EL JUEGO DE LOS MENSAJES SECRETOS

1. Escondiendo mensajes

Si queremos enviar un mensaje a alguien sin que nadie se entere, nos tendremos que inventar la forma de esconderlo. Se sabe que en la antigua Grecia, Histieo de Mileto, siendo prisionero de los persas en Susa, pudo enviar un mensaje secreto a su padre Aristágores incitándole al ataque contra los persas. Para ello, se sirvió de la siguiente estratagema: afeitó la cabeza de uno de sus hombres y le tatuó en la piel un texto en el que incitaba a Aristágores a rebelarse contra los persas. Luego, sólo tuvo que esperar a que le volviera a crecer el pelo, y le envió a a Aristógares con una carta absolutamente inocente. Cuando el mensajero llegó a su destino, informó de que debían afeitarle la cabeza, para poder conocer el verdadero mensaje.

Otros métodos para esconder mensajes a lo largo de la historia han sido:

- También en la antigua Grecia, utilizaban tablillas de madera, donde se grababa el mensaje, y que luego se cubría con cera
- En China, se escribía el texto en seda, se hacía una bolita recubierta de cera que luego se hacía comer al mensajero. Ahora, sólo había que tener un poco de paciencia (y un buen detergente...)
- También se han utilizado tintas invisibles, como el zumo de limón
- Los acrósticos son palabras o frases que se esconden en un texto. La forma más común son los poemas en los que la primera letra de cada verso forma la frase o palabra.

¿Y si alguien intercepta el mensaje? El código secreto

Si los persas hubieran pillado al mensajero de Histieo, seguro que no hubiera tenido que cortarse el pelo nunca más: seguramente se habría quedado sin cabeza ni siquiera. Y eso porque si el mensaje se interceptaba se podía leer perfectamente y enterarse del contenido. Otra forma de escribir el mensaje es hacerlo de forma que sólo el destinatario lo pueda comprender.

Por ejemplo, podemos pactar un código con un amigo o amiga con unas cuantas palabras claves:

Palabra	*Código*	*Palabra*	*Código*	*Palabra*	*Código*
Amigo	Ático	Cenar	Camello	Bici	Ballena
Amiga	Águila	Merendar	Murciélago	Moto	Mamífero
Cantar	Conejo	Encontrar	Elefante	Escuela	Ecología
Dormir	Domingo	Perder	Perro	Casa	Cuchara
Salir	Serpiente	Abrir	Araña	Mi	Molino
Entrar	Estrella	Cerrar	Caballo	Tu	Tucán

¿Qué podemos interpretar si recibimos un mensaje como este?

Elefante Serpiente Ecología Murciélago Tucán Cuchara

Encontrar Salir Escuela Merendar Tu Casa

Nos encontramos a la salida de la escuela para merendar en tu casa

Pero esto del código tiene algunos problemas:

- Hay demasiadas palabras que memorizar (aunque hay reglas de memoria que puedan servir – en nuestro código la palabra y la clave empiezan siempre por la misma letra-)
- Para hacer mensajes más complicados, necesitaremos más palabras, con lo que el código será cada vez más grande.
- Si alguien intercepta el código se acabó el secreto: tendremos que inventar un código nuevo.

Solución: Transformar el mensaje

Una solución consiste en transformar el mensaje de forma que quede ireconocible para cualquier persona que desconozca el método de transformación. Eso implica que el emisor y el receptor están de acuerdo en una regla para transformar el mensaje. El emisor aplica la regla en un sentido y el receptor en sentido contrario.

Veamos un ejemplo: Supongamos que emisor y receptor se ponen de acuerdo en invertir el orden de las letras de cada palabra, como si escribiéramos al revés,

Nos encontramos a la salida de la escuela para merendar en tu casa

Son somartnocne a la adilas de al aleucse arap radnerem en tu asac

A esto que acabamos de hacer se le llama **cifrar** un mensaje. La criptografía, es, precisamente, la rama de la ciencia que se encarga de estudiar las reglas que transforman mensajes en formas aparentemente incomprensibles para quien no conozca la regla que se ha aplicado para cambiar el mensaje.

- Llamamos **texto plano** o claro a un texto sin cifrar
- **Texto cifrado** es aquel que está codificado (encriptado)
- La regla para cifrar y descifrar el mensaje se llama **algoritmo**
- La mayoría de los algoritmos tienen un método que permite descifrar con mayor rapidez, al que se le llama **clave**. Al método para encriptar un mensaje se le llama **cifra**.

Texto plano	Nos encontramos a la salida de la escuela para merendar en tu casa
Algoritmo	Invertir el orden de las letras de la palabra
Clave	No tiene
Texto cifrado	Son somartnocne a la adilas de al aleucse arap radnerem en tu asac

Desordenar o cambiar

Los métodos más antiguos que se conocen de cifrar un mensaje se basan en:

- Desordenar las letras (algoritmos de transposición)
- Cambiar unas letras por otras o por otros símbolos (algoritmos de sustitución)

2. Métodos de cambiar

2.1. El código ATBAS

El código ATBAS es un código utilizado en algunos textos religiosos hebreos. El nombre viene a partir de las letras del alfabeto hebreo

Àlef	Bet	Guímel	...	Reix	Sin (Xin)	Tau
א	ב	נ	...	ר	ש	ת

Y del resultado de juntar la primera letra con la última, la segunda con la penúltima:

Alef – Tau – Bet (a) – Sin

En nuestro alfabeto el código ATBAS se construiría poniendo dos filas con el alfabeto en orden usual arriba e inverso abajo:

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

(Observa que con media tabla (la media de la izquierda hasta la N) sería suficiente:

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

Ahora cada vez que toque escribir una A, escribiremos una Z, cada vez que toque una Y, escribiremos una B, etc

Ejemplo:

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

v h g z x s f o z o z x i r k g l t i z u r z

Ejercicio:

1. Codifica el mensaje

“Nos vemos esta noche”

2. Descifra el mensaje:

“Vizhv fnz eva”

3. Inventa un mensaje en este código.

2.2. La cifra de Polibi

Descrito por el historiador del siglo III a.C., Polibi, para codificar cada letra utiliza una tabla de doble entrada, en la que cada letra viene representada por dos números:

	1	**2**	**3**	**4**	**5**
1	a	b/v	c	d	e
2	f	g	h	i	j
3	k/q	l	m	n	ñ
4	o	p	r	s	t
5	u	w	x	y	z

Ejemplo:

Texto plano	**Texto cifrado**
dinosaurio	14 24 34 41 44 11 51 43 24 41

Con este código, se pueden utilizar los dedos de las manos para codificar cada letra. Así:

Esta letra sería 25 -> J

Ejercicios:

1. Codifica el mensaje

   "Quien roba a un ladrón"

2. Descifra el mensaje:

   45 24 15 34 15 13 24 15 34 11 35 41 44 14 15 42 15 43 14 41 34

3. Inventa un mensaje escrito en cifra Polibi.

2.3. La cifra Pig Pen

Se basa en situar cada letra del alfabeto sobre una cuadrícula 3 x 3 o sobre un aspa formada por dos rectas. Una de las cuadrículas y una de las aspas tendrá además un punto. A continuación cada letra se representa por los segmentos de cuadrícula o de aspa que la rodean:

EJERCICIOS

1. Codifica con Pig-Pen el siguiente mensaje:

"Me encanta escribir mensajes que la gente no comprende"

2. Descodifica el siguiente mensaje:

|‾| \/ > _| |_ |‾| < |·_ |·‾ |‾|

\/ > |·‾ ‾| |‾| |·_ _| |_ |‾ |‾

|·‾ _| ‾| |‾| ‾·| |‾ ‾| ‾·| |‾| |‾·|

3. Intercambia un breve mensaje con tu compañero o compañera

2.4. La cifra de César

El método de César consiste en desplazar cualquier alfabeto. La clave del código será el número de lugares que se desplaza. Julio César siempre utilizaba el mismo valor: el 3. Así, la tabla de sustitución quedaba:

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

Ejemplo:

Texto plano	Texto cifrado
dinosaurio	AFKMPXROFM

Puedes construir una regleta como la del modelo, para fabricar alfabetos de César:

Ejercicios:

1. Construye dos tiras una con el alfabeto completo y otra el doble de larga con dos alfabetos seguidos. Procura que la separación entre letra y letra sea siempre la misma. Nos servirán para construir distintos alfabetos de César.
2. Construye un alfabeto de César con clave G.
3. Codifica este mensaje con clave G:

   "Quedamos donde siempre"
4. Descifra este mensaje escrito con clave S:

   "Ihvwkhlh ustsddwkh wl vhf vafwkh"
5. Inventa un mensaje escrito con cifra César, con la clave que tú elijas

3. Métodos de desordenar

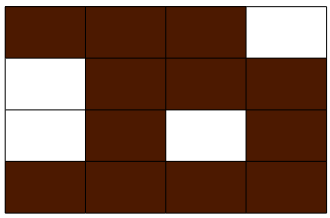
3.1. La rejilla giratoria

La rejilla giratoria

Lo primero que debe hacerse es fabricar una rejilla giratoria con huecos que hará de tapadera. La rejilla se construye de forma que:

- Tenga tantos huecos como la cuarta parte del total de la rejilla
- Al girar hasta cuatro veces, una casilla no puede quedar destapada dos veces
- Todas las casillas han de quedar destapadas alguna vez

Ejemplo:

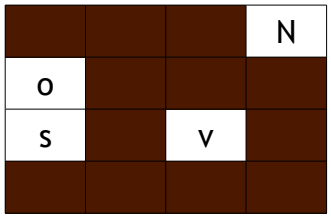


Ahora para codificar el mensaje, se prepara una tabla del mismo tamaño que la rejilla (en nuestro caso 4x4) y se copian ordenadamente de izquierda a derecha y de arriba abajo las letras en las casillas destapadas. Cuando se han terminado de llenar los huecos, se gira la rejilla en el sentido contrario a las agujas del reloj, y se sigue escribiendo el mensaje, y así sucesivamente hasta dar cuatro giros, momento en el que nos volvemos a encontrar en la posición inicial. Si el mensaje es más largo que el

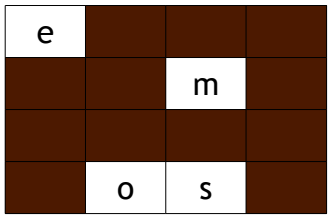
número de casillas de la tabla, se utiliza una nueva tabla, y si es más corto se completa con símbolos sin significado.

Ejemplo: “Nos vemos en el cine”

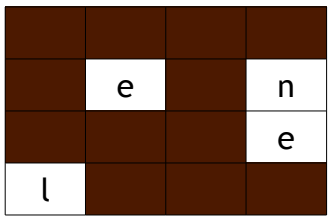
1)



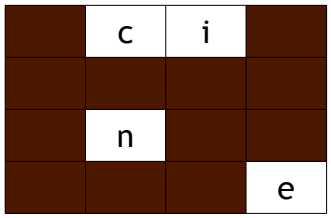
2)



3)



4)



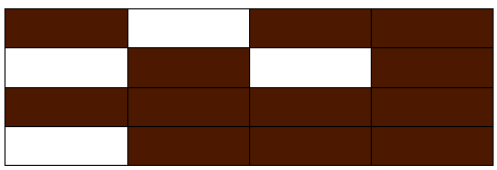
5)

e	c	i	n
o	e	m	n
s	n	v	e
l	o	s	e

“ecim oemn snve lose”

Ejercicios:

1. Inventa una rejilla giratoria 6 x 6 que reúna las condiciones necesarias para poder codificar. Intenta describir un método para construirla



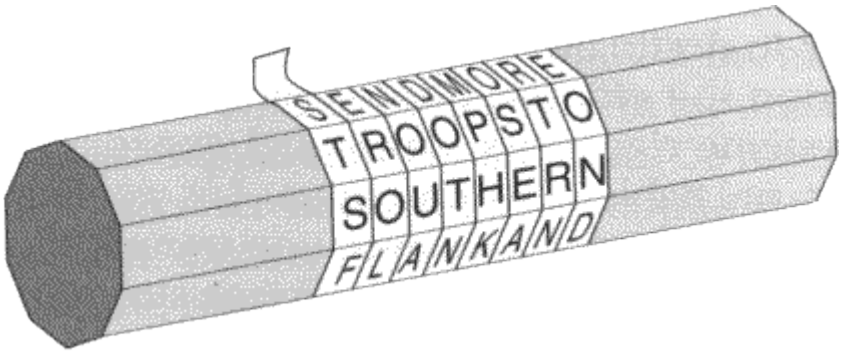
2. Codifica el mensaje “No te encuentro” con la rejilla:

3. Con la misma rejilla, descifra el mensaje: “aqte utee eoox xxmv”

4. Intercambia algún mensaje codificado con algún compañero o compañera.

3.2. La escítala espartana

En el siglo V antes de Cristo, los militares espartanos, para proteger el contenido de sus mensajes de los ojos de los enemigos, hacían lo siguiente:



1. Se enrollaba una cinta en un palo de madera de un diámetro determinado (En nuestro ejemplo un palo decagonal)
2. Se escribía el mensaje horizontalmente de izquierda a derecha.
3. Se desenrollaba la cinta y el mensaje quedaba escrito con las letras desordenadas.
4. La persona que recibía un mensaje, para leerlo, sólo necesitaba tener un palo del mismo diámetro y volver a enrollar la cinta.

3.3. La matriz: Combinación de desordenar y cambiar

La matriz

La escítala espartana se puede traspasar a una matriz (tabla) en la que lo único que se necesita conocer es el número de columnas.

Ejemplo:

s	i	v	i	e
n	e	s	a	l
b	a	r	t	e
i	n	v	i	t
o	x	x	x	x

“snbio ieanx vsrvx iatix eletx”

Este método también puede combinarse con el de desordenar las columnas a partir de una palabra clave, como se hacía con el método de ADFGVX.

<u>Ejemplo:</u>

1) Copiamos la tabla anterior, encabezándola con la palabra clave (por ejemplo: “libro”):

L	I	B	R	O
s	i	v	i	e
n	e	s	a	l
b	a	r	t	e
i	n	v	i	t
o	x	x	x	x

2) Reordenamos las columnas por orden alfabético:

B	I	L	O	R
v	i	s	e	i
s	e	n	l	a
r	a	b	e	t
v	n	i	t	i
x	x	o	x	x

3) Para acabar, se copia el mensaje de izquierda a derecha:

"visei senla rabet vniti xxoxx"

Ejercicios:

1. Codifica este mensaje con la palabra clave: "Bruja"

   "Guarda bien este secreto"

2. Descifra este mensaje con la palabra clave: "Reloj":

   "olvel erves wrhey xxxxe"

3. Intercambia un mensaje breve codificado con algún compañero de la clase.

4. Métodos de descifrado

4.1. Análisis de frecuencias

Si la **criptografía** es el arte de inventar algoritmos y claves que nos permiten escribir mensajes cifrados, el **criptoanálisis** es el arte de descubrir lo que dicen los mensajes aunque no se disponga de algoritmos ni de claves.

El primer libro conocido de criptoanálisis es una obra del filósofo árabe del siglo IX, Al Kindi. Este hombre se dio cuenta de que **"en todas las lenguas hay unas letras que aparecen más a menudo que otras"**.

Por ejemplo, en castellano, las letras más frecuentes son:

Altas	*Medias*	*Bajas*	*Muy Bajas*
E – 16.78%	R – 4,94%	Y – 1,54%	J – 0,30%
A – 11,96 %	U – 4,80%	Q – 1,53%	Ñ – 0,29%
O – 8,69%	I – 4,15%	B – 0,92%	Z – 0,15%
L – 8,37%	T – 3,31%	H – 0,89%	X – 0,06%
S – 7,88%	C – 2,92%	G – 0,73%	K – 0,00%
N – 7,01%	P – 2,78%	F – 0,52%	W – 0,00%
D - 6,87%	M – 2,12%	V – 0,39%	

Así, si en un texto plano las letras E y A son las más frecuentes, las letras por las que se sustituyan también serán las más abundantes. Por tanto, si contamos cuántas veces sale una letra en un texto cifrado y miramos las que salen más veces, tendremos las primeras pistas importantes.

Eso sí, cuanto más largo sea el texto, o más mesajes tengamos, más fácil será que coincidan las frecuencias, porque nos podemos encontrar con un mensaje en el que los datos de frecuencias no coincidan con los habituales:

"Dábale arroz a la zorra el abad"

(Demasiadas *des* y *zetas* para lo habitual).

4.2. Un ejemplo difícil

Apoyándote en las frecuencias absolutas de las letras que más se repiten, y ayudándote de tu intuición, intenta descifrar el siguiente mensaje:

U	K		W	O		G	U	V	C	F	K	U	V	K	E	Q		Ñ	G	V	G		N	C
	E	C	D	G	B	C		G	O		W	O		J	Q	T	O	Q		A		N	Q	U
	R	K	G	U		G	O		G	N		J	K	G	N	Q		R	W	G	F	G		
F	G	E	K	T		S	W	G		F	G		Ñ	G	F	K	C		G	U	V	C		
D	K	G	O																					

Busca en primer lugar las 8 letras que más se repiten y calcula su frecuencia relativa. Compáralas con las letras más frecuentes en castellano, que, como hemos visto antes, son:

Letras con frecuencia más alta en castellano
E – 16.78%
A – 11,96 %
O – 8,69%
L – 8,37%
S – 7,88%
N – 7,01%
D - 6,87%

4.3. Algunas ideas sobre criptoanálisis

Seguro que al intentar descifrar el mensaje anterior, has utilizado también alguna de las siguientes ideas, que suelen ser muy útiles en criptoanálisis:

- Si dos palabras seguidas acaban en una misma letra, y la primera es corta, es probable que esta letra sea la S (para los plurales).
- Las palabras de una letra pueden ser A, Y, O, y, en mucha menor frecuencia, E y U.
- Las palabras de dos letras son artículos, preposiciones o conjunciones: *el, la, un, al, de, en, si, ni...*
- Las palabras de tres letras también son del mismo estilo: *con, por, que...*
- Detrás de una Q siempre viene una U.

Por otro lado, es conveniente saber que los criptoanalistas no sólo atienden a las letras solas, sino también a los **digramas** (grupos de dos letras) y **trigramas** (grupos de tres letras) que más aparecen, ya que cada lengua tiene sus combinaciones más frecuentes. Así, por ejemplo, en castellano, algunos de los digramas más frecuentes son: ES, EN, EL, DE, LA, OS, AR, UE, RA, RE, ER, AS, ON, ST, AD, AL, OR, TA, CO, y algunos de los trigramas más frecuentes serían: QUE, DEL, POR, ENT, IEN, EST, CON, LOS, OSA, ENE.

4.4. Introducción a los métodos polialfabéticos

Los métodos como el anterior en el que cada letra se sustituye por otra, se llaman **método monoalfabéticos**.

Cuando un criptoanalista intenta descifrar un método sin saber el método ni la clave, se dice que **ataca** el código. En los métodos monoalfabéticos, el primer ataque siempre consiste en el análisis de frecuencias.

En el siglo XVII y XVIII, las cifras monoalfabéticas no resistían los ataques de los criptoanalistas. Los estados tenían a auténticos expertos lingüistas y matemáticos trabajando para descifrar al enemigo y para inventar nuevos códigos. Algunos de los trucos que se inventaron fueron:

1) Utilizar un signo para cada letra y otro para cada sílaba
2) Intercalar signos sin ningún significado

3) Hacer que algunos signos significasen instrucciones extrañas como “borra el anterior” o “borra los tres signos siguientes”.

Pero aún así, estas cifras con trampas podían resistirse un poco más, pero al final acababan siendo descifradas, cuando se disponía de muchos de mensajes o de algún mensaje muy largo.

En el siglo XVI, el rey español Felipe II utilizaba una de estas cifras con más de 500 símbolos, que era, sistemáticamente, descifrada por sus enemigos franceses. El monarca se quejó al Vaticano, porque “sólo un diablo podía descifrar esos mensajes”. El tal diablo no era otro que François Viete, uno de los más importantes algebristas de la época (uno de los descubridores de la fórmula que proporciona la solución general de una ecuación de tercer grado), que también trabajaba para el propio Vaticano.

Uno de los contraataques más interesantes fue **la cifra homofónica**, que utilizaba las propias frecuencias de cada letra para inventar un código. Por ejemplo, podemos hacer un código con 100 números (00, 01, 02, ..., 99). Si sabemos que la letra **T** sale un 6% de veces, le adjudicamos 6 números al azar, si la **M** tiene una frecuencia aproximada de 3% se le adjudican 3 números.

5. Un método casi definitivo: la cifra de Vigenère

5.1. La cifra de Vigenère

En el siglo XVI, el frances Blaise de Vigenère publicó su libro: “Tratado de las cifras o maneras secretas de escribir” donde explicaba su método de cifrado polialfabético:

“Una misma letra a lo largo del mensaje puede estar representada por otras de manera cambiante. Así, una **A** puede venir codificada a veces por una **D** o a veces por una **H**, pero, ¡atención! no siempre la **D** o la **H** codifican la **A**”

En el fondo, la cifra de Vigenère, lo que hace es utilizar varias veces la cifra de César con unos cuantos alfabetos a la vez. Pero el método es tan bueno que lo pudo publicar sin guardarlo en secreto, porque aunque el comienzo del mensaje diga claramente “Este mensaje está codificado con la cifra de Vigenère”, el desconocimiento de la clave hace prácticamente imposible su descifrado.

Veamos como funciona:

1. Se decide una palabra clave que sólo debe conocer el emisor y el receptor. Por ejemplo: “SOL”
2. Debajo de cada letra del mensaje escribimos la palabra clave:

Q	u	e	d	a	m	o	s		e	s	t	a		t	a	r	d	e		a		l	a	s
S	O	L	S	O	L	S	O		L	S	O	L		S	O	L	S	O		L		S	O	L
	c	i	n	c	o																			
	S	O	L	S	O																			

3. Ahora para codificar cada letra vamos a utilizar el alfabeto de César que hace coincidir la A con la letra de la clave que tiene debajo la letra que queremos

codificar. En nuestro ejemplo, como la clave es SOL, una palabra con tres letras, utilizaremos tres alfabetos de César, a saber, los que hacen coincidir la A con la S, con la O y con la L respectivamente:

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

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
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	Ñ

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

Así pues nuestro mensaje quedaría:

Q	u	e	d	a	m	o	s		e	s	t	a		t	a	r	d	e		a		l	a	s
S	O	L	S	O	L	S	O		L	S	O	L		S	O	L	S	O		L		S	O	L
j	j	o	v	o	w	h	h		o	l	i	l		m	o	c	v	s		l		d	o	d
	c	i	n	c	o																			
	S	O	L	S	O																			
	u	w	x	u	d																			

"jjovowhh olil mocvs l dod uwxud"

Observa que de las tres veces que aparece la **E** en nuestro texto, dos veces aparece codificada con la **O** y una vez con la **S**, es decir, no siempre viene codificada con la misma letra. Además, la **O**, representa, además de a la **E** a la **A**. Y hay pocos casos porque hemos escogido una palabra clave muy corta (con solo tres letras), si hubiéramos escogido una clave más larga, una letra podría venir representada hasta por 10 o 12 letras distintas.

Ejercicios

1. Codifica el mensaje "Esto no hay Dios que lo entienda" con la clave "Libro"
2. Con la misma clave, descifra el mensaje:

   "jw tz sxbjvbñw fkio kpuwqw"

3. Intercambia un mensaje breve codificado con un compañero o compañera de la clase.

5.2. Los trabajos de Kasiski y Babage

Durante casi tres siglos, nadie sabía cómo atacar la cifra de Vigenère, pero a mitad del siglo XIX, dos criptoanalistas, de forma independiente, encontraron su punto débil. Se trataba del oficial prusiano Kasiski, y del matemático inglés Babage, hoy conocido por sus aportaciones a los primeros ordenadores.

Estaba claro que la dificultad de la cifra de Vigenère era la clave, pero la clave tiene dos características: la longitud y las letras que la forman.

Como sucede en cualquier caso, para descifrar mensajes, conviene tener mensajes suficientemente largos que permitan un análisis más profundo.

Así, para adivinar la longitud de la clave, lo que se hace es buscar secuencias de letras que se repitan con una determinada frecuencia. Por ejemplo, la palabra QUE es una palabra muy usual en castellano, y si se usa con frecuencia en un mensaje es posible que más de una vez coincidan sus trascripciones. Se mide la distancia que hay entre unas repeticiones y otras, porque la longitud de la clave tiene que ser un divisor de esta distancia. Así, calculando el máximo común divisor de estas distancias, utilizando varios grupos de letras, podemos hallar un candidato posible a ser la longitud de la clave.

Cuando se sabe la longitud de la clave (por ejemplo 7), se sabe que cada 7 letras, están codificadas por el mismo alfabeto. Haciendo ahora un análisis de frecuencias, se puede atacar la cifra de forma similar a como se hacía con la cifra de César.

5.3. Contraatacando a Kasiski y Babage

Está claro que si no se descubriera la longitud de la clave, sería mucho más difícil de descifrar el código. Por tanto, caben dos soluciones:

1) La clave infinita: Si tenemos una clave tan larga como el texto, no nos la podrán encontrar. Por ejemplo, nos podemos coger un capítulo de un libro y utilizarlo como clave.
2) La clave al azar: Como los criptoanalistas tienen mucha paciencia, podrían encontrar el libro clave. Además, en un libro siempre va a haber palabras que se repitan con cierta frecuencia (que, de, en...), que pueden constituír puntos débiles para la clave. Así que se puede utilizar una clave al azar:

   fbvjewnbpojnzsfbjnaèobfn...

   Ahora bien, una clave al azar es imposible de recordar y muy pesada de utilizar. Lo normal es utilizar un algoritmo que permita construir la clave a una máquina (como por ejemplo, un ordenador). En algo de esto se basaba la máquina ENIGMA.

5.4. La máquina ENIGMA

La máquina ENIGMA fue desarrollada por los alemanes entre la primera y la segunda guerra mundial, y se basaba en un sistema de cifrado de Vigenère con una clave infinita aleatoria.

En su aspecto externo, la máquina ENIGMA simula una máquina de escribir, pero cuando se pulsa una letra se ilumina la codificada.

Internamente, la máquina tenía tres rodillos que conectaban cada punto de entrada con otro de salida descolocado respecto del primero. Cada vez que se pulsaba una letra, el primer rodillo se movía y cada vez que el primer rodillo giraba una vuelta completa, movía el segundo, y, este, hacía lo mismo con el tercero.

Como cada rodillo tiene 26 letras, no se volvía a estar en la misma posición que al principio, hasta después de 26^3 = 17576 movimientos. Además los rodillos eran distintos entre sí, por lo que no era lo mismo colocarlos en la posición 1 – 2 – 3 que en la posición 2 – 1 – 3, por ejemplo, así, pues, las posiciones iniciales eran, en total: 105456 posibilidades.

Pero es que, además, debajo del teclado, tenía un tablero que permitía intercambiar seis pares de letras entre sí: convirtiendo la A en la G, o la B en la U, lo que elevaba a más de dos mil billones las posibilidades iniciales.

El ejército alemán disponía de un libro para determinar la posición inicial de los rodillos y del tablero cada día. Pero además, cada mensaje empezaba con una secuencia repetida de tres letras. Así pues, para descifrar el mensaje que se recibía:

1. El decodificador situaba los rodillos y el tablero según la clave del día
2. Descodificaba las seis primeras letras, y le salía una secuencia repetida (por ejemplo ZFD ZFD), que indicaba como debía colocar los rodillos.
3. Colocaba los rodillos de la forma indicada en la secuencia inicial y descifraba el resto del mensaje.

5.5. Resolviendo ENIGMA

1) <u>El episodio de Polonia</u>

Los polacos disponían de una máquina ENIGMA, con lo que todo se reducía a encontrar la posición inicial del tablero y de los rodillos (lo que suponía quedarse con alguna de las más de dos mil billones de posibilidades). El matemático Rejewski se dio cuenta que el problema principal no era la posición del tablero, que sólo cambiaba una letra por otra, y que, una vez traducido el mensaje, podía hacerse bien a mano, sino las posiciones de los rodillos. La forma de atacar este método fue a partir de la repetición de las tres primeras letras al principio de cada mensaje, porque estas repeticiones iban informando sobre las posiciones de los rodillos. Después de analizar muchos mensajes, el ENIGMA estaba resuelto.

Los alemanes se dieron cuenta y construyeron dos rodillos más: cinco en total, de los cuales sólo introducían tres en la máquina. Ahora las posiciones iniciales de los rodillos pasaron de ser 17576 a ser casi 12 millones, que, combinadas con las posiciones del tablero, dan cerca de 160 trillones de posibilidades. Algo que complicaba demasiado las cosas

2) <u>El episodio de Inglaterra</u>

Polonia comenzó a colaborar con Inglaterra, que mantenía a centenares de personas trabajando en un pueblo de las cercanías de Londres para descodificar los mensajes.

El gran cerebro inglés que permitió el descifrado de ENIGMA fue Alan Turing (uno de los amigos del padre de Beth en la película “Los crímenes de Oxford”, y, precursor, como Babage, de los ordenadores modernos), y como ya no podía basarse en la secuencia de tres letras que repetían los alemanes al principio de cada transmisión, observó que en las primeras palabras de cada mensaje hablaban siempre de las condiciones meteorológicas, por lo que palabras como *tiempo, viento, frío...* se repetían con bastante frecuencia. Se apoyó en este hecho y en el de que la máquina ENIGMA estaba construida de forma que nunca una letra codificaba a ella misma, para descubrir los códigos.

El descubrimiento de los códigos de ENIGMA fue muy importante en la segunda guerra mundial, ya que pudieron evitarse ataques del enemigo y pudieron provocarse ataques por sorpresa, lo que, sin duda, influyó en el rumbo de la guerra.