Descifrando códigos

A.Manuel L.Pérez

2 de abril de 2011

1. El problema

> - ¡Qué cosa más absurdamente sencilla! - exclamé yo.
> - ¡Sencillísima! - dijo Sherlock un poco picado -. Una vez que se los explican a usted, todos los problemas resultan infantiles. Aquí tiene usted uno sin explicación. Veamos, amigo Watson, lo que usted saca del mismo.
>
> Me echó una hoja de papel encima de la mesa, y volvió a su análisis químico. Yo me quedé contemplando con asombro los jeroglíficos absurdos que tenía el documento y exclamé:
>
> - Pero, ¡Holmes, si este es un dibujo hecho por algún niño!

El párrafo anterior es un extracto del principio de "La aventura de los bailarines" del libro de Sherlock Holmes, escrito por Sir Arthur Conan Doyle. El dibujo anterior contiene un mensaje que conduce a la solución del caso. Como la novela es inglesa el mensaje está en inglés, y descifrarlo es un poco más complicado para un español. Pero ¿serías capaz de averiguar el significado del siguiente mensaje?

Jwswñw ñv etbmv ktbmwo. W dv jbivo bd znboñby. Gbyvy. Jwonw.

A este tipo de mensajes se les suele llamar mensajes cifrados. Un mensaje cifrado es un mensaje que solo lo pueden entender ciertas personas, aquellas que sepan cómo descifrar el mensaje. El problema que tiene Sherlock Holmes es descifrar el mensaje sin saber cómo hacerlo.

Con 15 años me quedé embelesado con la forma de razonar de este detective, porque de las observaciones más triviales es capaz de sacar conclusiones fantásticas. Y después de ver cómo descifra el mensaje con los dibujitos me entraron ganas de descifrar mensajes. ¿Sería capaz de descifrar yo algún tipo de mensaje?

Por aquel entonces estaba de moda entre las chicas de mi clase el enviarse mensajitos cifrados. De esa forma podían pasarse mensajitos en clase sin que los demás pudiésemos leerlos. Después de haber leído a Sherlock Holmes reté a un par de chicas a que me escribieran cada una de ellas dos cartas cifradas, cada carta cifrada de una forma diferente. Las reté y gané :)

¿Cómo fui capaz de descifrar las cartas? Confieso que me ayudé de alguna de las ideas que usa Holmes para resolver su problema. Veamos cómo podemos descifrar el mensaje anterior: para ello voy a usar un método un poco bestia.

Miremos de nuevo el mensaje:

Jwswñw ñv etbmv ktbmwo. W dv jbivo bd znboñby. Gbyvy. Jwonw.

Lo primero que tenemos que preguntarnos es por el método de cifrado, esto es, ¿cómo podemos cifrar un mensaje? Por ejemplo, si yo quiero cifrar la palabra "hola", ¿cómo puedo hacerlo?

El método más sencillo es lo que se conoce como el método del Cesar, porque ya lo usaba Julio Cesar para enviar mensajes. En este método cambiamos una letra por otra. Por ejemplo, en lugar de escribir la a escribimos la b, en lugar de

la b la c,..., en lugar de la p escribimos la q,..., en lugar de la y escribimos la z y en lugar de la z escricambiamos una letra por otra. Por ejemplo, en lugar de escribir la a escribimos la b, en lugar de la b la c,..., en lugar de la p escribimos la q,..., en lugar de la y escribimos la z y en lugar de la z escribimos la a. En este método de cifrado escribimos la siguiente letra. Usando este método podemos cifrar "hola" escribiendo "ipmb".

hola →ipmb

Descifrar este mensaje es muy sencillo. La h la convertimos en i, ya que la i es la letra que sigue a la h, para descifrar un mensaje basta con escribir una h en lugar de una i, la letra anterior a la escrita. De esta forma desciframos "ipmb" obteniendo "hola".

¿Serías capaz de averiguar el significado del siguiente mensaje codificado de igual forma?

Rvfebnpt nbobñb b mbt dvbusp

Pero ¿por qué al cifrar tenemos que coger la letra siguiente? ¿Por qué no coger la letra que se sitúa dos posiciones más adelante en el abecedario? En este caso escribiríamos una c en lugar de una a, una d en lugar de una b, ... Usando este método en lugar de escribir "hola" escribiríamos "jqnc", ya que la h la convertimos en una j puesto que la j es la segunda letra que va después de la h (h i j k ...), la o en una q,...

Y si en lugar de escribir la letra que se sitúa dos posiciones más adelante, ¿cogemos la que se sitúa 3 puestos? ¿Podríamos cifrar un mensaje? ¿Y si en lugar de escribir la letra que se situa 3 posiciones más adelante elegimos la que está 4? ¿ó 5? ¿ó 6? ...

Como se ve el método del Cesar admite muchas variaciones posibles. Pero ¿en qué se basa dicho método? Si nos paramos a pensar con un poco de detenimiento observamos que lo que hacemos es sustituir una letra por otra. La ventaja del método del Cesar radica enn que es muy sencillo recordar cómo sustituimos unas letras por otras. Pero ¿por qué no puedo sustituir la a por una j, la b por una c, y la c por una r? En principio no hay nada que me lo impida hacer, lo único importante es que a cada letra le asocie una única letra.

Si queremos usar éste método necesitamos construir una tabla que nos diga cómo transformamos unas letras en otras. La siguiente tabla muestra un ejemplo:

a	ñ
b	y
c	w
d	g
e	h
f	o
g	x

h	n
i	a
j	f
k	t
l	i
m	l
n	s

ñ	q
o	e
p	m
q	b
r	j
s	r
t	p

u	d
v	v
w	z
x	k
y	c
z	u

¿Esta tabla que quiere decir? En la primera fila encontramos un par de letras: la a y la $\tilde{n}$. Esto quiere decir que en lugar de una a voy a escribir una $\tilde{n}$. Como se ve la primeras dos columnas nos dice cómo escribir las letras desde la a hasta la g en el mensaje cifrado. Así, por ejemplo, en lugar de la letra e escribiremos una h, y en lugar de la g una x. Las columnas 3 y 4 nos dicen cómo escribir las letras desde la h hasta la n, las columnas 5 y 6 cómo escribir las letras desde la $\tilde{n}$ hasta la t, y las columnas 7 y 8 cómo hacerlo con las letras que van desde la u hasta la z. Notar que las columnas pares nos dan las letras en el mensaje original, mientras que las columnas impares nos dicen cómo vamos a escribir las letras realmente. Decimos que la tabla anterior nos cifra el mensaje.

Si queremos enviar a un amigo el mensaje transcendental

que sueño tengo

lo escribiremos como

bdh rdhqe phsxe

Para hacerlo basta con mirar la tabla anterior y ver que la letra q, que aparece en la cuarta fila de la quinta columna, la escribimos como b; que la u, que aparece en la primera fila de la séptima columna, la escribimos como d, y así sucesivamente.

Descifrar el código anterior es trivial si tenemos la tabla anterior. Para ello, buscamos la letra b en las columnas impares, encontrándola en la quinta columna. Miramos la letra que se encuentra a su lado, la q, y sabemos que es ésta letra la letra que tenemos que escribir. Repitiendo este proceso averiguamos el mensaje original. Si usas mucho un método de cifrado es más práctico tener dos tablas como la anterior: una, que nos dice cómo cifrar un mensaje (la tabla anterior), y otra que nos dice cómo descifrarlo (es la misma tabla pero cambiando de lugar la columna 2 por la 1, la 4 por la 3, la 6 por la 5 y la 8 por la 7, y ordenándolas).

Problema: ¿serías capaz de descifrar el mensaje "mahsre, idhxe hkarpe", dicho por un famoso filósofo francés. ¿Sabes de qué filósofo se trata?

Como observarás conociendo la tabla anterior es muy sencillo descifrar un mensaje escrito de esta forma. Pero ¿y si no conocemos la tabla anterior? ¿Podríamos hacerlo de alguna manera?

Volvamos a nuestro problema inicial: cómo descifrar el siguiente mensaje

Jwswñw ñv etbmv ktbmwo. W dv jbivo bd znboñby. Gbyvy. Jwonw.

Lo primero que nos preguntamos es, ¿este mensaje estará cifrado usando una tabla como la anterior? Esto es, a cada letra le corresponde una única palabra.

Supongamos que, efectivamente, este mensaje está cifrado de esta manera. ¿Cómo podemos averiguar la tabla usada? Para ello voy a usar una de las ideas usadas por Sherlock Holmes: lo habitual cuando escribes un mensaje es saludar, despedirse.

Si el mensaje anterior fuese más largo podíamos pensar que se trata de una carta, empezando con algo del estilo "Querido Pepito:", pero al ser un mensaje muy corto no es de esperar un saludo tan largo. El saludo debería ser mas bien del tipo: "Hola, Pepe", o un simple "Hola". ¿La primera palabra del mensaje será "hola"? Veamos a ver si encaja. La primera palabra es "Jwswñw" y tiene 6 letras, mientras que la palabra "hola" tiene 4. No nos sirve. La primera palabra no es hola.

¿Cómo nos solemos despedir en los mensajes? "Nos vemos", "Besos", "Hasta luego", "Ciao",... o simplemente con nuestro nombre. Vayamos probando todas estas posibilidades.

El mensaje cifrado termina con una única palabra "Jwonw", teniendo que descartar "Nos vemos", "Hasta luego" y demás despedidas de más de una palabra. "Besos" es una palabra ¿será la última? "Besos" tiene 5 letras y "Jwonw" también. ¡Esto pinta bien! ¿Podemos sustituir "Jwonw" por "Besos"? Pero basta con escribir una palabra encima de la otra para darnos cuenta de que "Jwonw" no puede corresponderse con "Besos":

J	w	o	n	w
B	e	s	o	s

La primera w la tendríamos que traducir como una e, mientras que la segunda como una s, lo cual no es posible, ya que una letra se tiene que cifrar siempre de igual manera. De esta forma concluimos que la última palabra no es besos.

Probemos con el nombre. El mensaje lo ha escrito "María". ¿Se habrá despedido escribiendo su nombre al final? La palabra "María" también tiene 5 letras al igual que "Jwonw". Escribamos una palabra encima de la otra:

J	w	o	n	w
M	a	r	i	a

¡Encaja perfectamente! Si la última palabra es realmente "María" (realmente no lo sabemos, es simplemente una suposición), todas las *j* en el mensaje corresponden a *m*, las *w* a *a*, las *o* a *r*, y las *n* a *i*. Con esto podemos traducir el mensaje inicial de la siguiente forma:

Jwswñw	Ma -a -a
ñv	- -
etbmv	- - - - -
ktbmwo.	- - - -ar.
W	A
dv	- -
jbivo	m - - -r
bd	- -
znboñby.	-i -r - - -.
Gbyvy.	- - - - -.
Jwonw.	María.

Mirando el mensaje traducido nos encontramos con que la primera palabra es "Ma -a -a". ¿Nos suena a algo? ¿Podría ser "mañana"? ¿Podemos hacer la siguiente traducción?

J	w	s	w	ñ	w
M	a	ñ	a	n	a

Traducir "Jwswñw" como "Mañana" quiere decir que la *s* se corresponde con una *ñ*, y la *ñ* con una *n*. Sabiendo esto podemos traducir el mensaje de la siguiente forma:

Jwswñw	Mañana
ñv	n -
etbmv	- - - - -
ktbmwo.	- - - -ar.
W	A
dv	- -
jbivo	m - - -r
bd	- -
znboñby.	-i -rn - - -.
Gbyvy.	- - - - -.
Jwonw.	María.

A la vista de la nueva traducción, ¿podemos intentar averiguar cómo traducir alguna letra más? La segunda palabra del mensaje se traduce como "n-", tiene dos letras, siendo la primera una *n*. ¿Qué palabras de dos letras empiezan por *n*? Como la segunda letra tiene que ser necesariamente una vocal, las posibles palabras de dos letras que podemos formar son *na*, *ne*, *ni*, *no*, *nu*, y de estas cinco posibilidades tan solo la segunda y la tercera tienen algo de sentido en el mensaje. Si nos quedamos con *ni* el mensaje empezaría: "Mañana ni...", mientras que si nos quedamos con *no*: "Mañana no...". De estos dos casos posibles, el segundo parece más probable. Supongamos por tanto que la segunda palabra *ñv* se traduce como un *no*, y que por tanto, la letra *v* se corresponde con la letra *o*. Sabiendo esto, el mensaje se traduce como:

Jwswñw	Mañana
ñv	no
etbmv	- - - - o
ktbmwo.	- - - - ar.
W	A
dv	-o
jbivo	m - - or
bd	- -
znboñby.	-i -rn - -.
Gbyvy.	- - - o -.
Jwonw.	María.

¿Cómo proseguir con la traducción? Lo primero que llama la atención al ver el mensaje es que tenemos de nuevo una palabra de dos letras casi traducida: la cuarta palabra *dv* se traduce como *-o*, y sabemos que esta palabra no puede ser *no*, ya que *no* se escribe en el mensaje cifrado como *ñv* y no como *dv*. ¿Qué palabras hay de dos letras que acaban en *o*? En principio se me ocurren *no* y el artículo *lo*. Pero ¿existe alguna más? Pensar que si existe alguna más y no la tenemos en cuenta, podemos obcecarnos a la hora de intentar traducir el mensaje diciendo que *dv* se traduce como *lo* y no ser cierto, en cuyo caso nunca conseguiríamos resolver nuestro problema.

Para estar seguro de qué palabras hay de dos letras que acaban en *o* basta con escribir todas las combinaciones posibles y quedarnos con aquellas que reconozcamos como palabras. Hagámoslo:

ao bo co do eo fo go ho io jo ko lo mo no
ño oo po qo ro so to uo vo wo xo yo zo

De todas estas combinaciones las únicas que tienen sentido son: *jo*, *lo*, *no*, *so*. Sabemos que *no* no es traducción, quedándonos como opciones *jo*, *lo* y *so*, y de estas tres la más probable es *lo*. Si esto fuese verdad, la quinta palabra del mensaje *dv* se tiene que traducir como *lo*, y por tanto, la *d* se traduce como una *l*:

Jwswñw	Mañana
ñv	no
etbmv	- - - - o
ktbmwo.	- - - - ar.
W	A
dv	lo
jbivo	m - - or
bd	-l
znboñby.	-i -rn - -.
Gbyvy.	- - - o -.
Jwonw.	María.

Mirando el mensaje traducido observamos que la octava palabra *bd* se traduce como *-l*. Como sabemos traducir las vocales *a*, *i* y *o*, *bd* ha de traducirse necesariamente como *el* o como *ul*. Y puesto que *ul* no es una palabra española, concluimos que *bd* se traduce como *el*, y por tanto, *b* como *e*. Ya sabemos como traducir todas las vocales excepto la *u*, y esto nos va a facilitar mucho nuestra tarea. Traduciendo *b* por *e* el mensaje se lee como

Jwswñw	Mañana
ñv	no
etbmv	- - e - o
ktbmwo.	- - e - ar.
W	A
dv	lo
jbivo	me-or
bd	el
znboñby.	-ierne-.
Gbyvy.	-e-o-.
Jwonw.	María.

En este mensaje se pueden leer la séptima y la novena palabra: es claro que *me-or* se traduce como *mejor*, y que *-ierne-* como *viernes*. Esto nos dice que *i* se traduce como *j*, *z* como *v* y *y* como *s*. El mensaje queda:

Jwswñw	Mañana
ñv	no
etbmv	- - e - o
ktbmwo.	- - e - ar.
W	A
dv	lo
jbivo	mejor
bd	el
znboñby.	viernes.
Gbyvy.	-esos.
Jwonw.	María.

Ya casi tenemos traducido nuestro mensaje. Es claro que la penúltima palabra es *Besos*, quedándonos por averiguar cómo traducir la tercera y la cuarta palabra lo cual lo podemos hacer por tanteo. ¿Serías capaz de acabar de traducir el mensaje?

2. Buscando una solución

En la sección anterior hemos visto un método para descifrar mensajes codificados por el método del Cesar. Nuestro método se basa bastante en el tanteo, ya que hemos ido probando a traducir letras y viendo si el resultado es coherente o no.

Siempre que tengamos un problema conviene ser conscientes de ellos, escribiéndolo lo más claramente posible. En nuestro caso podemos enunciar el problema de la siguiente manera: *Dado un mensaje codificado con el método del Cesar, dar un método para descifrarlo.*

La solución que se da a este problema se basa en la probabilidad. La pregunta es la siguiente: ¿cuál es la probabilidad de que una letra aparezca en un mensaje? En la wikipedia encontramos la siguiente tabla con la probabilidad, escrita como tanto por cien, de que aparezca una letra en un mensaje:

a	12.53
b	1.42
c	4.68
d	5.86
e	13.68
f	0.69
g	1.01

h	0.70
i	6.25
j	0.44
k	0.01
l	4.97
m	3.15
n	6.71

ñ	???
o	8.68
p	2.51
q	0.88
r	6.87
s	7.98
t	4.63

u	3.93
v	0.90
w	0.02
x	0.22
y	0.90
z	0.52

Esta tabla lo que nos dice es que en un texto suficientemente largo el 12.53 % de las letras que aparecen son *a*, el 1.42 % *b*, el 4.68 % *c*, ... Si el texto es muy pequeño estos porcentajes no se tienen que cumplir.

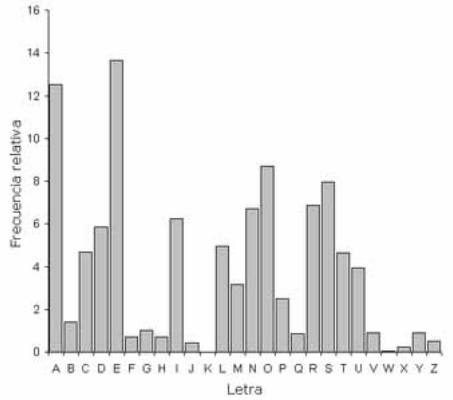

Figura 1: Diagrama de barras

Antes que continuar quiero hacer una pequeña observación: estos datos están sacados de wikipedia la cual es una enciclopedia que puede escribir cualquiera, que sepa de la materia o no sepa. ¿Por qué han de ser ciertos todos estos datos? De hecho si nos fijamos no aparece la probabilidad de encontrar una $\tilde{n}$ en un mensaje. ¿Esto quiere decir que las $\tilde{n}$ no las usamos en español? Como se ve la información de esta página es incompleta o errónea. En lo que sigue voy a considerar que esta tabla es correcta, si bien tenemos que ser conscientes de que su procedencia no es muy fiable.

De todas las letras ¿cuál es la que más suele aparecer? ¿cuál la que menos? Para responder a estas preguntas es más cómodo representar la tabla anterior en un diagrama de barras (figura 1). Basta con mirar esta figura para observar que es la letra *e* la que más aparece, seguida de la *a*.

¿Cómo podemos usar esto para descifrar un mensaje? Contemos las veces que aparece un símbolo en un mensaje y anotémoslo. El símbolo que más aparezca seguramente será una *e*, y el siguiente que más aparezca una *a*.

Veamos si funciona con el mensaje de la sección anterior:

Jwswñw ñv etbmv ktbmwo. W dv jbivo bd znboñby. Gbyvy. Jwonw.

Para ello contemos el número de veces que aparece cada símbolo en este mensaje. Así, por ejemplo, la *j* aparece tres veces, en la primera, séptima y la onceava palabra. La siguiente tabla indica el número de veces que aparece una letra en el mensaje anterior:

b	7
g	1
i	1
ñ	3
t	2
y	3

d	2
j	3
m	2
o	4
v	5
z	1

e	1
k	1
n	2
s	1
w	7

¿Qué símbolos son los que más aparecen? La *b* y la *w*. Y ¿qué letras son las que más frecuentemente aparecen en español? Ya lo vimos antes: la letra *e* es la que más aparece, siguiéndole a la zaga la letra *a*. Luego los símbolos *b* y *w* han de traducirse como *a* y *e* o al revés. Y, efectivamente, si miramos la traducción que hicimos en la sección anterior el símbolo *b* se traduce como *e*, mientras que el *w* como *a*.

Si antes dijimos que la letra *e* es la que más aparece en español, ¿por qué aparecen de igual forma la *a* y la *e* en nuestro mensaje? Porque el mensaje es muy corto. Recordar que la teoría de la probabilidad nos habla de certeza cuando hablamos de muchísimos objetos. En nuestro caso particular, decir que la probabilidad de que aparezca la letra *e* en un mensaje es del 13.68 % lo que

quiere decir es que cuando cojamos un texto muy largo, como puede ser "El Quijote", el 13.68 % aproximadamente de las letras será una *e*. Pero ¿y si el mensaje es muy corto como en nuestro caso? Ya no lo sabemos con certeza, no pudiendo afirmar nada con seguridad y teniendo que operar por tanteo.

Como se ve contar las veces que aparece una letra en un mensaje cifrado nos va a permitir sospechar qué símbolos corresponden a la *e* y cuáles a la *a*, lo cual nos va a facilitar mucho la traducción, siempre y cuando el mensaje esté codificado usando el método del Cesar.

Pero y ¿si el mensaje se codifica usando otro tipo de método? ¿Cómo podemos descifrarlo? La parte de las matemáticas que se encarga de resolver este tipo de problemas es la *criptografía*, la cual es de gran utilidad en la actualidad.

¿Para qué sirve en la actualidad encriptar (=cifrar) mensajes? Para poder acceder a una red social como tuenti, facebook,..., tienes que introducir una contraseña, la cual tuenti tiene que tener anotada en algún sitio. Como en el mundo hay mucho ladrón y gente con muy mala leche, tuenti está obligado a encriptar tu contraseña, de tal manera que si entrase algún ladrón y robase todas las contraseñas no pudiese leerlas. De hecho cuando una página es segura, lo más probable es que se esté encriptando toda la información que le envías a la página.

Otro uso más difundido en los EE.UU que en España es el de cifrar los mails. Cuando nosotros enviamos un mail, el mail no va directo al destinatario, sino que antes tiene que pasar por un montón de ordenadores. Así, por ejemplo, si yo envío un mail desde Yahoo hasta Gmail, el mail mínimo pasa mínimo por los siguientes ordenadores: el mío, donde escribo el mail; desde mi ordenador yo se lo envío a Yahoo y este se lo envía a un ordenador de Gmail, desde el que pasa al ordenador del destinatario del mail. Ahora bien, si Yahoo recibe mi mail, nada le impide hacer una copia de él, guardándoselo. Si mi mensaje de mail no está cifrado, cualquier persona que tenga acceso al ordenador de Yahoo podrá cotillear mi correspondencia, mientras que si está cifrado no podrá hacerlo.

3. Problemas

1. Inventa un código secreto, escribe un mensaje y pasáselo a un amigo. ¿Es capaz de descifrarlo?

2. ¿Serías capaz de crear un programa de ordenador para contar el número de veces que aparece cada letra en este artículo?

4. Soluciones a los problemas del artículo

1. "Rvfebnpt nbobñb b mbt dvbusp" →"quedamos mañana a las cuatro".

2. "mahsre, idhxe hkarpe" →"pienso, luego existo", dicho por René Descartes en su "Discurso del método"

3. "Jwswñw ñv etbmv ktbmwo. W dv jbivo bd znboñby. Gbyvy. Jwonw." se traduce como "Mañana no puedo quedar. A lo mejor el viernes. Besos."