



EXCMO. AYUNTAMIENTO  
DE CASTRO URDIALES



ESTÍMULO DEL TALENTO MATEMÁTICO



ESTALMAT  
Catalunya

# UCNRPIAPSTE OOGPROARFLIAA



REAL ACADEMIA DE CIENCIAS  
EXACTAS, FÍSICAS Y NATURALES  
DE ESPAÑA



C I E E M

Centro Internacional de Encuentros Matemáticos



un paseo por la criptografía...  
... y algo de Snap!



Purposeful  
Ventures

Guillem Bonet

Pura Fornals



Generalitat de Catalunya  
Departament  
d'Educació



Financiado por  
la Unión Europea  
NextGenerationEU



GOBIERNO  
DE ESPAÑA

MINISTERIO  
PARA LA TRANSFORMACIÓN DIGITAL  
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO  
DE TELECOMUNICACIONES  
E INFRAESTRUCTURAS DIGITALES



Plan de  
Recuperación,  
Transformación  
y Resiliencia



INSTITUTO NACIONAL DE CIBERSEGURIDAD



Universidad  
de Cantabria

# Ficha técnica

- Grupo: 2º
- Conocimientos previos:
  - **Aritmética modular**
  - ***Snap!*** básico.
- Objetivos:
  - Descubrir la **criptografía**
  - Usar las ventajas de la **programación** para **agilizar** la encriptación y desenscriptación de mensajes.

# Criptografía

¿Qué es la CRIPTOGRAFÍA?

KRIPTOS - ocultar

GRAPHOS - escritura

# Criptografía

## Por Ocultación

Se busca la forma de esconder el mensaje.

- Esconder el mensaje en la cabeza de un esclavo .
- Esconder el mensaje en un texto .
- Esconder el mensaje con simetrías .
- Esconder el mensaje ...

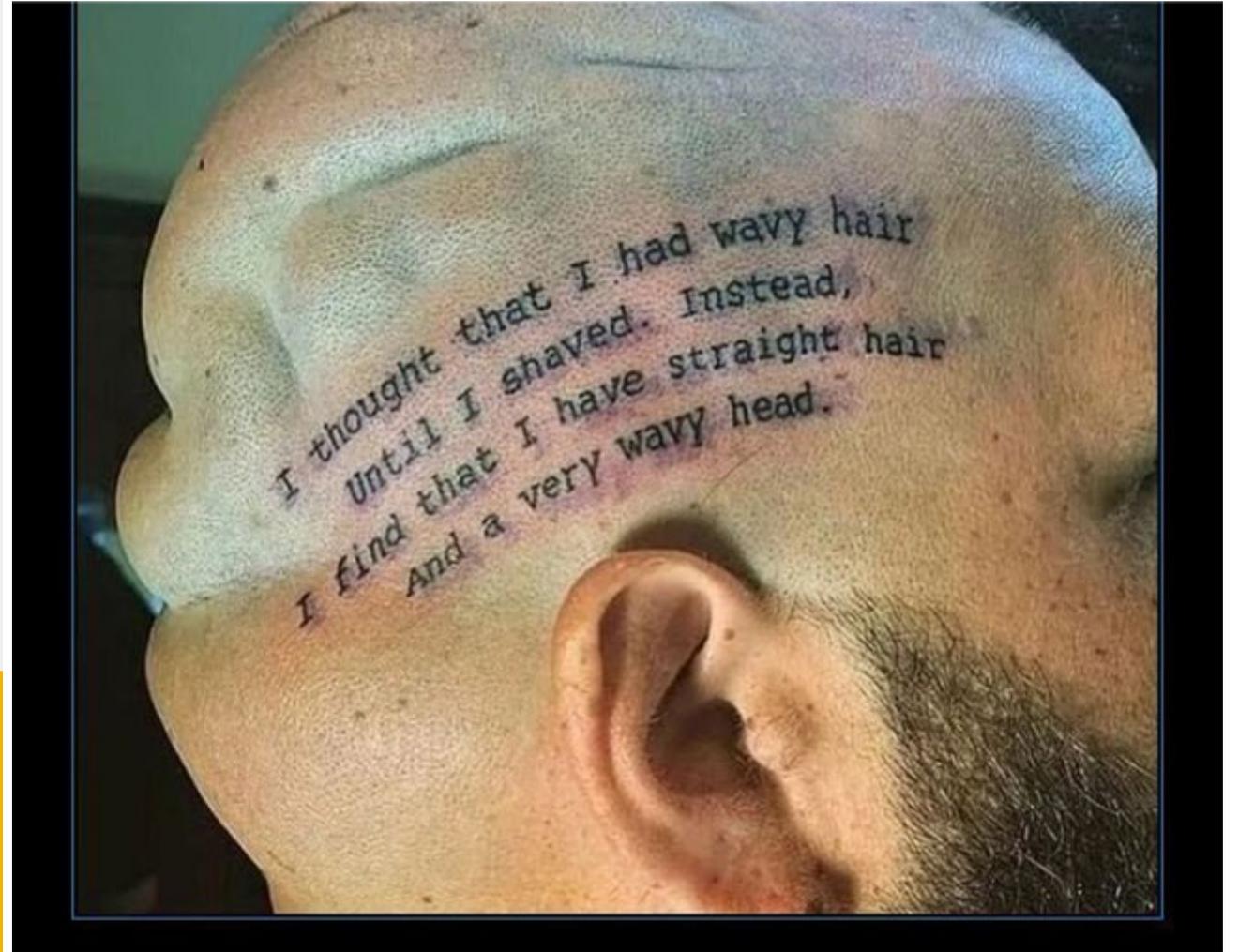
## CABEZA TATUADA

Se tatúa la cabeza rasurada de un esclavo y se le deja crecer el pelo.

### Problemas :

Supuesta fidelidad del esclavo

El esclavo debe llegar al destinatario.



Criptografía...

por Ocultación

## MENSAJE EN UN TEXTO

### Método :

Solamente algunas letras del texto tienen sentido real.

La clave y el texto viajan por separado.

### Problemas :

Si se pierde la clave o el texto, se pierde el mensaje.

Criptografía...

por Ocultación

*Despedida*

Distancia

Entre nuestros

Suaves cuerpos

Por

El abandono

De un sueño

Imposible

De

Amor

# ESCRITURA ESPECULAR

Método :

Se escribe el mensaje usando la simetría de un espejo.

Método usado por Leonardo Da Vinci.

Criptografía...

por Ocultación



## REJILLAS GIRATORIAS Y DE CARDANO

Método renacentista que consiste en repartir las letras en la base de tal forma que al superponer la rejilla perforada se pueda leer el mensaje.

La rejilla perforada tiene 8 posiciones distintas y no siempre es fácil leer el mensaje.

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

Criptografía...

por Substitución

## REJILLAS GIRATORIAS Y DE CARDANO

Método renacentista que consiste en repartir las letras en la base de tal forma que al superponer la rejilla perforada se pueda leer el mensaje.

La rejilla perforada tiene 8 posiciones distintas y no siempre es fácil leer el mensaje.

	U				N			P	
			A			S			S
	E			I					
		G							
					P				E
		R					L		
A			C			R		I	
	P			T			O		
		G				R			A
F			I		A				

Criptografía...

por Substitución

# Critografía

## Por Transposición

Cambia las posiciones de las letras en un mensaje.

- Método dientes de sierra
- Desordenar

## MÉTODO DIENTES DE SIERRA

Método :

Se escribe el mensaje en dos filas y se reescribe el mensaje tomando, por orden, una letra de cada fila.

Si se amplía el número de filas es más difícil descifrarlo.

**UCNRPIAPSTEOOGPROARFLIAA**

**UN PASEO POR LA  
CRIPTOGRAFIA**

Criptografía...

por Transposición

# Criptografía... por Transposición

Di ent es de Si err a

missatge **XVII SEMINARIO ESTALMAT**

Longitud **21**

files **3**

**XIMAOTMVSIREAA  
IENISLT**

**XVII SEMINARIO ESTALMAT**

X	I	M	A	O	T	M
V	S	I	R	E	A	A
I	E	N	I	S	L	T

**XIMAOTMVSIREAAIENISLT**

# Criptografía... por Transposició

Di ent es de Si err a

missatge **XVII SEMINARIO ESTALMAT**

Longitud **21** files **7**

**XISVNTIAAIRLSIM  
EOAMET**

**XVII SEMINARIO ESTALMAT**

X	I	S
V	N	T
I	A	A
I	R	L
S	I	M
E	O	A
M	E	T

**XISVNTIAAIRLSIMEOAMET**

## MÉTODO DIENTES DE SIERRA

### Programa Encriptación :

El primer acercamiento acostumbra a ser sencillo, ¿Qué puede fallar? ¿Qué se puede mejorar? ¿Dónde se desajusta el programa?

Con éstas preguntas rehacemos el programa las veces que haga falta.

Criptografía...

por Transposición

```
cuando se pulse bandera verde
  fijar missatge a 0
  fijar Longitud a 0
  fijar files a 1
  fijar mxifrat a 
  fijar PEntera a 1
  preguntar Anotate el missatge que vols encriptar. y esperar
  fijar missatge a respuesta
  fijar Longitud a longitud del texto missatge
  fijar missatge a mayúsculas del texto missatge
  preguntar En quantes files vols trencar el missatge? y esperar
  fijar files a respuesta
  fijar PEntera a suelo de Longitud / files
  para i = 1 hasta files
    para j = 1 hasta PEntera
      fijar lletra a letra (j - 1) x files + i de missatge
      fijar mxifrat a unir mxifrat lletra
    pensar mxifrat
```

## MÉTODO DIENTES DE SIERRA

### Programa DESencriptación :

Preguntas que debemos hacernos:

¿Cómo puedo deshacer la encriptación anterior? ¿Cuáles eran los puntos clave que me permitían esconder el mensaje?

Con éstas preguntas reacomodamos el programa las veces que haga falta.

Criptografía...

por Transposición

```
cuando se pulse la tecla d
  fijar missatge a 0
  fijar Longitud a 0
  fijar files a 1
  fijar mxifrat a 1
  fijar PEntera a 1
  preguntar Añota el mensaje criptado y esperar
  fijar missatge a respuesta
  fijar Longitud a longitud del texto missatge
  fijar missatge a minúsculas del texto missatge
  preguntar ¿En cuántas filas se ha roto el mensaje? y esperar
  fijar files a respuesta
  fijar PEntera a suelo de Longitud / files
  para i = 1 hasta files
    para j = 1 hasta PEntera
      fijar letra a
      letra (j - 1) x PEntera + i de missatge
      fijar mxifrat a unir mxifrat letra
    pensar mxifrat
```

## DESORDENAR

Escribimos el texto en horizontal y lo recuperamos en vertical.

Si además lo hacemos con una palabra clave i reordenamos las columnas según el orden alfabético de las letras de esa palabra clave, lo complicamos aún más.

H	O	L	A
Q	U	E	D
E	M	D	I
U	M	E	N
G	E	P	E
R	C	E	L
E	B	R	A
R	L	A	N
I	V	E	R
S	A	R	I



A	H	L	O
D	Q	E	U
I	E	D	M
N	U	E	M
E	G	P	E
L	R	E	C
A	E	R	B
N	R	A	L
R	I	E	V
I	S	R	A

Criptografía...

por Transposición

# Critografía

## Por Sustitución

Cambia las posiciones de las letras en un mensaje.

- Sustitución de algunos caracteres
- Método César
- Método Pigpen
- Método de Vigènere

# Critografía

## Por Substitución

Conserva la posición pero  
cambia las letras en un  
mensaje.

1N73LL1G3NC3

0261597H3802

874B1L17Y790

7064D4P73705

651CH4NG3248

-573PH3NH4WKING

# MÉTODO CÉSAR

	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
+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

El cifrado César consiste en sustituir cada letra del texto por la que está 3 lugares más adelante en el abecedario. Si cambiamos el valor 3 por otro, n, obtenemos otros casos. El valor sólo deben conocerlo el emisor y el receptor.

**FULSWRJUDILD =**

**=CRIPTOGRAFIA**

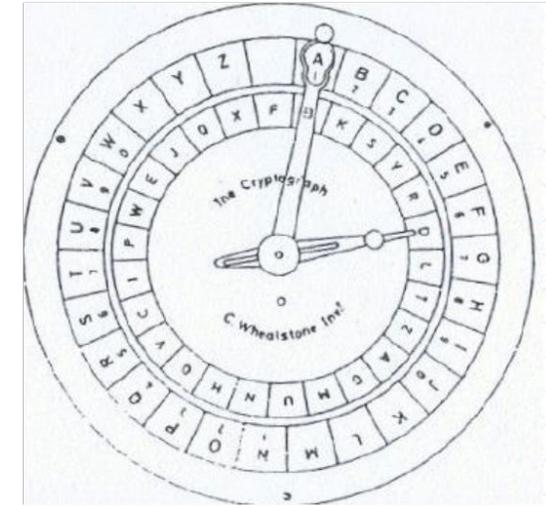
Criptografía...

por Substitución

# CÍRCULOS GIRATORIOS

Si usamos círculos donde las letras están ordenadas de formas distintas en ambos, la cantidad de códigos posibles es realmente exorbitante, sin embargo sigue siendo descifrable.

Ya los encontramos en el disco de Alberti (1450) o el criptógrafo de Wheatstone (1867).



Criptografía...

por Substitución

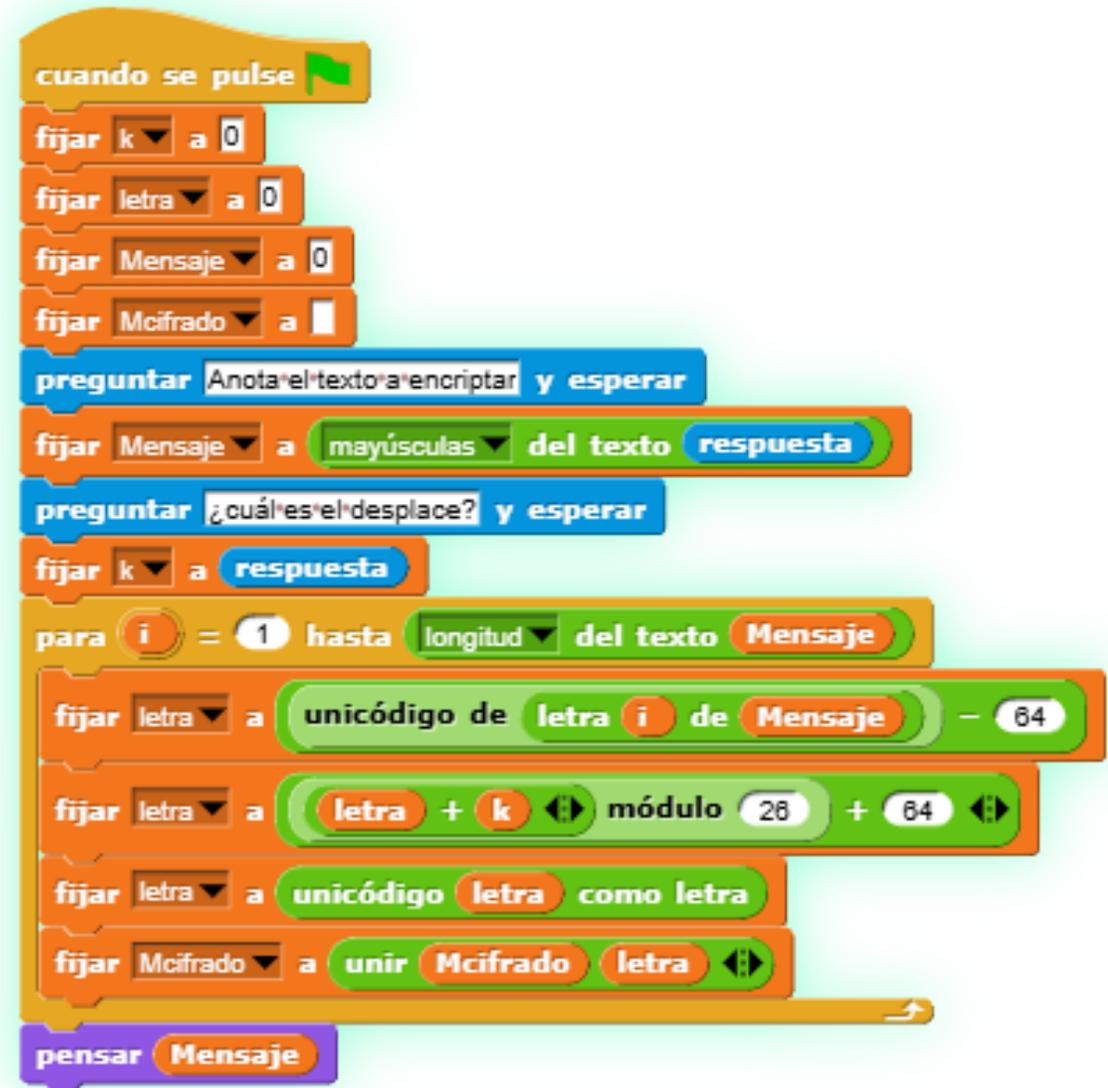
## Método CESAR

Ejercicio de encriptación con el método César usando la herramienta unicódigo para transformar letras en cifras.

Hay que prestar especial atención a acentos y caracteres como la tilde de la Ñ, etc.

Criptografía...

por Substitución



```
cuando se pulse
  fijar k a 0
  fijar letra a 0
  fijar Mensaje a 0
  fijar Mcifrado a 
  preguntar Añota el texto a encriptar y esperar
  fijar Mensaje a mayúsculas del texto respuesta
  preguntar ¿cuál es el desplace? y esperar
  fijar k a respuesta
  para i = 1 hasta longitud del texto Mensaje
    fijar letra a unicódigo de letra i de Mensaje - 64
    fijar letra a letra + k módulo 28 + 64
    fijar letra a unicódigo letra como letra
    fijar Mcifrado a unir Mcifrado letra
  pensar Mensaje
```

## César -2

Si desplazamos un solo elemento, en la palabra HAL la letra H pasa a la I, la A a la B y la L a la M, codificación que se usó en la película 2001: Una odisea del espacio en la que el ordenador que aparece se llamaba HAL, que equivaldría a IBM.

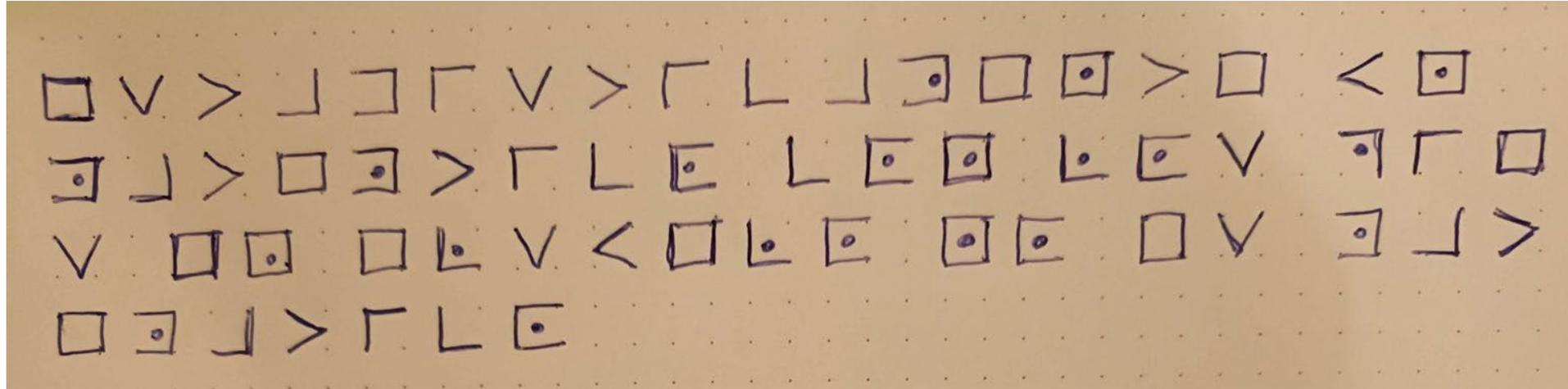


Criptografía...

por Substitución

## MÉTODO DE Pigpen

¿Te atreves a decodificar el siguiente mensaje?



Estadísticamente, un matemático con los pies en el suelo no es un matemático.

Criptografía...

por Substitución

## MÉTODO DE Pigpen

Sustituye cada letra por un símbolo, cogiendo la parte de la cuadrícula que la contiene, según el dibujo .

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	

Criptografía...

por Substitución

## MÉTODO DE VIGÈNERE

Se escoge una palabra clave y se sustituye cada letra del mensaje por la que ocupa la fila de la letra de la palabra clave i la columna de la del texto, correspondientes.

Invulnerable al análisis de frecuencias.

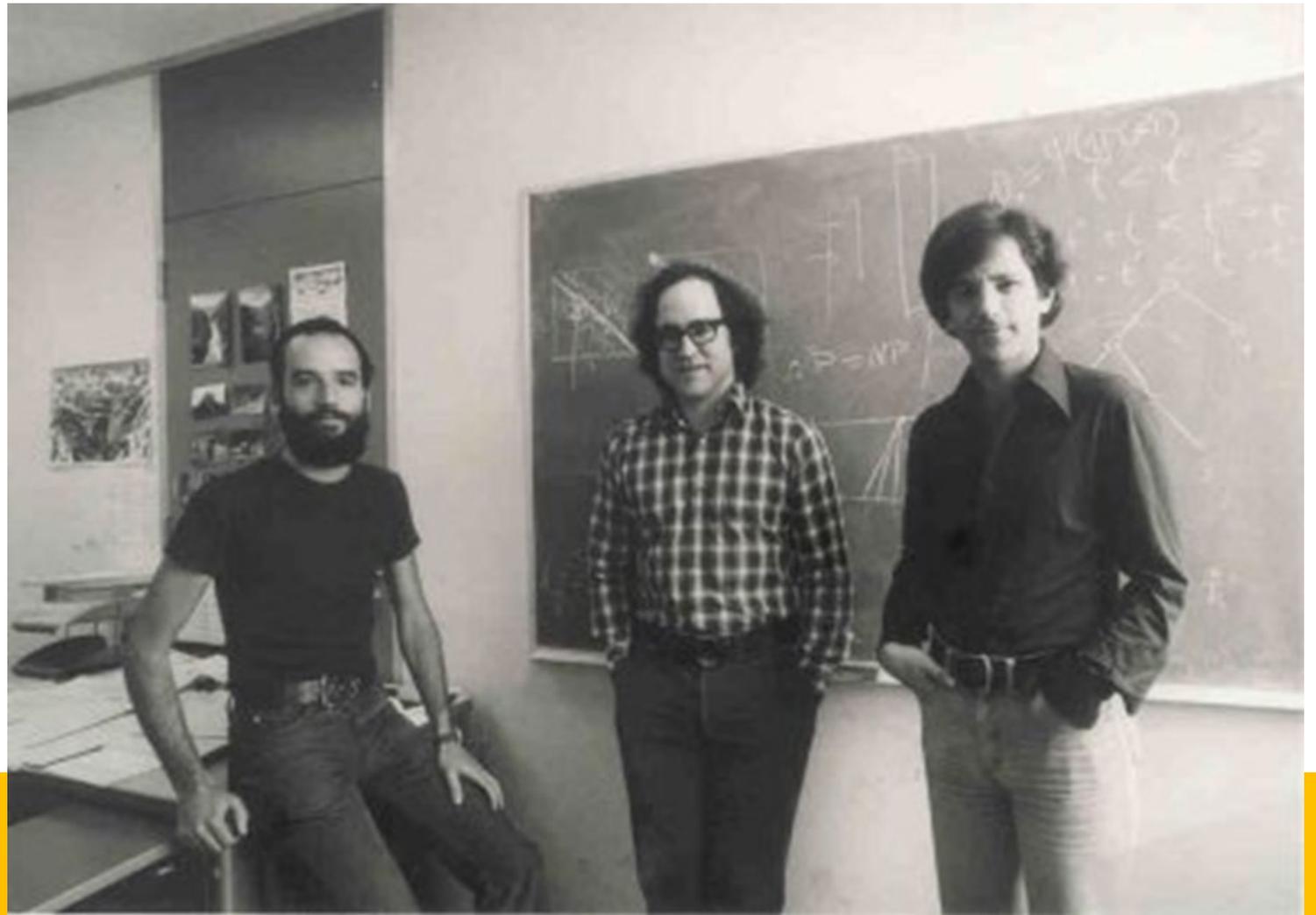
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	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
g	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
h	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
i	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
j	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
k	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
l	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
m	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
n	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
o	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
p	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
q	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
r	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
s	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
t	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
u	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
v	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
w	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
x	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
y	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
z	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

Criptografía...

por Substitución

## MÉTODO RSA

Su nombre sale de las iniciales de los tres matemáticos americanos que lo inventaron, en 1977: Ron **R**ivest, Adi **S**hamir i Leonard **A**dleman, del MIT.



Criptografía...

por Substitución

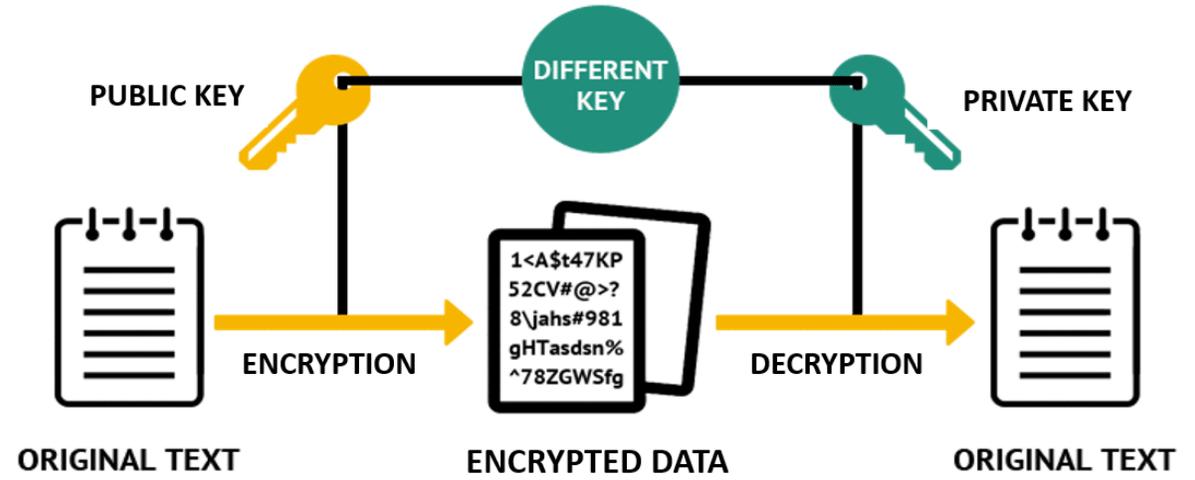
# MÉTODO RSA

Método de clave pública (N,e,d)

$N = p \cdot q$  (producto de dos primos)

$e$ , número invertible módulo  $M = (p-1) \cdot (q-1)$

$d$ , inverso de  $e$  módulo  $M$ .



Criptografía...

por Substitución

# MÉTODO RSA

$$N = 33, e = 3 \quad (p = 3, q = 11, d = 7)$$

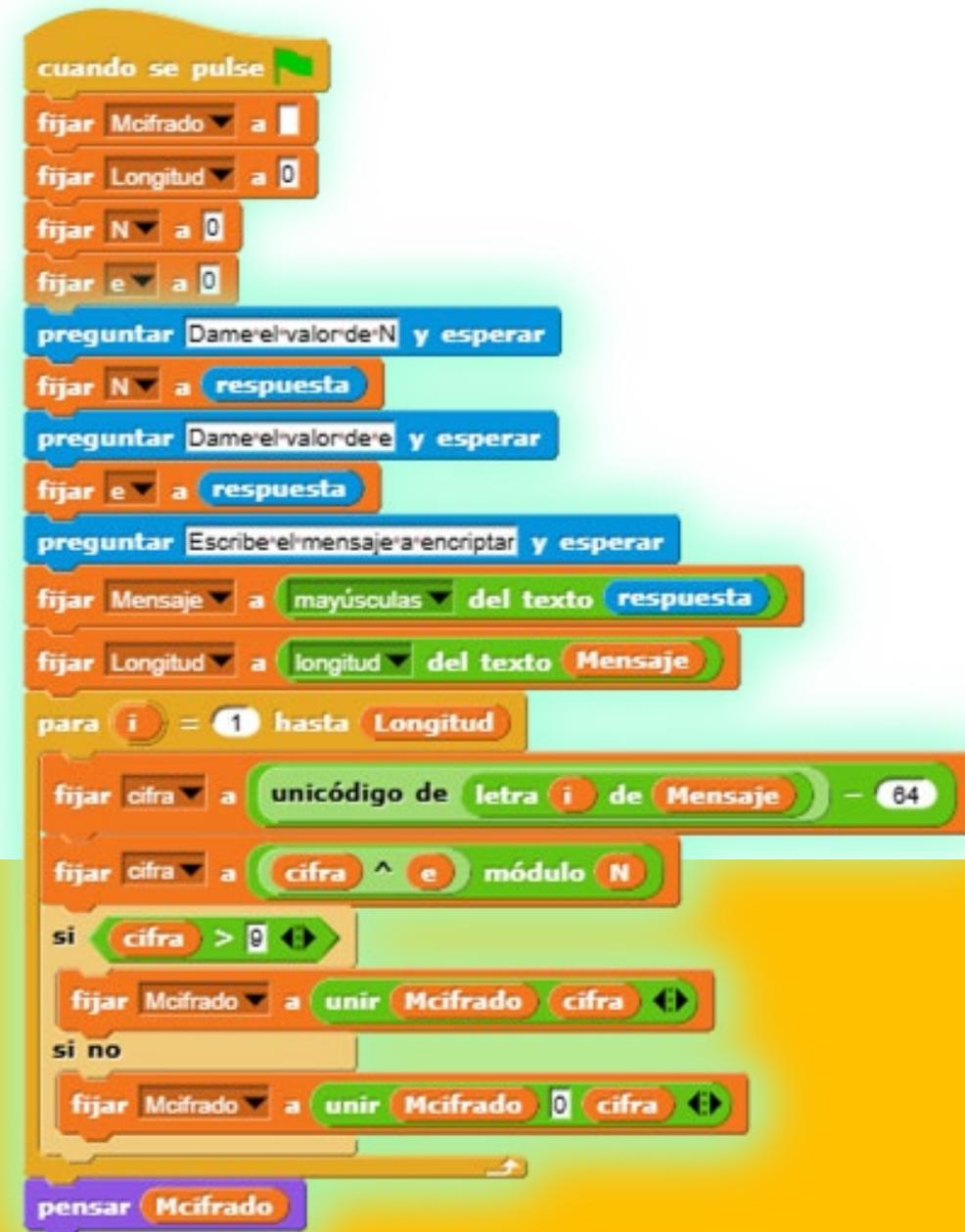
mensaje: **ESTALMAT - 05 19 20 01 12 13 01 20**

$$\begin{array}{ll} 5^3 = 125 \equiv 26 \pmod{33} & 19^3 = 6859 \equiv 28 \pmod{33} \\ 20^3 = 8000 \equiv 14 \pmod{33} & 1^3 = 1 \equiv 01 \pmod{33} \\ 12^3 = 1728 \equiv 12 \pmod{33} & 13^3 = 2197 \equiv 19 \pmod{33} \\ 1^3 = 1 \equiv 01 \pmod{33} & 20^3 = 8000 \equiv 14 \pmod{33} \end{array}$$

mensaje cifrado: **2628140112190114**

Criptografía...

por Substitución



```
cuando se pulse
  fijar Mcifrado a 
  fijar Longitud a 0
  fijar N a 0
  fijar e a 0
  preguntar Dame el valor de N y esperar
  fijar N a respuesta
  preguntar Dame el valor de e y esperar
  fijar e a respuesta
  preguntar Escribe el mensaje a encriptar y esperar
  fijar Mensaje a mayúsculas del texto respuesta
  fijar Longitud a longitud del texto Mensaje
  para i = 1 hasta Longitud
    fijar cifra a unicódigo de letra i de Mensaje - 64
    fijar cifra a cifra ^ e módulo N
    si cifra > 9
      fijar Mcifrado a unir Mcifrado cifra
    si no
      fijar Mcifrado a unir Mcifrado 0 cifra
  pensar Mcifrado
```



EXCMO. AYUNTAMIENTO  
DE CASTRO URDIALES



ESTÍMULO DEL TALENTO MATEMÁTICO



ESTALMAT  
Catalunya



REAL ACADEMIA DE CIENCIAS  
EXACTAS, FÍSICAS Y NATURALES  
DE ESPAÑA

# ¡MÁS OCHAS USUARIAS OCORRIÓ VUESTRA PRESENCIA!



C I E E M

Centro Internacional de Encuentros Matemáticos



Purposeful  
Ventures



Generalitat de Catalunya  
Departament  
d'Educació

Guillem Bonet

Pura Fornals



Financiado por  
la Unión Europea  
NextGenerationEU



GOBIERNO  
DE ESPAÑA

MINISTERIO  
PARA LA TRANSFORMACIÓN DIGITAL  
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO  
DE TELECOMUNICACIONES  
E INFRAESTRUCTURAS DIGITALES



Plan de  
Recuperación,  
Transformación  
y Resiliencia



INSTITUTO NACIONAL DE CIBERSEGURIDAD



Universidad  
de Cantabria