

Prólogo

”La Matemática es la más grande aventura del pensamiento”

Jesús Mosterín

”Al igual que las ciencias, la Matemática es una especie de juego donde el universo hace de contrario. Los mejores matemáticos, y los mejores profesores de Matemáticas, son evidentemente quienes mejor comprenden las reglas del juego y gozan experimentando la emoción de jugar”

Martin Gardner

La enseñanza de las Matemáticas, y sobre todo la motivación, en un Instituto de Secundaria es una labor de gran dificultad. La queja de muchos alumnos es ¿por qué nos enseñas estas matemáticas que nunca las usaremos en nuestra vida diaria?

La única mejora en la enseñanza de las Matemáticas con la LOGSE fue la incorporación de una nueva asignatura optativa en la ESO: El Taller de Matemáticas. Con un programa atractivo, podíamos acercar esta asignatura a los alumnos que hasta ahora habían fracasado en los estudios clásicos de Matemáticas. Es esta la razón de estos materiales, hasta ese momento apenas había textos para la nueva asignatura. Pero al igual que la LOGSE, El Taller de Matemáticas desapareció. Y hace dos cursos, en el primer ciclo de secundaria, aparece una optativa llamada ”optativa de ámbito científico”.

El material está estructurado en tres grandes bloques y una actividad extraescolar:

- Números y problemas.
- Geometría.
- Matemáticas en la vida cotidiana.
- Excursión por el monte Roldán.

Cada uno de estos bloques se divide en varios capítulos. Es obvio que estos capítulos están desarrollados siguiendo una iniciativa personal que quizás no concuerde con los gustos de cada lector. Y en todos los capítulos se incluye una biografía de destacados matemáticos relacionados con el tema tratado.

Y aunque no sean personas, sin su existencia esta tarea habría resultado imposible. Me refiero a Internet y a \LaTeX . El uso de Internet posibilita manejar una biblioteca, un archivo fotográfico, un diccionario, etc sin movernos de casa. \LaTeX permite escribir libros de una forma relativamente sencilla y sin estar vendidos a ciertos monopolios.¹

¹Bill Gates traducido a lenguaje hexadecimal se escribe 666.

Parte I

Números y problemas.

Capítulo 1

Criptografía

1.1 Introducción histórica

En el diccionario de la Real Academia de la Lengua aparece la definición clásica de criptografía: *arte de escribir con clave secreta o de un modo enigmático*. Hasta los años 50 se le consideró un arte, es con los trabajos de Shannon cuando pasa a ser una ciencia.

Desde la antigüedad indios, chinos, babilonios poseían signos equivalentes a las letras de sus alfabetos con los que comunicaban ordenes secretas a sus emisarios, en especial en tiempos de guerra.

Uno de los métodos más originales consistía en afeitarse la cabeza de un esclavo y escribir sobre su piel el mensaje que quería mandarse, esperando a que el pelo creciera podía enviarse al emisario sin que nadie sospechase que era transmisor de información.

En Esparta, durante los enfrentamientos con Atenas, se utilizaban largas tiras de papel sobre las que escribían una vez enrolladas sobre un bastón. Cuando se desenrollaba la tira resultaba ilegible para cualquiera que desconociera el método o no tuviera un bastón del mismo grosor.

Julio Cesar, en la Guerra de las Galias, utilizaba un sistema simple de sustitución para comunicarse con sus ejércitos.

La República Veneciana mezclaba caracteres griegos o hebraicos con los latinos al transmitir mensajes.

En el siglo XV aparecen los primeros tratados, el más importante el de Vigenere con un método de cifrado que lleva su nombre. En España, en 1738, Cristobal Rodríguez escribe el primer libro conocido.

Es en nuestro siglo, durante las dos guerras mundiales, cuando la criptología sufre un fuerte impulso ante la necesidad de comunicaciones confidenciales en los terrenos militar y diplomático. Es curiosa la utilización en el ejército de EEUU de indios navajos cuyo idioma no puede ser aprendido por alguien que no haya sido criado con ellos.

En la segunda mitad del siglo XX, con los avances de la informática, hay

un desarrollo inusitado de la criptología. No sólo para su uso en el terreno militar y en el diplomático, sino también para la confidencialidad en las operaciones comerciales.

Para terminar es obligatorio recordar el uso de la Criptografía en la obra de *Edgar Alan Poe El escarabajo de oro* donde escribe: "Se puede dudar que el ingenio humano sea capaz de construir un ingenio de este tipo que el ingenio humano sea capaz de descifrar". O también en el *Diccionario Filosófico* de *Voltaire*: "Los que se vanaglorian de saber leer cartas cifradas son más charlatanes que los que dicen saber descifrar un idioma que no conocen"

1.2 Cifrados monoalfabéticos: la cifra de Cesar.

Atribuido a Julio Cesar quien lo crearía durante la Guerra de las Galias. Consiste en sustituir cada letra del mensaje por otra que esté k posiciones detrás en el alfabeto. Julio Cesar siempre tomaba $k=3$, es decir, si el alfabeto español está formado por las letras

$$A, B, C, D, E, F \dots$$

cada una se sustituye por la letra que ocupa la misma posición después de correr tres posiciones el alfabeto.

$$D, E, F, G, H, I \dots$$

Así la palabra Cesar se sustituye por *FHVDU*. Si en el mensaje aparecen espacios o cualquier signo ortográfico (, . : ;) no los tendremos en cuenta. Si queremos enviar

mensaje enviado ayer

se convierte en

phqvdmhhqyldgrdbhu

Criptoanalizar este criptosistema es muy sencillo (porque ha sido muy sencilla su construcción) por fuerza bruta (probar todas las claves) variando k desde 1 a 26. Para descifrar tenemos que escribir dos alfabetos en dos papeles distintos. Ponemos un alfabeto encima del otro y vamos desplazando el de abajo hasta ver cuando el mensaje cifrado tiene sentido.

Ejercicio 1.2.1 *Construir la tabla para $k=7$ y traducir el mensaje "El paquete llegara a las once de la noche en el último tren"*

Ejercicio 1.2.2 *¿Cuál es el mensaje que se ha enviado y con qué clave k ?*
DKRUD KH FDPELDGR OD FODYH

El método de Cesar es un caso particular de los métodos de sustitución simple pues cada signo se sustituye por otro y siempre resultará el mismo. Este método consiste en hacer una permutación arbitraria de las letras, a cada letra se le hace corresponder otra letra. El alfabeto normal

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

lo sustituimos por

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

y el mensaje

MENSAJE ENVIADO AYER

se transmite como

CUDKVNNUUDQOVTFVXUJ

En total tendremos (usando la eñe)

$$27! = 10.888.869.450.418.352.160.768.000.000$$

sólo 10.888 **cuatrillones** de claves. Y si no usamos la eñe tendremos

$$26! = 403.291.461.126.605.635.584.000.000$$

403 **cuatrillones** de claves

Con este pequeño número de claves no podemos recurrir a la fuerza bruta y un buen método de criptoanálisis consistirá en el recuento de frecuencias: hacer un análisis de la frecuencia con que aparecen en el texto las letras y comparar con tablas standard de frecuencias. En el último mensaje la letra más repetida es la U, como en español la letra más frecuente es la E, es muy probable que la E se haya sustituido por la U.

Las letras que más aparecen en español son (por orden de más a menos frecuente):

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

El primer grupo está formado por letras de muy frecuente aparición constituyendo un 68% de la letras del mensaje. La E y la A destacan abrumadoramente en castellano y son las primeras que debes buscar. El siguiente grupo lo constituyen letras de aparición menos frecuente, un 25%. En el último grupo aparecen letras muy poco frecuentes que a menudo conviene descartar sin que importen demasiado para entender el mensaje.[3]

Ejercicio 1.2.3 Construir la tabla para un criptograma de sustitución simple y mandar un mensaje.

Ejercicio 1.2.4 Usando el análisis de frecuencias intentar descifrar el siguiente mensaje sabiendo que se ha cifrado la ñ
 UH CBS TSNOMGDS SNKS ZSRNUIS HY MRLMKY SR HU OURKMRU,
 UXYDU ZS SRDYHHY EUDU GUOMHMKUD SH TSNOMGDUTY Q
 CBS NSU GUOMH SH SISDOMOMY.

FRECUENCIAS RELATIVAS DE APARICION DE LAS LETRAS EN EL IDIOMA ESPAÑOL.

A 11.53	B 1.09	C 5.08
D 4.57	E 13.32	F 0.97
G 0.89	H 0.96	I 7.63
J 0.33	K 0.13	L 5.01
M 3.94	N 7.26	O 8.66
P 2.63	Q 0.86	R 5.77
S 5.50	T 5.82	U 4.02
V 0.76	W 0.09	X 0.28
Y 0.65	Z 0.26	

1.3 Cifrados polialfabéticos: Gronsfeld y bífido.

El cifrado polialfabético consiste en usar más de un alfabeto cifrado para poner en clave el texto y se cambia de uno a otro según se pasa de una letra del mensaje a otra.

Un primer caso es el cifradoalfabeto de Gronsfeld y vamos a verlo con un ejemplo de las tablas, ver figura 1.1, que se usaban antes de la era de los ordenadores.

Ahora cogemos una serie de dígitos como clave, por ejemplo 1203456987 y vamos a cifrar el mensaje EMBARCAMOS AL ANOCHECER. Escribimos la clave debajo del texto original las veces que sea necesario

EMBARCAMOS AL ANOCHECER
 1203456987 12 034569871

y sustituimos cada letra por la correspondiente del alfabeto que indica el número debajo suyo

HRDHCROLL DQ CUZPYGZXU