Criptografía

Taller de Talento Matemático

24-11-2017

José Luis Tornos

ÍNDICE

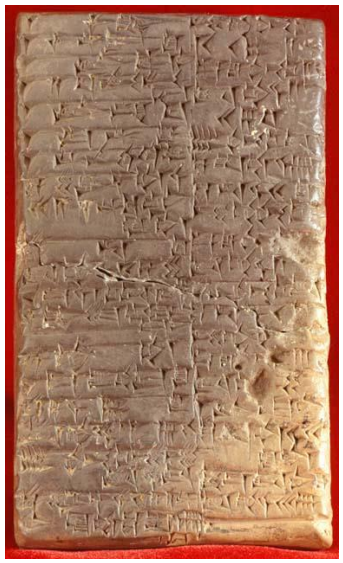
- ¿Codificar o cifrar?
- Criptografía clásica: ejemplos de criptografía clásica
- Criptografía moderna
- Ejemplos de criptografía moderna

Codificar o cifrar

- **Codificar:**
  - **2.** tr. Transformar mediante las reglas de un código la formulación de un mensaje.
- **Cifrar:**
  - **1.** tr. Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.

Asociación Taller de Talento Matemático de Aragón
TTM
www.unizar.es/ttm

Codificar



ABCDEFGHIJKLMN

ÑOPQRSTUVWXYZ

1234567890

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Cifrar

- **Cifrar:**
  - **1.** tr. Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.

DÑHD LDFWD HVW ➔ ¿?

Asociación Taller de Talento Matemático de Aragón
TTM
www.unizar.es/ttm

Criptografía clásica

- **Sustitución:** Se sustituyen los símbolos del mensaje por otros.

- **Transposición:** Los símbolos que componen el mensaje se desordenan siguiendo unos patrones preestablecidos.

Criptografía clásica

Transposición

Escítala: Sistema de transposición que emplea un par de varas con el mismo diámetro y en el que se enrollaba una tira de cuero en la que se escribía el mensaje

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Criptografía clásica

Transposición

Nuestro sistema: raretla le nedro ed sal sartel ed anu arbalap

Alterar el orden de las letras de una palabra

Otro sistema: frase una de palabras las sitio de cambiar

Cambiar de sitio las palabras de una frase

Y otro: tlaeanrr el droen de sal telras jedaodn sal rapes iuqates

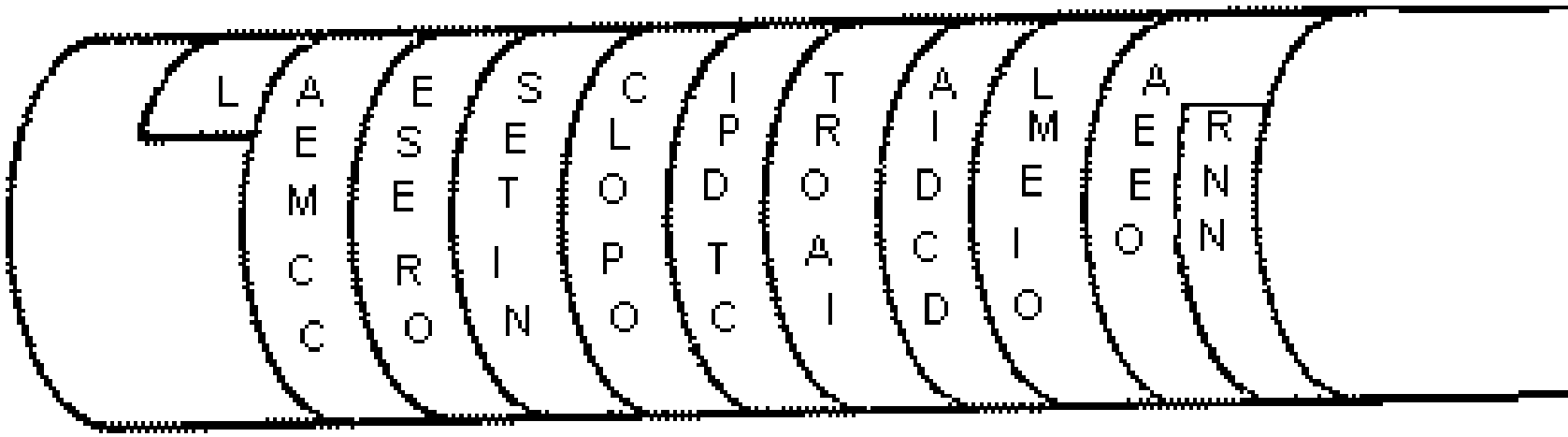
alternar el orden las letras dejando las pares quietas

Asociación Taller de Talento Matemático de Aragón

TTM

www.unizar.es/ttm

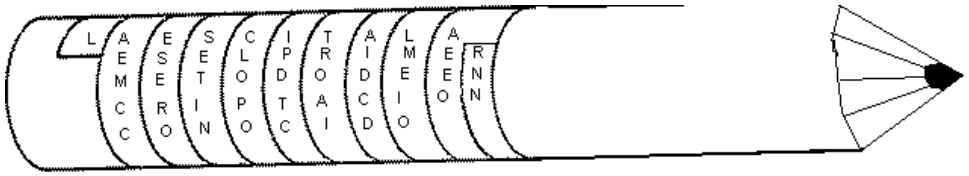
Criptografía clásica



LCCMEAORESENITESOPOLCCTDPIIAORTDCDIAOIEMLOEEANNR

Asociación Taller de Talento Matemático de Aragón
TTM
www.unizar.es/ttm

Criptografía clásica



HCEAOSCNDEUIRNFEBISOCTLIOIL

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Criptografía clásica

Sustitución

El cifrado César: Desplazar cada letra tres posiciones a la derecha. Si alcanzas el final, sigues desde el principio

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

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Criptografía clásica

Cifrado César

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

DÑHD LDFWD HVW

ALEA IACTA EST

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	26
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

$$C = M + 3 \pmod{27}$$

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Criptografía clásica

Sustitución

El cifrado Polibyus: Se construye una matriz como las dos de ejemplo en el que se introducen la letras del alfabeto.

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

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Se sustituye cada una de las letras por sus coordenadas en la tabla.

Criptografía clásica

El cifrado Polibyus

BC CD ED AE DC EA BD AE DB CC AE DC

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

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

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

Criptografía clásica

El cifrado Polibyus

BC CD ED AE DC EA BD AE DB CC AE DC

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

Hoy es viernes

Asociación Taller de Talento Matemático de Aragón
www.unizar.es/ttm

Criptografía clásica

Sustitución

El cifrado de Vigenère: cifrado de sustitución con la base del cifrado César, pero en el que el desplazamiento de las letras varía dependiendo de una clave que se repite. El cifrado de César es un cifrado Vigenère con clave “D”

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	26
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

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

- Ejemplo: Clave “Taller”

T ≡ 20 (mod 27)

A ≡ 0 (mod 27)

L ≡ 11 (mod 27)

L ≡ 11 (mod 27)

E ≡ 4 (mod 27)

R ≡ 18 (mod 27)

Mensaje a cifrar: Atacaremos al amanecer

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	26
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

A	T	A	C	A	R	E	M	O	S	A	L	A	M	A	N	E	C	E	R
T	A	L	L	E	R	T	A	L	L	E	R	T	A	L	L	E	R	T	A

Mensaje	0	20	0	2	0	18	4	12	15	19	0	11	0	12	0	13	4	2	4	18
Clave	20	0	11	11	4	18	20	0	11	11	4	18	20	0	11	11	4	18	20	0
Suma	20	20	11	13	4	36	24	12	26	30	4	29	20	12	11	24	8	20	24	18
Suma (mod 27)	20	20	11	13	4	9	24	12	26	3	4	2	20	12	11	24	8	20	24	18

Mensaje cifrado	T	T	L	N	E	J	X	M	Z	D	E	C	T	M	L	X	I	T	X	R

- Ejemplo: Clave “Taller”

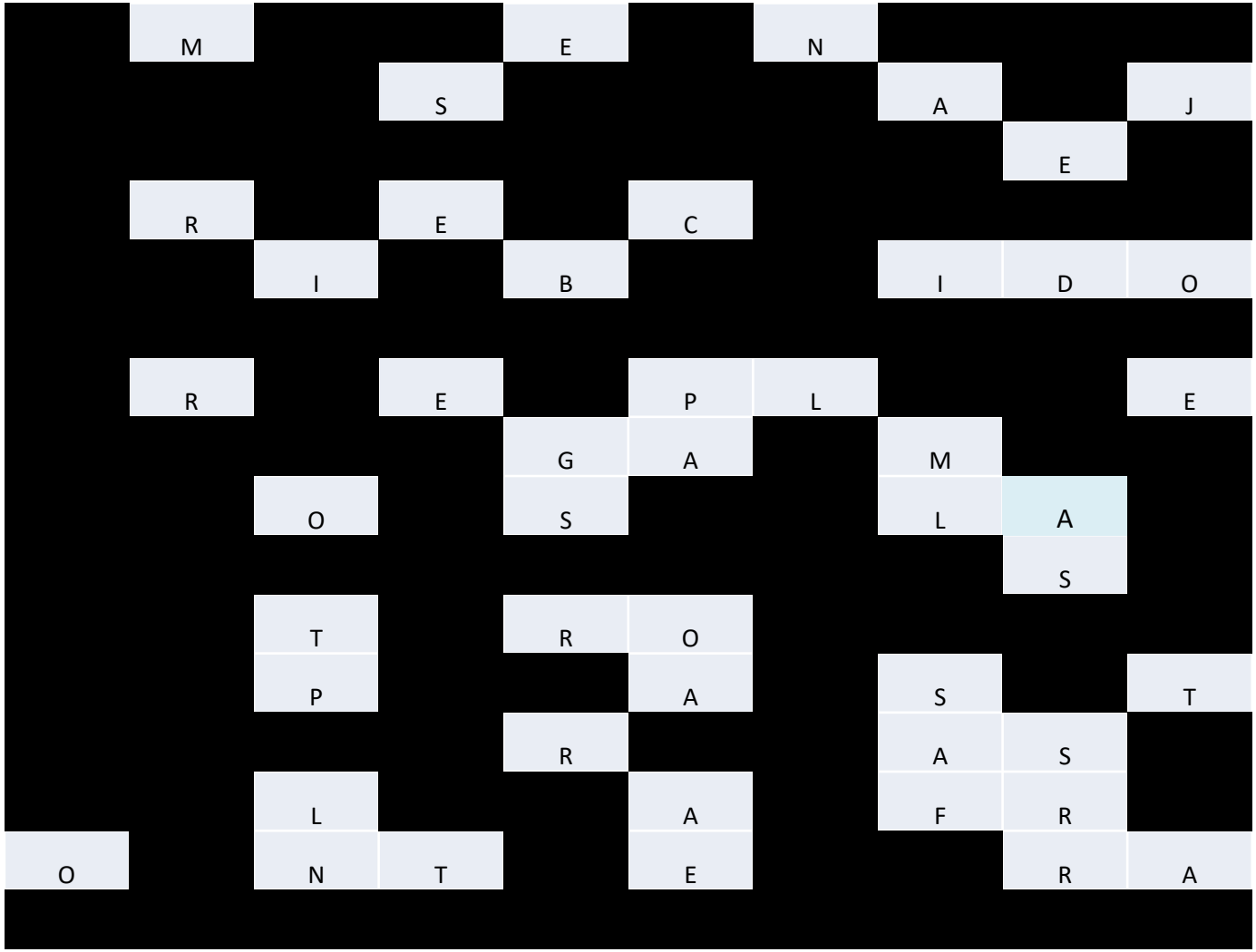
T ≡ 20 (mod 27) A ≡ 0 (mod 27) L ≡ 11 (mod 27) L ≡ 11 (mod 27) E ≡ 4 (mod 27) R ≡ 18 (mod 27)

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	26
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

Respuesta: LENSFZWO

	L	E	N	S	F	Z	W	O
	T	A	L	L	E	R	T	A
Mensaje cifrado	11	4	13	19	5	26	23	15
Clave	20	0	11	11	4	18	20	0
Resta	-9	4	2	8	1	8	3	15
Resta (mod 27)	18	4	2	8	1	8	3	15
Mensaje en claro	R	E	C	I	B	I	D	O

REJILLA DE CARDANO



ESTEGANOGRAFÍA

- La esteganografía (steganos) cubierto u oculto, y (graphos) escritura, es la parte de la criptología en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.
- Es decir, se trata de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

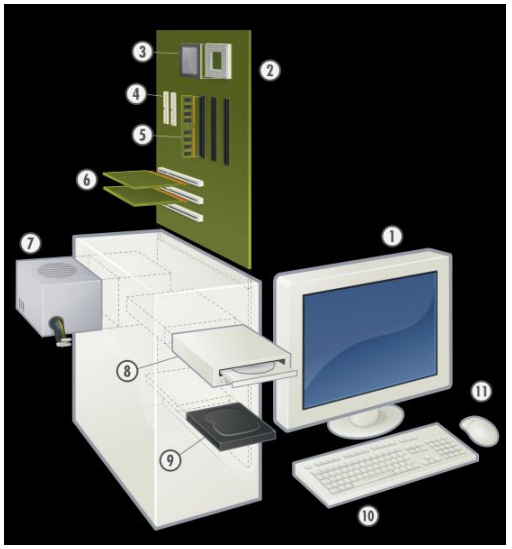
Criptografía clásica

- **Sustitución** y **Transposición**

- **¿Son seguros?...**

No son seguros
Existe técnicas de criptoanálisis como análisis de frecuencias que los rompen

Criptografía moderna



Asociación Taller de Talento Matemático de Aragón

TTM

www.unizar.es/ttm

Criptografía moderna

- Empleo de mecanismos electromecánicos: máquina enigma

- Empleo de ordenadores: criptografía simétrica y asimétrica

Criptografía moderna

- Máquina enigma:
  - Empleada por los alemanes en la 2ª Guerra Mundial
  - Emplea rotores y contactos eléctricos
  - Se varían las claves y el cifrado de una misma letra no siempre es el mismo

Criptografía moderna

- Máquina enigma:

http://enigmaco.de/enigma/enigma.swf

Asociación Taller de Talento Matemático de Aragón
www.unizar.es/ttm

Criptografía moderna

- Basada en aritmética modular
- Conexión entre ordenadores
- Cifrados simétricos y asimétricos

Criptografía moderna

- RSA (Rivest-Shamir-Adleman)
  - Dos primos: “p” y “q”
  - Módulo n = pq
  - Clave pública e primo respecto a $\phi(n) = (p-1)(q-1)$
  - Clave privada d ➔ $ed \equiv 1 \pmod{\phi(n)}$

  – Cifrado: $C \equiv M^e \pmod{n}$

  – Descifrado: $M \equiv C^d \pmod{n}$

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

RSA

- Clave pública (e, n)
- Clave privada (d)
  - Cifrado: $C \equiv M^e \pmod{n}$
  - Descifrado: $M \equiv C^d \pmod{n}$

http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/ejmrsa.html

Asociación Taller de Talento Matemático de Aragón
TTM
www.unizar.es/ttm

RSA

http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/ejmrsa.html

RSA

- Clave pública (3, 33)
- Clave privada (7)

- Cifrado: $C \equiv M^e \pmod{n}$
- Descifrado: $M \equiv C^d \pmod{n}$

Mensaje cifrado: 1 15 1 31 1

Asociación Taller de Talento Matemático de Aragón
TTM
www.unizar.es/ttm

RSA

- Clave pública (3, 33)
- Clave privada (7)

- Cifrado: $C \equiv M^e \pmod{n}$
- Descifrado: $M \equiv C^d \pmod{n}$

Mensaje cifrado: 1 15 1 31 1

Descifrar:

$1^7 = 1 \rightarrow 1 \pmod{33} \equiv 1$

$15^7 = 170859375 \rightarrow 170859375 \pmod{33} \equiv 27$

$31^7 = 27512614111 \rightarrow 27512614111 \pmod{33} \equiv 4$

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

RSA

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
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	27

Mensaje : 1 27 1 4 1

Descifrar:

1 ➔ A; 27➔ Z; 1➔ A; 4 ➔ D; 1 ➔ A

Mensaje en claro: AZADA

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

RSA

- Clave pública (3, 33)
- Clave privada (7)

- Cifrado: $C \equiv M^e \pmod{n}$
- Descifrado: $M \equiv C^d \pmod{n}$

Para cifrar elevar a 3 y reducir módulo 33

Si queremos cifrar la palabra azada con a ≡ 1;z ≡ 27; d ≡ 4

$1^3=1$ ➔ 1 (mod 33) ≡ 1

$27^3=19683$ ➔ 19683 (mod 33) ≡ 15

$4^3=64$ ➔ 64 (mod 33) ≡ 31

Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

Criptografía asimétrica

- Cifrar un mensaje
- Firmar un mensaje

Resumen

- **Criptografía clásica**:
  - Transposición
  - Sustitución

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

Divertida pero insegura

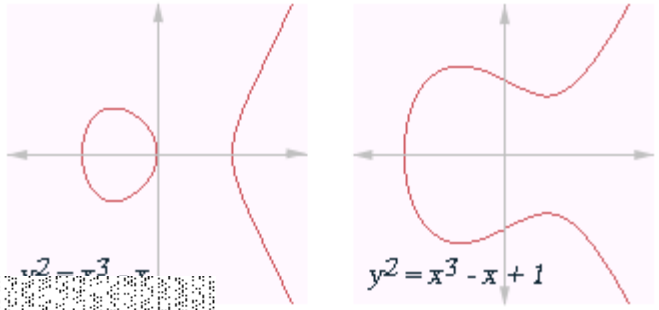
Asociación Taller de Talento Matemático de Aragón

www.unizar.es/ttm

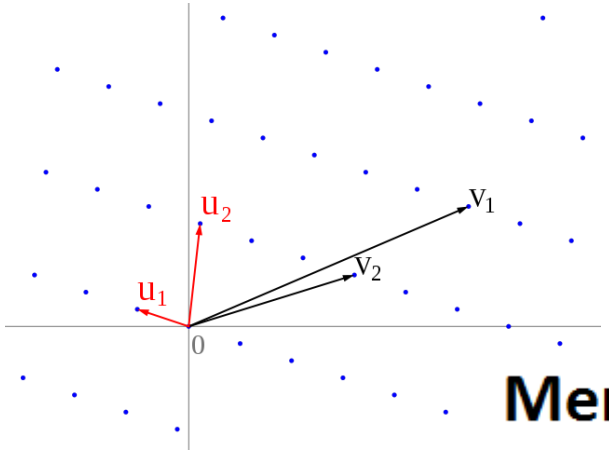
Resumen

- **Criptografía moderna**:

Segura y …¿divertida?



Fermat



Hipótesis de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}.$$

Mersenne

Sophie Germain

Asociación Taller de Talento Matemático de Aragón

TTM

www.unizar.es/ttm

Bibliografía y referencias

- Página de la asignatura de criptografía de la universidad de Zaragoza:

  criptosec.unizar.es

- Los códigos secretos. Simon Singh

- Imágenes: Wikipedia

Taller de Talento Matemático

Asociación TTM de Aragón

www.unizar.es/ttm

Muchas gracias por vuestra atención

¿?

Asociación Taller de Talento Matemático de Aragón

TTM

www.unizar.es/ttm