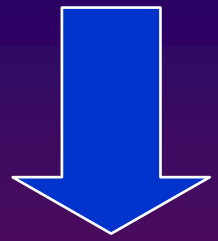
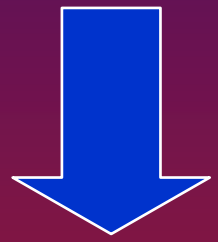
Firma Digital

2009

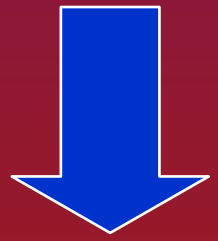
Vulnerabilidades Amenazas



SEGURIDAD



CONTRAMEDIDAS



CRIPTOLOGIA

Método de Clave Pública

Certificados de Clave Pública

Infraestructura de Clave Pública (PKI)

Función Hash

Firma Digital

SEGURIDAD INFORMATICA

- **Qué es seguridad informática?**
  - **Seguridad de la Información.**
  - **Seguridad de las Computadoras.**
  - **Seguridad de las Redes.**
  - **Seguridad Física.**
  - **Seguridad de las Personas.**

SEGURIDAD INFORMATICA

Aspectos de la seguridad de la información:

1. Ataques a la seguridad
2. Prestación de seguridad
3. Mecanismos de seguridad

SEGURIDAD INFORMATICA

Ataques a la seguridad

Cualquier acción que compromete la seguridad de la información perteneciente a la organización.

- **Vulnerabilidad**
- **Amenazas**
- **Contramedidas**

SEGURIDAD INFORMATICA

Vulnerabilidad:

1) Físicas.
2) Naturales.
3) Hardware/software.
4) Datos.
5) Emanaciones.
6) Comunicaciones.
7) Humanas.

SEGURIDAD INFORMATICA

Amenaza: Explotación de una vulne-rabilidad

a) Interrupción.

b) Interceptación.

c) Modificación.

d) Fabricación.

SEGURIDAD INFORMATICA

Clasificación de Amenazas.

1. Naturales
2. No intencionales.
3. Intencionadas

SEGURIDAD INFORMATICA

- **Ataque Pasivo.**

  a) Obtención de información.

  b) Análisis de tráfico.

SEGURIDAD INFORMATICA

- **Ataques Activos.**
  - **Alteración.**
  - **Fabricación.**
  - **Interrupción**

SEGURIDAD INFORMATICA

Servicio o Prestación de Seguridad

Emular funciones asociadas a documentos físicos

Desafíos: Copia – Alteración – Autenticidad.

SEGURIDAD INFORMATICA

Clasificación de los servicios de seguridad:

- Confidencialidad o secreto
- Integridad o precisión
- Disponibilidad
- Autenticación
- Reconocimiento o No repudio
- Control de accesos

SEGURIDAD INFORMATICA

Mecanismos de seguridad

Diseñados para detectar, prevenir o recuperar frente a un ataque a la seguridad.

Las transformaciones criptológicas de la información son el medio más usual de brindar seguridad.

SEGURIDAD INFORMATICA

Contramedidas.

1. Seguridad de las computadoras.
2. Seguridad de comunicaciones.
3. Seguridad física.

Criptología

TERMINOLOGIA

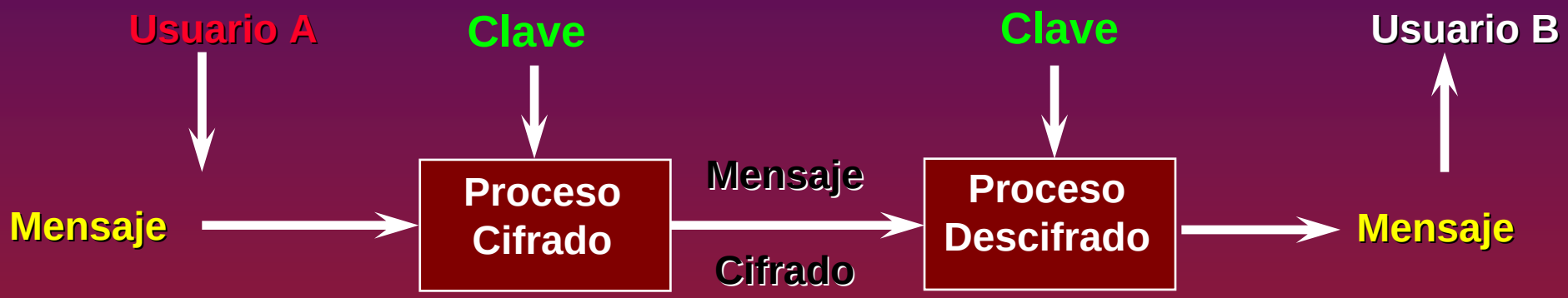
- Criptografía.
- Criptoanálisis.
- Cifrado.
- Descifrado.
- Texto claro.
- Texto cifrado.
- Clave.

Objetivos de la Criptografía

1. Confidencialidad
2. Integridad
3. Autenticación
4. Reconocimiento o No repudio

Proceso de Cifrado

La clave debe ser secreta y sólo conocida por el EMISOR y el RECEPTOR



Sistemas criptográficos

Clasificación

1. Tipo de operación que se realiza:
   - Sustitución
   - Trasposición.
2. Número de claves empleadas:
   - Simétrico
   - Asimétrico
3. Forma en que es procesado el texto claro:
   - Cifrado por bloque
   - Cifrado por flujo

Transposición

6	2	5	3	1	4
D	I	A	A	Y	E
R	R	O	B	O	S
E	E	S	M	E	R
A	L	D	A	V	E
R	D	E	Y	U	Q

Clave: 625314

Texto cifrado:

YOEVU IRELD ABMAY ESREQ AOSDE DREAR

CODIGO

- Características.
- Códigos Conocidos.
  - Morse.
  - Marconi.
  - INTERCO.

CODIGO

Orden	Palabra Código	Palabra Clara
00001	ABAAA	A
00002	ABAAB	ABAJO
00003	ABAAC	ABANDONE
00004	ABAAD	ABANDONADO
00005	ABAAE	ABANDONAR
00006	ABAAF	ABAJO

CODIGO DE UN ELEMENTO

ABAAA	A
ABACF	ABANDON AR
ABAHK	ABANDONARLO
ABAJL	ABANDONADO
.....	.....
ZYZYZ	ZAPARON

CODIGO DE DOS ELEMENTOS

A	HUIEH		ABABD	SUPUESTO
ABANDON AR	OPEBK		ABACF	COHERENCIA
ABANDONARLO	ZEWYU		ABAHK	MONTE
ABANDONADO	QPSEI		ABAJL	RAMPA
.....				.....
ZAPARON	OEWFJ		ZEWYU	ABANDONARLO

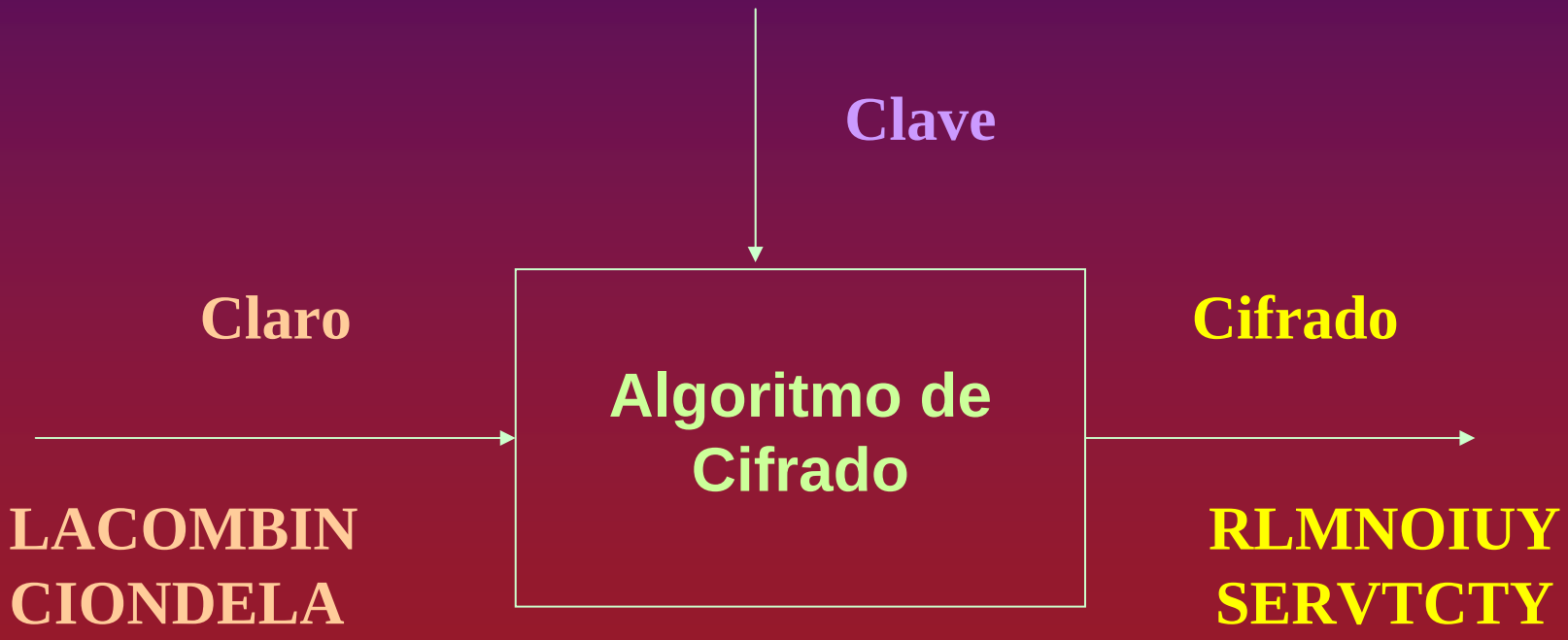
Converter M-209

CONVERTER M-209

	26	27																						
	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
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	M
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
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	Z
	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

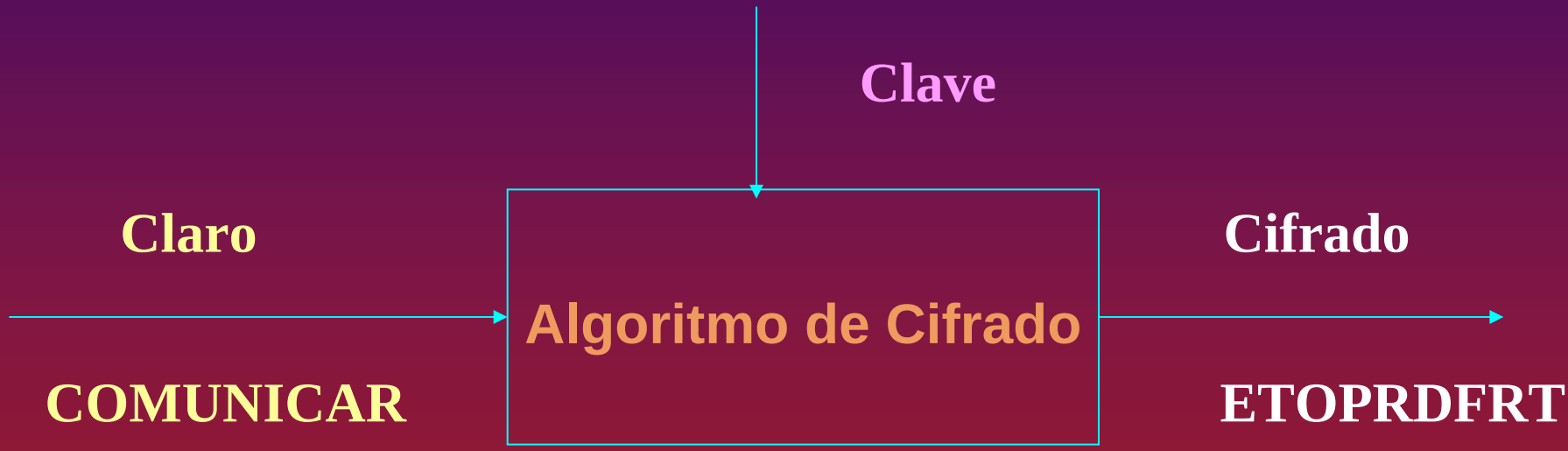
Cifrado en bloque y de flujo

Cifrados en bloque



Cifrado en bloque y de flujo

Cifrados de flujo



Sistemas Simétricos

- **Problemas de la Clave Simétrica.**
  - **El remitente tiene que divulgar su clave secreta para que el receptor de la información pueda leerla.**
  - **El remitente puede REPUDIAR la autoría de la información enviada.**
  - **El receptor puede modificar el texto original y volver a cifrarlo.**
  - **Administración de clave compleja:**

(n*(n-1) / 2)

Sistemas Asimétricos

CLAVE PUBLICA

- Fue diseñada para solucionar el problema del repudio, es decir para garantizar la identidad del autor del documento.
- La utilizan personas que no se conocen para intercambiar mensajes.
- Utiliza una clave distinta para cifrar que para descifrar.

Sistemas Asimétricos

CLAVE PUBLICA

- Tienen una enorme ventaja sobre los sistemas convencionales de manejo de claves:
- Cualquiera puede enviar un mensaje secreto a un usuario que desconoce
- Con un sistema de claves convencional se necesita una clave por cada par de usuarios.

Clave Pública

Características

- En 1974-75 Whitfield DIFFIE, Martin HELLMAN y Ralph MERKLE descubrieron este nuevo concepto en criptología que tuvo profundas implicancias en la tecnología.

- Funciones de un solo sentido.

Clave Pública

Características

- En un sistema de clave pública, cada usuario tiene dos claves: una pública y otra secreta.
- Cada clave opera como inversa una de la otra.
- Sean k_{priv} Clave Privada
  k_{pub} Clave Publica.

$$P = D(k_{priv}, E(k_{pub}, P))$$

Clave Pública

Características

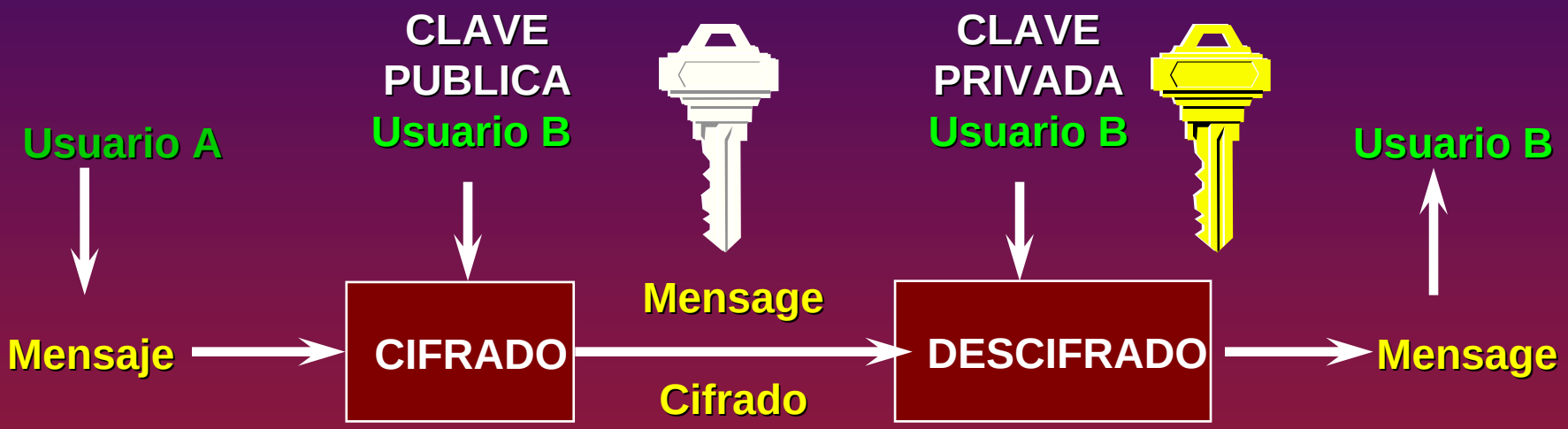
- Un usuario puede descifrar con su clave privada lo que otro cifró con su correspondiente clave publica.

$$P = D(k_{priv}, E(k_{pub}, P))$$

- Un usuario puede cifrar un mensaje con una clave privada y el mensaje sólo se puede descifrar con la clave publica.

$$P = D(k_{pub}, E(k_{priv}, P))$$

Cifrado con Clave Pública



Mediante un programa el usuario genera un PAR de claves (pública y privada)

Sistemas de Clave Pública.

- **Algoritmos de clave pública**

1. Problema de logaritmos discreto.
   - DSA (firmas digitales)
   - Diffie-Hellman (distribución de claves)
2. Problema de factorización de enteros.
   - RSA (cifrado, firmas digitales)
3. Problema de logaritmo discreto de curva elíptica.
   - El Gamal (distribución de claves, cifrado)

Sistemas de Clave Pública.

- **Función módulo.**

Consideremos el campo de los enteros módulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3 * 2 = 1 mod 5

Sistemas de Clave Pública.

- **Exponenciación**

$$2^4 * 2^2 = 2^{4+2} = 2^6$$

$$(2^4)^5 = 2^{4*5} = 2^{20}$$

Clave Pública

RIVEST-SHAMIR-ADELMAN (RSA).

- El algoritmo utiliza dos claves: d y e
- $C = P^e \bmod n$
- $P = C^d \bmod n$.
- Dada la simetría de la aritmética modular, el cifrado y descifrado son inversos mutuos y conmutativos.
- $P = C^d \bmod n = (P^e)^d \bmod n = (P^d)^e \bmod n$.