ABC, 30 de Abril de 2018
CIENCIA - El ABCdario de las matemáticas
Paz Jiménez Seral y Manuel Vázquez Lapuente

Además de Alan Turing, varios matemáticos polacos expertos en criptografía y permutaciones tuvieron un papel clave en un logro que contribuyó enormemente a la victoria de los Aliados

Comunicaciones cifradas alemanas durante la invasión de Francia - BUNDESARCHIV

Es bien conocida la participación fundamental de Alan Turing y su equipo para descifrar los mensajes que los alemanes mandaban encriptados con la máquina «Enigma», y que tanto contribuyó a acortar la II Guerra Mundial y a asegurar el triunfo aliado. Son menos conocidas las importantes aportaciones de **distintos matemáticos polacos, con Marian Rejewski** a la cabeza, así como las matemáticas que hay debajo de la compleja tarea que realizaron. Desvelaremos en este artículo ambos aspectos y veremos que es un asunto de plena actualidad: tiene algo en común con el cifrado que se usa en WhatsApp.

Permutaciones para cifrar mensajes

Las **distintas maneras de ordenar una determinada cantidad de objetos** en una fila llamó la atención de sabios y filósofos desde la antigüedad por resultar números muy grandes a partir de una cantidad pequeña de objetos. Por ejemplo, el número de las distintas formas de ordenar las 26 letras del alfabeto se calcula mediante los productos 26 x 25 x 24 x … x 3 x 2.

Para hacernos idea del tamaño de este número supongamos que para escribir cada una de esas formas, por ejemplo, la «hfaqkuiyolnjgswrcptezbmvdx», tardamos 10 segundos; si quisiéramos escribirlas todas **necesitaríamos más de 9000 millones de veces la edad del Universo** .

Por otra parte, desde el principio de las comunicaciones entre humanos preocupó el hecho de que un mensaje enviado a un receptor pudiera ser interceptado y leído por alguien no deseado. En el caso de las comunicaciones internas en un ejército preocupaba sobretodo que lo leyera el enemigo. **La criptografía es la ciencia que estudia las posibles transformaciones de un mensaje** para que sólo el receptor al que está dirigido pueda recomponer el mensaje inicial y conocer lo que se le está trasmitiendo.

El número tan enorme de posibles ordenaciones de las letras del alfabeto invitaba a utilizar alguna de esas ordenaciones como procedimiento de cifrado.

Si tomamos como punto de partida la ordenación natural de las 26 letras del alfabeto, o sea «a b c …», cada ordenación nos proporciona una transformación de las letras, de manera que con ella se puede cifrar un mensaje. Por ejemplo, colocando **la ordenación que hemos indicado anteriormente debajo de la ordenación alfabética**

, como en este cuadro:

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
h	f	a	q	k	u	i	y	o	l	n	j	g	s	w	r	c	p	t	e	z	b	m	v	d	x

Tenemos que cada letra se transforma en la letra que tiene debajo. Así el mensaje «hoy ha salido el sol», se transforma en «ywdyh thjoq wkjtw j». **Sólo si se conoce esa trasformación, que los matemáticos denominamos permutación**
, se puede recomponer el mensaje inicial.

Es muy útil representar una permutación mediante sucesiones de letras encerradas en paréntesis de manera que **cada letra se aplique en la siguiente**, y la última de cada paréntesis en la primera de ese mismo paréntesis. Por ejemplo, la permutación anterior se representaría de esta forma: *(ahydqc)(bfuzxv)(giowm)(eknst)(jl)(pr)*
.

Añadamos que cada paréntesis recibe el nombre de ciclo, y claramente un mismo ciclo se puede reordenar trasladando sus letras en un sentido u otro. Por ejemplo, el primer ciclo de la permutación anterior coincide con el *(ydqcah)*. El lector advertirá que **a cada permutación se le asocia una sucesión de números**
que indican las longitudes de los ciclos que forman parte de esa permutación, es el tipo de la permutación. La del ejemplo anterior tiene como tipo: 6, 6, 5, 5, 2, 2.

Julio César ya utilizaba un clase especial de permutaciones de las letras del alfabeto para cifrar sus mensajes, bastaba deslizar el alfabeto un número determinado de lugares. Ese método junto con sus múltiples variantes ha sido utilizado hasta fechas recientes. Pero no fue en criptografía sino en otra parcela de las matemáticas, la de resoluciones de ecuaciones, donde las permutaciones brillaron con gran esplendor.

El álgebra y las permutaciones

En el siglo XVIII, matemáticos como **Lagrange,Ruffini, Cauchy, Abel y Galois se ocuparon en la búsqueda de fórmulas** para expresar las soluciones de ecuaciones de quinto grado, análogas a la fórmula que nos da las soluciones de la ecuación de segundo grado, fórmula bien conocida por nuestros bachilleres. Este problema les llevó a desarrollar una complicada teoría de permutaciones, partiendo del hecho de que si componemos dos permutaciones, es decir, si aplicamos una a continuación de la otra, se obtiene una nueva permutación. Por ejemplo, si aplicamos la permutación anterior y después la permutación:
(ju)(li)(oc)(es)(ar)
.

El resultado es: *(ahydqowmgluzxvbfjicrp)(ekn)(st)*.

Utilizando como herramienta básica las permutaciones y la composición de las mismas, Évariste Galois resolvió el problema anterior probando que no existe ninguna fórmula que exprese las soluciones de ecuaciones de quinto grado. Estos estudios dieron lugar a la bonita y fructífera teoría de los grupos de permutaciones, que posteriormente se extendió a la teoría de grupos en general, con aplicaciones a la Física.

Pero volvamos a la criptografía, y trasladémonos a finales de los años 20 del siglo pasado. Por aquel entonces un polaco, **Marian Rejewski, seguía un curso sobre permutaciones en la Universidad de Poznan** . Este estudiante de matemáticas reconocería años más tarde la importancia que tuvo ese curso en el descifrado de la máquina Enigma, que en aquellos años comenzaba a utilizar el ejército alemán para cifrar sus comunicaciones.

Marian Rejewski - WIKIPEDIA

En 1929, la Oficina de Cifra polaca organizó un curso de criptografía entre estudiantes de matemáticas de la Universidad de Poznan. Esta universidad se encontraba en territorio de influencia alemana por lo que sus alumnos dominaban la lengua germánica. Como consecuencia de ello tres participantes de ese curso, Marian Rejewski y otros dos colegas, fueron contratados por los servicios secretos polacos, en principio de forma temporal, y a partir de 1932 entraron a formar parte de la plantilla de la Oficina de Cifra con sede en Varsovia. El propio Rejewski reconoce que el jefe de los servicios secretos polacos «apreció mucho antes que sus adversarios de otras oficinas de cifra la importancia de requerir a sus criptoanalistas no solo que fueran conocedores de lenguas sino también que **fuesen graduados matemáticos** ».

Rejewski fue sin duda la pieza clave en la rotura de Enigma. Abordó el problema mucho antes que Alan Turing y estableció los procedimientos para el descifrado de los mensajes de Enigma. Dedicó 13 años a su estudio, en condiciones y con medios mucho menores de los que dispuso Turing. Los dos llegaron a conclusiones parecidas, y fue Turing quien pudo aprovecharse de los avances del polaco.

Rejewski y la teoría de grupos

Rejewski se dio cuenta muy pronto que **Enigma era una endiablada máquina generadora de permutaciones** , así que desempolvó sus apuntes sobre teoría de grupos en la asignatura de Teoría de Galois y recordó todo el lenguaje y manipulación de las permutaciones de las 26 letras del alfabeto.

Por ejemplo, recordó la siguiente propiedad: si una permutación se multiplica a su izquierda por otra y a su derecha por la inversa de esta última, la permutación resultante tiene el mismo tipo que la inicial. Para resaltar la importancia de esta sencilla propiedad baste citar que ha sido calificada como **el teorema que hizo ganar la Segunda Guerra Mundial**. El recorrido que la corriente eléctrica realizaba en el interior de Enigma cada vez que se tecleaba una letra era de «ida y vuelta», simulando productos de permutaciones, una de ellas la inversa de la otra. Ese teorema tan especialmente denominado se podía aplicar a Enigma obteniendo unas primeras conclusiones, por ejemplo, que la misma clave serviría para cifrar que para descifrar, o que nunca una letra se cifraba en ella misma.

Nuestro matemático polaco, **en escasamente dos meses** y utilizando abundante material criptográfico, proveniente de los servicios de escucha del ejército polaco, e incluso de la información suministrada por un traidor alemán a través de los servicios secretos franceses, y por supuesto sus conocimientos de permutaciones, resolvió el primer secreto de Enigma que fue el **reconstruir el cableado interno de esta máquina**, cableado que es el que generaba esas permutaciones que servían para cifrar mensajes.

	(efwyxz)(codmtu)(aknqp)(blrsv)(gj)
(ahydqc)(bfuzxv)(giowm)(eknst)(jl)(pr)	(......)(......)(.....)(.....)(..
(acekyx)(fgvojq)(bdupl)(hwmtz)(is)(nr)	(......)(......)(.....)(.....)(..

La solución es:

(efwyxz)(codmtu)(aknqp)(blrsv)(gj)(hi)
(hydqca)(vbfuzx)(owmgi)(knste)(pr)(jl)
(jqfgvo)(ekyxac)(bdupl)(wmtzh)(is)(rn)

	(bcxyzuh)(dfijkgm)(awpq)(et
(dlphrvf)(iyqmztw)(agns)(ekju)(bo)(cx)	(.......)(.......)(....)(..
(afeozmb)(gqrusth)(ckny)(iwvj)(dx)(lp)	(.......)(.......)(....)(..