Criptografía para principiantes: Método de Playfair (Wheatstone)

por
Óscar Carrión Lostal
(IES Valdespartera)

Ya en anteriores artículos sobre «Criptografía para principiantes» vimos distintos métodos de cifrar y descifrar mensajes, con actividades dirigidas a alumnos y alumnas de último ciclo de Primaria y primer ciclo de Secundaria. En este nuevo artículo vamos a tratar el método de Playfair.

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

— Introducción histórica.
— Reglas del método.
— Cifrado y descifrado de mensajes sin/con clave.

Playfair y Wheatstone

Este método lleva por nombre Playfair ya que fue el que se lo presentó a las autoridades inglesas, aunque el verdadero inventor del método fue su amigo el físico Charles Wheatstone, que lo creó para realizar comunicaciones telegráficas secretas en el año 1854, y se utilizó durante la Primera Guerra Mundial.

Charles Wheatstone fue un inventor y científico inglés del siglo XIX muy conocido por el aparato eléctrico que lleva su nombre, el *puente de Wheatstone*, que sirve para medir la resistencia eléctrica.

El método usa una matriz alfabética 5×5 donde se incluyen las letras del alfabeto inglés (25 de las 26 letras). En castellano el alfabeto tiene 27 letras, por tanto adaptaremos dicha tabla haciendo que las letras N y Ñ, y las letras V y W ocupen la misma celda dentro de la tabla.

Figura 1. Charles Wheatstone

Figura 2. Lyon Playfair

La siguiente tabla es la que se usa para el método sin clave:

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

El método de cifrado de Playfair es un método de sustitución que cifra pares de caracteres o letras, mediante una tabla (sin/con clave).

Las reglas para cifrar una secuencia de caracteres son las siguientes:

— El número de caracteres tiene que ser par. Si fuera impar se debe añadir una letra *nula*, por ejemplo la letra *x*. Como ejemplo vamos a codificar la palabra «matemáticas» que tiene 11 letras. Por ello le añadiremos al final una *x*, y por tanto se codificará la palabra «matemáticasx», que ya tiene 12 letras.

— Se separa en pares de letras la palabra o texto a codificar. Si entre esas parejas aparece alguna con letras repetidas hay que romper dicha repetición introduciendo una letra nula entre ellas, por ejemplo la letra *x*. Si al final nos saliera un número impar de letras, también habría que añadir al final de la secuencia otro carácter nulo, es decir, una letra *x*.

Una vez hecho los pasos previos anteriores, se aplican las siguientes reglas para codificar la secuencia de caracteres que queremos codificar:

— Si los dos caracteres o letras se encuentran en la misma fila de la tabla, se eligen los caracteres situados a su derecha, teniendo en cuenta que esta operación de ir a la derecha es módulo 5. Así que al codificar la pareja AE se convierte en BA, ya que a la derecha de la A está la B y a la derecha de la E está la A. Al ir a la derecha de la letra E, que es la última de la primera fila de la tabla, volvemos a empezar de forma cíclica la fila, por lo que la secuencia es A−B−C−D−E−A−…

— Si los dos caracteres o letras se encuentran en la misma columna, se eligen los caracteres situados justamente debajo de ellos, operación módulo 5 también. Así FU se convertirá en KA, ya que debajo de la letra F está la letra K y debajo de la letra U está la letra A, ya que es al seguir la primera columna cíclicamente, la secuencia es A−F−K−P−U−A−…

— Si los dos caracteres o letras se encuentran en filas y columnas distintas, entonces se forma el rectángulo en el que los extremos de una de sus diagonales la forman los dos caracteres a codificar, mientras que los extremos de la otra (leídos en el orden de filas de la tabla) serán los que la sustituyan en la codificación. Así la pareja GR se codifica como HQ.

Una vez expuestas las *reglas de juego* pasamos a codificar la secuencia de caracteres: «matemáticasx» (12 letras).

Para ello debo codificar los pares de letras: MA−TE−MA−TI−CA−SX.

Como no se repite ningún par de caracteres una vez separados de dos en dos, estamos en condiciones de proceder a su cifrado:

MA: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado KC.

TE: Se encuentran en la misma columna por lo tanto los debemos sustituir por los que están justamente debajo, teniendo en cuenta el recorrido cíclico de la columna, y obtenemos como cifrado ZJ.

MA: Ya la hemos codificado antes.

TI: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado SJ.

CA: Se encuentran en la misma fila por lo tanto los debemos sustituir por los que están justamente a su derecha, teniendo en cuenta el recorrido cíclico de la fila, y obtenemos como cifrado DB.
SX: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado RY.

Por tanto el cifrado de «matemáticasx» es KCZJKCSJDBSX.

Para conseguir un método más robusto, y que sea más difícil que nos descodifiquen los mensajes codificados, se puede utilizar una clave. Para ello se empieza a rellenar la tabla 5×5 anterior con las letras de la clave sin que se repita ninguna letra. Como ejemplo vamos a usar la palabra clave PLAYFAIR, en la que como vemos se repite la letra *a*. Por tanto al rellenar la tabla lo haremos con PLAYFIR y luego vamos añadiendo en orden todas las letras del alfabeto castellano, sin incluir las letras usadas ya con la clave, sin olvidar que debemos dejar en una misma celda las letras N y Ñ, y las letras V y W. Dicha tabla con su clave nos quedará ahora:

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

Las reglas a aplicar son las mismas que en el caso anterior. Como ejemplo volveremos a codificar la secuencia de caracteres «matemáticasx»:

MA: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado OP.
TE: Se encuentran en la misma columna por lo tanto los debemos sustituir por los que están justamente debajo, teniendo en cuenta el recorrido cíclico de la columna, y obtenemos como cifrado PM.
MA: Ya la hemos codificado antes.
TI: Se encuentran en la misma columna por lo tanto los debemos sustituir por los que están justamente debajo, teniendo en cuenta el recorrido cíclico de la columna, y obtenemos como cifrado PE.
CA: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado BY.
SX: Como se encuentran en distintas filas y columnas, se forma el rectángulo correspondiente y obtenemos como cifrado QZ.

Por tanto el cifrado de «matemáticasx» usando como clave PLAYFAIR es OPPMOPPEBYQZ.

Para descifrar secuencias de caracteres con el método de Playfair se siguen las reglas anteriores, pero ahora con el algoritmo inverso. Por lo tanto, las reglas para descifrar una secuencia de caracteres son las siguientes:

— Si los dos caracteres se encuentran en la misma fila, se eligen los caracteres situados a su izquierda, teniendo en cuenta que esta operación de ir a la izquierda es módulo 5.
— Si los dos caracteres o letras se encuentran en la misma columna, se eligen los caracteres situados justamente encima de ellos, teniendo en cuenta que esta operación de ir hacia arriba es módulo 5.
— Si los dos caracteres o letras se encuentran en filas y columnas distintas, entonces se forma el rectángulo en el que los extremos de una de sus diagonales la forman los dos carácteres del texto codifacado mientras que los extremos de la otra (leídos en el orden de filas de la tabla) serán los que corresponderán al texto descodificado.

Ejercicio 1. Descifrar la secuencia de caracteres ABBYDRQOKMIKTHBLOQ sabiendo que en su codificación con el método de Playfair se ha usando la clave PLAYFAIR (ver tabla anterior).

Ejercicio 2. Codificar la secuencia de caracteres «canalla» usando las tablas anteriores.

(Pista: la palabra que hay que codificar, por un lado tiene 7 caracteres y por otro al formar parejas de caracteres ca−na−ll−a, aparece la pareja de caracteres ll repetido. Por tanto debemos añadir un carácter de forma que sumen 8 caracteres y se rompa la repetición).

Ejercicio 3. Practica con distintas secuencias de caracteres para codificarlas y descifrarlas con las tablas que aparecen anteriormente.

Ejercicio 4. Inventad con otro compañero de clase vuestra propia tabla con una clave propia y practicad a cifrar y descifrar mensajes.

Conclusiones

Este método es también de sustitución al igual que el cifrado de César, lo único que en el método de Playfair se usan pares de letras o caracteres, en vez de ir de letra en letra. Al trabajar por pares de letras, si la secuencia a codificar o descifrar tiene un número impar de letras, hay que añadir una letra nula (en nuestro caso hemos usado la letra *x*). Ver la analogía con el método de la escítala, en el que si el número de letras era un número primo, se añadía un nuevo carácter, en este caso un guión (−), para que el número de caracteres fuera un número compuesto, y así tener divisores y más opciones de cuadrículas para codificar y decodificar mensajes. Además se usa también una tabla de 5×5 caracteres, lo que implica que se trabaje en módulo 5 (cíclico), ya sea por filas o por columnas. Al igual que en los métodos vistos con anterioridad, si queremos aumentar la seguridad del método, incluimos una clave: recordar que el cifrado de César si se incluye una clave se convertía en el método de Vinègere.

Referencias bibliográficas

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*, Playfair, consultada en <https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto14.html>.

Cifrado de Playfair (2021), en *Wikipedia*, recuperado el 30 de mayo de 2021 de <https://es.wikipedia.org/wiki/Cifrado_de_Playfair>.

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

Director: Ricardo Alonso Liarte (IES Salvador Victoria, Monreal del Campo)

Consejo de Redacción: Alberto Elduque Palomo (Departamento de matemáticas de la Universidad de Zaragoza), M.ª Ángeles Esteban Polo (CEIP Josefa Amar y Borbón, Zaragoza), Julio Sancho Rocher (IES Avempace, Zaragoza).

Entorno Abierto es una publicación digital bimestral que se edita en Zaragoza por la Sociedad Aragonesa «Pedro Sánchez Ciruelo» de Profesores de Matemáticas. *Entorno Abierto* no se identifica necesariamente con las opiniones vertidas en las colaboraciones firmadas.

Envío de colaboraciones a <sapmciruelos@gmail.com>

Blog: <http://sapmatematicas.blogspot.com.es/>

Twitter: @SAPMciruelos

Mayo de 2021
ISSN: 2386-8821e