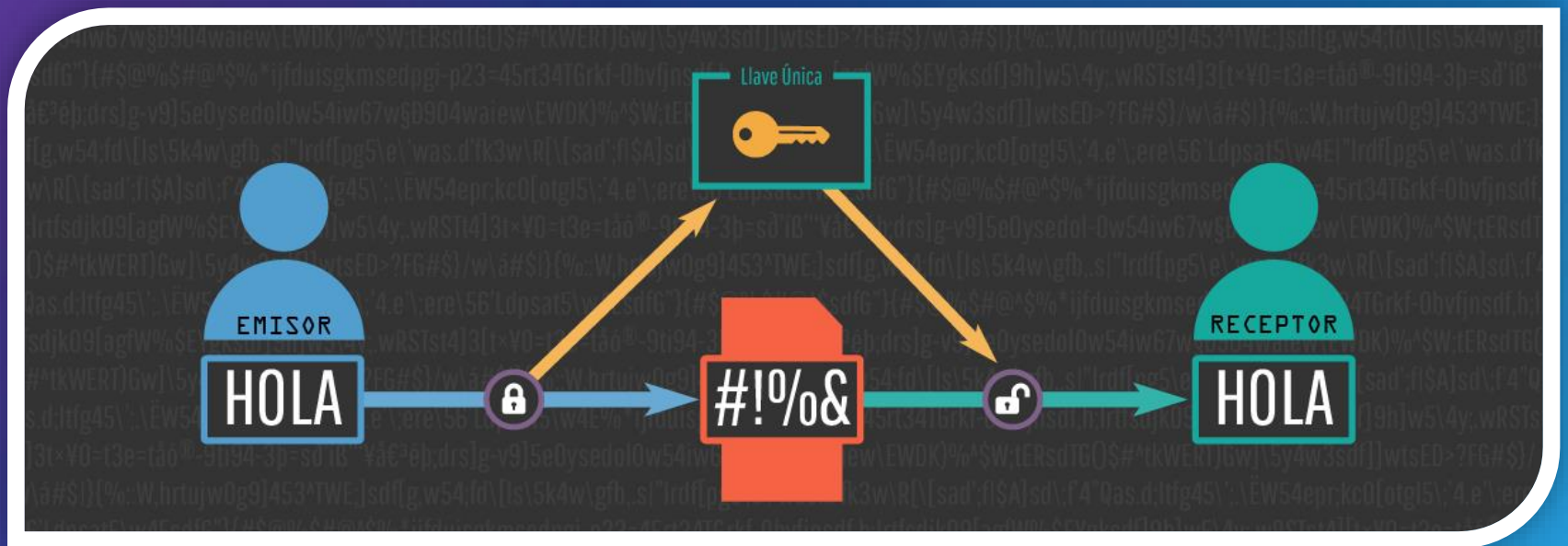




Universidad
Rafael Landívar
Tradición Jesuita en Guatemala

Criptografía



Facultad de ingeniería

Criptografía

- Es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales.

¿Para qué se usa?

- Para permitir un intercambio de mensajes de forma confidencial por un medio inseguro.



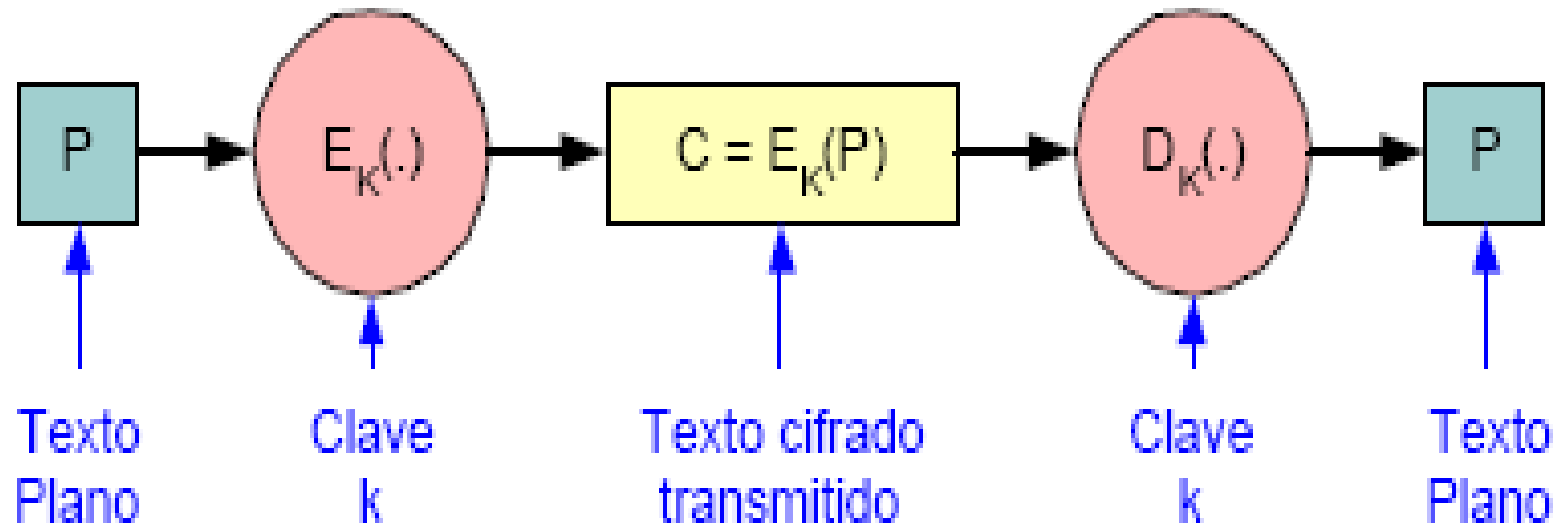
Donde:

a = 0001
b = 0002
c = 0003
d = 0004
...

a "cifrada" = 0036 = (valor numérico de "a" + clave)²

0036 "descifrado" = a = $\sqrt{\text{valor cifrado} - \text{clave}}$

¿Cómo funciona el cifrado?



E_k : Función para Encriptar (Cifrar)

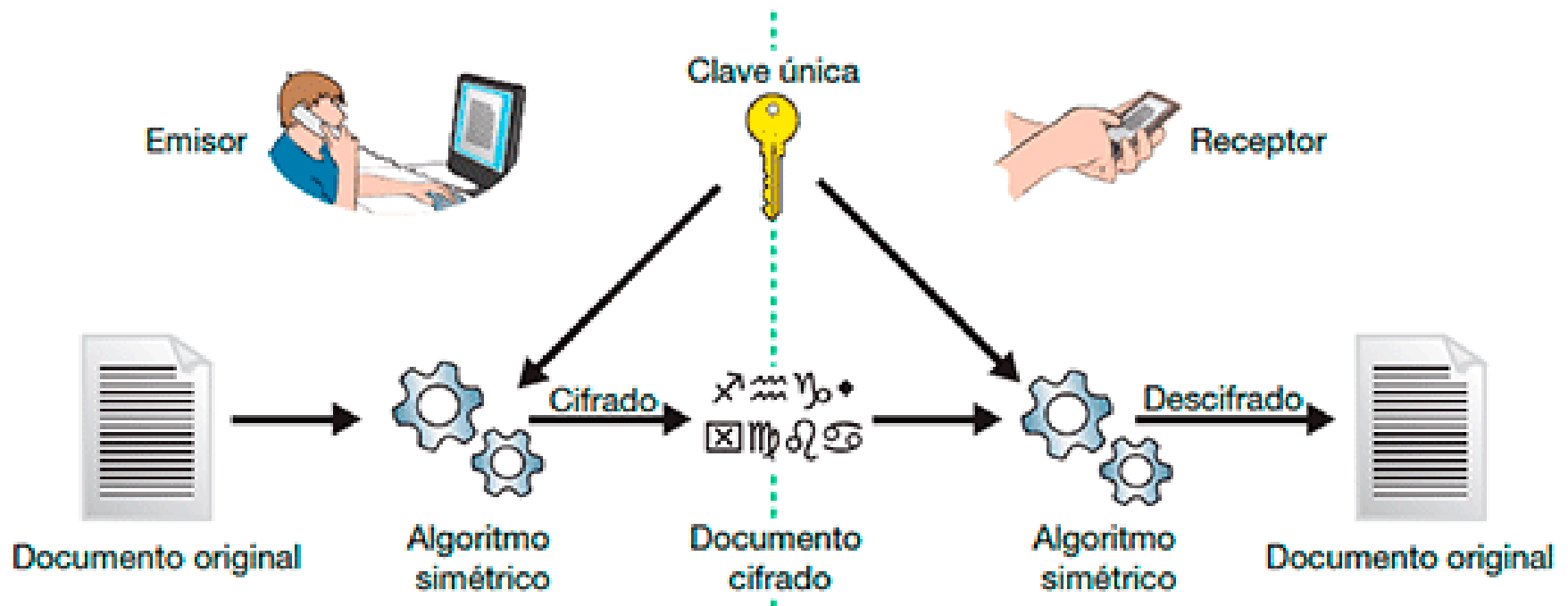
D_k : Función para Desencriptar (Descifrar)

Tipos de Cifrado

Una vez que el emisor y receptor acuerdan que algoritmo de cifrado usar, se distinguen dos tipos de cifrado:

Cifrado simétrico

Se considera **simétrico** si la clave de cifrado y descifrado son las mismas

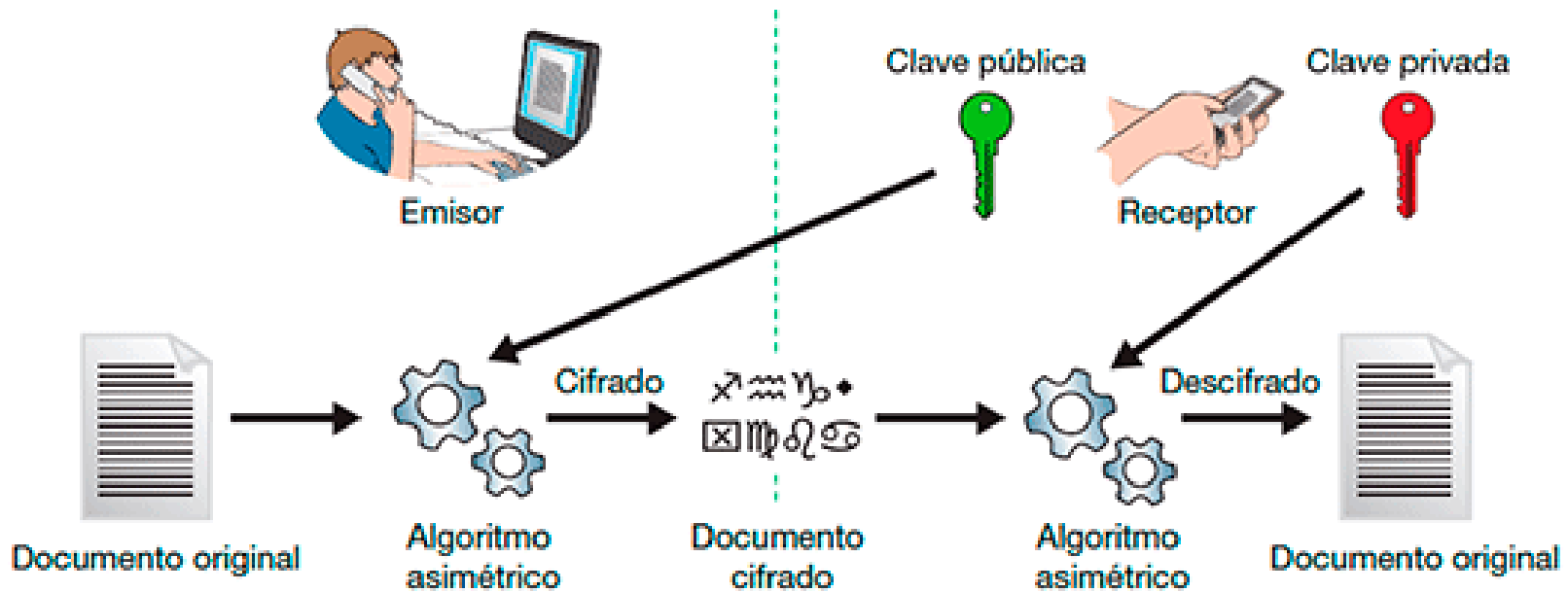


Cifrado asimétrico

Se hace uso de dos claves distintas:

Pública: Generalmente para cifrar.

Privada: Generalmente para descifrar.



Métodos de encriptación de la Información

- Cifrado César
- Código por sustitución de letras
- Código por transposición
- Criptografía de clave secreta. DES
- Criptografía de clave pública. RSA

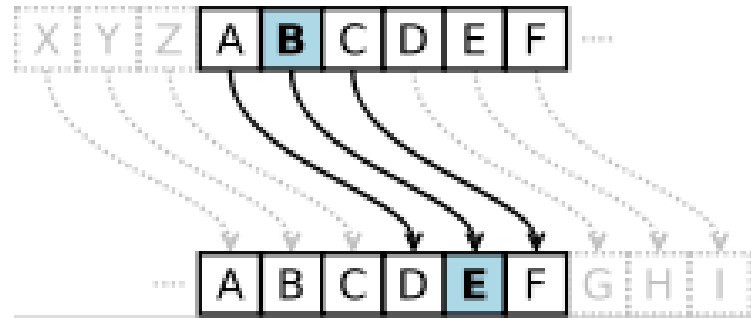
Cifrado César(I)

Funcionamiento:

- **Reemplaza** cada letra del alfabeto por otra más adelante en el alfabeto. Siempre a la misma distancia.
- La **clave** especifica la distancia.

Ejemplo:

Clave de sustitución: 3



Para cifrar y descifrar:

$$E_n(x) = x + n \mod 27. \quad D_n(x) = x - n \mod 27.$$

Donde n es la clave, x la letra a cifrar y 27 el número de letras del alfabeto.

Código por Sustitución de Letras(I)

Funcionamiento:

- **Reemplaza** cada letra del alfabeto por otra.
- La **clave** especifica el tipo de sustitución.

Ejemplo:

Clave de sustitución:

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

Cifrar:

. EJEMPLO

OSOQJRW

. HOLA

LWRI

Problema.

Puede romperse fácilmente para textos planos usando la frecuencia relativa de las letras.

(Ejemplo: la 'a' es la letra más usada en español).

Mejora.

Cambiar la sustitución de cada letra de acuerdo con un patrón periódico (sustitución múltiple).

Ejemplo. Sustitución múltiple.

Seleccionamos un periodo L. Por ejemplo $L=2$;

La clave de sustitución sería:

0:	A	H	L	O
	O	L	A	H

1:	A	H	L	O
	L	O	H	A

Posición:	0	1	0	1
T. Cifrado:	O	H	H	O
T. Plano:	H	O	L	A

Ejercicio: Cifrado de César

Desarrolle un programa simple que realice el cifrado de cesar. El usuario debe ingresar la clave a utilizar.

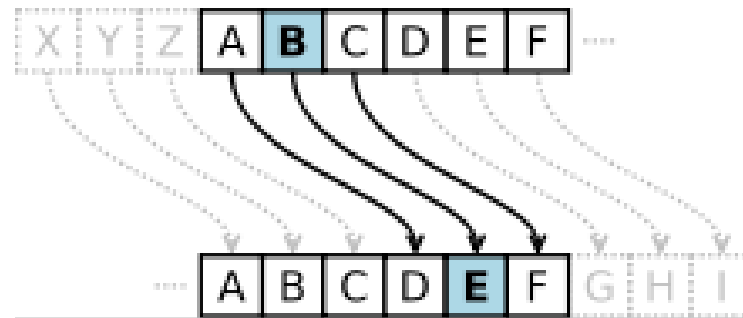
Tome en cuenta un alfabeto de 27 letras.

Ejercicio: Cifrado de César

Encripte la siguiente cadena utilizando una clave de sustitución igual a 20

Ejemplo:

Clave de sustitución: 3



Para cifrar y descifrar:

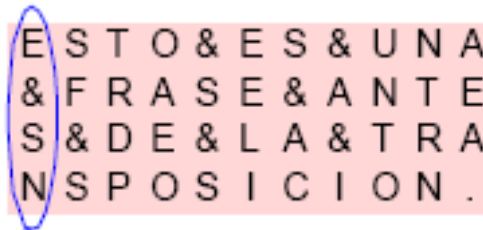
$$E_n(x) = x + n \mod 27. \quad D_n(x) = x - n \mod 27.$$

Donde n es la clave, x la letra a cifrar y 27 el número de letras del alfabeto.

Código por Transposición

Para aplicarlo, se considera el texto en filas de **L (11 por ejemplo)** letras cada una, y se envía el texto columna a columna:

P = ESTO&ES&UNA&FRASE&ANTES&DE&LA&TRANSPOSICION.



E	S	T	O	&	E	S	&	U	N	A
&	F	R	A	S	E	&	A	N	T	E
S	&	D	E	&	L	A	&	T	R	A
N	S	P	O	S	I	C	I	O	N	.

C = E&SNSF&STRDPOAEO&S&SEELIS&AC&A&IUNTONTNRAEA.

- El código se puede romper probando varias longitudes de fila distintas.
- Combinando sustitución con transposición se puede alcanzar una seguridad fiable con algoritmos de bajo coste computacional.

Criptografía de Clave Pública

A diferencia de los algoritmos simétricos, ahora vamos a disponer de 2 tipos de claves (por cada usuario) :

- Clave pública
- Clave privada

La clave pública la conoce todo el mundo y la privada es secreta y va ligado a un usuario.

Es imposible (ó muy difícil) deducir la clave secreta a partir de clave pública.

Comparativa entre Simétrica y Asimétrica

	Simétrico	Asimétrico
Más seguro		X
Más rápido	X	
Número de claves	1	2
Problema más significativo	Distribución de claves	Velocidad

¿ Qué es lo deseado ?

Combinar la velocidad con la seguridad

→ **Criptosistemas híbridos**

Criptografía de Clave Pública

El algoritmo más conocido es el RSA

Fue desarrollado en 1977.

(Rivest, Shamir, Adleman)

Actualmente es el primer sistema criptográfico y el mas utilizado.

Podemos cifrar y firmar digitalmente.

Investigación (Grupos – 2 pts.)

Investigar el funcionamiento de los siguientes algoritmos por medio de un ejemplo:

1. DES
2. RSA
3. Diffie-Hellman
4. PGP
5. GnuPG
6. Firma digital

La explicación debe ser grabada en un video, subirlo a la nube y publicarlo en el portal

Fecha entrega: Lunes 16 de noviembre