suma+ 61
Junio 2009, pp. 17-26

Criptografía y matemáticas

La criptografía nació en el mismo momento en que se empezó a usar la escritura. El arte de codificar mensajes para burlar a los enemigos y el arte de descodificar los mensajes captados a los mismos, ha ido cambiando de estrategias y métodos a lo largo de la historia hasta llegar a convertirse en lo que es hoy en día: una ciencia que usa a las matemáticas como herramienta perfecta para sus intereses. En este artículo se da un breve repaso a los métodos criptográficos más famosos de la historia así como una breve muestra de aquellos que usan las matemáticas para la codificación y descodificación de mensajes.

The cryptography was born in the same moment in which it was begun using the writing. The art of codifying messages to avoid the enemies and the art of decoding the messages caught to the enemy, has been changing strategies and methods along the history up to managing to turn what is today: a science that uses the mathematics as ideal tool to mask messages. Here it is given a brief revision to the most famous cryptographic methods of the history as well as a brief sample of those cryptographic methods that use the mathematics for the codification and decodification of messages.

Una vez fui testigo presencial, en una conferencia que no logro recordar con total clarividencia, de la siguiente afirmación sobre la Teoría de Números: "La teoría de números es como la música o el ajedrez: no sirven para nada pero entretienen". Por suerte he tenido la oportunidad de comprobar que no tenía razón en la totalidad de su afirmación, ya que la teoría de números, siendo bonita y entretenida, sí que tiene muchas aplicaciones. En concreto, la teoría de números es el eje fundamental sobre el que giran todos los estudios que, últimamente, se están haciendo en relación con la *criptografía*, tema que es el motivo de este artículo.

La Real Academia de la Lengua define la *criptografía* como "el arte de escribir con clave secreta o de un modo enigmático", y ciertamente es una definición acertada, pues la criptografía se considera actualmente como la ciencia dedicada a estudiar métodos para *codificar* (*cifrar o encriptar*) mensajes secretos; evidentemente el objetivo último de la criptografía es la imposibilidad, por parte de cualquier persona ajena al mensaje, de descifrar un mensaje codificado, pues hay que contar siempre con la existencia gratuita de un adversario, que pondrá todos los medios posibles a su alcance para descifrar los *mensajes secretos*. A la ciencia que estudia los métodos que permiten descifrar mensajes encriptados se le conoce como *criptoanálisis*, y a la unión de ambas ciencias se le ha denominado *criptología*.

Aunque actualmente la criptografía basa todos sus métodos en la teoría de números, la estadística y distintas teorías de la información, la criptografía se originó en el mismo momento en que apareció la escritura. Siempre han existido situaciones en las que el hombre ha necesitado comunicar mensajes de vital importancia a sus semejantes, intentado que sus enemigos no los conocieran, ya que estos mensajes solían estar referidos a las estrategias militares que pudieran usar.

En una primera parte se hace un sucinto recorrido por los métodos criptográficos más relevantes que se han usado a lo largo de la historia, y en una segunda parte se muestra la maquinaria matemática de una serie de métodos criptográficos que se usan o solían usar en una época más reciente.

La utilización de métodos criptográficos de cierta importancia se remonta a 400 años antes de Cristo, en Esparta, donde los espartanos usaban un sistema secreto de escritura durante los enfrentamientos con Atenas. Este sistema de codificación de mensajes consistía en algo tan simple como lo siguiente: el emisor del mensaje y el receptor de éste poseían, cada uno, cilindros idénticos con bases de igual radio, el emisor enrollaba una tira de papel en el cilindro como si de una

Juan José Ortiz Muñoz
IES Miguel Fernández. Melilla

venda se tratara, y una vez enrollada escribía el mensaje a lo largo del cilindro; una vez escrito el mensaje original, se desenrollaba la tira de papel, quedando un mensaje aparentemente caótico que se mandaba al receptor, única persona capaz de descifrar el mensaje a menos que el cilindro fuera robado, único método que puede aportar el criptoanálisis. Los historiadores griegos denominaban a este método *la scitala espartana*.

Scitala espartana

En el siglo II a. C, el historiador griego Polibio, miembro de la Liga Aquea cuando era dirigida por Filipémenes[1] y que fue derrotada por los romanos, usaba un sistema de encriptación y desencriptación muy original y que comunicaba a través de nueve antorchas. Concretamente su método consistía en insertar el alfabeto en una tabla de doble de entrada de cinco filas y cuatro columnas asignando a cada letra el número formado por el número de la fila y el número de la columna en la que la letra estaba situada, como si de coordenadas se tratara. Teniendo en cuenta que el alfabeto romano constaba de veintiuna letras, la I se agruparía junto con la K, y la tabla quedaría así:

	1	2	3	4
1	A	B	C	D
2	E	F	G	H
3	I/K	L	M	N
4	O	P	Q	R
5	S	T	V	X

(Se elegirá I o K según el contexto)

De esta forma al corresponderse la letra T con el número 52, ésta se comunicaría encendiendo las cinco primeras antorchas y las dos últimas. Este método, conocido como *cuadrado de Polibio*, tiene variaciones que hacen de él un buen método, pues a diferencia de lo que ocurre con los cifrarios monoalfabéticos de sustitución, que analizaremos a continuación, altera la frecuencia de los caracteres.

Una de las variaciones más conocidas del cuadrado de Polibio es la conocida como *Cifrado Bífido de Polibio*, usado en los siglos XIX y XX por los nihilistas rusos. En este caso el cuadro de Polibio está compuesto por cinco filas y cinco columnas, y consiste en: primero desordenar el alfabeto escribiendo primero una palabra clave; en segundo lugar y una vez obtenidos todos los números del texto, se disponen en dos filas, de forma que se vuelve a obtener un mensaje numérico que transformaremos en texto codificado usando el cuadrado de Polibio en sentido contrario tomando como números de dos cifras cada uno de los pares numéricos que forman las nuevas columnas. Como ejemplo tomemos como palabra clave CLAVE, la cual permitirá desordenar el alfabeto, y codifiquemos la palabra POLIBIO:

	1	2	3	4	5
1	C	L	A	V	E
2	B	D	F	G	H
3	I/J	K	M	N	O
4	P	Q	R	S	T
5	U	W	X	Y	Z

La palabra POLIBIO será entonces 41351231213135. Ahora La disponemos en dos filas:

4135123
1213135

De esta forma sale el texto numérico 41123153112335, que corresponde con PLIXCFO.

El proceso de desencriptación consiste entonces en hallar la serie numérica del mensaje codificado y disponerlo en dos filas, la primera formada por los números de los lugares impares y la segunda formada por los de lugares pares; una vez hecho esto se coloca la segunda fila consecutiva de la primera que será la serie numérica del texto original.

En el siglo I a. C. el general romano Julio César creó un sistema de encriptación muy simple, consistente en sustituir unas letras por otras. Más concretamente, la sustitución que Julio César utilizó consistía en asignar a cada letra del alfabeto la letra que estaba tres lugares más a su derecha, adoptando el criterio lógico de que tras la letra Z se empezaba de nuevo por la letra A.

La clave de encriptación del conocido como *Cifrario de César* es por tanto el número "3". Teniendo en cuenta que el alfabeto romano sólo tenía veintiuna letras, el cifrario de César se basa en la siguiente sustitución de letras:

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

La primera línea es el alfabeto sin cifrar y la segunda línea es el alfabeto de cifrado. Así por ejemplo, la frase ALEA IACTA EST *(la suerte está echada)*, que Julio César usó en el 49 a. C. cuando decidió atravesar el Rubicón con sus legiones, utilizando su cifrario se convierte en: DOHD MDFAD HXA.

Evidentemente, el cifrario de Julio César es uno de los 20 cifrarios que se pueden hacer de este tipo, basta con ir rotando el alfabeto de la línea de cifrado (la segunda línea).

El cifrario de Julio César está enmarcado dentro de los denominados *cifrarios monoalfabéticos de sustitución*, cuya clave de encriptación es el nuevo alfabeto encriptado. Así pues el cifrario de Julio César es el cifrario de sustitución por excelencia al ser el primero que se conoce a lo largo de la historia. Los cifrarios monoalfabéticos de sustitución perduraron a lo largo del tiempo; así por ejemplo, la Orden de Los Templarios usaba en el siglo XII un método criptográfico de sustitución que asociaba a cada letra del alfabeto un símbolo gráfico.

La ventaja que tienen estos cifrarios es la facilidad con que se encriptan los mensajes, pero unido a esta facilidad a la hora de encriptar mensajes, nos encontramos también con la facilidad de desencriptarlos cuando se dispone de tiempo suficiente.

Un fascinante e ingenioso ejemplo sobre cómo descifran un mensaje codificado por medio de un cifrario de sustitución se encuentra en la obra "El escarabajo de oro" de Edgar Alan Poe. El método que se utiliza en esta obra consiste prioritariamente en conocer cuáles son las letras, parejas de letras y tríos de letras que aparecen con mayor frecuencia en el idioma en que se ha escrito el mensaje original, e intentar encontrar el mensaje original por ensayo-error teniendo estos datos en cuenta. En España, la frecuencia relativa con la que aparecen las letras en los textos depende del estudio estadístico que se realice, pues no se obtiene el mismo resultado si se estudia directamente el diccionario de la Real Academia Española que si estudia libros de texto en general; a continuación se muestran, en orden descendente de aparición, las letras, pares de letras y tríos de letras de nuestro idioma sobre estudios realizados en libros de texto:

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

ES, EN, EL, DE, LA, OS, UE, AR, RA, RE, ON, ER, AS, ST, AL, AD, TA, CO.

QUE, EST, ARA, ADO, AQU, CIO, DEL, NT, EDE, OSA, PER, NEI, IST, SDE.

Pero como es lógico, los criptógrafos, una vez que se dan cuenta de la vulnerabilidad del método, intentan encontrar variantes de los métodos para que éstos no sean tan vulnerables. Este es el caso de los cifrarios *homofónicos* y los *nomenclátores*, cifrarios monoalfabéticos de sustitución que intentan luchar contra el análisis estadístico de los textos cifrados. Los *cifrarios homofónicos* consisten en considerar el alfabeto con unas cuantas letras repetidas, principalmente las de mayor frecuencia de aparición en el idioma, y en el alfabeto cifrado colocar tantos símbolos distintos como letras se han insertado en el alfabeto original. De esta forma se consigue que las frecuencias de aquellas letras más relevantes queden disminuidas.

La forma de codificar un mensaje original es igual que en los anteriores, salvo para aquellas letras que aparecen repetidas en el alfabeto original, para las cuales habrá una regla para determinar qué letra escoger. El primer cifrario homofónico del que se tiene constancia se utilizó en 1401 en la correspondencia cruzada entre la Corte de Mantua y Simeone de Crema. En el siguiente ejemplo de cifrario homofónico la palabra MAREA es sustituida por AHD%$:

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

S T U V W X Y Z
C R & F G V T B

Desde el siglo XVI hasta la primera mitad del siglo XIX, el sistema de cifrado más utilizado en las correspondencias diplomáticas fue un sistema mixto que se denomina *nomenclátor*. Los cifrarios nomenclátores están formados por dos núcleos: un primer núcleo formado por un cifrario homofónico, y un segundo núcleo compuesto por una serie de símbolos especiales que se corresponden con algunas palabras o frases concretas. De entre los cifrarios nomenclátores más famosos se encuentra el empleado en 1571 por el embajador en Francia de la Reina Isabel de Inglaterra.

Paralelamente a los cifrarios nomenclátores, se usaban con mucha frecuencia los denominados *cifrarios polialfabéticos de sustitución*, que tal y como su nombre indica, utilizan varios alfabetos a la hora de encriptar un mensaje. De entre estos cifrarios, el más importante es el conocido como *cifrario de Vigenère*[2]. La clave de este cifrario es una *palabra-clave*; se trabaja sobre una tabla formada por 26 alfabetos dispuestos uno bajo el otro de forma que el segundo alfabeto empieza por la letra B, el tercero por la letra C, y así sucesivamente hasta el último que empezará por la letra Z. A continuación se muestra cómo queda la disposición de la tabla:

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

Para encriptar un mensaje con el cifrario de Vigenère, debajo del mensaje que se va a encriptar se escribe la palabra clave tantas veces como sea preciso y, en su caso, truncarla al final del texto. De esta forma, cada letra del mensaje posee una letra clave que se encuentra mediante la intersección de la columna cuya primera letra es la original con la fila cuya primera letra es la letra clave correspondiente. Con un ejemplo se comprenderá mejor: supongamos que la palabra clave es DIA, y que queremos codificar la palabra RAREZAS, entonces se tiene la siguiente situación:

R A R E Z A S
D I A D I A D

La letra clave correspondiente a la primera R es la letra D, entonces la letra que se genera mediante este cifrario es la letra U, ya que la intersección de la columna que empieza peor la letra R con la fila que empieza con la letra D es la letra U. De esta forma la palabra codificada será:

UIRHHAV

Desencriptar un mensaje codificado por este cifrario es bastante fácil: se escribe debajo de la palabra codificada la palabra clave tantas veces como haga falta, como se hace para el proceso de codificación, y para encontrar cada letra original se busca la letra codificada en la fila de la correspondiente letra clave, miramos la letra inicial de la columna a la que pertenece y ésta determina la letra original.

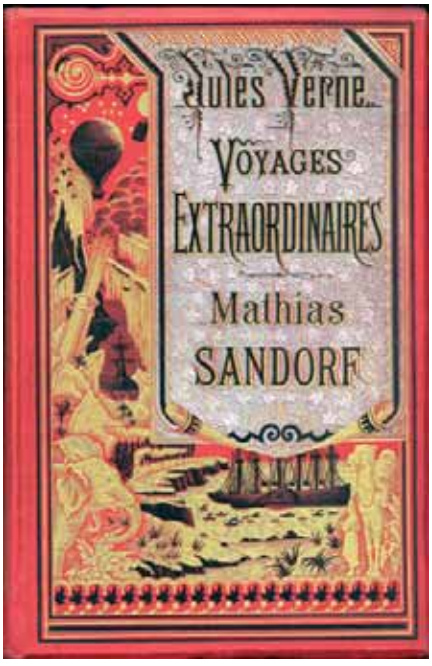
Como se puede observar el proceso descrito para la descodificación es tan sólo el proceso inverso al de codificación.

Existen otros cifrarios polialfabéticos de sustitución que utilizan una tabla un poco más pequeña que el cifrario de Vigenère, y para los que la clave, en vez de ser una palabra, es un *número-clave*.

Un ejemplo de este tipo de cifrario son los conocidos como *cifrarios de Gronsfeld*. Estos cifrarios no tienen demasiada importancia teórica por ser en esencia cifrarios de Vigenère; la diferencia radica en los métodos de encriptación y desencriptación, los cuales son leves modificaciones de los utilizados en aquel.

En cierto modo, podemos afirmar que todos los métodos de desencriptación vistos hasta ahora proceden del cifrario de César, ya que todos son cifrarios de sustitución. Sin embargo la *scitala espartana* no es un cifrario de sustitución, sino un *cifrario de transposición*. Los métodos criptográficos por transposición quedaron en olvido hasta que alrededor del siglo XVI el científico, excelente y prolífico matemático italiano Cardano introdujo los cifrarios de *rejillas.* Estos cifrarios reciben este nombre porque gran parte de los códigos secretos que se utilizan se basan en el empleo de un conjunto de distintas rejillas perforadas. Las rejillas se colocan sobre un cuadro polialfabético determinando, gracias a éstas, las letras codificadas.

En la obra *Mathias Sandorf* de Julio Verne, a veces la trama se centra en temas de criptografía relacionados con la utilización de ciertas rejillas perforadas que permiten encriptar y desencriptar mensajes secretos de gran importancia. Esta obra deja además constancia del gravísimo problema que tiene este tipo de cifrarios: la desencriptación la puede hacer toda persona que posea la rejilla adecuada, y puede ocurrir, como bien lo plasmó en la obra su autor, que la rejilla sea robada por una persona no deseada.



Los cifrarios de transposición y los de sustitución, tanto monoalfabéticos como polialfabéticos, cayeron en desuso en la primera mitad del siglo XIX cuando a finales del siglo XVIII se dio lugar la denominada hoy en día *Revolución Industrial*. La nueva corriente filosófica que esta revolución trajo consigo hizo que los criptógrafos inventaran sistemas criptográficos basados en las máquinas. Es por este motivo que a los cifrarios anteriormente mencionados se les denominan vulgarmente *cifrarios de lápiz y papel*.

El cifrario mecánico más antiguo que se conoce fue creado a finales del siglo XVIII por el que fuera presidente de los Estados Unidos: Thomas Jefferson. Este cifrario, conocido como *el cilindro de Jefferson*, tras caer en el olvido al no ser usado por su inventor, fue reconstruido por un famoso criptógrafo llamado Etienne Bazeries alrededor del año 1890. A partir de ese momento, el cilindro de Jefferson fue de gran utilidad, hasta tal punto que fue utilizado por los EEUU durante la segunda Guerra Mundial, y esporádicamente en la postguerra. El cifrario de Jefferson consiste en un cilindro formado por 26 discos iguales (el que construyó Bazeries sólo tenía 20 discos) que rotan sobre un eje que atraviesa los centros de los discos. Cada disco tiene su borde exterior dividido en 26 partes iguales, en los que se colocan aleatoriamente las 26 letras del alfabeto, intentado que cada disco tenga una ordenación diferente del alfabeto. El mensaje a codificar se agrupa en bloques de 26 letras, y si el último bloque no completa las 26 letras, se colocan letras nulas hasta completarlo. De esta forma, después de rotar los discos hasta conseguir escribir el bloque original, el bloque cifrado es el que se lee en la línea que, contada al rotar el cilindro en sentido positivo, nos indica la clave.

Cilindro de Jefferson

El cifrario de Jefferson fue el precedente de cifrarios mecánicos que, basándose en la rotación, son de mecánica mucho más complicada. Tal es el caso de la famosa máquina encriptadora *Enigma*, usada por los alemanes en la Segunda Guerra Mundial. El funcionamiento de esta máquina se basa en el cifrario de Jefferson, solo que en este caso cada disco giratorio tiene 26 nodos eléctricos (uno por cada letra del alfabeto) en cada cara, de forma que cada nodo de un disco está en contacto con cada nodo del disco siguiente. Cuando se inserta en la máquina una letra, el primer disco gira un lugar, si es el giro número 26 el segundo disco gira también un lugar, si en el segundo disco también es el número 26 entonces el tercer disco también gira un lugar, y así sucesivamente. Una vez que se producen los giros de discos, una señal eléctrica que parte del nodo correspondiente a la letra original, pasa por los nodos de contacto alineados con él; el nodo activado en el último disco corresponde a una letra que será la letra codificada de la inicial.

La clave de *Enigma* queda determinada por la estructura interna de los rotores y por su posición inicial. A pesar de que utilizaban distintas máquinas y distintos tipos de discos, como todas funcionaban mediante el mismo mecanismo, cuando los criptoanalistas británicos y polacos conocieron dicho funcionamiento, los ingleses recurrieron a enormes máquinas de calcular que le permitieron descifrar los mensajes encriptados de los alemanes. Este hecho está muy bien reflejado en la obra *Fuerteventura* de Alberto Vázquez Figueroa, la cual basa su trama en el intento de adquisición, por parte de la inteligencia Británica, de una *Enigma* incorporada en un submarino del ejército Alemán.

Máquina Enigma

Es importante mencionar que el ejército estadounidense, al mismo tiempo que usaba el cilindro de Jefferson, encontró un

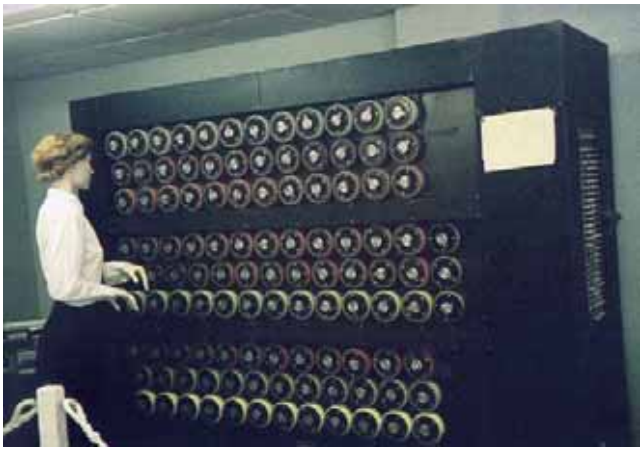
método criptográfico muy sencillo pero no por ello menos fiable. Quizás es el método más fiable de todos los comentados anteriormente: incluían en su ejército indios navajos, cuyo idioma no puede ser aprendido por nadie que no fuese criado entre ellos, y transmitían los mensajes en ese idioma. Se dice que sus mensajes no fueron descifrados nunca.

Si recordamos, el problema fundamental que tienen los cifrarios de rejillas recae en que si alguna persona no deseada se apodera de la rejilla entonces el mensaje es fácilmente descifrable. Este problema es igualmente aplicable al cifrario de Jefferson y a Enigma, que una vez en manos enemigas, es más fácil desenmascarar su sistema de cifrado y descifrado. A finales del siglo XIX, el criptógrafo holandés Auguste Kerckhoffs estableció una serie de recomendaciones que deben cumplir los sistemas criptográficos para considerarlos óptimos. Las recomendaciones establecidas por Kerckhoffs son:

1º) El sistema de cifrado debe ser impenetrable, si no en teoría, el menos en la práctica.
2º) El hecho de que el sistema se vea comprometido no debe dañar a los corresponsales.
3º) La clave debe ser fácil de memorizar y fácil de sustituir.
4º) Los criptogramas deben ser idóneos para su comunicación por los medios de transmisión habituales.
5º) El aparato y los documentos de cifrado deben ser fáciles de transportar; es necesario que la operación de cifrado la pueda realizar una sola persona.
6º) El sistema debe ser sencillo, no se debe basar en el conocimiento de largas listas de normas ni requerir esfuerzos mentales excesivos. Al menos la complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

Como se puede observar, los sistemas criptográficos comentados anteriormente no cumplen, entre otras, la primera de las seis recomendaciones.

La invención de máquinas gigantes de cálculo con el objetivo de intentar desenmascarar a *Enigma* es sin duda el comienzo de la era informática. La informática desde su comienzo hasta nuestros días ha avanzado a un ritmo vertiginoso que ha desembocado, entre otros logros, en la creación de redes informáticas de comunicación, como es el caso de Internet. La utilización de estas redes informáticas ha hecho necesario el uso de criptosistemas seguros para cifrar mensajes, ya que los mensajes transmitidos a través de estas redes pueden ser capturados por miles de personas. Debido a este motivo se hace imprescindible utilizar sistemas de encriptación que sean impenetrables, si no en teoría sí en la práctica. Es alrededor de 1975 cuando se crean criptosistemas con las características propias que los hacen óptimos. Estos sistemas de encriptación basan su funcionamiento en la teoría de números, aprovechando al servicio de la criptografía la increíble capacidad de cálculo numérico que poseen los ordenadores. Es aquí donde entra la parte puramente matemática y cuando la criptología en general deja de ser considerada un arte para pasar a ser considerada una ciencia.



Bomba de Turing en Bletchley Park

En principio se hace necesario buscar un modo de trasladar las letras a números. Esto no es una novedad histórica, ya que el código Morse que se usaba en el telégrafo utiliza rayas y puntos para caracterizar cada letra del alfabeto. Cambiando puntos por ceros y rayas por unos, cada letra del alfabeto se corresponderá de esta forma con un número cuyos dígitos solo cuentan con ceros y unos, es decir, cada letra del alfabeto se corresponderá con un número del sistema binario.

Sin embargo, esta forma de trasladar letras a números no es la que nos conviene para los sistemas criptográficos actuales, sino que nos conviene la que asigna a cada letra el número de dos cifras que refleja el lugar que ocupa en el alfabeto, es decir:

A = 00 B = 01 C = 02 D = 03 E = 04 F = 05 G = 06
H = 07 I = 08 J = 09 K = 10 L = 11 M = 12 N = 13
Ñ = 14 O = 15 P = 16 Q = 17 R = 18 S = 19 T = 20
U = 21 V = 22 W= 23 X = 24 Y = 25 Z = 26

Para trabajar con estos criptosistemas numéricos hay que recurrir a la teoría de números congruentes *módulo n*, siendo "n" un número natural (n=27 en el ejemplo anterior). Los números congruentes van a ser por tanto una invención matemática que va ser útil, a diferencia de otros mundos abstractos inventados por los matemáticos, y que además será de vital importancia para conseguir el objetivo que nos proponemos: encontrar un criptosistema que sea prácticamente imposible de vulnerar en su puesta en práctica y que además verifique las recomendaciones de Kerchoffs.

Se recuerda rápidamente que los números *módulo n*, n número natural, son los números naturales que van desde el cero

hasta el número n-1, ambos inclusive. En sí esto no parece tener mucha importancia, pero sí que la tiene: los números mayores o iguales que "n" y los números negativos se identifican con alguno de los números módulo n a través de la siguiente regla:

El número entero p se identifica con el número q, siendo $0 \leq q < n$, si el resto de dividir p entre n resulta ser q, en cuyo caso se escribe en la forma: "$p \equiv q \pmod{n}$" y se nombra *p es congruente con q módulo n.*

La primera aplicación que podemos hacer de los números módulo n es bastante curiosa. Recuérdese por un momento cuál era el método utilizado en el cifrario de Julio César: sustituir cada letra por la situada tres lugares más allá. Si convertimos las letras en números según la tabla correspondiente, el sustituir una cierta letra por la situada tres lugares más allá, no es sino que sumar a su número de identificación tres unidades, teniendo en cuenta de que cuando nos pasamos de 25 hay que empezar de nuevo por 0. Este método de sustitución numérica es muy fácil de expresar por medio de congruencias módulo 27 en la siguiente forma: Si m representa la letra original y h representa la letra cifrada, entonces el cifrario de Julio César es el resultante de aplicar la sencilla fórmula $\eta \equiv \mu + 3 \pmod{27}$.

Con la notación modular y con los números modulares es más fácil detallar todos los distintos cifrarios de sustitución como los de Julio César, ya que todos ellos siguen la regla: $\eta \equiv \mu + k \pmod{27}$ para $0 \leq k < 27$. Es por este motivo por el que se puede afirmar de nuevo que existen 26 cifrarios de Julio César diferentes cuando el alfabeto tiene 27 letras. Está claro entonces que en estos casos la clave será el número k.

A continuación se muestran una serie de criptosistemas basados todos ellos en la teoría de números. Los tres últimos, a diferencia de los dos primeros, tienen en común el hecho innovador de hacer pública una parte de la clave del sistema; concretamente suele ser la clave de codificación la que se da a conocer públicamente mientras que la de descodificación se mantiene en secreto. De esta forma se resuelve el problema de comunicar previamente la clave entre el emisor y el receptor del mensaje, problema que se encuentra principalmente en encontrar un canal seguro para transmitir dicha clave.

Criptosistemas matriciales

Los cifrarios matriciales son un tipo de sistemas criptográficos que basan su funcionamiento en la teoría de matrices. El primer paso consiste en disponer las letras del mensaje original en forma de tablas, es decir, disponerlas en un número determinado de filas y columnas. Una vez dispuestas en forma de tablas de tamaños predeterminados, cada letra se sustituye por su homólogo numérico, obteniendo así una matriz.

La clave del sistema está compuesta por dos números enteros positivos k y n, y una matriz inversible U de tamaño k y de matriz inversa U^{-1} módulo 27, es decir m.c.d.(det(U), 27)=1. Para cifrar un mensaje se deben seguir los siguientes pasos:

1º) Escribir el mensaje original en bloques de k filas y de n columnas.
2º) Sustituir las letras de cada bloque por sus números correspondientes, obteniendo así matrices M de k filas y de n columnas (es decir, son matrices de $M_{k \times n}$). Se les llaman matrices originales.
3º) Para cada matriz original M, calculamos su matriz cifrada C mediante la relación siguiente:
$C \equiv U \cdot M \pmod{27}$
4º) Sustituir los términos de cada matriz C por sus letras homólogas.

De esta forma se obtiene una serie de bloques de letras de k filas y de n columnas que al deshacerlos nos dará el mensaje cifrado. Como el receptor sabe que se está trabajando con matrices de k filas y de n columnas, éste seguirá los siguientes pasos para desencriptar el mensaje recibido:

1º) Escribir el mensaje cifrado en bloques de k filas y de n columnas.
2º) Sustituir las letras de cada bloque por sus números correspondientes, obteniendo así las matrices cifradas C.
3º) Calcular las matrices originales M mediante la siguientes relación: $M \equiv U^{-1} \cdot C \pmod{27}$.
4º) Sustituir los términos de cada matriz M por sus letras homólogas.

Criptosistema DES (Data Encryption Standard)

Este criptosistema fue creado en los Estados Unidos en el año 1977 con el fin de ser un sistema de protección de información utilizado en los diferentes estados bajo un sistema criptográfico común, admitido como estándar. El sistema DES fue desarrollado por IBM e inspirado en un sistema anterior que consistía en una concatenación de transformaciones.

El algoritmo en que se basa el sistema DES es un algoritmo de cifrado-descifrado que usa concretamente bloques de ocho filas por ocho columnas, es decir, bloques de 64 números. Dar explícitamente el algoritmo es muy engorroso, basta con tener una clara idea de su funcionamiento.

La clave del sistema es privada, está compuesta por 16 subclaves $k_1, \ldots, k_{16}$ y otra clave que es una permutación P de los 64 números que componen cada bloque obtenido a raíz del texto original. Para cada bloque B, el algoritmo es el siguiente:

1º) Aplicar la permutación P al bloque, obteniendo así un nuevo bloque B´ con los mismos números pero en un orden diferente.
2º) El bloque B´ se divide en dos subbloques de 32 números: L_0 y R_0. Es decir B = (L_0 | R_0).
3º) Mediante la clave k_1, R_0 se transforma en R_1,y como bloque L_1 se toma R_0.
4º) Mediante la clave k_2, R_1 se transforma en R_2, y como bloque L_2 se toma R_1.
.....
.....
17º) Mediante la clave k_{15}, R_{14} se transforma en R_{15}, y como L_{15} se toma R_{14}.
18º) Mediante la clave k_{16}, R_{15} se transforma en R_{16}, y como L_{16} se toma R_{15}.
19º) Al nuevo bloque B´´ = (R_{16} | L_{16}) se le aplica la permutación inversa de P, obteniendo así el bloque cifrado.

Criptosistema Exponencial

El cifrario exponencial fue creado en 1978. Tiene como clave pública un número primo "p" y como clave privada un número entero "e" de forma que el máximo común divisor de "e" y "p – 1" es uno: m.c.d. (e, p – 1) = 1, es decir, e y p son tales que de entre los divisores de e y de p –1 no existen comunes a ambos salvo quizá el 1. La clave de descifrado también es secreta al ser un número "d" tal que $d \cdot e \equiv 1 (\mathrm{mod}\ p - 1)$.
La forma de encriptar un mensaje mediante el cifrado exponencial es la siguiente:

1º) Se convierten las letras del mensaje en sus equivalentes numéricos.
2º) Buscamos un número m de forma que 2m sea el mayor número natural tal que todos los bloques de números correspondientes a 2m letras sean menores que p.
3º) Se agrupan los números resultantes del primer paso en bloques de 2m dígitos. Si el último bloque no cubriera los 2m dígitos, se implementarían letras nulas.
4º) Cada bloque μ del mensaje original se cifra siguiendo la relación $\eta \equiv \mu^e \pmod p$, obteniendo para cada bloque original el codificado η.

De esta forma el texto codificado obtenido estará formado por una serie de números enteros menores que p, pues para cada bloque pedimos que se obtenga un número de entre los números módulo p. Cada entero obtenido se corresponde con cada uno de los bloques iniciales.

El emisor del mensaje, a la hora de codificarlo toma la clave pública (e, p) del receptor para que al mandarlo sea el receptor la "única" persona que puede descodificarlo, ya que es éste quien únicamente conoce la clave secreta d. La forma en que se realiza la desencriptación del mensaje recibido es fácil, pues sólo requiere los siguientes pasos:

1º) A cada número entero menor que p se le hace la siguiente operación: $\mu^* \equiv \eta^d \pmod p$.
Teniendo en cuenta que $\eta \equiv \mu^e \pmod p$ y que $d \cdot e \equiv 1 \pmod{p-1}$, con un poco de álgebra y un poco de teoría de números se deduce que $\mu^* \equiv \mu$.
2º) Una vez obtenidos los bloques de números originales, cada dos números tiene su letra correspondiente, dando así el mensaje original.

Obsérvese que mientras mayor sea el número primo p, más difícil debe ser para el criptoanalista descifrar el mensaje. Aun conociendo una parte del texto inicial μ y la correspondiente parte codificada η, el criptoanalista debe encontrar un número e de forma que $\eta \equiv \mu^e \pmod p$, y por tanto debe ser un logaritmo de η en base μ módulo p. Cuando el número primo p es muy grande se requieren una cantidad tal de operaciones para encontrar el mencionado logaritmo, que los ordenadores más modernos con los métodos actuales tardarían miles de años.

Criptosistema RSA

Este cifrado fue presentado, paralelamente al cifrado exponencial, en 1978. Recibe este nombre por los apellidos de sus creadores: R. L. Rivest, A. Shamir y L. Adleman.

El criptosistema RSA tiene como clave pública un par de números (e, N) con las siguientes condiciones:

- N = p·q, donde p y q son dos números primos.
- El número e debe ser tal que mcd (e, ϕ(N)) = 1, donde ϕ(N) es el número de enteros que son menores que N y primos con él (función ϕ de Euler).

La clave privada para el par (e, N) es un número "d" inverso de "e" en el conjunto de los números módulo ϕ(N), es decir: tal que $d \cdot e \equiv 1 \pmod{\phi(N)}$.

La forma de encriptar un mensaje mediante el cifrado RSA es la siguiente:

1º) Se convierten las letras del mensaje en sus equivalentes numéricos.
2º) Se agrupan los números resultantes en bloques de números del mayor tamaño posible y con un número par de dígitos. Si el último bloque no cubriera los 2m dígitos, se implementarían letras nulas.
3º) Cada bloque μ del mensaje original se encripta siguiendo la relación $\eta \equiv \mu^e \pmod N$, obteniendo para cada bloque original el bloque codificado h.

Cada persona tendrá una clave (e, N) que hará pública y un número "d" inverso de "e" módulo N que será su clave privada. De esta forma si una persona quiere mandar un mensaje,

a la hora de codificarlo tomará la clave pública (e, N) del receptor para que de esta forma sea el receptor la "única" persona que puede desencriptar el mensaje codificado, ya que es ella quien únicamente conoce la clave secreta "d".

La forma en que se realiza la desencriptación del mensaje recibido es fácil, pues sólo requiere los siguientes pasos:

1º) A cada bloque de números h se le hace la siguiente operación: $\mu^* \equiv \eta^d \pmod p$.
Teniendo en cuenta que $\mu^* \equiv \eta^e \pmod N$ y que $d \cdot e \equiv 1 \pmod{\phi(N)}$, con un poco de álgebra y un poco de teoría de números se deduce que $\mu^* \equiv \mu$.
2º) Una vez obtenidos los bloques de números originales, cada dos números tiene su letra correspondiente, dando así el mensaje original.

Como se ha podido observar los dos criptosistemas son muy parecidos, pero es algo más sutil que una simple similitud, ya que el sistema RSA es una generalización del sistema Exponencial. Esta generalización se ve más clara con las siguientes precisiones:

Criptosistema Exponencial	Criptosistema RSA
Clave pública modular: Número primo p Clave exponencial de cifrado: Numero privado e con mcd (e, p) =1	Clave pública modular: Producto de dos primos, es decir un número N tal que N = p·q Clave exponencial de cifrado: Número público e tal que mcd (e, p·q)=1
Clave exponencial de descifrado: Número privado d tal que es el inverso de e módulo p-1.	Clave exponencial de descifrado: Número privado d tal que es el inverso de p·q módulo ϕ(p·q). **Observación:** Cuando p y q son primos se verifica que ϕ (p·q) = (p-1)·(q-1).

El criptosistema RSA es uno de los más útiles hoy en día. Esta utilidad se debe principalmente a dos hechos importantes:

1º) Existen hoy en día algoritmos muy rápidos para crear números primos. Estos algoritmos son tales que, con los ordenadores de hoy en día, en pocos minutos se encuentran números primos del orden de cien o más dígitos, lo cual permite encontrar el número N fácilmente. Del mismo modo existen algoritmos muy rápidos para calcular el inverso de e módulo ϕ(N) conocidos p y q.
2º) Por el contrario no se conocen algoritmos rápidos para descomponer un número compuesto. Con los métodos que se conocen hoy en día, ni los ordenadores actuales más potentes tardarían menos de algunos miles de años en descomponer un número que sea producto de dos números primos de cien dígitos cada uno (¡El producto de dos números de cien dígitos tiene al menos ciento noventa y nueve dígitos!)

Como la desencriptación de un mensaje por parte de una persona ajena al mensaje pasa por conocer el número d, esta persona tiene dos caminos posibles: encontrar la descomposición factorial del número N en sus dos números primos y así conocer ϕ(N), o encontrar f(N) directamente. Por desgracia para los criptoanalistas, si ya es difícil encontrar la factorización en números primos del número N, no es menos difícil encontrar directamente el número ϕ(N). Esto hace al sistema infalible en la práctica.

Aún así, se hace recomendable dar una serie de recomendaciones a la hora de escoger los números primos p y q para evitar posibles métodos especiales de factorización:

- p – 1 y q –1 deben tener grandes factores primos.
- El m.c.d.(p – 1, q – 1) debe ser pequeño.
- Los números primos p y q deben tener una cantidad de dígitos similares.

Criptosistema de ElGamal

El criptosistema que se muestra a continuación es otro criptosistema de clave pública basado también en la exponenciación modular. Para trabajar con el sistema de ElGamal, se necesita fijar un número primo "p", y encontrar un número "α" tal que $0 \le \alpha \le p-1$ y $\alpha^{p-1} \equiv 1 \pmod p$. Ambos números son números fijos para todos los usuarios, y por tanto en cierto modo forman parte de la clave pública.

Cada usuario debe escoger al azar un número natural "r" tal que $2 \le r \le p-1$; este número r será su clave secreta. La clave pública será el número "b" con $0 \le b \le p-1$ que verifica $b \equiv \alpha^r \pmod p$.

Para cifrar un mensaje original el emisor tomará la clave pública del receptor y realizará la siguientes operaciones:

1º) Transformar el mensaje original en su homólogo numérico. Tomar bloques de números pares, siempre con un número de dígitos menor que el que tiene el número primo p. Los denotaremos por μ.
2º) Escoger al azar un entero "k" y calcular a^k módulo p.
3º) Cifrar cada bloque original m mediante la relación:
$\eta \equiv \mu \cdot (b^k) \pmod p$
4º) Transmitir el par $(\alpha^k, \ \eta)$.

El resultado de la transmisión se puede ver como el texto original cubierto con una máscara b^k junto con una pista α^k que sirve para desenmascarar el texto cifrado. Lo bueno del méto-

do es que la pista sólo podrá usarla quien conozca el número r.

Como el receptor del mensaje tiene su clave privada de descifrado, tan sólo tendrá que realizar la siguientes operaciones:

1º) Calcular el número β tal que $\beta \equiv (\alpha^k)^r \pmod p$.
2º) Calcular η/β, cuyo resultado será el mensaje numérico original μ.

A pesar de que los sistemas de encriptación de clave pública tienen bastantes ventajas, ninguno de ellos puede competir en rapidez con los sistemas de clave secreta como el sistema DES.

Actualmente lo que se intenta es aprovechar las ventajas del RSA y la rapidez del DES, obteniendo de esta forma lo que se ha denominado como *sistemas híbridos*, pero este tema habrá que estudiarlo con mucho detenimiento.

NOTAS

1 La Liga Aquea era una confederación de doce ciudades-estados de la región costera Acaya en el norte del Peloponeso en la Antigua Grecia. Filipémenes fue uno de sus más destacados generales.

2 Diplomático francés que vivió en la segunda mitad del siglo XVI.

REFERENCIAS BIBLIOGRÁFICAS

ABRAMSON N. (1981): *Teoría de la Información y Codificación*. Paraninfo.

ALLAN POE, E. (1991): "El escarabajo de Oro" en *Cuentos*. Planeta, Barcelona.

CABALLERO, P. (1996)*: Introducción a la Criptografía*. Ra-Ma, Madrid.

CESID (1991): *Glosario de términos de Criptología*. CESID. Madrid.

DE GUZMÁN, M.(1996): *Aventuras matemáticas. Una ventana hacia el "caos" y lo impredecible*. Pirámide, Madrid.

MOLINA MATEOS, J. M. (1994): *Seguridad, información y poder*. Incipit.

RIFÁ, J. y HUGUET, LL. (1991): *Teoría matemática de la información. Criptología*. Masson, Barcelona.

SGARRO, A. (1990): *Códigos secretos*. Pirámide, Madrid.

TUCHMAN, B. W. (1984): *El telegrama Zimermann*. Argos-Vergara.

VACCA, J. (1997): *Los secretos de la Seguridad en Internet*. Anaya Multimedia.

VAZQUEZ FIGUEROA, A. (1999): *Fuerteventura*. Plaza y Janés, Barcelona.