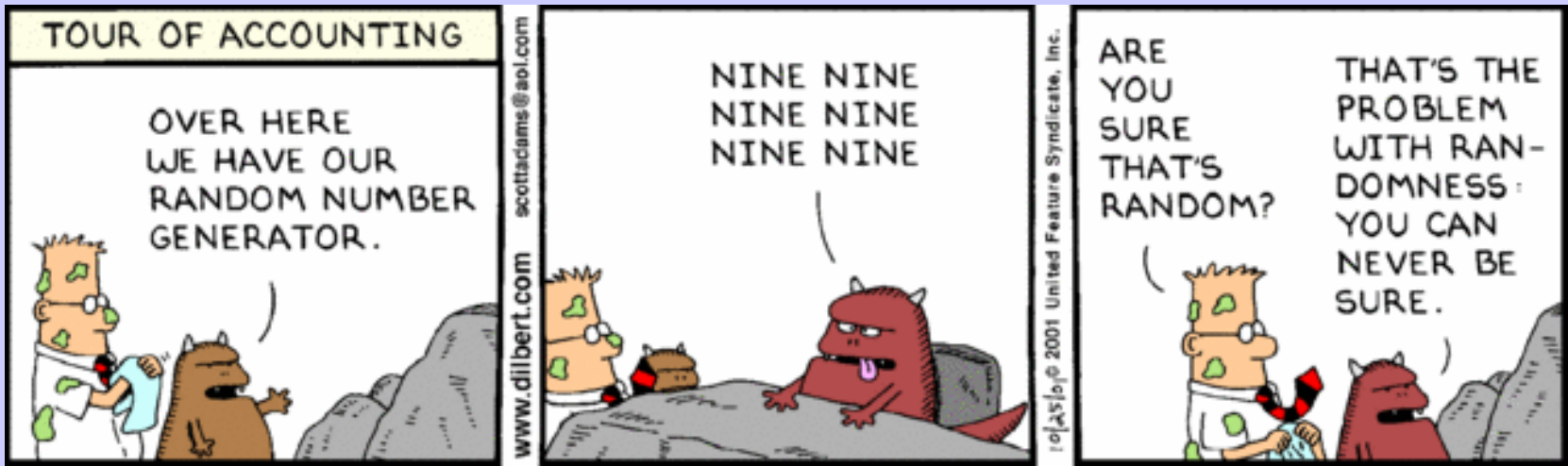
Secreto Perfecto

Demostrado para el OTP por Claude Shannon

- Texto original (M): secuencia de bits
- Secuencia cifrante (K): secuencia de bits aleatorios
- Texto cifrado (C): M XOR K (suma módulo2)
- **Ejemplo** :

M : 011 001 001 000 100 010
K: 001 010 001 101 110 101
C: 010 011 000 101 010 111





Ejemplo de Cifrado de Vernam

Carácter	ASCII	Carácter	ASCII
A	0100 0001	W	0101 0111
B	0100 0010	X	0101 1000
C	0100 0011	Y	0101 1001
D	0100 0100	Z	0101 1010
E	0100 0101	0	0011 0000
F	0100 0110	1	0011 0001
G	0100 0111	2	0011 0010
H	0100 1000	3	0011 0011
I	0100 1001	4	0011 0100
J	0100 1010	5	0011 0101
K	0100 1011	6	0011 0110
L	0100 1100	7	0011 0111
M	0100 1101	8	0011 1000
N	0100 1110	9	0011 1001
O	0100 1111	+	0010 1011
P	0101 0000	-	0010 1101
Q	0101 0001	*	0010 1010
R	0101 0010	:	0011 1010
S	0101 0011	=	0011 1101
T	0101 0100	<	0011 1100
U	0101 0101	;	0011 1011
V	0101 0110		

Tabla 1.2. *Código ASCII.*

- Cifrado:

11101111100101110001111 1

- Clave:

10111100110110000101001 1

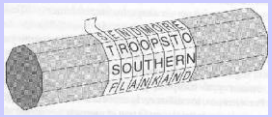
- Descifrado:

01010011010011110100110 0

SOL

Pasado, Presente y Futuro.

- < s. XX:
  - s. V a.C., escítala en Grecia (**Transposición**: Permuta los símbolos del texto original, garantizando **difusión** al propagar la información a lo largo del mensaje cifrado)
  - s. I d.C, cifrado de César (**Sustitución**: Cambia las unidades del texto original por otras, garantizando **confusión** al esconder la relación entre texto claro, texto cifrado y clave)



SimonSinghRailFence

- s. XX:
  - Telegrama Zimmermann (I Guerra Mundial)
  - **Máquina Enigma** (II Guerra Mundial)
  - **Clave Pública** (1976, **Diffie y Hellman → RSA**)
- s. XXI:
  - 2001: Cambio en el estándar de cifrado (**DES → AES**)
  - Crecimiento de la criptografía **elíptica**
  - Futuro: Criptografía **cuántica y post-cuántica**

Máquina Enigma

- Inventada por un ingeniero alemán durante la I Guerra Mundial, utilizada posteriormente en la II GM por los alemanes.
- Las claves se definían inicialmente mediante 3 rotores. Cada rotor es una permutación arbitraria del alfabeto. La salida de un rotor se encuentra conectada a la entrada del rotor siguiente.
- Una vez posicionados los rotores se tecleaba el carácter a cifrar y se obtenía iluminado como resultado el carácter cifrado. Se cifraba así, sucesivamente todo el texto. Tras cada letra cifrada, el rotor se desplazaba permitiendo romper la redundancia estadística del idioma.
- Para descifrar el mensaje era necesario tener la misma máquina y conocer la posición inicial de los rotores.
- Criptógrafos polacos e ingleses lograron romper la máquina enigma.

youtube

Sustitución

César : VENI VIDI VICI																							
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c
ZHQL ZLGL ZLFL																							

https://www.cryptool.org/en/cto/caesar

Desplazamiento: Cada letra se sustituye por otra que ocupa k posiciones mas allá en el alfabeto.

SimonSinghShifth

IBM > HAL

A>Z, B>A, C>B,...,Z>Y

Con alfabeto invertido: Cifrado Atbash

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
z	y	x	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

El Cifrado Indescifrable

Cifrado de Vigenere: La 1ª letra se sustituye por la que ocupa k_0 posiciones mas allá, la 2ª por la que está k_1 posiciones mas allá,...

Clave: SOL
M.Or.: DES AST RES
M.Ci.: VSD SGE JSD

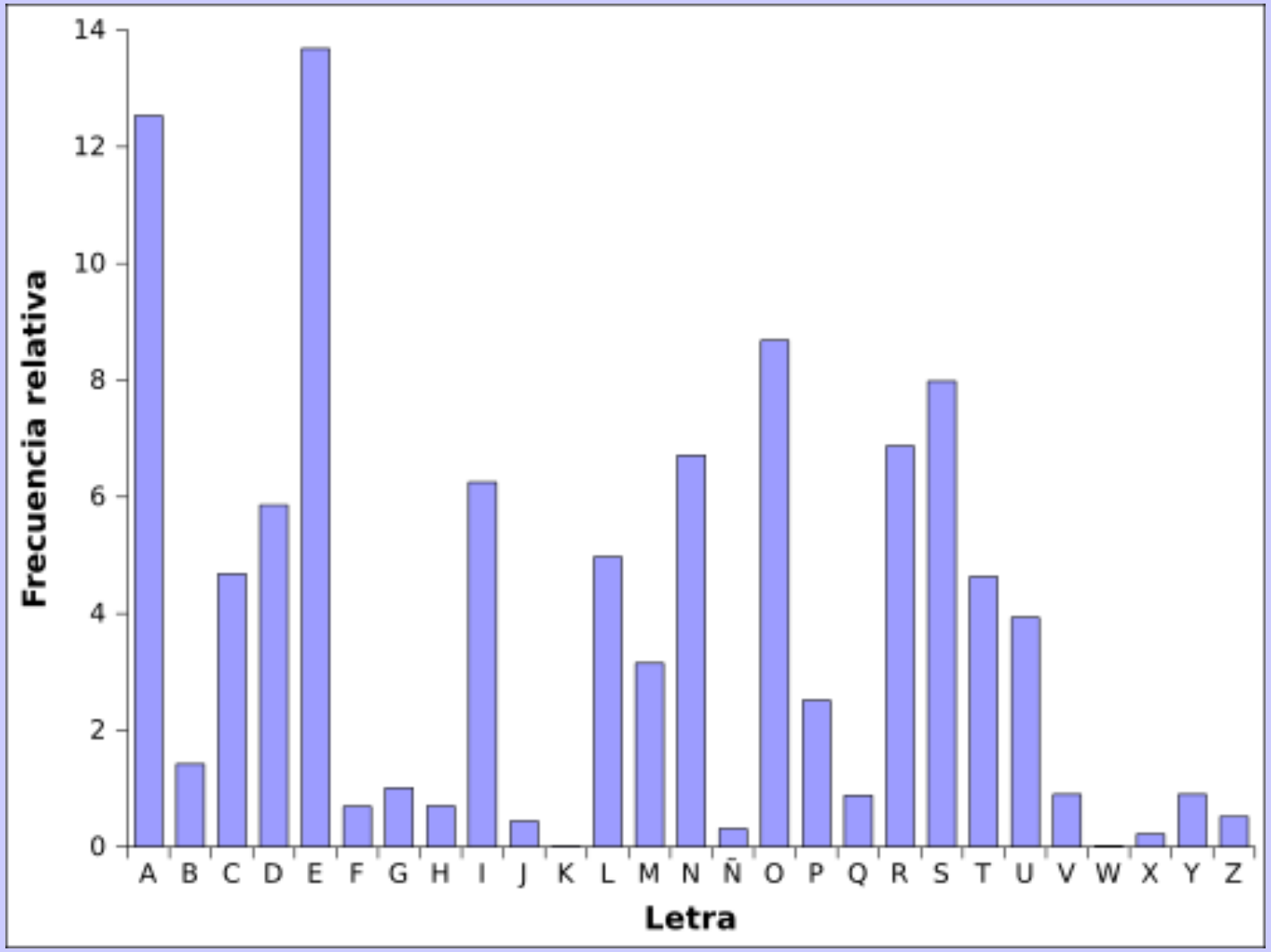
Clave: 18 14 11 18 14 11 18 14 11
M.Or.: 03 04 18 00 18 19 17 04 18
M.Ci.: 21 18 03 18 06 04 09 18 03

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

SimonSingh
Vigenere

CryptULL

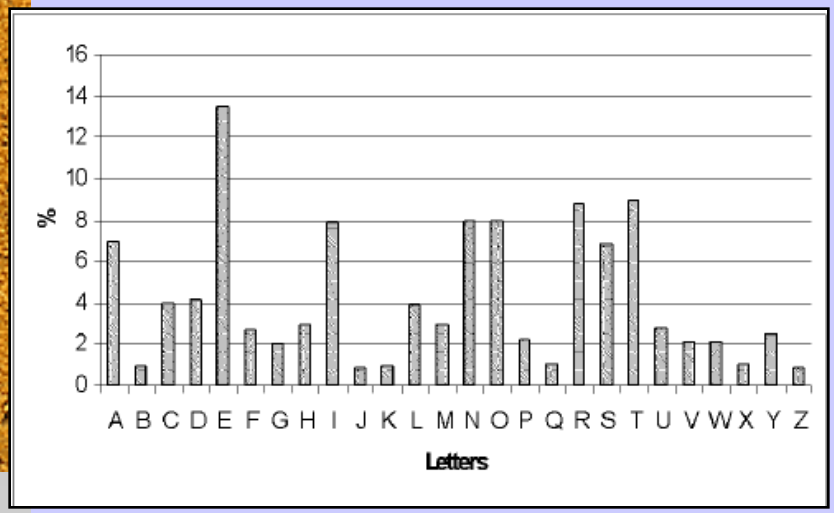
Criptoanálisis Estadístico

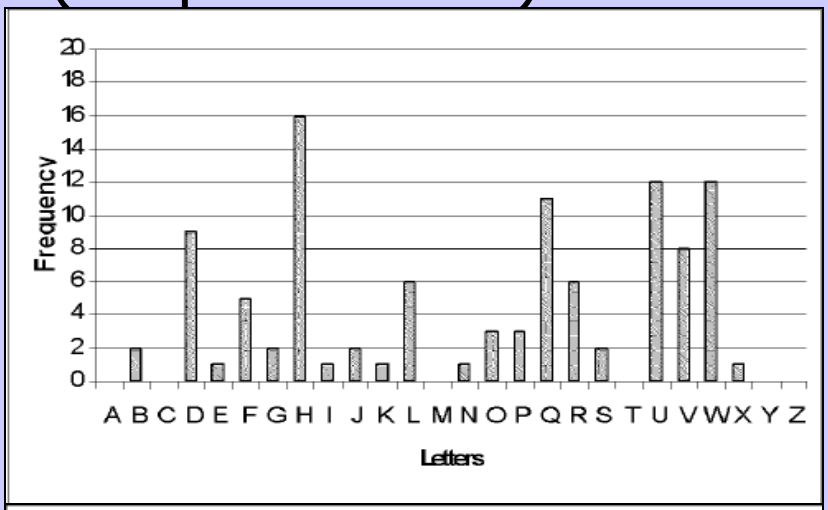


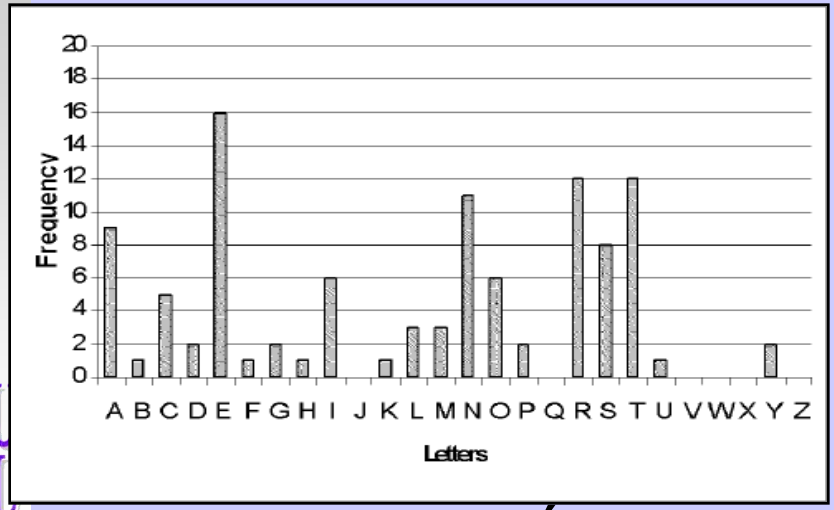
CryptULL

Criptoanálisis Estadístico

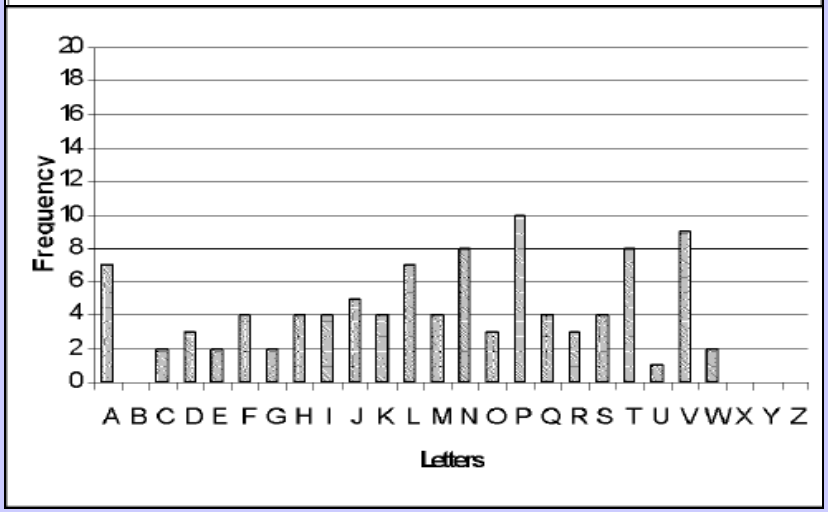
Sustitución monoalfabética (Desplazamiento)







Transposición



Sustitución polialfabética

Aritmética Modular

- Usa un conjunto finito de enteros en el que se pueden realizar de manera eficiente cálculos complejos y se puede calcular la inversa de varias operaciones.
- **Relación de congruencia:** Dados dos números enteros a y b, se dice que a es congruente con b módulo n

$$a \equiv b \pmod{n}$$

si y sólo si existe algún entero k tal que

$$a - b = k * n$$

(b es el resto de a dividido por n)

Sustitución: Cifrado/Descifrado

- Cifrado de César:

$$C \equiv E(M) \equiv M + 3 \pmod m$$

$$C - 3 \equiv M \pmod m$$

- Desplazamiento:

$$C \equiv E_K(M) \equiv M + K \pmod m$$

$$C - K \equiv M \pmod m$$

- Sustitución con alfabeto invertido:

$$C \equiv E_K(M) \equiv - M + K \pmod m$$

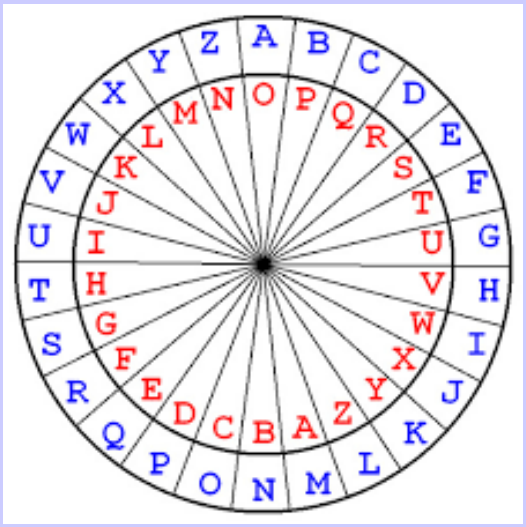
$$- C + K \equiv M \pmod m$$

- Cifrado de Vigenere con clave $K=(k_0,k_1,\ldots,k_{r-1})$:

$$C_i = E_K(M_i) \equiv M_i + k_{(i \bmod r)} \pmod m$$

$$C_i - k_{(i \bmod r)} \equiv M_i \pmod m$$

Ejemplo de Cifrado de Vigenere



Alfabeto de 26 letras

Plaintext: ATTACK
Key: LEMONL
Ciphertext: LXFOPV

Operaciones (mod 26)

Plaintext:	**0**	**19**	**19**	**0**	**2**	**10**
Key:	**11**	**4**	**12**	**14**	**13**	**11**
Ciphertext:	**11**	**23**	**31**	**14**	**15**	**21**
			5			
	L	**X**	**F**	**O**	**P**	**V**

https://www.cryptool.org/en/cto/vigenere

Herramientas online

https://www.simonsingh.net/The_Black_Chamber/

https://www.cryptool.org

https://gchq.github.io/CyberChef/

https://www.academia.edu/48962247/The_Manga_Guide_to_Cryptography_Masaaki_Mitani

https://www.incibe.es/ed2026/talento-hacker/academia-hacker/retosdescargables