NÚMEROS
Revista de Didáctica de las Matemáticas
http://www.sinewton.org/numeros
ISSN: 1887-1984
Volumen 74, julio de 2010, páginas 5–17

Las matemáticas de lo secreto

Mikel Lezaun Iturralde (Universidad del País Vasco)

Fecha de recepción: 3 de febrero de 2010
Artículo solicitado al autor por la revista

Resumen

En un mundo en que el que cada vez más los medios de comunicación son electrónicos, la seguridad de las transacciones electrónicas nos afecta a todos. La criptografía, la seguridad de la información en general, actualmente está basada en métodos matemáticos, son un campo de nuestra vida cotidiana en el que el aporte de las matemáticas es esencial. En este artículo se muestran algunos sistemas de cifrado artesanales de la criptografía clásica y se introducen los algoritmos de cifrado, de autentificación de documentos y firma digital hoy en día más utilizados: los RSA, que están basados en un resultado clásico de la teoría de números. El estilo del artículo es narrativo, todos los métodos se explican con ejemplos, con comentarios históricos. Su contenido se puede utilizar para diseñar un "taller de matemáticas" dirigido a estudiantes de nivel preuniversitario.

Palabras clave Criptografía, Sistema RSA, Firma digital

Abstract

In a world where more and more media are electronic, security of electronic transactions is an issue that affects us all. Cryptography, in general the security of information, is currently based on mathematical methods; it is an area of everyday life in which the contribution of mathematics is essential. This article shows some artisanal ciphers systems of classical cryptography and introduces the encryption method, authentication of documents and digital signature more used today: the RSA algorithm, which is based on a classical result of number theory. The style of the article is narrative; all methods are explained with examples, with historical comments. Its content can be used to design a math workshop for pre-college students.

Keywords Cryptography, RSA algorithm, Digital Signature

A P E R T U R A

1. Introducción

Junto con la necesidad de comunicarnos, convive un interés por hacerlo sin que terceras personas se enteren de lo que decimos. Cuando hablamos en presencia de otros bajamos la voz, nos tapamos la boca o simplemente nos apartamos para que no nos escuche nadie. Cuando se trata de un mensaje escrito, tener la seguridad de que su contenido sólo llegará a su destinatario es algo muy difícil de conseguir.

Las primeras formas de asegurar el secreto de un mensaje importante consisten en ocultarlo, ya sea camuflándolo dentro de otros textos, escribiéndolo con tintas invisibles, modificando su soporte físico o disimulando su misma existencia. Así, Herodoto cuenta cómo un tal Histieo, para contactar con su yerno y solicitarle ayuda en su empeño de rebelarse contra el rey persa, afeitó la cabeza de su

esclavo más leal, le tatuó en ella el mensaje secreto, esperó a que le creciera el pelo, y envió al esclavo con la instrucción de que le afeitara la cabeza.

La criptología es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. Esta ciencia está dividida en dos grandes ramas: la criptografía, ocupada del cifrado de mensajes en clave y del diseño de criptosistemas, y el criptoanálisis, que trata de descifrar los mensajes en clave, de romper el criptosistema.

Históricamente, el primer sistema que no era un mecanismo de ocultación y que los criptólogos reconocen como propio, se debe a Julio César. En él, cada letra se reemplazaba por su desplazada tres lugares en el alfabeto. Así, CICERON se sustituía por FLFHURP. Todavía hoy, una sustitución obtenida desplazando las letras del alfabeto un número cualquiera de posiciones se denomina “alfabeto de Julio César”. En la actualidad, el sistema criptográfico más utilizado tanto para cifrar como para autentificar documentos es el denominado RSA, iniciales de sus autores, los matemáticos y profesores de Ciencias de la Computación Ronald L. Rivest (1947-), Adi Shamir (1952-) y Leonard Adleman (1945-), que lo inventaron en 1977.

Este artículo lo hemos dividido en tres partes. En la primera mostramos algunos sistemas de cifrado artesanales fáciles de poner en práctica y que dan una visión panorámica de la criptografía clásica, en la segunda se introduce el sistema de cifrado RSA, y en la tercera la autentificación de documentos y firma digital RSA. Todos los métodos se explican con ejemplos, con comentarios históricos, por lo que el resultado pretende ser un artículo didáctico, cuyo contenido se pueda utilizar para diseñar un “taller de matemáticas” dirigido a estudiantes de nivel preuniversitario.

2. De la época artesanal a las máquinas de cifrar

Hasta comienzos del siglo XX, se puede decir que la criptografía era una actividad artesanal. Para cifrar mensajes, además de técnicas de ocultación, básicamente se han utilizado dos tipos de procedimientos: la trasposición y la sustitución. La trasposición consiste en cambiar el orden de las letras del texto, mientras que la trasposición reemplaza cada letra del mensaje por otro símbolo. Para ponerlos en práctica se han usado métodos manuales y métodos mecánicos basados en aparatos diseñados al efecto. Veamos algunos ejemplos históricos ilustrativos.

2.1. Rejilla de Cardano

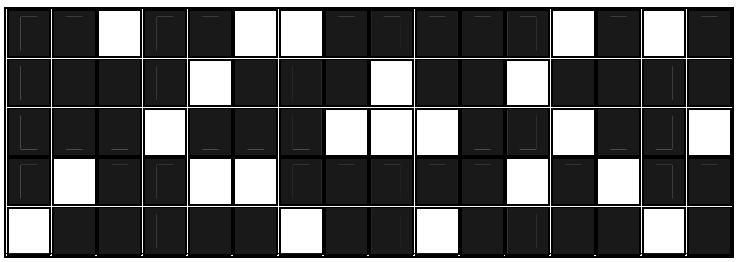


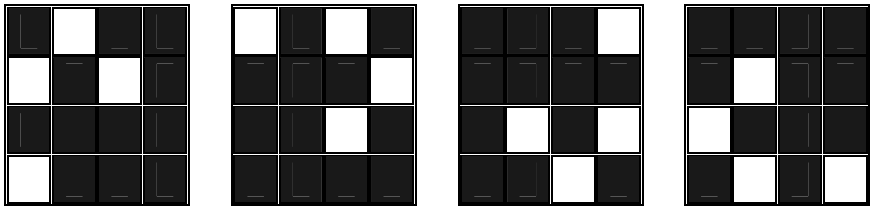
Figura 1. Rejilla de Cardano

La rejilla ideada por Gerolamo Cardano (1501-1576) es una placa metálica delgada en la cual se han agujereado unas ventanas rectangulares (ver la figura 1). Quien desee cifrar un mensaje lo escribe letra a letra en las ventanas, luego retira la placa y rellena el resto del espacio con un texto anodino.

Así el mensaje queda escondido en todo el texto. Para recuperarlo, se vuelve a poner una placa similar sobre el texto y en los huecos aparecerá el mensaje. Se trata pues de un procedimiento de ocultación.

2.2. Rejilla giratoria

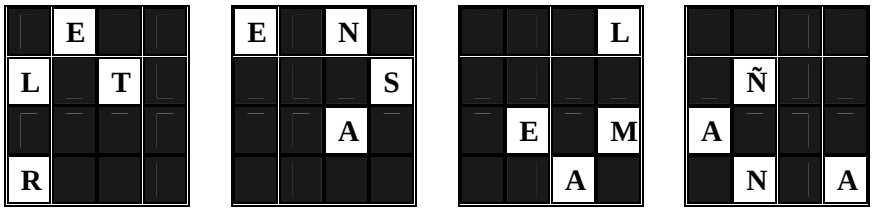
Una rejilla giratoria es una placa metálica cuadrada dividida en un número cuadrado par de cuadrículas: 4, 16, 36, etc. Para fijar las ideas consideremos el caso de 16 cuadrículas. De las 16 se agujerean 4 de forma que entre la posición inicial y las tres obtenidas girando la placa sobre sí misma sucesivamente 90 grados, en sentido de las agujas del reloj, dejen al descubierto las 16 posiciones (ver la figura 2). Para cifrar un mensaje se descompone en bloques de 16 letras y cada uno de ellos se escribe paso a paso en las ventanas que quedan al descubierto al realizar las cuatro posiciones giradas anteriores. Así, en las ventanas de la posición inicial se escriben las 4 primeras letras, en las de la segunda obtenida girando la placa 90 grados las 4 siguientes, las otras 4 en los huecos de la tercera posición obtenida tras un nuevo giro de 90 grados, y en las de la cuarta posición las 4 últimas letras. De esta forma se obtiene un texto con las 16 letras de cada bloque del mensaje totalmente desordenadas.



Posición 1 Posición 2 Posición 3 Posición 4

Figura 2. Las cuatro posiciones de la rejilla giratoria

Veamos un ejemplo. El mensaje en claro es: EL TREN SALE MAÑANA A LAS OCHO DE BILBAO. Empecemos con el primer bloque de 16 letras. Escribimos las letras de 4 en 4 tal y como se ha explicado anteriormente. Las letras de cada posición se muestran en la figura 3.



Posición 1 Posición 2 Posición 3 Posición 4

Figura 3. El texto de cada una de las cuatro posiciones de la rejilla giratoria

Si después de las cuatro escrituras se levanta la rejilla el resultado es el de la figura 4.

E	**E**	**N**	**L**
L	**Ñ**	**T**	**S**
A	**E**	**A**	**M**
R	**N**	**A**	**A**

Figura 4. Resultado final de la rejilla giratoria

Poniendo las letras en fila, el mensaje cifrado es un texto con las mismas letras pero desordenadas: EENLLÑTSAEAMRNAA. Lo mismo se haría con el segundo bloque de 16 letras. Estamos pues ante un ejemplo de trasposición. Para descifrarlo se necesita una placa similar y se tienen que hacer las mismas operaciones.

2.3. Cifrado de Playfair

A pesar de que el nombre del Barón de Playfair (1818-1898) esté asociado a uno de los cifrados clásicos más conocidos, fue su amigo, el científico Charles Wheatstone (1802-1875), quien lo concibió. Después de su creación en 1854, el barón consiguió que el gobierno británico adoptara oficialmente el uso de este sistema, de ahí el nombre. Así, el cifrado de Playfair fue utilizado por el Reino Unido en la Primera Guerra Mundial.

El cifrado de Playfair es un método de sustitución. Está basado en una matriz 5×5 con las letras del alfabeto. Como en el alfabeto castellano hay 27 letras, para trabajar con 25, previamente en todo texto a cifrar hay que sustituir la Ñ por N y la W por V. La matriz se construye a partir de una palabra clave, en el ejemplo MUSICO, que se coloca en los primeros lugares. Luego se escriben las letras restantes en el orden natural del alfabeto (ver la figura 5).

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

Figura 5. Matriz de cifrado de Playfair

Una vez que se tiene la matriz, se descompone el mensaje en claro en pares de letras. Si el número de letras es impar, se le añade la letra X al final. Cada par de letras sólo puede tener tres localizaciones en la matriz: las dos letras están en la misma fila, las dos están en la misma columna o las dos están en filas y columnas diferentes. Por tanto, para la sustitución sólo hay que aplicar tres reglas a los pares de letras:

1. Si las dos letras están en la misma fila, cada una de ellas se sustituye por la de su derecha. Si una de las dos está en el último lugar de la fila, se sustituye por la primera de su misma fila.
2. Si las dos letras están en la misma columna, cada una de ellas se sustituye por la de abajo. Si una de las dos está en el último lugar de la columna, se sustituye por la primera de su misma columna.
3. Si las dos letras están en filas y columnas diferentes, las dos son vértices opuestos de un cuadrilátero. En este caso cada una de las letras se sustituye por la letra del vértice siguiente de ese cuadrilátero, en el sentido de las agujas del reloj.

Veamos un ejemplo. El mensaje en claro es: HAN DESAPARECIDO LOS DOCUMENTOS. Su descomposición en parejas de letras es: HA ND ES AP AR EC ID OL OS DO CU ME NT OS. Para fijar las ideas vamos a mostrar algunas parejas.

La pareja OL en la que las dos letras están en la primera columna se cifra en FT; la pareja CU en la que las dos letras están en la primera fila se cifra en MS; y la pareja AR en la que las dos letras están en diferente fila y columna se cifra en EN (ver la figura 6).

El resultado es el mensaje cifrado: GB AQ BC BN EN KE DJ FT MB EA MS CO VL MB.

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

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

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

Figura 6. Cifrado de Playfair

Se observa, lo cual es muy importante, que en el mensaje en claro aparece cuatro veces la letra O, de las cuales dos veces se sustituye por M y las otras por F y A. A la inversa, en el mensaje cifrado aparece tres veces la letra E, que proviene en un caso de A, en otro de C y en otro de D. Estamos pues ante una sustitución polialfabética.

Para descifrar el mensaje hay tener la misma matriz de letras que lo ha cifrado, y para ello basta con que el receptor sepa la clave que la ha generado, en este caso MUSICO. Una vez que se tiene la matriz se realizan las mismas operaciones pero en sentido inverso.

2.4. Cilindro de Jefferson

Este dispositivo de cifrado fue inventado por Thomas Jefferson (1743-1826), el autor de la declaración de independencia de los Estados Unidos, aunque el primero en fabricarlo en serie fue Etienne Bazeries en 1891. Desde 1923 hasta 1942, el ejército estadounidense utilizó un cilindro de Jefferson para cifrar sus mensajes. Se llamó M-64.

1	2	3	4	5	6	7	8
A	Z	R	T	J	C	A	L
V	C	U	H	R	W	I	G
Y	F	X	Z	P	O	D	B
S	**E**	**C**	**R**	**E**	**T**	**O**	**S**
E	L	D	V	J	Ñ	C	H
D	K	W	B	U	A	F	Q
G	N	F	L	Z	S	M	K

Figura 7. Cilindro de Jefferson

Este aparato consiste en una serie de discos cilíndricos de igual diámetro que giran independientemente alrededor de un mismo eje. En el canto de cada disco están escritas todas las letras del abecedario, pero en cada una de ellos en orden distinto. Por ejemplo, el modelo M-64 constaba de 26 discos de aluminio. Para cifrar un mensaje, el emisor primero lo descompone en grupos

que contengan tantas letras como discos tenga el aparato. Para cada grupo mueve los discos hasta escribir en una línea longitudinal el mensaje en claro. Conseguido esto, elige cualquiera de las otras líneas y lo escrito en ella será el mensaje del grupo cifrado.

En la figura 7 se tiene una imagen frontal de un cilindro de Jefferson con 8 discos. Para cifrar la palabra SECRETOS se han girado los discos hasta escribirla en una línea. Se elige cualquier otra fila, por ejemplo la segunda de la figura, y sus letras conformarán el mensaje cifrado: VCUHRWIG.

El receptor, utilizando un aparato idéntico, escribe en una línea el mensaje recibido, mira las otras líneas, y se queda con la que contenga un texto con significado, que será el mensaje en claro.

Una característica muy importante de este sistema es que el cifrado no es determinista, el emisor puede elegir cualquier fila como mensaje cifrado.

2.5. Máquinas de cifrar

Como hemos visto, a comienzos del siglo XX se utilizaban artilugios diseñados para cifrar mensajes. Pero hasta terminada la Primera Guerra Mundial no aparecen en Europa las primeras máquinas de cifrar. Estas máquinas tenían el aspecto de las primitivas máquinas de escribir y consistían principalmente de un teclado normal de 26 letras. Eran engorrosas de manejar, pesaban más de una decena de kilos y, al menos las versiones básicas, no imprimían, se contentaban con cifrar y descifrar. La más famosa de todas es la alemana Enigma, que fue adoptada por el ejército del Tercer Reich. En Internet se pueden encontrar muchas páginas con fotografías de estas máquinas.

Las máquinas Enigma estaban basadas en un perfeccionamiento del cilindro de Jefferson, y automatizaban considerablemente los cálculos necesarios para realizar las operaciones de cifrado y descifrado de mensajes. Para romper la codificación de Enigma, los ingleses montaron la operación Ultra, que al final de la guerra llegó a contar con siete mil personas dedicadas a tareas de criptoanálisis. Todo ese esfuerzo dio sus frutos y el equipo dirigido por el brillante matemático Alan Turing (1912-1954) consiguió romper el Enigma de la flota naval de los alemanes. Así, desde mediados de 1941, los ingleses leían los códigos alemanes, lo cual éstos nunca sospecharon pues tal era su confianza en la máquina Enigma, que siempre la tuvieron por indescifrable.

2.6. Criptógrafos y matemáticos

Muchos criptógrafos también fueron brillantes matemáticos. Del siglo XVI ya hemos citado a Cardano y del XX a Turing. Un poco posterior a Cardano es François Viète (1540-1603), que como matemático fue el primero en introducir de forma sistemática la notación algebraica. Viète, consejero privado de los reyes de Francia Enrique III y Enrique IV, se hizo indispensable para descifrar, durante las guerras de la Liga, los despachos secretos que intercambiaban sus enemigos, españoles e italianos principalmente. En el siglo XVII, John Wallis (1616-1703), que como matemático obtuvo la fórmula de aproximación del número π que lleva su nombre, fue criptógrafo del parlamento inglés y descifró los mensajes del rey Carlos I de Inglaterra. Ya en nuestra época, como se ha indicado en la introducción, el sistema RSA fue concebido por tres matemáticos americanos.

3. Criptosistema RSA

Terminada la Segunda Guerra Mundial, una gran restricción de créditos produjo prácticamente la desmantelación de los departamentos militares dedicados a la criptografía. En consecuencia, los cerebros que trabajaban en ellos tuvieron que recolocarse en ocupaciones civiles. A la par, el surgimiento de los ordenadores y de la informática, a los que tanto contribuyó el desarrollo de las máquinas de cifrar como la inglesa Colossus, supuso un cambio radical del escenario criptográfico, que pasó del dominio militar al civil. La globalización de las infraestructuras de comunicaciones hizo que los bancos, las compañías de seguros, las administraciones y otras instituciones vislumbraran la necesidad de proteger la gran cantidad de datos que manipulaban, salvaguardaban y transferían. Así, importantes compañías americanas como Bell e IBM montaron equipos de criptógrafos civiles encargados de concebir los futuros productos ligados a esas necesidades.

Una característica común a todos los sistemas criptográficos clásicos y máquinas de cifrar es la simetría existente entre emisor y receptor. En ellos, el cifrado y descifrado son operaciones inversas que para su realización necesitan compartir el mismo artilugio o máquina y la misma clave, que se mantiene en secreto. Esto supone una debilidad y una gran traba para su uso extensivo. En este contexto, el año 1976, Whitfield Diffie (1944-) y Martin Hellman (1945-) inventaron el concepto de clave pública. Su propuesta consistía en idear un sistema en el que la clave tuviera dos partes interdependientes: una pública para cifrar y una privada para descifrar. Ahora bien, de ninguna forma se debería poder obtener la clave privada a partir de la clave pública. Entonces, para enviar un mensaje cifrado a un receptor, éste publicaría su clave de cifrado, el emisor cifraría el mensaje en esa clave, pero sólo el receptor sería capaz de descifrar el mensaje con la clave privada. Esto solventaría el problema de la distribución masiva de claves secretas y supuso una revolución en la criptografía.

Los primeros en presentar un sistema criptográfico de clave pública fueron R. Rivest, A. Shamir y L. Adleman en el año 1977. El algoritmo que diseñaron se denomina RSA. Como veremos a continuación, los mensajes enviados se representan mediante números, y su funcionamiento se basa en el producto (conocido) de dos números primos muy grandes elegidos al azar y que se mantienen en secreto. Su seguridad radica en la imposibilidad actual de factorizar números enteros grandes.

Los lectores interesados en una historia completa de la criptografía pueden consultar el libro (Singh, 2000), en el artículo (Fernández, 2004) encontrarán distintas técnicas criptográficas desarrolladas a lo largo de la historia, y en el libro (Stern, 1998), además de historia, planteamientos más conceptuales relacionados con la criptografía.

3.1. Resultados matemáticos en que se basa el algoritmo RSA

Los resultados matemáticos en los que se basa el algoritmo RSA son muy anteriores al algoritmo y sus enunciados son fáciles de comprender. Se pueden encontrar en el artículo (Sangróniz, 2004). Los escribimos a continuación.

Teorema de Euler (1736). Sean p y q dos números primos distintos y k un número tal que $k-1$ sea divisible por $p-1$ y $q-1$. Sea n el producto de p y q: $n = pq$. Entonces, para cualquier número entero m, si calculamos la potencia m^k, tanto m^k como m tienen el mismo el resto al dividirlos por el número n.

Corolario. Supongamos además que k está descompuesto en dos factores e y d: $k = ed$ y calculemos $c = m^e$. Como $m^k = m^{ed} = (m^e)^d = c^d$, del Teorema de Euler se sigue que c^d y m tienen el mismo resto al dividirlos por n.

Para completar los resultados básicos escribimos dos elementales.

- Si *m* es un número entero menor que *n*, el resto de la división de *m* por *n* es él mismo.

- Sean *c* y *d* dos números enteros cualesquiera. Sea *r* el resto de dividir *c* por *n*. Entonces las potencias c^d y r^d tienen igual resto al dividirlas por *n*. En efecto, como $c = qn + r$ con $r < n$, escribiendo $c^d = (qn + r)^d$, del binomio de Newton se sigue que c^d y r^d tienen igual resto al dividirlos por *n*.

Consecuencia. Supongamos verificadas las hipótesis del Teorema de Euler y que *k* está descompuesto en los factores *e* y *d*: $k = ed$. Sea *m* un número inferior a *n*. Calculemos $c = m^e$ y luego su resto *r* al dividirlo por *n*. Entonces el resto de la división de r^d por *n* es igual a *m*. Esta es la base del método RSA para cifrar mensajes.

3.2. Método RSA

Para ilustrar el método RSA vamos a representar una situación un tanto novelesca. Supongamos que James Bond ha decidido que todo mensaje destinado a él debe estar cifrado utilizando el método RSA. James Bond sabe que este método es muy seguro y que aunque se intercepten los mensajes, no se podrán descifrar y conocer su contenido. Para ello James Bond hace una elección adecuada de los números *p, q, e, d,* $n = pq$ y $k = ed$ de forma que verifiquen las hipótesis del Teorema de Euler. En la realidad, los números primos *p* y *q* son muy grandes, mayores que 10^{200}. Hecho esto, James Bond publica los números *e* y *n* para cifrar los mensajes que le vayan a enviar. Esos números constituyen la clave pública. Los números *p, q* y *d* se los guarda en secreto para él sólo. Así nadie podrá recrear los parámetros del algoritmo y sólo él será capaz de descifrar los mensajes que le dirijan. Los números *p, q* y *d* constituyen la clave privada.

Está claro que la clave pública y la privada son interdependientes. La cuestión es tener la seguridad de que no se pueda obtener la clave privada a partir de la pública. Pues bien, esto es así ya que actualmente no se es capaz de factorizar un número *n* muy grande, es decir no es posible obtener los factores *p* y *q* de *n*, y en consecuencia tampoco se puede obtener el número *d*, imprescindible para el descifrado.

Cuando el Agente 043 del servio secreto inglés quiere enviar un mensaje cifrado al Agente 007 sigue los siguientes pasos.

1. Convierte el mensaje en una secuencia de números m_1, m_2, ….., m_t, cada uno de ellos menor que *n*.
2. Cifra el mensaje con la clave pública *e* y *n* de 007. Para ello eleva los números m_1, m_2, ….., m_t a la potencia *e*, divide los resultados obtenidos por *n* y retiene los restos r_1, r_2, ….., r_t de las divisiones. Estos números constituyen el mensaje cifrado.
3. El Agente 043 hace llegar a 007 el mensaje cifrado sin ningún tipo de preocupación por el secreto. Lo puede por ejemplo publicar en un anuncio de periódico. Eso sí, tiene que estar seguro de que el destinatario lo va a leer.

Al recibir el mensaje, James Bond lo tiene que descifrar con su clave privada. Para ello eleva los números r_1, r_2, ….., r_t a la potencia *d*, divide los resultados por *n*, y los restos que obtiene son los

números m_1, m_1, m_2, ….., m_t del mensaje en claro. James Bond convierte los números en letras y puede leer lo que le comunican.

James Bond sabe que hoy en día la única forma de recuperar los números en claro es utilizando el número *d*. Como actualmente este número no se puede obtener a partir de la clave pública y sólo él lo conoce, James Bond está seguro de que aunque lo hayan leído, nadie habrá conseguido descifrar el mensaje que le ha enviado 043. Por eso no le ha molestado que haya aparecido en un periódico.

Como ejemplo muy sencillo, con números pequeños, supongamos que James Bond ha elegido $p=3$, $q=11$, $e=3$, $d=7$ y en consecuencia $n=33$ y $k=21$. La clave pública son los números $e=3$ y $n=33$. La privada $p=3$, $q=11$ y $d=7$.

En el transcurso de una misión, James Bond se encuentra sin saberlo en peligro y el Agente 043, sin levantar sospechas, le quiere dejar el siguiente aviso: LARGATE SIGUEN TUS PASOS. ¿Cómo lo hace?

1. El Agente 043 convierte el mensaje en una secuencia de números sustituyendo cada letra por el número del lugar que ocupa en el alfabeto. Obtiene así el mensaje numérico en claro de la tabla 1.

L	**A**	**R**	**G**	**A**	**T**	**E**	**S**	**I**	**G**	**U**	**E**	**N**	**T**	**U**	**S**	**P**	**A**	**S**	**O**	**S**
12	1	19	7	1	21	5	20	9	7	22	5	14	21	22	20	17	1	20	16	20

Tabla 1. Mensaje en claro que 043 quiere enviar a 007

2. 043 cifra el mensaje numérico con la clave pública de 007, elevando cada número a la potencia 3, dividiendo los resultados por 33 y reteniendo los restos. Estos restos constituyen el mensaje cifrado de la tabla 2. Por ejemplo, para $m=5$ se tiene $5^3=125$ y el resto de su división por 33 es 26. El resto de la división de $19^3=6859$ por 33 es 28. Así, 5 lo cifra en 26 y 19 en 28.

12	1	28	13	1	21	26	14	3	13	22	26	5	21	22	14	29	1	14	4	14

Tabla 2. Mensaje numérico cifrado con la clave pública de 007

3. El Agente 043 deja el mensaje cifrado en el hotel de 007 sin preocuparse de que pueda ser interceptado, eso sí, teniendo la seguridad de que se lo van a entregar.
4. James Bond recibe el mensaje y lo descifra con su clave privada, elevando cada número a la potencia 7 y calculando los restos al dividirlos por 33. Por ejemplo, 26^7 es 8031810176 y su resto al dividirlo por 33 es 5. El resto de dividir $28^7=13492928512$ por 33 es 19. Por tanto 26 lo descifra en 5 y 28 en 19. El resultado que obtiene son los números iniciales. Convirtiendo los números en letras (ver la tabla 3) James Bond recupera el mensaje en claro, se da cuenta del peligro en el que se encuentra y consigue esquivar a sus perseguidores.

12	1	19	7	1	21	5	20	9	7	22	5	14	21	22	20	17	1	20	16	20
L	**A**	**R**	**G**	**A**	**T**	**E**	**S**	**I**	**G**	**U**	**E**	**N**	**T**	**U**	**S**	**P**	**A**	**S**	**O**	**S**

Tabla 3. Recuperación del mensaje en claro con la clave privada de 007

4. Autentificación de documentos con RSA

Otra cuestión paralela a ésta es la autentificación de los documentos y la denominada firma digital. Supongamos ahora que una persona o una institución desea emitir un documento autentificado, es decir que quien lo reciba tenga la seguridad de que el autor es el emisor, y que no ha sido violado. Aquí el texto puede ser público, pero se trata de estar seguro de su autenticidad. Para conseguirlo dispone del sistema RSA. Como antes, el emisor empieza haciendo una elección adecuada de los números *p, q, e, d,* $n = pq$ y $k = ed$ y publica los números *e* y *n* de su clave pública. Hecho esto, convierte su documento en una lista de números m_1, m_2, ….., m_s menores que *n* y los cifra con su clave privada que sólo él conoce. Para ello eleva cada número a la potencia *d*, divide los resultados por *n* y los restos r_1, r_2, ….., r_s forman el documento cifrado. El emisor difunde juntos el documento abierto y el cifrado. El receptor de los dos documentos eleva los números cifrados r_1, r_2, ….., r_s a la potencia *e*, los divide por *n*, retiene los nuevos restos y éstos, por la misma consecuencia del teorema de Euler escrita anteriormente, deben ser m_1, m_2, ….., m_s. Por tanto, al convertir estos números en letras, el texto obtenido debe coincidir con el documento abierto. Si es así tiene la seguridad de que el documento no ha sido manipulado y que el autor es quien dice que lo es. Si no, repudia el documento.

4.1. Ejemplo

Volvamos a James Bond y a su algoritmo RSA con la clave pública $e = 3$ y $n = 33$ y la privada $p = 3$, $q = 11$ y $d = 7$. James Bond está cansado y quiere enviar a todos sus amigos y adversarios el siguiente texto: LO DEJO ESTOY ENAMORADO. Para que todos estén seguros de que 007 es el autor, para que nadie piense que es una trampa, lo tiene que autentificar. Veamos cómo.

1. 007 convierte el texto en la secuencia de números de la tabla 4.

L	**O**	**D**	**E**	**J**	**O**	**E**	**S**	**T**	**O**	**Y**	**E**	**N**	**A**	**M**	**O**	**R**	**A**	**D**	**O**
12	16	4	5	10	16	5	20	21	16	26	5	14	1	13	16	19	1	4	16

Tabla 4. Texto en claro emitido por 007

2. Cifra esos números con su clave privada. Para ello los eleva a la potencia 7, los divide por 33 y retiene los restos. Por ejemplo para $m = 10$ se tiene que 10^7 es 10000000 y su resto al dividirlo por 33 es 10. En la tabla 5 se tiene el texto cifrado con la clave privada de 007.

12	25	16	14	10	25	14	26	21	25	20	14	20	1	7	25	13	1	16	25
L	**X**	**O**	**N**	**J**	**X**	**N**	**Y**	**T**	**X**	**S**	**N**	**S**	**A**	**G**	**X**	**M**	**A**	**O**	**X**

Tabla 5. Texto cifrado con la clave privada de 007

3. El Agente 007 publica juntos el texto en claro LO DEJO ESTOY ENAMORADO y el cifrado LXONJXNYTSNSAGXMAOX.
4. Quienes leen los dos textos, convierten las letras del cifrado en números y éstos los descifran con la clave pública de 007. Para ello elevan los números cifrados a la potencia $e = 3$ de Bond, los resultados los dividen por 33 y, si todo está bien, los restos serán los números en claro (ver la tabla 6).

12	16	4	5	10	16	5	20	21	16	26	5	14	1	13	16	19	1	4	16
L	**O**	**D**	**E**	**J**	**O**	**E**	**S**	**T**	**O**	**Y**	**E**	**N**	**A**	**M**	**O**	**R**	**A**	**D**	**O**

Tabla 6. Recuperación del texto en claro con la clave pública de 007

Volviendo a convertir los números en letras, los amigos y rivales de 007 comprueban que el texto obtenido (tabla 6) coincide con el texto abierto emitido por James Bond. En consecuencia el texto es auténtico y todos saben que el Agente 007 se retira por causa mayor.

4.2. Firma digital

Internet permite intercambiar mensajes (electrónicos) escritos entre personas que se encuentran a gran distancia. Ahora bien, los usuarios utilizarán este medio para hacer, por ejemplo, transacciones comerciales, sólo si tienen el pleno convencimiento de que los documentos así intercambiados son fiables. Esto exige que el tráfico documental se haga de manera que se cumplan estos tres requisitos:

- *Identidad del autor*. Quien recibe el mensaje debe estar completamente seguro de que el autor es quien lo envía.

- *Integridad del contenido*. El receptor debe tener la seguridad de que el documento que le ha llegado es el original, que no ha sido violado en el camino.

- *No rechazo en origen*. Quien haya enviado el documento de ninguna forma puede negar que él es quien lo ha remitido.

El procedimiento técnico que garantiza que se cumplen estas tres condiciones es la firma digital. La firma digital está basada en técnicas criptográficas. La más usada es el algoritmo RSA de autentificación de documentos que acabamos de describir. Veamos cómo funciona en la práctica.

Supongamos que el emisor Ander quiere enviar al receptor Walter una propuesta comercial. Tanto Ander como Walter tienen su clave pública y privada que les ha suministrado y gestiona un tercero, un prestador de servicios de certificación. Los pasos que Ander y Walter deben seguir son los siguientes.

1. Ander redacta el mensaje que quiere enviar electrónicamente a Walter. Como el texto puede ser largo y su codificación laboriosa, Ander le aplica una “función hash” que le ha proporcionado el prestador de servicios de certificación. El cometido de estas funciones es generar a partir de un conjunto grande de información uno mucho más pequeño, de forma que si dos resultados de una misma función son diferentes, las dos entradas que los generaron también lo son. Este nuevo documento, que puede ser numérico, se denomina texto-resumen o texto hash e identifica unívocamente el texto inicial. En Internet es fácil encontrar información sobre las funciones hash.
2. Según el procedimiento descrito en la sección anterior sobre autentificación de documentos, Ander debe enviar a Walter dos textos: el escrito en claro y su versión cifrada con su clave privada. En la práctica las cosas son un poco más complicadas. Así, de hecho Ander primero cifra el texto hash con su clave privada y luego envía a Walter un correo electrónico con dos elementos: el texto completo en claro y la firma. Ésta contiene dos ficheros: el texto hash que ha cifrado Ander con su clave privada y su certificado electrónico, el cual a su vez contiene su identificación y su clave pública. Este certificado se lo ha proporcionado el prestador de

servicios de certificación y está cifrado con la clave privada del prestador. A veces puede ocurrir que el texto de Ander tiene que ser confidencial, por lo que éste previamente a aplicarle la función hash, lo tiene que cifrar con la clave pública de Walter.

3. Al recibir el correo, Walter descifra el certificado electrónico de Ander utilizando la clave pública del prestador de servicios, que la ha puesto a disposición de todos sus clientes en su página web. Ahora ya, Walter tiene el mensaje en claro, el texto hash cifrado que ha recibido de Ander y la clave pública e identidad de éste en claro.
4. Por un lado, Walter descifra con la clave pública de Ander el texto hash. Por otro, aplica al texto completo en claro la misma función hash que ha utilizado Ander y que el prestador de servicios también le ha proporcionado. Después compara el resultado con el texto hash que acaba de descifrar. Si son idénticos todo está bien, Walter está seguro de que Ander es el autor de la propuesta que ha recibido y la toma en consideración. Si no coinciden, el mensaje ha sido alterado por un tercero. Si el resultado es ininteligible, no ha sido cifrado por Ander, alguien ha tratado de suplantarle.

En el caso en que para garantizar su confidencialidad Ander haya cifrado su texto completo con la clave pública de Walter, éste, después de autentificar el mensaje cifrado recibido, lo debe descifrar con su clave privada.

Por último, en el intercambio de mensajes electrónicos es importante que se pueda establecer con certeza la fecha exacta en la que se han enviado. Esto se consigue por medio de los llamados sellos temporales, que son funciones atribuidas generalmente a los prestadores de servicios de certificación, los cuales fijan la fecha al texto resumen hash de los mensajes electrónicos firmados digitalmente.

	Clave privada	**Clave pública**
Ejemplo 1	$p=3,\ q=11,\ d=7$	$e=3,\ n=33$
Ejemplo 2	$p=3,\ q=17,\ d=11$	$e=3,\ n=51$
Ejemplo 3	$p=3,\ q=23,\ d=9$	$e=5,\ n=69$
Ejemplo 4	$p=5,\ q=13,\ d=7$	$e=7,\ n=65$
Ejemplo 5	$p=5,\ q=13,\ d=29$	$e=5,\ n=65$
Ejemplo 6	$p=7,\ q=37,\ d=31$	$e=7,\ n=259$
Ejemplo 7	$p=7,\ q=43,\ d=23$	$e=11,\ n=301$
Ejemplo 8	$p=11,\ q=17,\ d=23$	$e=7,\ n=187$
Ejemplo 9	$p=11,\ q=23,\ d=17$	$e=13,\ n=253$
Ejemplo 10	$p=13,\ q=43,\ d=101$	$e=5,\ n=559$
Ejemplo 11	$p=13,\ q=47,\ d=79$	$e=7,\ n=611$
Ejemplo 12	$p=61,\ q=53,\ d=2753$	$e=17,\ n=3223$

Tabla 7. Ejemplos de parámetros del sistema RSA

5. Comentario final

Como se ha indicado varias veces, la seguridad del algoritmo RSA recae en el convencimiento de que el adversario no va a poder factorizar el número *n* de la clave pública. Dado que tanto los algoritmos como la tecnología se perfeccionan constantemente, hay que tener presente que lo que hoy está dentro de los límites de seguridad, posiblemente no lo estará mañana. Por lo tanto, para mantener el nivel de seguridad que compense esas mejoras, el tamaño de las claves, esencialmente el número *n*, tiene que aumentar progresivamente. En el artículo (Buchmann, 1999) se hace un recorrido por las principales técnicas de factorización.

Queda un último detalle por aclarar. Para disponer de un sistema RSA, hay que empezar eligiendo dos números primos *p* y *q* muy grandes, aproximadamente del mismo tamaño, pero que no estén muy próximos. La pregunta obvia es ¿cómo se puede hacer esto? No vamos a entrar aquí en detalles, baste decir que existen criterios muy eficientes para decidir si un número, sin importar que sea grande, es primo o compuesto. El lector interesado puede encontrarlos en el libro (Koblitz, 1987). Por tanto, se empieza probando si un número impar (grande) elegido al azar es primo. Si no lo es, se prueba con el siguiente impar y así hasta que se logre dar con un primo. En la tabla 7 se muestran distintas elecciones de los parámetros del sistema RSA con números pequeños.

A la vista de todo lo anterior, está claro que la criptografía moderna reposa en las matemáticas y que es una ciencia viva. Así, la investigación sobre el modo de aumentar la seguridad de la información y comunicación es incesante, y está dando lugar a avances apasionantes tanto en las matemáticas involucradas, Teoría de números, Geometría algebraica, como en la criptografía propiamente dicha. Los libros (Koblitz, 1987) y (Stinson, 2002) son una buena referencia para tener una panorámica más general de la criptografía moderna y de las matemáticas implicadas en ella.

Bibliografía

Buchmann, J. (abril 1999). Factorización de números grandes. *Investigación y Ciencia.*

Fernández, S. (2004). La Criptografía clásica. Revista *SIGMA*, 24, 119-141.

Koblitz, N. (1987). *A course in number theory and cryptography*, Springer. New York.

Sangróniz, J. (2004). Criptografía de clave pública: el sistema RSA. Revista *SIGMA*, 25, 149-165.

Singh, S. (2000). *Los códigos secretos.* Editorial Debate.

Stern, J. (1998). *La science du secret*, Editions Odile Jacob. Paris.

Stinson, D. (2002). *Cryptography theory and practice*, 2nd ed. CRC Press Inc., New-York.

Mikel Lezaun Iturralde es Catedrático de Matemática Aplicada de la Universidad del País Vasco/Euskal Herriko Unibertsitatea. Licenciado en Matemáticas por la Universidad de Zaragoza y Doctor por la Universidad del País Vasco, ha publicado artículos de investigación en revistas de prestigio. Su trabajo *Predicciones del Tiempo y Matemáticas* fue galardonado con el III Premio Sema de Divulgación en Matemática Aplicada. Actualmente dirige el Grupo de Transferencia de Tecnología Matemática, con contratos para empresas como Metro Bilbao, EuskoTren, FEVE, Cespa, Aguas de Barcelona, Sidenor y Eroski.