Criptografía para principiantes: Método Della Porta

por
Óscar Carrión Lostal
(IES Valdespartera)

Ya en anteriores artículos sobre criptografía para principiantes se vieron distintos métodos de cifrar y descifrar mensajes, como el de Julio César, el de Vinegère y el de la Escítala.

En este artículo vamos a tratar el método de Della Porta. Este método utiliza distintos alfabetos (filas de la tabla que veremos más adelante) y una palabra clave para cifrar y descifrar mensajes.

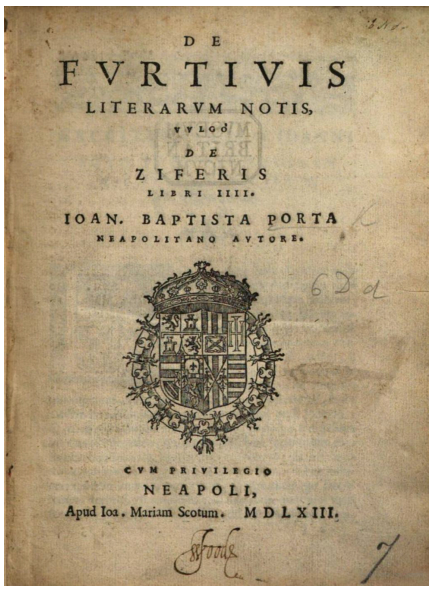
Para desarrollar dicho método en clase la propuesta didáctica es la siguiente:

— Introducción histórica.
— Cifrado y descifrado de mensajes con la tabla y la palabra clave correspondiente.

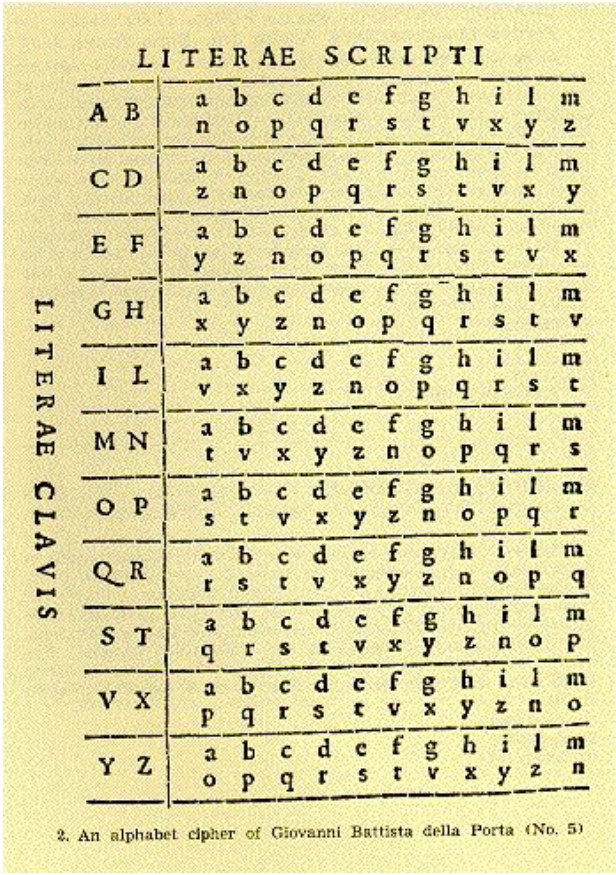
Della Porta

Este método lleva por nombre el de un famoso científico italiano, Giovanni Battista Della Porta (Vico Equense, 1535 – Nápoles, 1615),que además fue un filósofo, alquimista, comediógrafo de fines del siglo XVI y principios del XVII. Cuando tenía 28 años, en 1563, escribió el libro que le dio gran renombre como criptólogo: *De furtivis literarum notis-vulgo de ziferis*. Está compuesto por cuatro volúmenes que tratan, respectivamente, de cifras de la antigüedad, de cifras modernas, del criptoanálisis y de las características lingüísticas que facilitan el descifrado. La obra representa una recapitulación de los procedimientos clásicos de sus predecesores.

Della Porta clasifica los procedimientos en tres categorías: el cambio de la orden de las letras (transposición), de sus formas (sustitución por símbolos) y de su valor (sustitución por un alfabeto criptográfico). Estableció la división de los procedimientos, actualmente clásica, en dos principios: transposición y sustitución. Finalmente, fue el inventor del primer sistema literal de llave doble.



La tabla 1 es la original que usó Della Porta y que sale en el libro citado con anterioridad.



LITERAE SCRIPTI

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

LITERAE CLAVIS

2. An alphabet cipher of Giovanni Battista della Porta (No. 5)

Tabla 1

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

Tabla 2

Como se ha indicado, este método utiliza distintos alfabetos y una palabra clave. La tabla 2 es la que se debe utilizar. En ella se considera *Ch* como una letra para adaptarla al castellano (nótese que escribimos *Ch*, y no *CH*, ya que en caso contrario se podría confundir con la letra *H* que está incluida en la quinta fila de la tabla).

Préstese atención al hecho de que la tabla consta de catorce alfabetos (filas) cuando la original de Della Porta constaba de once alfabetos distintos.

Para su construcción hay que fijarse que cada alfabeto consta de dos letras que pueden formar parte de la palabra clave y de dos filas de letras que dan la correspondencia entre las del texto a cifrar y el cifrado. La primera fila de cada alfabeto es fija, y la segunda se va trasladando. Por ejemplo en el primer alfabeto (*A B*) la letra *a* está asociada a la letra *n*, sin embargo en el segundo alfabeto, la letra *a* está asociada a la letra *z*, que corresponde a trasladar la segunda fila un lugar hacia la derecha, y así sucesivamente.

Al cifrar un texto con este método se debe uno fijar en la palabra clave, (para el ejemplo supondremos que la palabra clave es CLAVE). Para la primera letra del texto a cifrar, nos debemos fijar en el alfabeto de la letra C, que es la segunda fila de la tabla derecha anterior, y sustituimos la letra del texto a cifrar por la letra que está encima o debajo de ese alfabeto, en nuestro caso la letra *m* hay que sustituirla por la letra *y*. Y así sucesivamente.

Veamos un ejemplo:

Texto a cifrar	m	a	t	e	m	a	t	i	c	a	s
Palabra clave	*C*	*L*	*A*	*V*	*E*	*C*	*L*	*A*	*V*	*E*	*C*
Texto cifrado	Y	U	G	U	X	Z	M	V	R	Y	G

Ejercicio 1. Cifrar el texto «taller de matemáticas», utilizando como palabras clave: a) PORTA y b) MATES.

a)

Texto a cifrar	t	a	l	l	e	r	d	e	m	a	t	e	m	a	t	i	c	a	s
Palabra clave	*P*	*O*	*R*	*T*	*A*	*P*	*O*	*R*	*T*	*A*	*P*	*O*	*R*	*T*	*A*	*P*	*O*	*R*	*T*
Texto cifrado																			

b)

Texto a cifrar	t	a	l	l	e	r	d	e	m	a	t	e	m	a	t	i	c	a	s
Palabra clave	*M*	*A*	*T*	*E*	*S*	*M*	*A*	*T*	*E*	*S*	*M*	*A*	*T*	*E*	*S*	*M*	*A*	*T*	*E*
Texto cifrado																			

En el siguiente ejemplo se procede al revés. Ahora hay que descifrar el mensaje que nos dan cifrado conocida la palabra clave (que en este caso es PORTA):

Texto cifrado	R	S	C	V	Z	S	B	N	S	N	A
Palabra clave	*P*	*O*	*R*	*T*	*A*	*P*	*O*	*R*	*T*	*A*	*P*
Mensaje	m	a	t	e	m	a	t	i	c	a	s

Ejercicio 2. Sabiendo que la palabra clave es CLAVE, descifrar los mensajes: a) «ÑKVAIChÑEPIUU», b) «QLGPOULGYNZ», y c) «DIBQYNRYZOZZ».

a)

Texto cifrado	Ñ	K	V	A	I	Ch	Ñ	E	P	I	U	U
Palabra clave	*C*	*L*	*A*	*V*	*E*	*C*	*L*	*A*	*V*	*E*	*C*	*L*
Mensaje												

b)

Texto cifrado	Q	L	G	P	O	U	L	G	Y	N	Z
Palabra clave											
Mensaje											

c)

Texto cifrado	D	I	B	Q	Y	N	R	Y	Z	O	Z	Z
Palabra clave												
Mensaje												

Ejercicio 3. Cifrar y descifrar diferentes mensajes entre vosotros por el método de Della Porta, donde uséis como palabra clave diferentes palabras clave.

Bibliografía

MÜLLER, D., P. BONAVOGLIA y J. SAVARD (s.f.), *Criptología*, *Giambattista Della Porta*, recuperado el 21 de marzo de 2021 de <https://web.archive.org/web/20091012192837/http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTPLOGIA/de%20la%20porta.htm>.

TÁBARA, J. L. (s. f.) *Breve historia de la Criptografía Clásica*, descargada de <http://www.openboxer.260mb.com/asignaturas/criptografia/metodosCriptograficos.pdf?i=2>.

— *Criptografía clásica*, Della Porta, consultada en <https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto10.html>.

Giovanni Battista della Porta (2020), en *Wikipedia*, recuperado el 21 de marzo de 2021 de <https://es.wikipedia.org/wiki/Giovanni_Battista_della_Porta>.

Talleres de Conexión Matemática impartidos por el autor del presente artículo.