colección
MIRADAS MATEMÁTICAS

María Isabel González Vasco

Las matemáticas de la criptología

Secretos demostrables y demostraciones secretas

CATARATA

María Isabel González Vasco

Las matemáticas de la criptología

SECRETOS DEMOSTRABLES Y DEMOSTRACIONES SECRETAS

colección
MIRADAS MATEMÁTICAS

DISEÑO DE CUBIERTA: ESTUDIO SÁNCHEZ/LACASTA

LAS MATEMÁTICAS DE LA CRIPTOLOGÍA.
SECRETOS DEMOSTRABLES Y DEMOSTRACIONES SECRETAS

ISBN: 978-84-9097-505-3
E-ISBN: 978-84-9097-513-8
DEPÓSITO LEGAL: M-19.825-2018
IBIC: PDZ/GPJ

A Carlos, María y Nacho, mis usuarios honestos, pero infinitamente curiosos.

A Palmira, depositaria de todos los secretos.

Introducción

Como casi todas las cosas importantes en la vida, la criptografía me encontró en un pupitre del colegio. Mi amiga Sara, sentada dos filas delante, tenía algo que contarme y escribía pequeños renglones en fragmentos de papel cuadriculado que intentaba hacerme llegar escondidos en su goma o en la caña de un bolígrafo. Sin duda, burlar la vigilancia de al menos dos potenciales entidades interesadas en nuestros mensajes (a la sazón, mi compañero de pupitre y don Primitivo, nuestro profesor de cuarto) era la principal razón de ser de este intercambio de información. Nuestra técnica fue, por tanto, ganando en sofisticación: una vez vimos claro que no bastaba con intentar esconder la existencia de la transmisión que nos ocupaba, comenzamos a pensar en ocultar no la presencia de los mensajes, sino su contenido.

Este tipo de procesos se repiten cada día en miles de aulas de educación primaria a lo largo del mundo. Esto no es sorprendente, pues la criptología, definida como "ciencia y práctica del diseño de sistemas de comunicación que son seguros en presencia de adversarios"[1], surge de modo inseparable de la necesidad de comunicación del ser humano. Existen evidencias históricas de métodos para la ocultación de la transmisión de la información (técnicas esteganográficas)[2] y esquemas de cifrado elementales contemporáneos de los lenguajes más antiguos conocidos. Por ejemplo, la escritura cuneiforme de los sumerios o el lengua-

je jeroglífico de los egipcios son métodos de comunicación cuyo fin es transmitir información no de manera universal, sino a ciertos receptores autorizados. Un *esquema de cifrado*, la herramienta criptográfica más conocida y antigua, persigue exactamente eso: no el ocultar que existe transmisión de información, sino limitar el acceso a la información transmitida por medio de instrumentos matemáticos.

La criptología tiene dos vertientes bien diferenciadas: una constructiva y otra crítica o destructiva. La primera, llamada criptografía, se ocupa del diseño de herramientas, mientras que la segunda, el criptoanálisis, es el estudio crítico de las mismas. Criptógrafos y criptoanalistas llevan siglos enzarzados en una pugna cuyo resultado son construcciones cada vez más seguras para todo tipo de aplicaciones relacionadas con la gestión, transmisión y almacenamiento de información. Ambos buscan sus armas en un arsenal inagotable y precioso: las matemáticas. El papel de las matemáticas en criptología es central desde dos puntos de vista. Por un lado, como fuente de problemas cuya dificultad mantendrá bajo control a adversarios externos y usuarios maliciosos de un cierto sistema. Por otro, las matemáticas proporcionan el único lenguaje formal adecuado para la cimentación de demostraciones rigurosas e irrefutables de seguridad.

Hasta finales del siglo pasado, las construcciones criptográficas eran fundamentalmente esquemas de cifrado, diseñados para conseguir transmitir de manera segura información entre dos usuarios. En los últimos cuarenta años, sin embargo, las reglas del juego han cambiado radicalmente. La forma en que hoy compartimos, gestionamos y almacenamos la información plantea escenarios de aplicación fascinantes que suponen un reto constante para criptógrafos y criptoanalistas.

Este libro es una introducción a la criptología desde una perspectiva moderna. En cada capítulo presentaremos al lector

un tipo de construcción criptográfica, profundizando en las herramientas matemáticas que pueden usarse para su implementación. Queremos acercar al lector a la criptología de manera amena y divulgativa, y presentarle además las ideas y conceptos matemáticos que subyacen en diferentes construcciones criptográficas. Nuestra ambición es proporcionar al lector un beneficio doble: aprender matemáticas a través de la criptología y desarrollar la inquietud por la criptología moderna desde el placer del formalismo matemático. Así, este libro proporciona a los profesores de educación secundaria algunos ejemplos novedosos con los que motivar a sus alumnos en el aprendizaje. Con ese fin plantearemos distintos retos o ejercicios sencillos, que pueden ser abordados con éxito por estudiantes de este nivel.

Capítulo 1

Criptografía simétrica. Al César lo que es del César

Volvamos atrás, quizá no tantos años, hacia un pasado sin internet, sin mensajería instantánea, sin móviles. Un pasado en el que los mensajes eran complejos en fondo y forma, redactados con paciencia y pulcritud. Entonces, los destinatarios eran pocos y selectos, y en la mayoría de los casos no se enviaba más de una carta cada mes, precedida de varios encuentros cara a cara. Este escenario, que parece rescatado de una infancia en blanco y negro, era el marco habitual de la comunicación hasta hace menos de treinta años. Es en cierta manera el ideal al que se aspira: cada día se intenta simular cientos de veces a través de la comunicación digital. La razón es sencilla; querríamos confiar en la autenticidad y confidencialidad de un archivo de datos recibido por *e-mail* igual que hacemos al recibir un sobre inmaculado (sin trazas de manipulación) por correo ordinario.

Este escenario en blanco y negro es el hábitat natural de la llamada *criptografía simétrica* (también llamada criptografía clásica o de clave privada). Parte del supuesto de que los interlocutores involucrados comparten un secreto *grande*, acordado en una fase previa completamente confiable, como podría ser un encuentro en persona. En este contexto, *grande* significa difícil de predecir o, en términos técnicos, de *alta entropía*. Actualmente, se considera que una cadena de ceros y unos (bits) es de alta entropía si su longitud es, al menos, de 180 bits. En contraposición,

cadenas de 30 bits o menos suelen considerarse de baja entropía; ese es, por ejemplo, el caso de las contraseñas que somos capaces de memorizar. La entropía puede definirse rigurosamente como una medida para cuantificar la incertidumbre: en física, por ejemplo, sirve para medir el desorden, la desorganización de un sistema.

El secreto que comparten los dos usuarios, emisor y receptor, es la consigna que servirá para enviar mensajes entre ellos. Esta clave servirá tanto para cifrar (transformar el mensaje original en otro que, en caso de ser interceptado, sea inteligible si no se dispone de la clave) como para descifrar los mensajes (recuperar el mensaje original, a partir del mensaje cifrado, para poder leerlo).

Formalicemos matemáticamente esta idea. Nombramos, como es habitual en los libros de criptología, Alice a nuestra emisora y Bob al receptor. Todos los objetos involucrados en la transmisión viven en una estructura algebraica X, es decir, un conjunto en el que está definida una cierta operación (por ejemplo, los números enteros y la operación suma). Tanto el conjunto de posibles mensajes sin cifrar (al que llamaremos M) como el de mensajes ya cifrados (llamémosle C) están contenidos en X. Distinguiremos un subconjunto especial, K, dentro de X, donde estarán las llamadas claves simétricas. Estas claves son los elementos indispensables para transformar un texto claro en un texto cifrado, y también para revertir esta transformación.

Formalmente, un esquema de cifrado se definirá haciendo explícitos tres procesos o *algoritmos*[3]:

- Un *algoritmo de generación de clave*, denotado KeyGen, que sirva para seleccionar cada una de las claves utilizadas a partir de un valor prefijado, llamado pará-

metro de seguridad. Este suele ser una medida de la fortaleza del esquema en cuestión.

- Un *algoritmo de cifrado*, que denotaremos Enc, que recibe como entrada una clave y un mensaje claro y da como salida un texto cifrado.
- Un *algoritmo de descifrado*, denotado por Dec, que recibe como entrada una clave y un texto cifrado y da como salida un mensaje claro.

Así, un esquema de cifrado = (KeyGen, Enc, Dec) será correcto si el algoritmo de descifrado permite recuperar el texto claro m que subyace a un texto cifrado c, siempre que se le dé como entrada la clave k que sirvió para construir c. En símbolos:

$$Enc(k, m) = c \quad Dec(k, c) = m$$

para toda clave k que haya sido seleccionada por KeyGen.

Alice será la encargada de ejecutar Enc, mientras que Bob tendrá que usar el algoritmo Dec para descifrar. En principio, si ambos usan la misma clave y nadie más la conoce, todo irá bien.

Un poco de historia

Un ejemplo clásico de cifrado simétrico usando la notación anterior es el *cifrado de César*. Gracias a los escritos de Suetonio[4], datados en el siglo segundo antes de Cristo, sabemos que el emperador romano Julio César empleaba un sencillo sistema para cifrar sus misivas más delicadas. Simplemente, César sustituía cada letra del alfabeto latino por la que ocupaba tres posiciones más adelante, volviendo a las primeras letras desde el final para cifrar las tres últimas. Así, podemos decir que efectuaba una simple sustitución utilizando una tabla como esta:

Tabla 1
Cifrado de César

A	B	C	D	....	W	X	Y	Z
D	E	F	G		X	A	B	C

La primera fila contendría las letras del texto claro y la segunda el resultado tras cifrar. Así, el mensaje "TAMBIÉN TÚ, BRUTO" —obviando la coma y los acentos— quedaría cifrado como "WDPELHQ WX EUXWR".

Este método es muy sencillo, pero presenta ciertos problemas. El primero es que no hay variabilidad, es decir, al cifrar el mismo texto claro siempre obtendremos el mismo texto cifrado como resultado. Esta característica, llamada *determinismo*, es evidentemente una debilidad. Todo aquel que conozca el descifrado de un texto concreto podrá identificar las palabras contenidas en este que se repitan en envíos posteriores. Por ejemplo, la cadena "QR" en los textos cifrados siempre quiere decir "NO". Un espía que sepa que una respuesta "QR" de César es negativa, sabrá reconocer la palabra "NO" contenida en cualquier mensaje que se envíe, pues el cifrado de esta siempre será "QR".

Pasemos a describir formalmente el esquema de César para así entender de manera más general dónde está el problema. El conjunto X que nos sirve de estructura básica será el alfabeto latino, que codificaremos con los números del 0 al 25.

La operación de cifrado es, por tanto, sumar 3 al número que representa cada letra del texto claro. Pero al llegar a la última letra, se vuelve a empezar desde el comienzo. Así, la X se cifraría con la A, la Y con la B y la Z con la C (como pasa con el reloj, al llegar al 12, se vuelve a pasar al 1). Esta operación se llama *suma módulo 26*. Operamos, por tanto, identificando cada número con el resto que da al dividirse por 26. En el caso concreto de sumar tres, cuando el resultado de la suma sea superior a 25, res-

tamos a este 26 (para obtener, de nuevo, un número en el rango adecuado). Para manejarnos con este tipo de aritmética es útil pensar que el 26 se transforma en un cero. Así, al sumar o restar —las veces que queramos— 26 a un número X, nos quedamos en el mismo número.

Tabla 2
Codificación para el cifrado de César

A	B	C	D	....	X	Y	Z
0	1	2	3		23	24	25

Para descifrar, de nuevo, utilizamos la codificación numérica descrita en la tabla 2 y restamos a cada número recibido el 3, ajustando (sumando 26, si obtenemos un número negativo) para tener siempre números entre 0 y 25.

Así, nuestro conjunto X es el de los enteros {0, 1, …, 25}, y la operación de cifrado puede describirse como

$$Enc(m) = m + 3 \bmod 26$$

siendo el descifrado

$$Dec(m) = m - 3 \bmod 26$$

donde la expresión "mod 26" se traduce como "divide entre 26, y quédate con el resto". En efecto, estamos usando, en realidad, una estructura algebraica clásica, el grupo aditivo que se define en el conjunto de números enteros {0, …, n – 1} denotado por Z_n con la operación suma mod n anteriormente descrita (para n = 26).

Ejercicio 1. Ya hemos razonado que al trabajar con aritmética modular, el módulo (en el texto, el número 26) desempeña el papel del neutro para la suma. Utiliza esta idea para argumentar, sin hacer la división, que el resto de 52.002 al dividirse entre 26 es 2.

Y, en este caso, ¿cuál es la clave? Dicho de otra forma: ¿qué valor de $X = Z_{26}$ es imprescindible conocer para cifrar y descifrar? La respuesta es sencilla: el número 3. El tamaño del "salto" con el que ciframos y desciframos determina la clave y, además, se mantiene estable. Esto nos permite deducir que Julio César, o bien no tenía demasiadas ocasiones para acordar claves de cifrado con sus homólogos, o no tenía un elevado concepto del talento matemático de sus adversarios.

En términos modernos, una descripción de este método que nos dejaría más tranquilos sería una terna de algoritmos descritos como sigue:

- KeyGen(n) = k Z_n
- Enc(k, m) = m + k mod n
- Dec(k, c) = c – k mod n

El parámetro de seguridad, n, fijaría el tamaño del alfabeto utilizado en la comunicación y la seguridad del método dependería esencialmente del diseño del algoritmo KeyGen. Si para un n fijado (por ejemplo, n = 26) la salida de KeyGen fuese siempre el mismo número (otra vez, por no llevar la contraria al César, el 3), estaríamos de nuevo con una construcción determinista. Yéndonos al extremo contrario, forzaríamos que cualquier valor entre 0 y 25 tuviese la misma probabilidad de resultar como salida de KeyGen. Esta es, evidentemente, la mejor estrategia para ganar seguridad en un diseño de este tipo[5].
Demos a la construcción recién descrita una vuelta más, concre-

tamente, cifrando cada letra con un método como el anterior, pero con clave distinta. Esta evolución del cifrado de César se conoce con el nombre de *cifrado de Vigenère*, más conocido como el código indescifrable (*le chiffre indéchiffrable*, en francés).

Blaise de Vigenère

Blaise de Vigenère fue un diplomático, criptógrafo y químico francés del siglo XVI, que ejerció de secretario de la cámara del rey Enrique III de Francia. Curiosamente, él no inventó el cifrado que ha pasado a la historia con su nombre; este fue descrito, en realidad, por un criptógrafo italiano: Giovan Battista Belasso.

Veamos cómo funciona. Para cifrar mensajes de longitud t, esta sería la descripción de los algoritmos involucrados:

- KeyGen(n, t) = k = $(k_1, \ldots, k_t)$ con $k_i \quad Z_n$ para i = 1, …, t
- Enc(k, m) = c

  siendo $m = (m_1, \ldots, m_t)$ y $c = (c_1, \ldots, c_t)$

  donde para i = 1, …, t

  $c_i = m_i + k_i \bmod n$
- Dec(k, c) = m,

  donde para i = 1, …, t,

  $m_i = c_i - k_i \bmod n$

Este método, del que se tiene constancia desde el siglo XVI, heredó la debilidad del método usado por Julio César. De nuevo, el algoritmo KeyGen utilizado era esencialmente determinista, pues la clave quedaba fijada a través de una tabla que, además, en muchos casos, se resumía utilizando una palabra clave corta.

La tabla 3 ejemplifica este método, donde las claves asociadas k = (k_1,…, k_t) van de 0 a 25 en la primera columna de la izquierda. La tabla 4 representa la misma clave, pero sin codificación numérica[6].

Tabla 3
Tabla Vigenère numérica

Clave K	A	B	C	D		W	X	Y	Z
0	0	1	2	3		22	23	24	25
1	1	2	3	4		23	24	25	0
2	2	3	4	5		24	25	0	1
3	3	4	5	6		25	0	1	2
4	4	5	6	7	...	0	1	2	3
...						...			
23	23	24	25			19	20	21	22
24	24	25	0			20	21	22	23
25	25	0	1			21	22	23	24

Tabla 4
Tabla Vigenère alfabética

Clave K	A	B	C	D		W	X	Y	Z
0	A	B	C	D		W	X	Y	Z
1	B	C	D	E		X	y	X	A
2	C	D	E	F		Y	Z	A	B
3	D	E	F	G		Z	A	B	C
4	E	F	G	H	...	A	B	C	D
...						...			
23	X	Y	Z			T	U	V	W
24	Y	Z	A			U	V	W	X
25	Z	A	B			V	W	X	Y

Ejemplo 1
Así, para cifrar la palabra "FÁCIL", si utilizáramos la secuencia de clave (0, 1, 2, 3, 4), tendríamos como resultado el texto cifrado "FBELP". Si queremos que la secuencia de clave no sea siempre de la forma (0, 1, …, t), podemos usar una palabra clave que señale qué filas de la tabla Vigenère se usarán para cada letra. Por ejemplo, si usamos la palabra clave "MISTERIO", estamos señalando a las filas 12, 8, 18, 19, 4, 17, 8 y 14. Así, por ejemplo, para cifrar la palabra "ALMA" haremos:

m = (A, L, M, A), k = (12, 8, 18, 19) y así, el texto
cifrado c = (c_1, …, c_t) se construirá con la fórmula

$$c_i = m_i + k_i \bmod 26$$

de donde obtenemos, codificando numéricamente el texto claro m como (0,