

# SEGURIDAD DE LA INFORMACIÓN

## TEMA 2

### **TÉCNICAS CRIPTOGRÁFICAS BÁSICAS** **(Y SERVICIOS DE SEGURIDAD ASOCIADOS)**

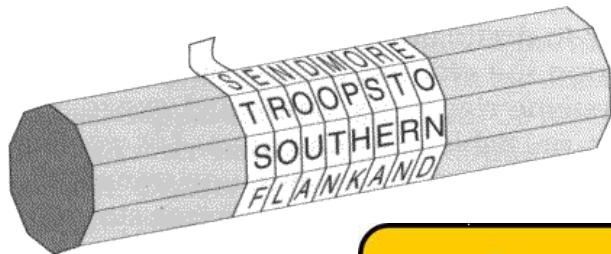
# Índice del tema (I)

- Introducción a la criptografía clásica
  - Cifrados por sustitución y transposición. Ejemplos
  - Cifrado producto
  - Cifrado Vernam (one-time pad)
- Algoritmos simétricos
  - Fundamentos
  - Algoritmo DES
  - Algoritmo triple-DES
  - Algoritmo AES
  - Otros algoritmos simétricos
  - Modos de operación para algoritmos simétricos
  - Ventajas y desventajas de los algoritmos simétricos

## Indice del tema (II)

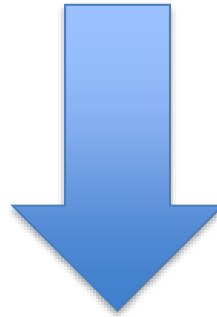
- Algoritmos asimétricos (o de clave pública)
  - Cifrado/descifrado
  - Firma Digital
  - Intercambio de Claves
  - Algoritmo de Diffie-Hellman
  - Algoritmo RSA
- Otras primitivas criptográficas
  - Funciones hash
  - Códigos de autenticación de mensajes
- Referencias bibliográficas

# Introducción a la criptografía clásica



# Cifrado: Criptografía, Criptoanálisis, Criptología

- Como se ha visto en la última tabla del capítulo anterior, un **algoritmo de cifrado** es uno de los mecanismos para la implementación de servicios de seguridad



- **Criptografía**: ciencia que estudia cómo mantener la seguridad en los mensajes ( $M$ )
  - usando, entre otros mecanismos, los algoritmos de cifrado
- **Criptoanálisis**: ciencia que estudia cómo romper los textos cifrados
- **Criptología**: Criptografía + Criptoanálisis

- El algoritmo de **cifrado** es un mecanismo que transforma un texto en claro en texto ininteligible
  - Su objetivo es dar cobertura al servicio de Confidencialidad
  - El algoritmo de cifrado se denota por **E** (del inglés “encrypt”) y opera sobre el **texto en claro**  $M$  (mensaje) para producir el **texto cifrado**  $C$  (criptograma)

$$E(M) = C$$
- La transformación inversa, o sea, de un texto cifrado en un texto en claro, se denomina algoritmo de **descifrado**
  - El algoritmo de descifrado se denota por **D** (“decrypt”) opera sobre  $C$  para producir el mensaje  $M$ 

$$D(C) = M$$
- Se cumple que:

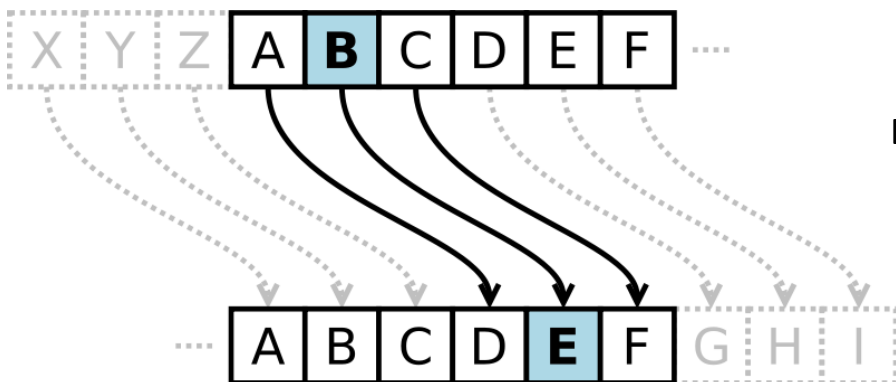
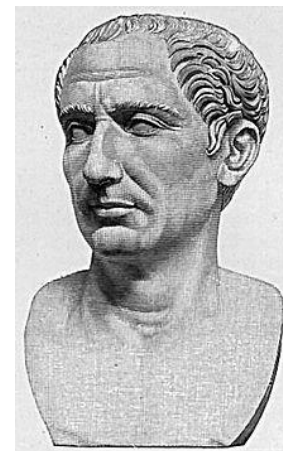
$$D(E(M)) = M$$

- Antes de la existencia de ordenadores, la criptografía clásica consistía en algoritmos basados en caracteres
- Los algoritmos criptográficos clásicos o bien sustituían caracteres o bien los transponían
  - Cifrado por **sustitución**:
    - cifrado en el que cada carácter del texto en claro se sustituye por otro carácter en el texto cifrado
      - $A \rightarrow V$
      - $V \rightarrow W$
      - ...
  - Cifrado por **transposición**:
    - consiste en realizar una permutación de las posiciones que ocupan los símbolos en el mensaje en claro
      - $HOLA \rightarrow ALHO$

## Ejemplo: cifrado por sustitución César

- Consiste en una transformación única. Cada carácter de texto en claro se reemplaza por el carácter tercero a la derecha, módulo 27

$$C: M \rightarrow M + 3 \pmod{27}$$



Ejemplo texto cifrado: WX WDPELHQ, EUXWR, KLMR PLR

¿Cómo sería el descifrado de este texto cifrado?

- Generalizado después a un sistema de cifrado con 27 posibles combinaciones

$$C: M \rightarrow M + i \pmod{27} \quad 1 \leq i \leq 27$$



- Ese algoritmo da ventaja al criptoanalista, porque la frecuencia de aparición de las letras es bien conocida. Así:

Some typical letter frequencies in different european languages



#### English

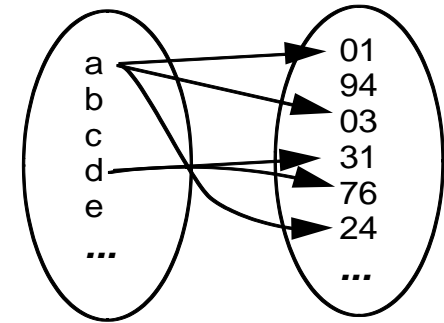
E	12.4%	H	6.5%	U	2.7%	G	2.0%	K	0.7%
T	8.9%	S	6.2%	M	2.5%	Y	2.0%	Q	0.1%
A	8.0%	R	6.1%	W	2.3%	P	1.6%	X	0.1%
O	7.6%	D	4.6%	C	2.2%	B	1.3%	J	0.1%
N	7.0%	L	3.6%	F	2.2%	V	0.8%	Z	0.0%
I	6.7%								

#### Spanish

E	13.0%	S	6.9%	U	3.6%	V	1.0%	J	0.3%
A	11.1%	T	5.3%	P	3.0%	F	0.8%	Z	0.3%
O	9.7%	C	5.2%	M	2.9%	Y	0.7%	X	0.2%
I	8.2%	D	4.5%	G	1.4%	H	0.6%	W	0.1%
N	8.0%	L	3.6%	B	1.3%	Q	0.6%	K	0.0%
R	7.7%								

## Ejemplo: cifrado por sustitución homofónico

- Se basa en la idea de asignar a un símbolo del alfabeto fuente varios del alfabeto cifrado, solventando el problema de la frecuencia de letras
- Correspondencia uno a muchos  $\Rightarrow$  al cifrar un mensaje podemos obtener varios criptogramas



- Ejemplo:

Letra	% (redondeado)	Símbolos asignados
A	8	10, 11, 23, 45, 76, 79, 87, 98
L	6	02, 15, 21, 25, 56, 60
N	3	44, 63, 71
O	8	04, 16, 28, 29, 37, 52, 69, 90
P	2	30, 88
T	2	24, 77

“PLATON” se cifra como “882110772963”

- | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| V | K | L | s | w | e | M | N | U | f | a | b | Q | r | S | t | o | j | l | P | x | s | Ñ | h | d | Z | w |

- | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| z | g | X | Y | a | b | D | K | L | P | q | s | t | U | O | Ñ | Q | k | e | c | H | W | M | N | f | g | i |

- [illegible]

- [illegible]

# Ejemplo: cifrado por sustitución polialfabética

- Alfabeto para posiciones impares:

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
V	K	L	s	w	e	M	N	U	f	a	b	Q	r	S	t	o	j	I	P	x	s	Ñ	h	d	Z	W

- Alfabeto para posiciones pares:

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
z	g	X	Y	a	b	D	K	L	P	q	s	t	U	O	Ñ	Q	k	e	c	H	W	M	N	f	g	i

- Cifrado del texto: “***HOLA A TODOS***”

H	O	L	A	A	T	O	D	O	S
N	Ñ	b	z	V	H	t	Y	t	c

- Descifrado:

N	Ñ	b	z	V	H	t	Y	t	c
H	O	L	A	A	T	O	D	O	S

## Ejemplo: cifrado por transposición

- La forma más simple de transposición: el texto en claro se escribe como secuencia de filas (con una cierta profundidad) y se lee como secuencia de columnas
- Ejemplo: “EN ANDALUCIA, EL MULHACEN Y EL VELETA, SON LAS MONTAÑAS MAS ALTAS”

ENANDALUCIAELMULHACENYELVE  
LETASONLASMONTAÑASMASALTAS

- Mensaje cifrado:

ELNEATNADSAOLNULCAISAMEOLNMTUALÑHAASCMEANSYAELLTVAES

## Ejemplo: cifrado por transposición con clave

- Se podría complicar el procedimiento anterior estableciendo una restricción en el número de columnas cuyo valor va a depender del tamaño que tenga una **clave**
- Ejemplo:
  - Texto en claro: ***“HOLA A TODOS, QUE TENGÁIS UN BUEN DÍA”***
  - Clave: **“SECRETO”** con un tamaño de 7

S	E	C	R	E	T	O
H	O	L	A	A	T	O
D	O	S	Q	U	E	T
E	N	G	A	I	S	U
N	B	U	N	D	I	A

- Para el cifrado se puede poner la condición siguiente: se va a ir cogiendo las letras de aquellas columnas por orden alfabético del secreto, es decir: **C, E, E, O, R, S, T**, resultando en: “\_\_\_\_\_”

## Ejemplo: cifrado por transposición con clave

- Se podría complicar el procedimiento anterior estableciendo una restricción en el número de columnas cuyo valor va a depender del tamaño que tenga una **clave**
- Ejemplo:
  - Texto en claro: ***HOLAA TODOS, QUE TENGÁIS UN BUEN DÍA***
  - Clave: **”SECRETO”** con un tamaño de 7

S	E	C	R	E	T	O
H	O	L	A	A	T	O
D	O	S	Q	U	E	T
E	N	G	A	I	S	U
N	B	U	N	D	I	A

- Para el cifrado se puede poner la condición siguiente: se va a ir cogiendo las letras de aquellas columnas por orden alfabético del secreto, es decir: **C, E, E, O, R, S, T**, resultando en: **“LSGUOONBAUIDOTUAAQANHIDENTESI”**

## Ejemplo: cifrado por transposición Railfence

- El cifrado consiste
  - en escribir diagonalmente el texto en claro con una profundidad  $P$  específica
  - el criptograma se escribe leyendo las filas
- Ejemplo:  $M = \text{“Hola a todos”}$ , con una profundidad de  $P=4$ , entonces el criptograma es: **Hoot d laosas**  
por simplemente computar:

```
H      o
o    t  d
l  a    o
a      s
```

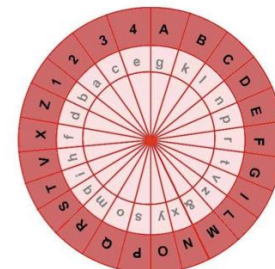


# Ejemplo: métodos polialfabéticos y nomenclátore

- Para complicar el proceso de cifrado, se puede hacer uso del disco de Alberti junto con nomenclátore, los cuales consisten en asociar a determinados palabras, códigos específicos

Felipe II	123
Rey	124
Walshingan	122

- Se desea descifrar el siguiente texto: “*baa&hpmiyvsvoiylrlxckngkl*”
- Uso del disco:
  - Cada diez letras descifradas, se ha de girar el disco externo (de las mayúsculas) dos posiciones en el sentido de las agujas del reloj
  - En el disco de Alberti, la **u** se identifica con la **v** al cifrar. Al descifrar, por el sentido de la frase, se puede conocer si se ha de escribir una u otra letra



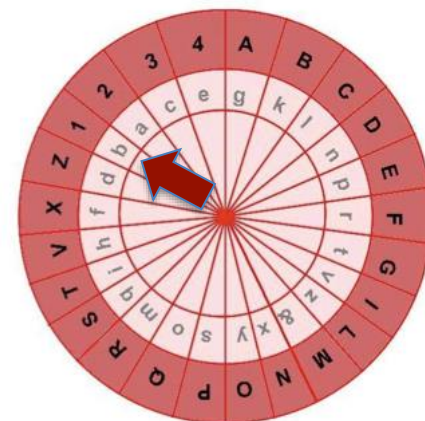
# Ejemplo: métodos polialfabéticos y nomenclátore

- Funcionamiento para cifrar:

- Posicionar los disco en el estado inicial

b	a	a	&	H	p	m	i	Y	V
1	2								

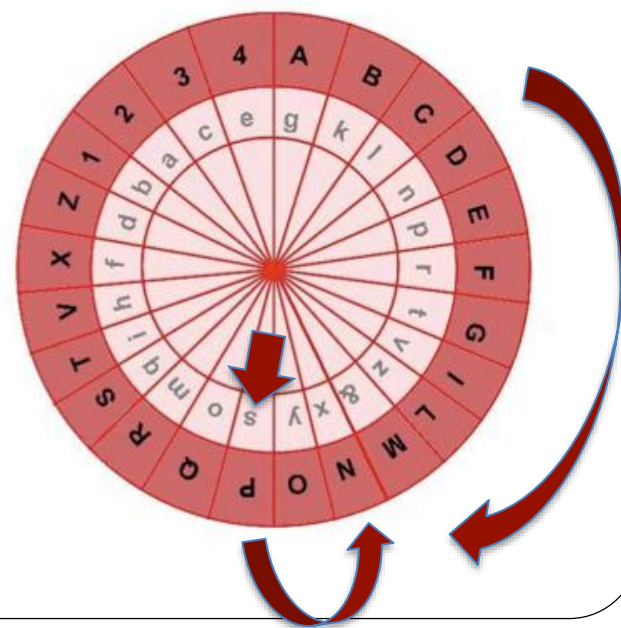
***"baa&hpmiyvsvoiyrlrxckngkl"***



- Con el disco externo girar 2 posiciones en el sentido de las agujas del reloj (sólo en cada diez letras descifrada):

s	v	o	l	Y	l	r	l	X	C
N	F								

***"baa&hpmiyvsvoiyrlrxckngkl"***



# Ejemplo: métodos polialfabéticos y nomenclátore

- Funcionamiento:

- Con el disco externo volver a girar 2 posiciones en el sentido de las agujas del reloj:

k	n	g	k	L
2	4	1	2	3

***“baa&hpmiyvsvoiyrlxckngkl”***

- Por consiguiente, el texto en claro es:

b	a	a	&	H	p	m	i	Y	V
1	2	2	M	V	E	R	T	O	I

s	v	o	I	Y	I	r	I	X	C
N	F	O	R	M	A	D	A	L	1

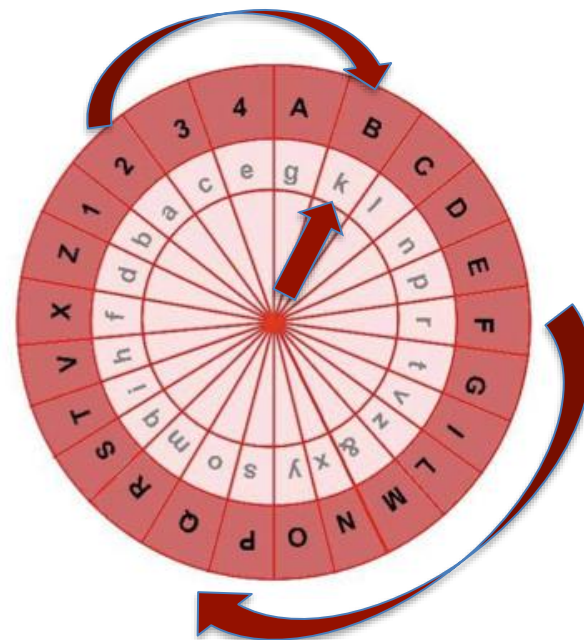
k	n	g	k	L
2	4	1	2	3

**“1 2 2 M V E R T O I N F O R M A D A L 1 2 4 1 2 3”**

- Si, además, añadimos los nomenclátore + la restricción de la V → U:

Felipe II	123
Rey	124
Walshingan	122

**“WALSHINGAN MUERTO INFORMAD AL REY FELIPE II”**



# Cifrado Producto

- Combina sustitución y transposición
- Se pueden considerar como la aplicación sucesiva de varios cifrados  $E_i$

$$E = E_1 \cdot E_2 \cdot \dots \cdot E_r$$

$$E(M) = E_1(E_2(\dots(E_r(M))))$$

- La composición de funciones de descifrado  $D_i$  se realiza en orden inverso

$$D = D_r \cdot D_{r-1} \dots D_1$$

$$M = D(C) = D_r(D_{r-1}(\dots(D_1(C))))$$

- Es un esquema utilizado para obtener un alto grado de seguridad con sistemas relativamente sencillos aplicados reiterativamente
- Dan lugar a sistemas de cifrado complejos, seguros, difíciles de atacar, fácilmente trasladables a un ordenador

# Cifrado Vernam

- Variante del cifrado llamado **one-time pad (OTP)**
- Un one-time pad es un *conjunto infinito y no repetitivo* de letras aleatorias
- Cada letra del pad se usa para cifrar una única letra del texto en claro, en módulo  $n$  (longitud del alfabeto)



Texto : THIS IS SECRET  
OTP: X VHE UW NOPGCZ

-----  
Cifrado : QCPW CO FSRXHS



- Otro dos ejemplos:

- Aquí se observan grupos de tres filas, que se corresponden con texto en claro (en decimal), clave y criptograma

Fuente: <http://www.caslab.cl/che.php>

B	A	R	R	O	Y	C	A	Ñ	A	B	R	A	V	A	← MCl
1	0	18	18	15	25	2	0	14	0	1	18	0	22	0	← Clave (tan larga como el mensaje)
E	D	S	A	S	A	C	E	T	N	I	E	V	E	D	← MCl + Clave
4	3	19	0	19	0	2	4	20	13	8	4	22	4	3	← Criptograma
5	3	10	18	7	25	4	4	7	13	9	22	22	26	3	
F	D	K	R	H	Y	E	E	H	N	J	V	V	Z	D	

Fuente: <http://bit.ly/2cqBu8D>

Cifrado: (carácter del texto en claro + key ) + mod 27

Descifrado: (carácter del criptograma - key ) + mod 27

- En los ordenadores, el OTP aleatorio de longitud infinita se combina mediante XOR con el texto en claro. Ejemplo:

Texto en claro	1	1	0	0	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	$\oplus$
OTP	1	0	0	1	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	0	1	0	=
Criptograma	0	1	0	1	0	0	0	1	1	0	1	0	1	1	1	0	1	0	1	0	0	1	$\oplus$
OTP	1	0	0	1	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	0	1	0	=
Texto en claro	1	1	0	0	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	

- Inconvenientes del cifrado Vernam:
  - las letras del OTP (o bits si se usa en ordenador) han de generarse aleatoriamente
  - el OTP no se vuelve a usar

## Relación de ejercicios

1. Considerando el alfabeto común (incluyendo la ñ en el alfabeto) y un desplazamiento de 3 posiciones para el proceso de cifrado o descifrado, aplicar la técnica de sustitución Caesar para cifrar el siguiente texto:

“EL PATIO DE MI CASA ES PARTICULAR”

Nota: se empieza a contar desde la posición 1 (A del alfabeto)

**SOLUCIÓN:** HÑ SDWLR GH OL FDVD HV SDUWLFXÑDU



## Relación de ejercicios

2. Dado el criptograma  $C = \text{"FMIRZIRMHS E PE EW MKREXYVE HI WIKYVMHEH HI PE MRJSVQEGMKR"}$  descifrar el contenido del mismo, sabiendo, además, que hay que usar la técnica de sustitución Caesar con un desplazamiento de 4 posiciones modulo  $n=26$

Nota: se empieza a contar desde la posición 1 (A del alfabeto)

**SOLUCIÓN:** BIENVENIDO A LA ASIGNATURA DE SEGURIDAD  
DE LA INFORMACIÓN

## Relación de ejercicios

3. El siguiente algoritmo aplicará una sustitución monoalfabética, pero esta vez teniendo en cuenta la siguiente regla:  $C_i = M_i + K_i \bmod 26$  donde  $K$  representa una clave de longitud  $L$ . El objetivo es cifrar el texto original usando el alfabeto inglés

¿Cuál sería el criptograma del mensaje  $M = \text{“HOLA AMIGOS”}$  usando una clave  $K = \text{CIFRA}$ ?

Nota: se empieza a contar desde la posición 1 (A del alfabeto)

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

<b>H</b>	<b>O</b>	<b>L</b>	<b>A</b>	<b>A</b>	<b>M</b>	<b>I</b>	<b>G</b>	<b>O</b>	<b>S</b>
8	15	12	1	1	13	9	7	15	19
<b>C</b>	<b>I</b>	<b>F</b>	<b>R</b>	<b>A</b>	<b>C</b>	<b>I</b>	<b>F</b>	<b>R</b>	<b>A</b>
<b>+3</b>	<b>+9</b>	<b>+6</b>	<b>+18</b>	<b>+1</b>	<b>+3</b>	<b>+9</b>	<b>+6</b>	<b>+18</b>	<b>+1</b>
<b>K</b>	<b>X</b>	<b>R</b>	<b>S</b>	<b>B</b>	<b>P</b>	<b>R</b>	<b>M</b>	<b>G</b>	<b>T</b>
11	24	17	19	2	16	18	13	32→7	20

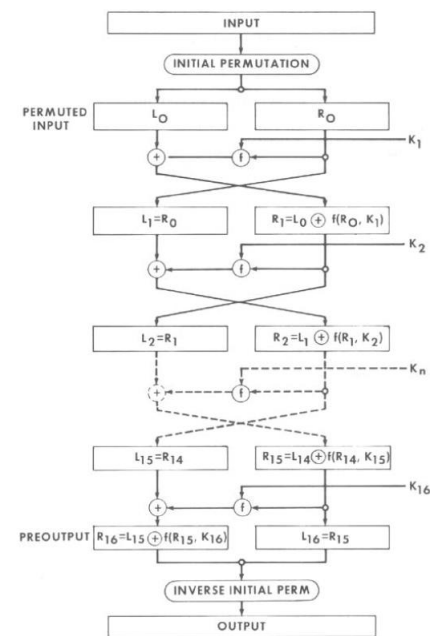
**SOLUCIÓN:** KXRS BPRMGT

## Relación de ejercicios

4. Mediante la técnica Railfence, determinar el criptograma correspondiente al mensaje “*Nos han descubierto, debemos huir*” con una profundidad  $P=7$  (alfabeto inglés) y sin contar espacios

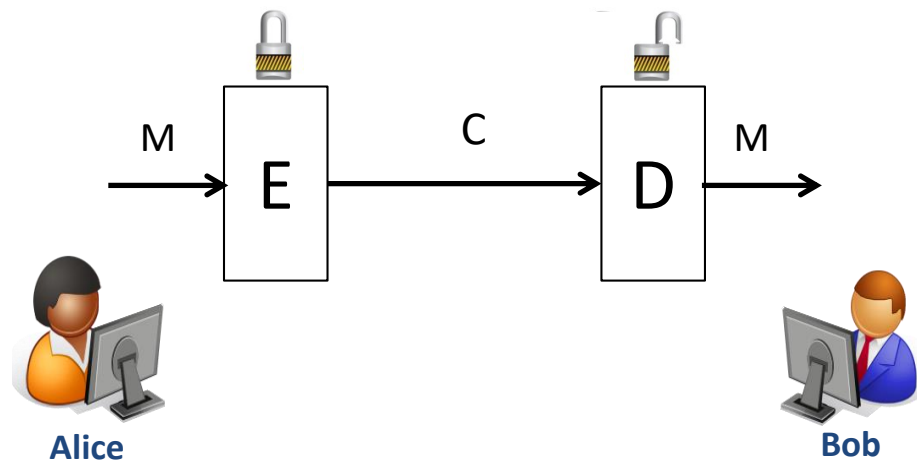
**SOLUCIÓN:** Nihobesusuroihctmrasoenedbde

# Algoritmos simétricos

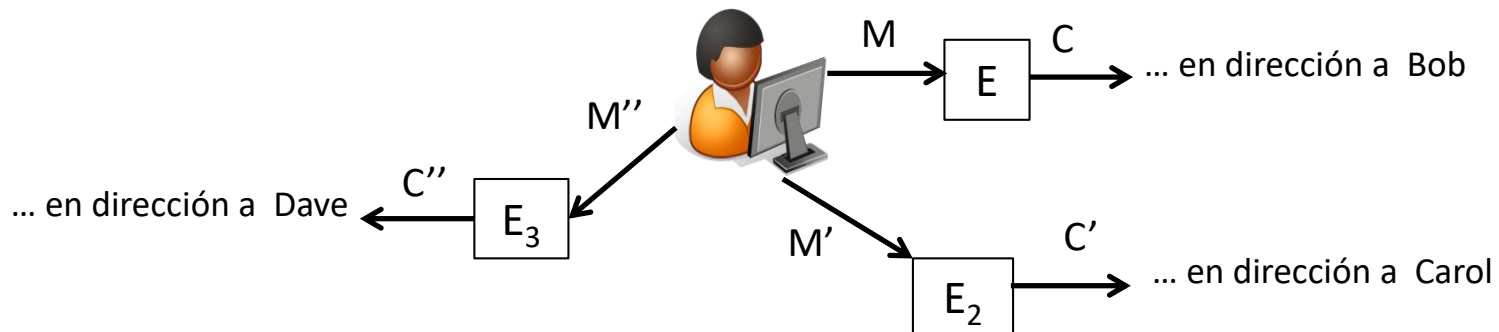


# Fundamentos

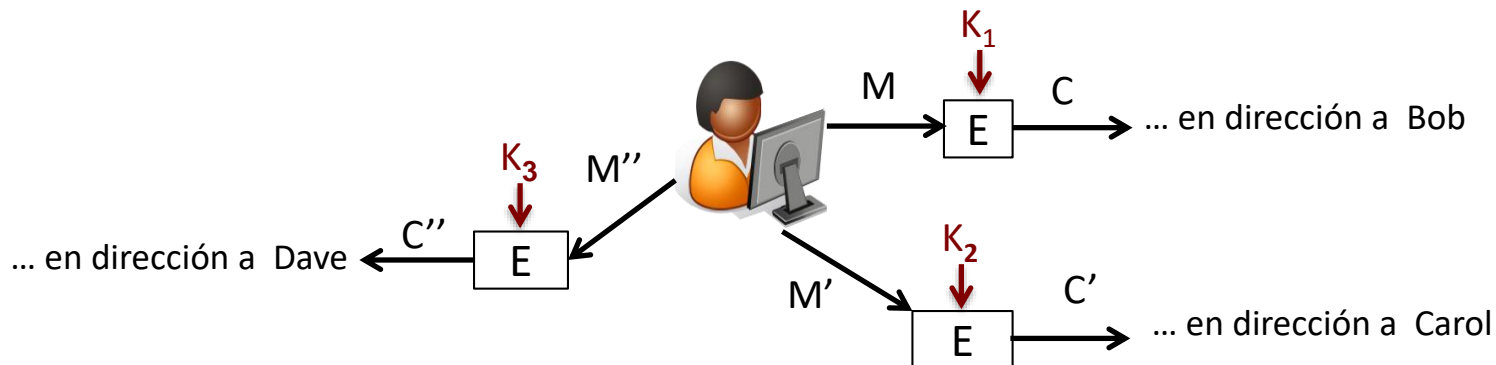
- En la mayoría de los ejemplos de la sección anterior la comunicación entre los usuarios puede representarse como sigue:



- El esquema anterior es útil siempre que se mantengan en "secreto" la transformación  $E$  y su inversa  $D$ 
  - Esto es factible para un intercambio de información entre dos usuarios específicos (por ejemplo, *Alice* y *Bob*)
  - Sin embargo, esta forma de funcionamiento resulta **no escalable**
    - Es decir, cuando *Alice* necesite comunicar con alguien distinto de *Bob*, habría de usar un algoritmo distinto a  $E$ , como muestra la figura inferior
    - Más concretamente, *Alice* necesitaría un **algoritmo distinto para cada usuario** con quien necesitara contactar

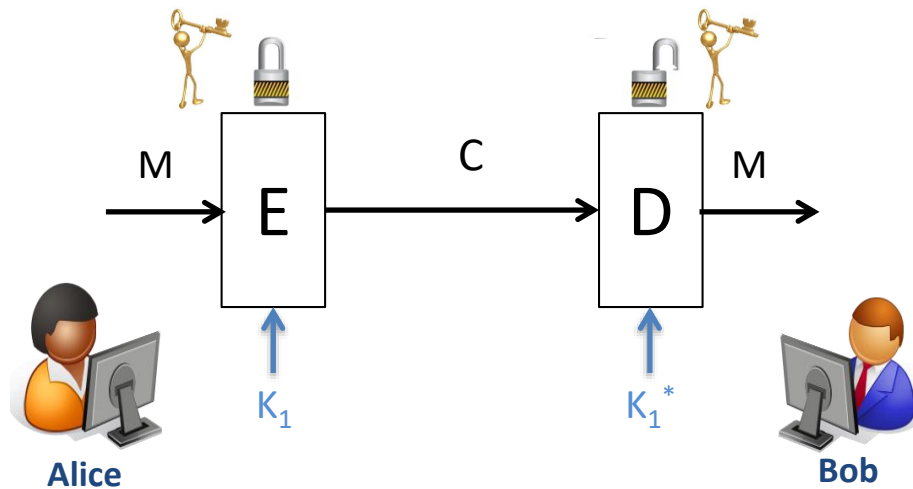


- Esta problemática se puede solucionar introduciendo un parámetro adicional, la **clave secreta**  $K$ , en el algoritmo de cifrado  $E$ 
  - De esta forma, *Alice* puede usar el mismo algoritmo  $E$  en sus comunicaciones con todos los usuarios (*Bob*, *Carol*, *Dave*, ...), pero selecciona una clave  $K$  distinta para cada uno de ellos





- En esta situación, el mismo algoritmo de descifrado  $D$  será usado por todos los receptores, pero cada uno necesitará la clave correspondiente de descifrado ( $K_1^*$ ,  $K_2^*$ ,  $K_3^*$  ...)
- En resumen, para la comunicación específica entre *Alice* y *Bob*:



$$D_{K_1^*} ( E_{K_1} (M) ) = M$$