CRIPTOGRAFÍA: UNA CUESTIÓN DE CÓDIGOS

Rodrigo Berrondo - Noelia Cabrera - Gustavo Franco - Mathías Frederico - Franco Mariani - Lester Rodríguez

berryberrondo@gmail.com - manoeliacabrera@gmaill.com - gfrancoc@hotmail.com - mathiasafg@hotmail.com - francomar_88@hotmail.com - lesrod77@gmail.com

Instituto de Profesores "Artigas" (IPA) - Uruguay

Tema: Pensamiento numérico

Modalidad: Mini Curso

Nivel educativo: No específico

Palabras clave: Criptografía, cifrar, descifrar, métodos de cifrado.

Resumen

¿Qué es la criptografía? ¿Cuáles son sus orígenes? ¿Cuáles son algunos de los métodos que se han utilizado a lo largo de la historia para cifrar mensajes? En este mini curso daremos respuestas a estas preguntas y a muchas otras, al tiempo que propondremos una serie de actividades que luego podrán ser utilizadas por el profesor en la clase de matemática.

Introducción

En este mini curso expondremos algunos de los muchos métodos criptográficos utilizados a lo largo de la historia. Propondremos actividades cuya resolución permitirá comprender dichos métodos de una manera participativa y colaborativa. Estas actividades, que buscan recrear los momentos de creación matemática, pueden adaptarse para ser propuestas en distintos niveles educativos y en diferentes bloques curriculares. Consideramos que la criptografía puede utilizarse como un recurso didáctico para motivar a los alumnos a interesarse por algunos contenidos matemáticos: ¿cómo la divisibilidad puede ayudarnos a descifrar un mensaje? ¿Cuáles son las características geométricas de la escítala espartana que, una vez cifrado un mensaje, permitirían descifrarlo? ¿Cómo se vinculan el conteo, la probabilidad y la estadística con la criptografía? En relación a esta última pregunta, y a modo de adelanto, podemos decir que el conocimiento de la frecuencia relativa de cada letra en un cierto idioma permite, en algunos casos, que un mensaje se pueda descifrar. Este revolucionario método fue creado por Al-Kindi y sirvió para descifrar mensajes que se cifraban con un procedimiento que se utilizó durante el primer milenio de nuestra era.

Por otra parte, en el cifrado RSA (en el que está presente la aritmética modular), los números primos cobran un gran protagonismo, ya que la fortaleza del sistema radica en la dificultad que tiene para una computadora la factorización de un número compuesto como el producto de dos números primos (cuando dichos números tienen más de 200 cifras). Por lo tanto, algunos de los contenidos presentes en los programas de enseñanza media, que muchas veces parecerían no tener ninguna aplicación práctica, encuentran una utilidad dentro de la criptografía.

¿Qué es la criptografía?

A lo largo de la historia se ha tenido la necesidad de enviar mensajes secretos. Si el emisor y el receptor estaban a una distancia relativamente pequeña podían encontrarse personalmente y comunicarse el mensaje en forma oral. Pero, ¿qué sucedía si era imposible reunirse debido a distancias de separación muy grandes entre los participantes de la comunicación? En ese caso el mensaje tenía que ser enviado de alguna forma segura. Si bien actualmente utilizamos medios electrónicos o informáticos para hacerlo, también puede llevarse a cabo escribiendo el texto en un papel y enviándolo como se acostumbraba a hacer antes de la era digital. No importa la forma en que enviemos el mensaje, siempre se corre el riesgo de que alguien externo lea su contenido sin nuestro consentimiento. Es por esto que se puede optar principalmente por dos alternativas: la de *ocultar el mensaje* de alguna manera para que nadie sepa de su existencia salvo su receptor, y la de *ocultar el significado del mensaje* para que si alguien lo intercepta no entienda su contenido. La *esteganografía* es la ciencia que se encarga de la primera mientras que de la segunda se ocupa la *criptografía*.

La criptografía estudia los códigos secretos o códigos cifrados (en griego *kripto* significa secreto y *grapho*, escritura). Es una disciplina muy antigua, cuyos orígenes se remontan al nacimiento de nuestra civilización. Su único objetivo era el de proteger la confidencialidad de informaciones militares y políticas (Fernández, 2004). Actualmente no solo tiene ese propósito sino que son cuatro que resumimos a continuación:

- privacidad o confidencialidad de la información
- autenticación de la misma (el emisor del mensaje es quien dice ser y no otra persona)
- su integridad (el mensaje que se recibe es el mismo que se envió)
- su no repudio (el emisor no puede negar haber enviado el mensaje)

A lo largo de la historia se han utilizado distintas maneras de enviar mensajes y es interesante estudiarlas porque cada civilización puso a prueba su ingenio para hacerlo. Pero antes corresponde aclarar algunos términos que utilizaremos a lo largo de este documento. Se llama *texto plano* al texto o contenido original que se quiere enviar, y *texto cifrado* al que resulta de haber aplicado un determinado algoritmo al texto plano con el objetivo de que sea ilegible para cualquiera, salvo el destinatario.

Por otro lado, *cifrar* un mensaje consiste en convertir el texto plano en cifrado y *descifrar* implica realizar el proceso inverso. Para lograr que el descifrado de un mensaje implique una ardua tarea a un tercero, se debe seleccionar adecuadamente un método de cifrado. (Castañeda & Cavallero, 1997)

Criptografía simétrica y asimétrica

Los métodos de cifrado pueden dividirse en dos grandes grupos: los *simétricos* y los *asimétricos*.

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave tanto para cifrar como para descifrar. El principal problema de seguridad de estos sistemas reside en el intercambio de claves entre el emisor y el receptor, ya que ambos deben usar la misma. Es por este motivo que se busca un canal de comunicación que sea seguro para el intercambio de la clave. Es muy importante que dicha clave sea difícil de averiguar, sobre todo hoy día debido al uso de computadoras y de otras tecnologías. Otro inconveniente que presenta este sistema es que si se quiere tener un contenido totalmente confidencial con distintas personas, el emisor debe asignar y recordar una clave por cada persona con la que se quiera comunicar, volviéndose problemático para él cuando se trate de una cantidad numerosa de receptores.

Los sistemas de cifrado asimétrico o también llamados sistemas de cifrado de clave pública, se basan en el uso de dos claves diferentes. Una es la *clave pública* y se puede enviar a cualquier persona sin ningún inconveniente y la otra se denomina *clave privada*, la cual debe resguardarse para que nadie tenga acceso a ella. Cuando se envía un mensaje, el emisor usa la clave pública del receptor para cifrar el mensaje. Una vez que el receptor lo descifra con su clave privada, podrá leer el mensaje original del emisor. La seguridad de estos sistemas radica en que luego de cifrado un mensaje, no se puede descifrar utilizando la clave pública: el único que tiene la posibilidad de hacerlo es el receptor que es quien posee la clave privada.

La escítala espartana

Uno de los primeros métodos de cifrado fue el que se utilizó en la guerra entre Atenas y Esparta.

Para comunicarse los militares espartanos enrollaban en forma de espiral una tira de cuero en una escítala (palo o bastón). Sobre esa tira se escribía el mensaje longitudinalmente, luego se desenrollaba y se enviaba a destino. Si alguien interceptaba el mensaje, aunque leyera la tira no entendería su contenido debido a que las letras aparecerían mezcladas. Este método requería que el receptor dispusiera de una escítala idéntica a la utilizada para cifrar el mensaje, para que, enrollando la tira en el bastón, pudiera descifrarlo.

El cifrado del César

Este método de cifrado debe su nombre a Julio César debido a que lo utilizó para enviar mensajes en la Roma Imperial. Es un procedimiento por sustitución ya que cada letra en el texto plano se reemplaza por la que está tres lugares después en el alfabeto. Es decir, la A se suplanta por la D, la B por la E, y así sucesivamente hasta que la Z se convierte en la C, como lo muestra la siguiente tabla:

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

Por ejemplo, el mensaje ATAQUEN POR LA NOCHE queda cifrado como DWDTXHP SRU ÑD PRFKH.

Actualmente a cualquier cifrado que consista en "correr" una determinada cantidad de lugares las letras del alfabeto original, se le llama cifrado del César.

Por otra parte, a cada letra se le puede asociar un natural del 0 al 26: la A se corresponde con el 0, la B con el 1, y así hasta que la Z se corresponde con el 26. Si llamamos x al natural que se corresponde con una letra del texto plano, la siguiente ecuación nos permite determinar el número que le corresponde a la letra del texto cifrado $\big(E(x)\big)$: $E(x) = x + k(m\acute{o}d\ 27)$, en donde k es el corrimiento establecido al cifrar el texto plano.

A partir de lo anterior se podrían plantear algunas actividades para la clase de matemática: la relación E definida anteriormente, ¿es función? En caso afirmativo, ¿existe su función inversa? Y si existe, ¿cuál sería su utilidad? Otras cuestiones que se

podrían investigar son: ¿qué desventajas tiene este tipo de cifrado? ¿Cómo se puede descifrar un mensaje que se haya interceptado sin saber cuál cifrado del César se utilizó para cifrarlo?

A lo largo de la historia los mecanismos de cifrado mediante sustitución fueron multiplicándose y sofisticándose, obteniendo como resultado criptogramas mucho más difíciles de descifrar. No es sino hasta la llegada del llamado "padre de la filosofía árabe", Abu Al-Kindi (801-873 d.C), que aparece un procedimiento que permite descifrar estos tipos de criptogramas de una manera genérica, llamado *criptoanálisis* o *análisis mediante frecuencias*. Este procedimiento de descifrado de criptosistemas se basa en estudiar la frecuencia con la que aparecen los distintos símbolos en el lenguaje del texto plano y luego estudiar la frecuencia con la que aparecen en el texto cifrado, y de esta manera establecer una relación biunívoca entre los caracteres para finalmente obtener el texto descifrado. Con la aparición del criptoanálisis, todos los mensajes cifrados por mecanismos de sustitución, si eran lo suficientemente extensos (para así tener una mayor muestra), eran descifrados con mucha facilidad.

Cifrado de Vigenère

El cifrado de Vigenère (nombrado así en honor al criptógrafo Blaise de Vigenère) es un cifrado simétrico y *polialfabético* o de *sustitución múltiple* (el cifrado de cada carácter varía en función de la posición que ocupe en el texto plano), a diferencia del cifrado del César que es *monoalfabético* (donde el texto cifrado mantiene la misma distribución de frecuencias de caracteres que el texto plano). Si bien recibe este nombre, la idea original fue de Giovan Battista Belasso en 1553, aunque Vigenère desarrolló un sistema más completo. Este tipo de cifrado posee mayor seguridad a la hora de enviar un mensaje pues, a diferencia del cifrado del César, utiliza más de un alfabeto.

Supongamos que se quiere cifrar el mensaje: "El sol sale por el este". En primer lugar se debe elegir una palabra clave, la cual determinará los cifrados del César que se utilizarán. A continuación se escribe la frase a cifrar y debajo la palabra clave repetida tantas veces como sea necesario. Si consideramos como palabra clave "LUNA", tendríamos:

E	L		S	O	L		S	A	L	E		P	O	R		E	L		E	S	T	E
L	U		N	A	L		U	N	A	L		U	N	A		L	U		N	A	L	U

Debajo de la primera "E" aparece una "L". Esto se debe interpretar de la siguiente forma: se cifra la letra E utilizando el método del César en que a la A le corresponde la L. Por lo tanto, a esta primera letra, en el texto cifrado, le corresponde la O. Empleando el mismo procedimiento para cifrar las otras letras se obtiene el siguiente texto cifrado: OA FOW NNMO KBR OA QSEY

El sistema de Vigenère tuvo vigencia hasta 1863, año en que el prusiano Friedrich Kasiski logró encontrar una forma para romperlo. El método creado por Kasiski tiene como finalidad determinar la longitud de la palabra clave. De esta forma se pueden agrupar las letras para emplear el análisis de frecuencia y así obtener el texto plano. Observando el ejemplo anterior vemos que, cada cuatro letras, el cifrado empleado es el del César en el que a la letra A le corresponde la L. Al agrupar todas las letras que poseen este corrimiento, podemos analizarlas utilizando el análisis estadístico del cifrado del César.

El sistema RSA

Es un sistema criptográfico de clave pública desarrollado en 1977 por **R**on Rivest, Adi **S**hamir y Leonard **A**dleman, del Instituto Tecnológico de Massachusetts (MIT). ¿Cómo funciona? Como en todo sistema de clave pública cada usuario tiene dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con dicha clave, y una vez que el mensaje cifrado llega al receptor, este se encarga de descifrarlo usando su clave privada.

¿Cómo cifrar un mensaje? Supongamos que la clave pública del receptor es el par (e, n) (que puede estar publicada en una guía de claves públicas) y que el mensaje que se desea cifrar es un cierto número m, con $1 \leq m \leq n-1$ y $\text{MCD}(m, n) = 1$. El mensaje cifrado será el número c tal que $c \equiv m^e \, (mód\, n)$. Por ejemplo, supongamos que la clave pública del Sr. X es $(11, 65)$ y que el mensaje que se quiere cifrar es $m = 57$, entonces el mensaje cifrado es $c \equiv 57^{11} (mód\ 65)$, por lo que $c = 8$. Ahora bien, ¿cómo el receptor descifra el mensaje? Si la clave privada es el par (d, n), el mensaje plano m se obtiene a partir del mensaje cifrado c resolviendo la ecuación $m \equiv c^d (mód\ n)$. Siguiendo con el ejemplo anterior, si la clave privada del Sr. X es $(35, 65)$, para descifrar el mensaje que le han enviado deberá resolver la ecuación $m \equiv 8^{35} (mód\ 65)$. De este modo obtendrá $m = 57$.

El procedimiento anterior queda justificado a partir de una proposición matemática, pero antes de presentar su enunciado veamos cómo se obtiene la clave pública y la privada. Para determinar la clave pública se siguen los siguientes pasos:

(1) Se eligen dos números primos grandes p y q (del orden de 10^{200}, para que sea inviable hoy día hallarlos con computadoras).

(2) Se calcula $n = p.q$ y $\varphi(n) = (p-1)(q-1)$ (φ es la función de Euler, es decir, la función que a cada natural n mayor que 0 le hace corresponder la cantidad de naturales menores o iguales que n que son coprimos con n).

(3) Se elige un entero arbitrario e tal que $1 < e < \varphi(n)$ y $\text{MCD}(e, \varphi(n)) = 1$.

La clave pública será el par (e, n).

Por ejemplo, consideremos $p = 5$ y $q = 13$. Calculamos $n = 5.13 = 65$ y $\varphi(65) = (5-1)(13-1) = 48$. Podemos elegir $e = 11$, ya que $1 < 11 < \varphi(65)$ y $\text{MCD}(11, \varphi(65)) = 1$. La clave pública será entonces: $(11, 65)$.

¿Y la clave privada? Para obtener la clave privada se halla el único d que verifica: $1 < d < \varphi(n)$ y $e.d \equiv 1 (mód\ \varphi(n))$. La clave privada será: (d, n).

Volviendo al ejemplo anterior, se debe hallar d tal que $1 < d < \varphi(65)$ y $11.d \equiv 1 (mód\ \varphi(65))$, de lo cual resulta que $d = 35$ y, por lo tanto, la clave privada es $(35, 65)$.

Por último, el teorema que está por detrás del sistema RSA plantea lo siguiente (Criptografía, 2007):

Consideremos los enteros positivos p, q, n, d, e y m mencionados anteriormente. Si m es el mensaje plano y c el mensaje cifrado, se cumple que si $c \equiv m^e (mód\ n)$, entonces $m \equiv c^d (mód\ n)$.

¿Dónde radica la dificultad para descifrar un mensaje si no se posee la clave privada? Como se vio más arriba, para hallar m conociendo c hay que resolver la ecuación $m \equiv c^d (mód\ n)$, para lo cual es suficiente con conocer d (ya que n es parte de la clave pública). A su vez d verifica que $e.d \equiv 1 (mód\ \varphi(n))$, en donde e es conocido (ya que es parte de la clave pública), por lo que bastaría conocer $\varphi(n)$ para poder hallar d. Ahora bien, $\varphi(n) = (p-1)(q-1)$ es fácil de calcular si conociéramos los números primos p y q, para lo cual se debería poder factorizar n como el producto de factores primos. Y es aquí dónde radica la dificultad: ¡es muy difícil factorizar números naturales grandes! (Graña, Jancsa, Jeronimo, Pacetti & Petrovich, 2010)

Conclusiones

La utilización de sistemas de cifrado como los abordados en este trabajo representan una fuente de recursos didácticos para la introducción y enseñanza de diversos contenidos matemáticos. A través de la criptografía se pueden plantear problemas que susciten el interés de los estudiantes y promuevan un auténtico trabajo matemático en contraposición a la realización de actividades rutinarias que solo requieren la aplicación de procedimientos mecánicos. (Además, a partir del trabajo en grupos, se estimula la participación y la cooperación.) Como si se tratara de un juego, los alumnos tienen que descubrir y comprender el funcionamiento del cifrado utilizando distintos conceptos matemáticos para lograr el objetivo final: descifrar un mensaje.

Referencias

Graña, M., Jancsa, A. P., Jeronimo, G., Pacetti, A. & Petrovich, A. (2010). *Los números. De los naturales a los complejos*. Recuperado de http://www.ifdcvm.edu.ar/tecnicatura/Ciencias_Nat_y_las_Matematicas/14.pdf

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

Castañeda, C. y Caballero, P. (1997). Sistemas criptográficos de sustitución. *NÚMEROS. Revista de Didáctica de las Matemáticas 30*, 15-30.

Criptografía. (s. f.). En *Notas del curso Matemática Discreta 2 (2007)*. Facultad de Ingeniería. UdelaR. Recuperado de https://www.fing.edu.uy/imerl/matdisc2/cursos_anteriores/md2%202008/criptog08.pdf