SEGURIDAD DE LA INFORMACIÓN

TEMA 2

TÉCNICAS CRIPTOGRÁFICAS BÁSICAS

(Y SERVICIOS DE SEGURIDAD ASOCIADOS)

KIT-KAT

GRUPOA	Sem	Hora	Practica	Lugar	Docente
2023-09-12	M	12:45-14:30		2.0.5	CAT, RRP
2023-09-14 (EXCEPCIÓN)	J	8:45-10:30		2.0.5	CAT
2023-09-18	L	10:45-12:30		2.0.5	CAT
2023-09-19	M	12:45-14:30	👷 (MAT)	LAB_3.1.9	RRP
2023-09-21	J	8:45-10:30	👷	LAB_3.1.7	RRP
2023-09-25	L	10:45-12:30		2.0.5	CAT
2023-09-26	M	12:45-14:30	👷 (MAT)	LAB_3.1.9	RRP
2023-09-28	J	8:45-10:30	👷	LAB_3.1.7	RRP

GRUPO B	Sem	Hora	Practica	Lugar	Docente
2023-09-12	M	8:45-10:30		3.0.11	CAT, RRP
2023-09-15	V	8:45-10:30		3.0.11	CAT
2023-09-18	L	12:45-14:30		3.0.11	CAT
2023-09-19	M	8:45-10:30	👷	LAB_3.1.6	RRC
2023-09-22	V	8:45-10:30	👷	LAB_3.1.2	RRC
2023-09-25	L	12:45-14:30		3.0.11	CAT
2023-09-26	M	8:45-10:30	👷	LAB_3.1.6	RRC
2023-09-29	V	8:45-10:30	👷	LAB_3.1.2	RRC

Indice 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

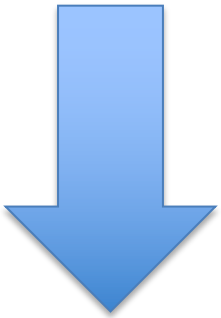
Indice del tema (II)

- 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

Criptografía, Criptoanálisis, Criptología

- Ya se sabe por el tema anterior que un **algoritmo de cifrado** es un mecanismo fundamental para el desarrollo de servicios de seguridad, como puede ser la confidencialidad



- 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, caracterizado por E (del inglés "*encrypt*"), opera sobre el texto en claro *M* (mensaje) para producir el texto cifrado *C* (criptograma)

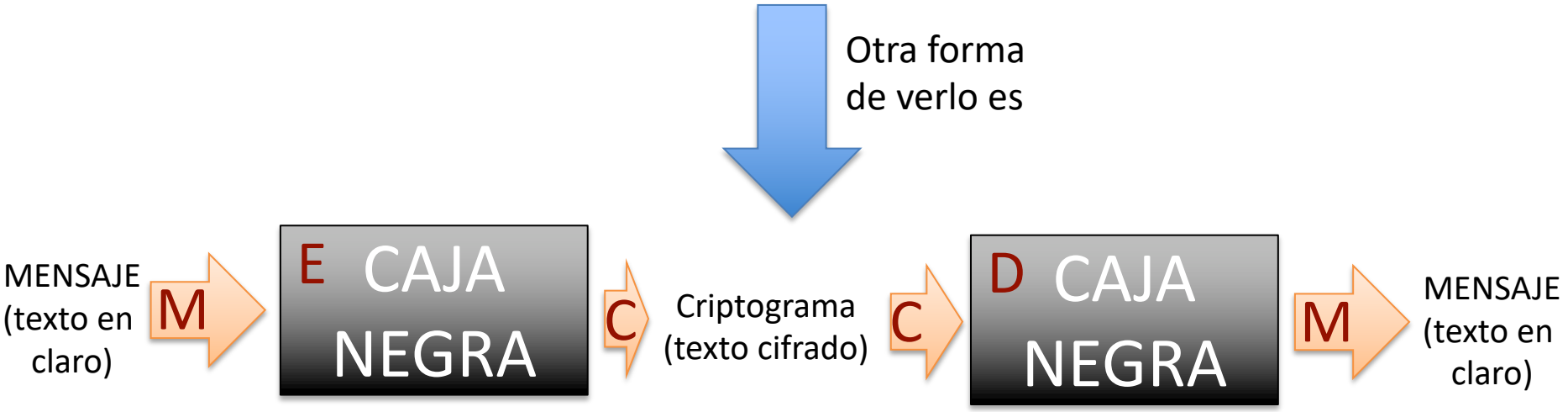
- La transformación inversa de un texto cifrado a un texto en claro, se denomina ALGORITMO DE DESCIFRADO
  - El algoritmo se denota por la letra D ("*decrypt*") y opera sobre *C* para producir el mensaje *M*

$$D(C) = M$$

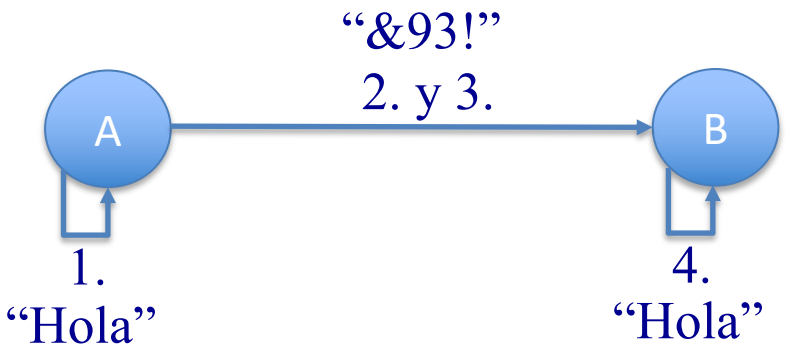
- Se cumple también que:

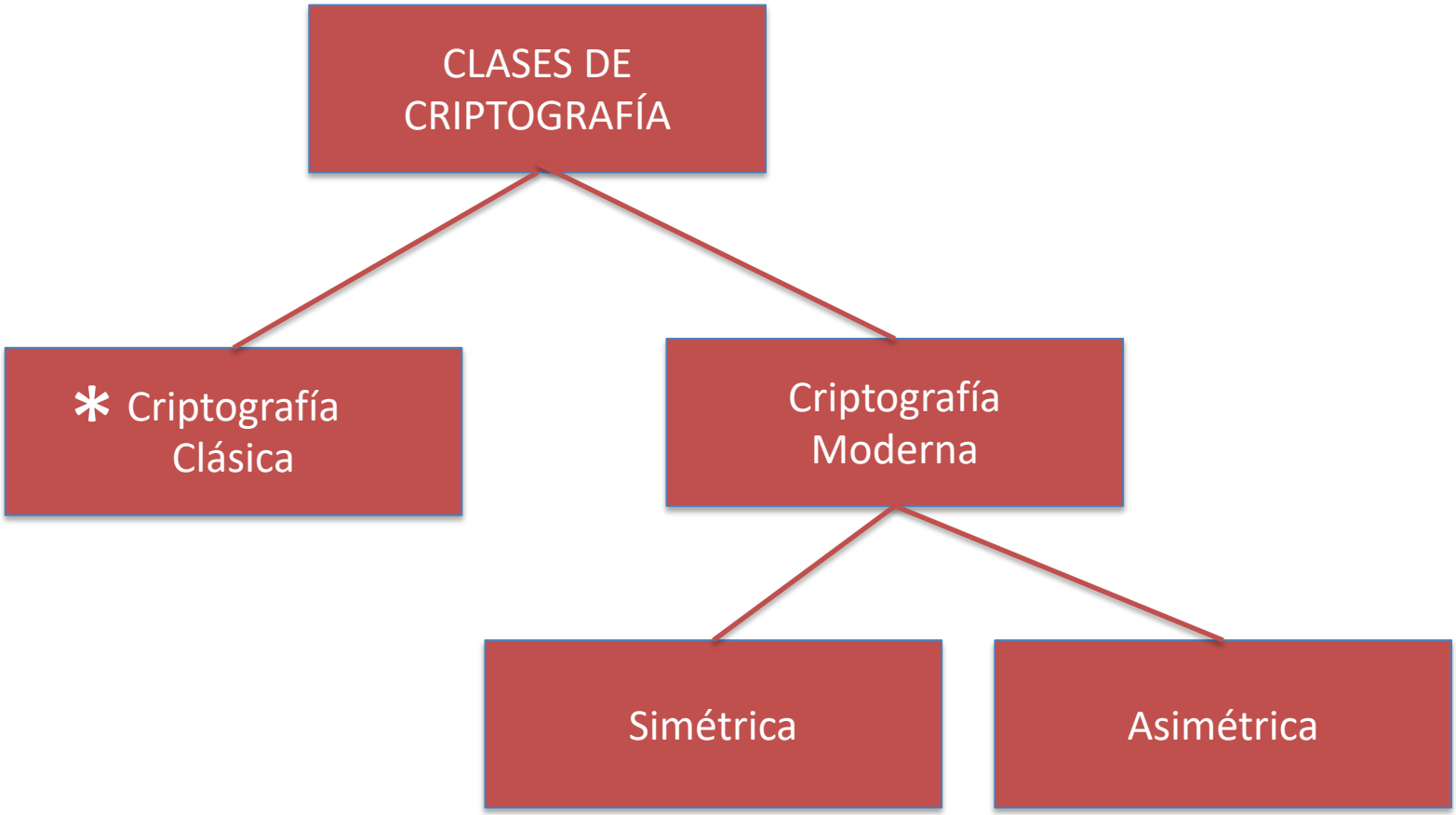
$$D(E(M)) = M$$

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



- Ejemplo:
  1. A genera un texto en claro: “Hola”
  2. A computa: E(“Hola”) = “&93!”
  3. A envía a B el criptograma: “&93!”
  4. B computa: D(“&93!”): “Hola”



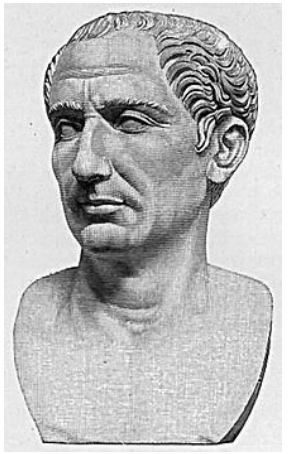

CLASES DE CRIPTOGRAFÍA
* Criptografía Clásica
Criptografía Moderna
Simétrica
Asimétrica

Criptografía clásica

- Antes de la existencia de ordenadores, la criptografía clásica consistía en algoritmos basados en caracteres
- Estos algoritmos se basaban en dos técnicas principales:
  - **Cifrado por sustitución:**
    - Objetivo: cada carácter del texto en claro se sustituye por otro carácter en el texto cifrado
      - A→ V
      - V → W
      - …
  - **Cifrado por transposición:**
    - Objetivo: realizar una permutación con respecto a las posiciones que ocupan los símbolos en el mensaje en claro
      - HOLA → ALHO

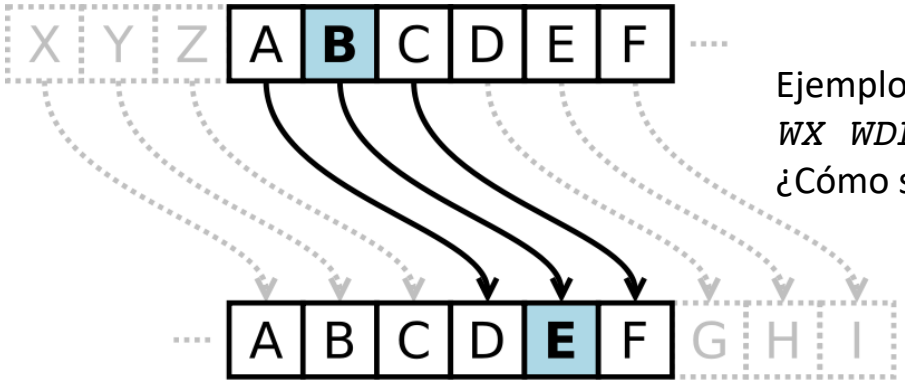
EJEMPLOS
SUSTITUCIÓN

Ejemplo 1: cifrado por sustitución César



- Objetivo:
  - Cada carácter de texto en claro se reemplaza por aquel posicionado a tres posiciones a la derecha (módulo 27)

$$C: M \rightarrow M + 3 \ (mod\ 27)$$

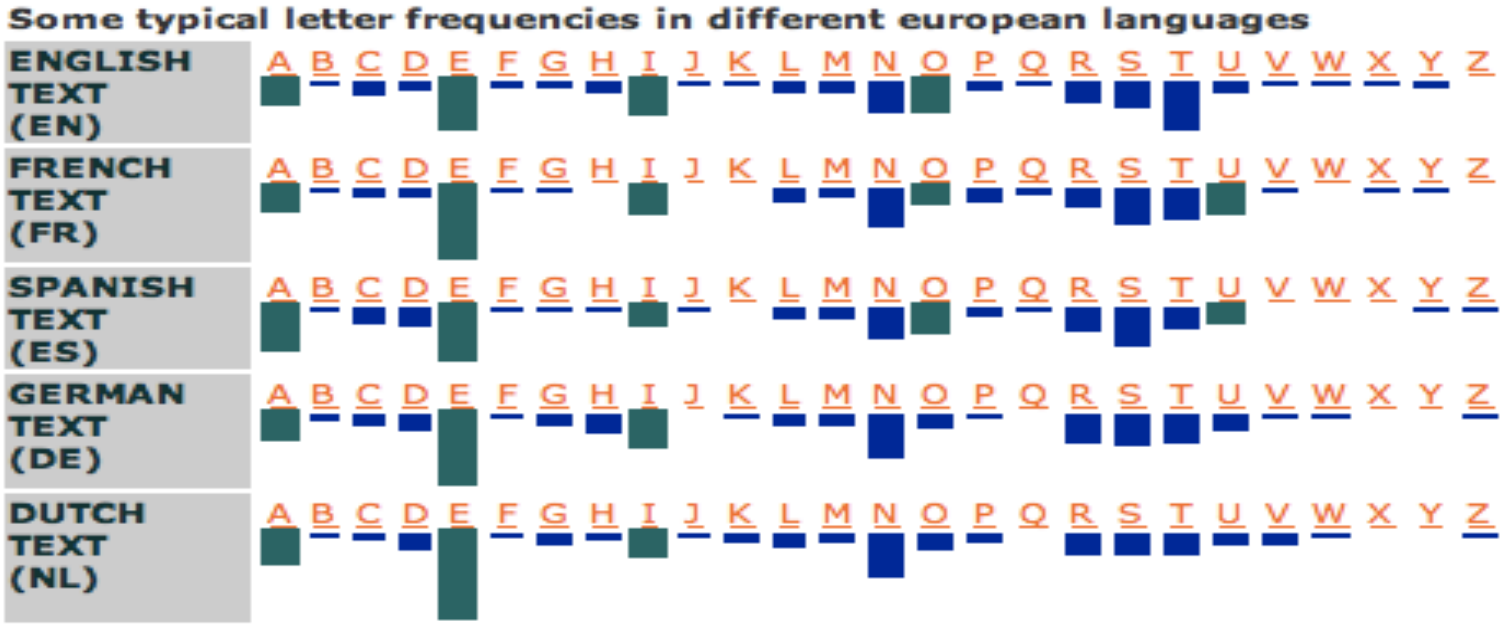


Ejemplo texto cifrado:
WX WDPELHQ, EUXWR, KLMR PLR
¿Cómo sería el descifrado de este texto cifrado?

- Se puede generalizar a un sistema de cifrado con 27 posibles combinaciones

$$C: M \rightarrow M + i \ (\mathbf{mod}\ 27) \quad 1 \leq i \leq 27$$

- El algoritmo proporciona ventajas al criptoanalista, porque la frecuencia de aparición de las letras es bien conocida. Así:



English

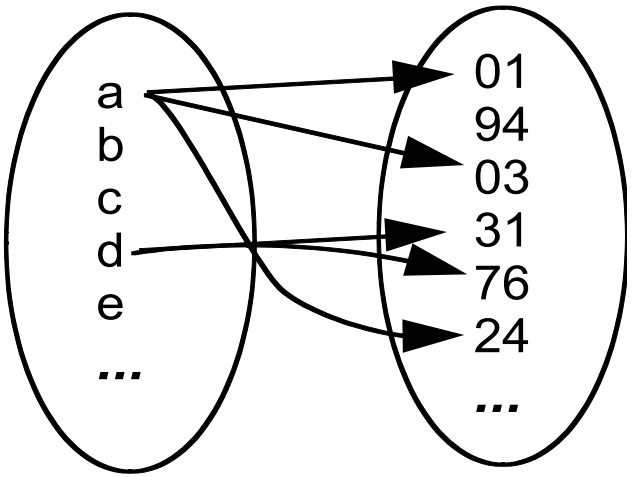
E	12.4%	H	6.5%	U	2.7%	G	2.0%	K	0.7%
T	8.9%	S	6.2%	M	2.5%	Y	2.0%	Q	0.1%
A	8.0%	R	6.1%	W	2.3%	P	1.6%	X	0.1%
O	7.6%	D	4.6%	C	2.2%	B	1.3%	J	0.1%
N	7.0%	L	3.6%	F	2.2%	V	0.8%	Z	0.0%
I	6.7%								

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 2: 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 ⇒ 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"

Ejemplo 3: cifrado por sustitución POLIalfabética

[Intipedia]

- 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

- Descifrado:

Ejemplo 3: cifrado por sustitución POLIalfabética

[Intipedia]

- 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

EJEMPLOS
TRANSPOSICIÓN

Ejemplo 4: cifrado por transposición

- Objetivo: el texto en claro se escribe como secuencia de filas (con una cierta profundidad X) y se lee como secuencia de columnas

Restricción a nivel de fila

H	O	L	A	M	U	N
D	O	Y	A	S	Í	C
O	N	T	O	D	O	I

- Ejemplo:
  - "EN ANDALUCIA, EL MULHACEN Y EL VELETA, SON LAS MONTAÑAS MAS ALTAS" - profundidad 26

ENANDALUCIAELMULHACENYELVE

LETASONLASMONTAÑASMASALTAS

Hay que quitar los espacios, los símbolos, etc.

  - Mensaje cifrado:
    ELNEATNADSAOLNULCAISAMEOLNMTUALÑHAASCMEANSYAELLTVAES
  - Mensaje descifrado: **ELNEATNADSAOLNULCAISA ….**

Ejemplo 5: cifrado por transposición con CLAVE

[Intipedia]

- 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**

Restricción a nivel de fila

H	O	L	A	M	U	N
D	O	Y	A	S	Í	C
O	N	T	O	D	O	I

Restricción a nivel de columna

- 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

Ejemplo 5: cifrado por transposición con CLAVE

[Intipedia]

- 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

- Podemos fortalecer la seguridad si añadimos más restricciones:
  - Por ejemplo, coger las letras de aquellas columnas por orden alfabético del secreto, es decir: **C, E, E, O, R, S, T**, resultando en:"LSGUOONBAUIDOTUAAQANHDENTESI"

Cifrado Producto

- **Combinación de algoritmos: sustitución y transposición**
- Se pueden considerar como la aplicación sucesiva de varios cifrados E_i

$$E = E_1 \,.\, E_2 \,.\, \cdots \,.\, E_r$$

$$E\,(M) = E_1\,(E_2\,(\cdots\,(E_r\,(M))$$

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

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

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

- 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 y difíciles de atacar, así como fácilmente trasladables a un ordenador

EJEMPLOS
CIFRADO DE PRODUCTO

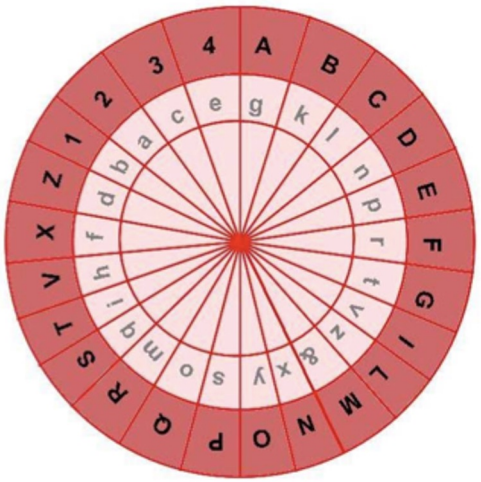
Ejemplo 6: métodos polialfabéticos y nomenclátores

[Intipedia]

- Se hace uso del disco de Alberti junto con nomenclátores
  - Los nomenclátores consisten en asociar a determinadas palabras códigos específicos
- El proceso debería ser:
  - Cifrado: 1) nomenclátores, y 2) disco de Alberti
  - Descifrado: 1) disco de Alberti y 2) nomenclátores

Felipe II	123
Rey	124
Walshingan	122

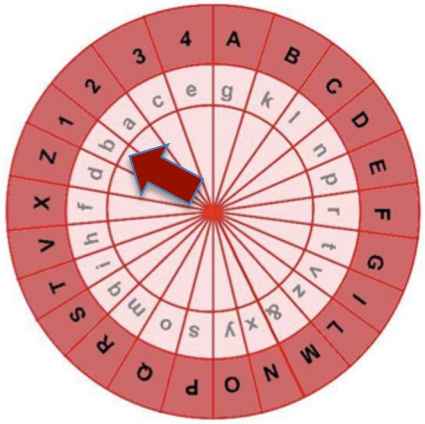
- Se desea **descifrar** el siguiente texto: "***baa&hpmiyvsvoiylrlxckngkl***"
- Usaremos el disco y las siguientes condiciones:
  - Cada diez letras descifradas, se ha de girar el disco externo (de las mayúsculas) dos posiciones en el sentido de las agujas del reloj
  - En el disco de Alberti, la **u** 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 6: métodos polialfabéticos y nomenclátores

[Intipedia]

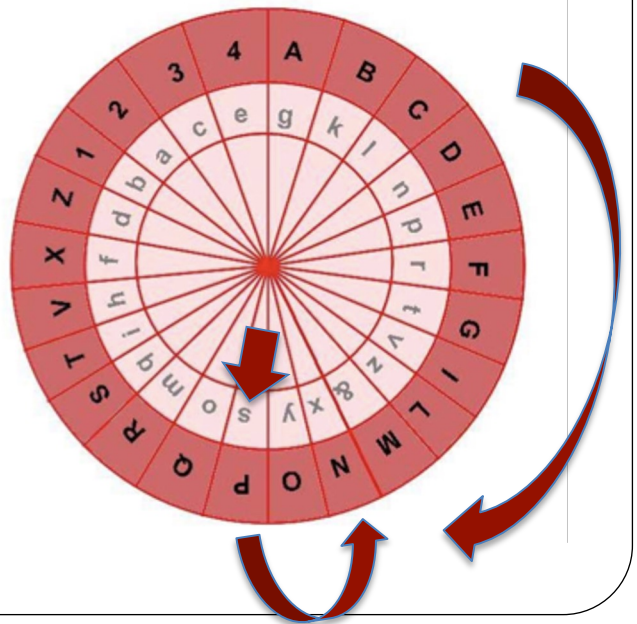
- Funcionamiento para cifrar:
  - Posicionar los disco en el estado inicial



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

"baa&hpmiyvsvoiylrlxckngkl"

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



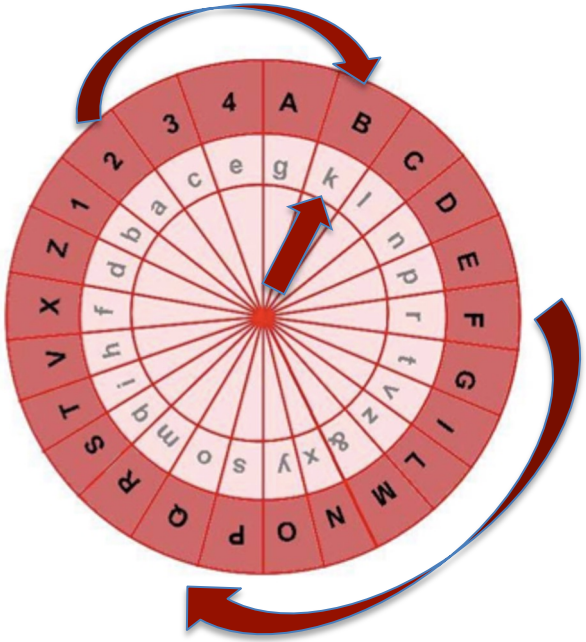
s	v	o	i	Y	l	r	l	X	C
N	F								

"baa&hpmiyvsvoiylrlxckngkl"

Ejemplo 6: métodos polialfabéticos y nomenclátores [Intipedia]

- 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&hpmiyvsvoiylrlxckngkl"

- 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	l	Y	l	r	l	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 nomenclátores + la restricción de la V → U:

Felipe II	123
Rey	124
Walshingan	122

"WALSHINGAN MUERTO INFORMAD AL REY FELIPE II"

Ejemplo 7: Cifrado Vernam

- Aplica el concepto de **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 : T H I S I S S E C R E T

OTP: X V H E U W N O P G C Z

Cifrado : Q C P W C O F S R X H S

One-time pad booklet and microdot reader,concealed in a toy truck and used by an illegal agent that operated in Canada
© Canadian Security Intelligence Service

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

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

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

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

- Ejemplo:
  - 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	⊕
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**	⊕
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 (CASA)

Relación de ejercicios

1. Considerando el alfabeto inglés (sin incluir la ñ) 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"

SOLUCIÓN: HO SDWLR GH PL FDVD HV SDUWLFXODU

Relación de ejercicios

2. Dado el criptograma C = “FMIRZIRMHS E PE EWMKREXYVE HI WIKYVMHEH HI PE MRJSVQEGMSR” 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 (Alfabeto inglés)

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 = "HOLA AMIGOS" usando una clave K = CIFRA?

   Nota: (i) se empieza a contar desde la posición 0 (A del alfabeto); (ii) se puede repetir la clave K tantas veces como sea necesario

Relación de ejercicios

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

H	O	L	A	A	M	I	G	O	S
7	14	11	0	0	12	8	6	14	18
C	***I***	***F***	***R***	***A***	***C***	***I***	***F***	***R***	***A***
+2	**+8**	**+5**	**+17**	**+0**	**+2**	**+8**	**+5**	**+17**	**+0**
J	**W**	**Q**	**R**	**A**	**O**	**Q**	**L**	**F**	**S**
9	22	16	17	0	14	16	11	31→5	18

SOLUCIÓN: JWQR AOQLFS

- Con https://cryptii.com,es possible probar algunos otros algoritmos de cifrado clásicos y básicos