Revista Digital Universitaria
10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

ARTICULO

LAS MATEMÁTICAS Y SUS APLICACIONES EN COMUNICACIONES DIGITALES

Dr. Guillermo Morales-Luna
Departamento de Computación
Centro de Investigación y Estudios Avanzados del IPN,
Cinvestav-IPN
gmorales@cs.cinvestav.mx

10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

Las Matemáticas y su aplicación en las Comunicaciones Digitales

Resumen:

Bosquejamos aplicaciones matemáticas en las comunicaciones digitales: en la Teoría de Códigos para ilustrar su importancia en la transmisión de información, y en la Criptografía para mostrar sus aportes a la seguridad de la información. Hemos querido seguir un enfoque cronológico pero también hacer una somera descripción de las matemáticas utilizadas. Al final queremos enfatizar que la influencia de las matemáticas en las comunicaciones está lejos de haberse agotado y plantea problemas de intensa investigación actual.

Matemáticas puras según Hardy

En la primera mitad del siglo XX, el profesor Godfrey Harold Hardy (1877-1947), de la Universidad de Cambridge en Inglaterra, se distinguió como un gran matemático con contribuciones importantes en Teoría de Números, perteneció a la generación que incluyó a Bertrand Russell, Alfred North Whitehead, J. E. Littlewood y Alan M. Turing, entre otros. Su libro de texto, en coautoría con Wright,[1] es un clásico vigente en cursos en todo el mundo. En su célebre Apología,[2] publicada en 1940, Hardy formuló apreciaciones de su visión de las matemáticas puras que se han convertido en aforismas, entre muchas otras las siguientes[3]:

- Me intereso en las matemáticas sólo por ser un arte creativo.
- Arquímedes será recordado cuando Esquilo haya sido olvidado, porque los idiomas perecen pero las ideas matemáticas, no. “Inmortalidad” es una palabra zonza, pero tal vez un matemático es quien tiene mayor posibilidad de alcanzarla.
- Nunca he hecho nada “útil”. Ningún descubrimiento mío ha redundado o ha parecido redundar, para bien o para mal, en una mejora al mundo.
- Los matemáticos pueden regocijarse de que la lejanía de su ciencia de las actividades humanas ordinarias la mantendrá noble y pulcra.
- Una ciencia se califica de útil sólo cuando contribuye a acentuar las desigualdades sociales o incluso a destruir la vida humana.
- Nadie ha descubierto un propósito bélico que se apoye en la Teoría de Números o en la Relatividad, y parece poco plausible que esto ocurra en los próximos años.

1 Hardy, G. H., and Wright, E. M. An Introduction to the Theory of Numbers. fifth ed. Oxford: Clarendon Press, 1979.

2 Hardy, G. H. A Mathematician’s Apology. Cambridge University Press, January 1992. Available at http:// www.math.ualberta.ca/~mss/misc/A%20Mathematician’s%20Apology.pdf

3 Traducciones libérrimas mías (GML), todas provenientes de: Hardy, G. H. A Mathematician’s Apology. Cambridge University Press, January 1992. Available at http:// www.math.ualberta.ca/~mss/misc/A%20Mathematician’s%20Apology.pdf

]

La última de estas aseveraciones ha sido constantemente objeto de refutaciones. Lamentablemente menos de un lustro después de haber sido formulada, el Proyecto Manhattan mostró la aplicación, aun cuando se quisiese marginal de la Relatividad en la construcción de la bomba atómica. Por lo que respecta al uso de la Teoría de Números, ésta se ha utilizado también desde entonces en las comunicaciones, tanto civiles como militares, tal como lo apuntaba Levinson desde los años 70.[4]

Códigos

Recordemos que en la década de los 40 del siglo XIX, Samuel Morse (1791-1872) inventó su célebre esquema de codificación del alfabeto latino en un lenguaje consistente de palabras sobre un alfabeto de tres símbolos: punto, raya y blanco. En 1874, el francés Emile Baudot (1845-1903) inventó una codificación que a cada carácter lo identificaba con una cadena de 5 bits, con lo cual proporcionó facultades de impresión a las comunicaciones telegráficas; como sólo hay cadenas de 5-bits, se utilizaba dos plantillas de caracteres, por lo que se tenía un código de 64 símbolos; este código se usó durante largo tiempo e incluso en 1932, el Comité Consultatif International Télégraphique et Téléphonique (CCITT) estandarizó un código basado en cadenas de 5 bits para teleimpresoras. A finales del XIX, el norteamericano Herman Hollerith (1860-1929), inventó el código para tarjetas perforadas, las cuales eran de uso común en la industria textil decimonónica; el código de Hollerith se mantuvo en uso hasta la década de los 70 del siglo XX.

En 1963 se adoptó como un estándar el código ASCII (American Standard Code for Information Interchange), el cual codificaba un alfabeto consistente de 96 caracteres (alfanuméricos y especiales) con cadenas de 7 bits (las 2^7 - 96 = 32 cadenas restantes correspondían a símbolos de control y a "variantes nacionales" estandarizadas en 1967 como la ISO (International Organization for Standardization) Recommendation 646), un octavo bit era "de paridad" de cada cadena de 7 bits y se utilizaba para detección de errores; en la actualidad ese octavo bit ha dejado de cumplir con su papel de revisión y ha servido para extender el código ASCII a 2^8 = 256 caracteres. El código Latin-1 (ISO 8859-1), una extensión de ASCII/ISO 646, contiene los caracteres acentuados propios de idiomas romances como el nuestro. En las décadas de los 60 y los 70, IBM desarrolló el código EBCDIC (Extended Binary Coded Decimal Interchange Code) también con 2^8 = 256 caracteres. En los 80 se inició un proyecto para establecer un Unicode (Unification Code) utilizando 16 bits para codificar cada símbolo, y ya últimamente, el ISO/IEC DIS 10646 se ha desarrollado como un estándar multilingüe que codifica caracteres con cadenas de 32 bits (es decir 4 octales o bytes) y por tanto posee una capacidad de hasta 2^{32} = 4,294,967,296 caracteres. Así pues en las comunicaciones electrónicas el alfabeto de codificación ha consistido de cadenas de una longitud fija, sobre un alfabeto pequeño, usualmente de tan sólo dos caracteres.

El lenguaje del código

Dos tareas importantes que ha de cumplir cualquier codificación son la detección y la corrección de errores. Cuando una parte, digamos Alicia, se quiere comunicar con otra, digamos Beto, el canal de transmisión que utilicen podría alterar las cadenas de bits enviadas por Alicia. Además de que sería altamente ineficiente que Beto le devolviera a Alicia, con el propósito de verificar que sean correctas, las cadenas que hubiera ella transmitido, se tendría que en ese viaje de regreso podrían introducirse nuevas alteraciones. Por ello, Alicia y Beto pueden convenir de antemano un lenguaje de código, es decir, un conjunto de cadenas, o palabras, que han de servir como códigos. Así, si Beto recibe una cadena y ésta no está en el lenguaje de código convenido, entonces Beto podrá detectar que hubo un error. Si además Beto puede localizar

4 Levinson, N. Coding theory: A counterexample to G. H. Hardy's conception of applied mathematics. American Mathematical Monthly 77, 3 (1970), 249-258.

10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

la palabra de código que se parece más a la recibida, entonces podrá sustituir a la cadena recibida por aquella en el código que más se le parezca y corregir así el error detectado.

El conjunto GF(2) que consta de los valores 0 y 1, o sea el conjunto de bits, posee una estructura algebraica de campo, es decir posee una suma (x + y es 0 sólo cuando x = y) con respecto a la cual es un grupo, y posee una multiplicación (x.y es 1 sólo cuando ambos x e y sean 1) con respecto a la cual los elementos no-nulos forman un grupo (en este caso el grupo multiplicativo trivial que consta sólo del 1), y la multiplicación se distribuye respecto a la suma.[5] Para cada entero n, el conjunto de cadenas de bits de longitud n forma un espacio vectorial, GF(2,n), de dimensión n, sobre el campo GF(2). Se dota así de una estructura geométrica al conjunto de cadenas de longitud n. Todo subespacio vectorial V puede ser descrito por una base de él y al colocar a los vectores de una base como columnas en un arreglo rectangular se obtiene una matriz generatriz de V. Este espacio tiene un complemento ortogonal, digamos Orto(V), y una generatriz suya se dice ser una matriz de paridad de V. Con todo esto se tiene que una cadena está en V siempre que al multiplicarla por una matriz de paridad se obtiene la palabra nula, es decir aquella de longitud n consistente sólo de valores 0. El peso de una palabra en GF(2,n) es el número de valores distintos de 0 en ella. Dadas dos palabras, la distancia entre ellas es el peso de su suma. GF(2,n) resulta así ser un espacio métrico vectorial, es un objeto matemático en el que se puede desarrollar un análisis geométrico completo.

Pues bien, si se elige como lenguaje de código a un subespacio lineal, la detección de errores se realizará multiplicando cada palabra recibida por una matriz de paridad. Si el resultado, llamado síndrome, no fuese nulo, entonces se detecta un error. Dada una palabra en la que aparezca un error, se calcula aquella palabra en el lenguaje de código que minimice la distancia a esa palabra, con lo cual se la habrá de corregir. Las codificaciones construídas así se llaman códigos lineales. A la fecha se ha reportado una gran variedad de éstos: los de Hamming, los polinomiales, los cíclicos, los de Golay, los de Reed-Muller, los de Reed-Solomon, etc.

Un curso muy descriptivo sobre la Teoría de Códigos es: Fundamentals of error-correcting codes, de Huffman, W. C., AND Pless, V. , editado por la Universidad de Cambridge en 2003; un recuento de tipo histórico, técnico y lógico es: Coding theory and cryptography: From Enigma and Geheimschreiber to quantum theory, de Joyner, D que se encuentra disponible en esta dirección: http://web.usna.navy.mil/~wdj/papers/cryptoday.html.

Unas prácticas con Mathematica de Gachkov, I. están disponibles en: http://library.wolfram.com/infocenter/MathSource/5085/; y unas notas propias, en estado de desarrollo, aparecen en: http://delta.cs.cinvestav.mx/~gmorales/TeoriaDeCodigos/.

Los códigos de Reed-Muller

Los códigos de Reed-Muller fueron inventados en los años 50, Muller los presentó formalmente en su artículo: “Application of Boolean algebra to switching circuit design and to error detection”,[6] Reed presentó el método de decodificación en: “A class of multiple-error-correcting codes and the decoding scheme”,[7]

5 Un buen curso de campos finitos es: Lidl, R., AND NIEDERREITER, H. Finite Fields. Reading, MA: Addison-Wesley, 1983. Encyclopedia of Mathematics and its Applications, Volume 20.

6 Muller, D. E. “Application of Boolean algebra to switching circuit design and to error detection”. IEEE Trans. on Electronic Computers 3 (1954), 6-12.

7 Reed, I. S. “A class of multiple-error-correcting codes and the decoding scheme”. IEEE Trans. on Information Theory 4

y en los 70 fueron utilizados para el envío de fotografías por naves espaciales Voyager y Mariner. Los códigos de Reed-Solomon fueron presentados en 1960 en el texto: "Polynomial codes over certain finite fields"[8] (Irving S. Reed (1923- -) y Gustave Solomon (1930-1996) eran investigadores del Instituto Tecnológico de Massachussets en ese entonces) y han sido utilizados en CD's, DVD's y discos Blu-ray, así como en sistemas de comunicaciones DSL, WiMAX, DVB y ATSC. En la década de los 80 Philips y Sony Corporation establecieron el CIRC (Cross Interleaved Reed-Solomon Code) como un estándar en la detección y corrección de errores en el sistema de audio para discos compactos. Así que toda vez que se utiliza un disco compacto, sea de audio o de datos, se está aprovechando servicios otorgados mediante códigos lineales.

Esta es pues una aplicación muy relevante de las matemáticas en la vida moderna, en particular es una aplicación de la Teoría de Números, contradiciendo la hipótesis de Hardy. De hecho, en la actualidad se ha planteado una conjetura: Toda área de Matemáticas, sin importar cuán abstracta sea, a la larga ha de sustentar una aplicación práctica. Pero ésta no es la única aplicación relevante. La Criptografía moderna se basa esencialmente en las matemáticas.

Criptografía

La criptografía desde siempre, desde los tiempos de la Grecia Clásica en la Cultura Occidental por ejemplo, ha sido una componente esencial de la seguridad en las comunicaciones. Si bien hasta mediados del siglo XX era del dominio casi exclusivo de sectores gubernamentales (militares y diplomáticos) o de grandes corporaciones (la Iglesia Católica por ejemplo) en la actualidad se utiliza por toda la sociedad, en cualquier comunicación digital. La criptografía proporciona servicios de confidencialidad, de integridad de mensajes, de autenticación de mensajes y de usuarios y de establecimiento de compromisos (no-repudio, avales, pronósticos, apuestas, etc.) entre muchos otros. En las comunicaciones a través de la world wide web, las transacciones seguras se hacen con el protocolo https y cualquier navegador las identifica mostrando un candado a cada usuario. De hecho la capa de seguridad de Internet, SSL (Secure Socket Layer) o TLS (Transport Layer Security),[9] implementa procedimientos criptográficos y éstos son de uso universal acaso de manera inconsciente por los usuarios. Al hacer uso de cajeros automáticos o de consultas bancarias en-línea, de tiendas con comercio electrónico, de votaciones electrónicas, de firmas electrónicas ante la Secretaría de Hacienda[10] en el caso mexicano o ante cualquier autoridad hacendaria en cualquier otro país, se está utilizando a la criptografía. Incluso varios países, España[11] entre ellos, tienden a expedir carnets de identidad a sus ciudadanos en los que se integra una firma electrónica a la identidad de cada uno de ellos. La criptografía de clave pública se usa de manera extensa y se ha estandarizado;[12] cualquier proveedor de servicios criptográficos debe ajustarse a los estándares técnicos establecidos, tanto en lo tocante a la codificación de la información como a la implementación de los

(1954), 38-49.

8 Reed, I. S., AND SOLOMON, G. "Polynomial codes over certain finite fields". Journal of the Society for Industrial and Applied Mathematics 8, 2 (1960), 300-304.

9 IETF Secretariat. Transport layer security (tls). Report, 2008. http://www.ietf.org/html.charters/tls-charter.html.

10 Servicio de Administración Tributaria. Firma electrónica avanzada (fiel). URL, 2008. http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/

11 Gobierno de España, Ministerio de Fomento. Documento nacional de identidad electrónico. URL, 2008. http://www.dnielectronico.es/.

12 RSA Laboratories. Public-key cryptography standards (PKCS). Standards Initiatives, 1991-2008. http://www.rsa.com/rsalabs/node.asp?id=2124.

10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

procedimientos matemáticos.

En todo esquema criptográfico hay objetos sintácticos de tres tipos: mensajes, cifrados y claves (o si se quiere, llaves), y dos funciones determinantes, una de cifrado (en inglés, encryption) y otra de descifrado (en inglés, decryption). Dada una clave de cifrado, la función de cifrado transforma cada mensaje en un cifrado único; recíprocamente, dada una clave de descifrado, la función de descifrado transforma cada cifrado en un mensaje único. Dos claves, una de cifrado y otra de descifrado, corresponden entre sí toda vez que al descifrar con la clave de descifrado, el cifrado obtenido con la función y la clave de cifrado en un mensaje, se obtiene ese mismo mensaje, y, recíprocamente, al cifrar con la clave de cifrado, el mensaje obtenido con la función y la clave de descifrado en un cifrado, se obtiene ese mismo cifrado. Los esquemas criptográficos en los que toda clave corresponde consigo misma se dicen ser simétricos o de clave secreta. En ellos cualquier usuario que conozca una clave podrá cifrar y descifrar cualesquiera mensajes y cifrados obtenidos de ellos con esa clave. Por eso, el dueño de cada clave la debe mantener en secreto, y compartirla sólo con sus corresponsales autorizados, y evitar así intrusiones no-autorizadas. Cuando la clave de cifrado es distinta de su correspondiente de descifrado, el esquema criptográfico se dice ser asimétrico o de clave pública. Cada usuario, digamos Alicia, ha de poseer dos claves: una para cifrar, llamada clave pública, que denotaremos CPubA, y otra para descifrar, llamada clave privada, que denotaremos CPrvA. Alicia puede publicar su clave CPubA, por lo que todo corresponsal, digamos Beto, puede cifrar mensajes que le quiera enviar a Alicia, aunque sólo ella, siendo la única poseedora de CPrvA podrá descifrar. Alicia, junto con sus corresponsales, mantiene así la confidencialidad de los mensajes dirigidos a ella. Por otra parte, dado un mensaje originado por Alicia, ella le puede concatenar el descifrado del mensaje obtenido con su clave privada CPrvA. Cuando Beto recibe el mensaje y ese descifrado, a este último lo cifra con la clave pública CPubA y al ver que el resultado coincida con el mensaje tendrá evidencia de que éste proviene efectivamente de Alicia. El descifrado hace pues las veces de una firma criptográfica y sirve para autenticar a Alicia ante Beto.

En suma, en todo sistema criptográfico se tiene una función de cifrado $E:\{Claves\}\times\{Mensajes\}\rightarrow\{Cifrados\}$ y una de descifrado $D:\{Claves\}\times\{Cifrados\}\rightarrow\{Mensajes\}$ tales que para cada clave CPub existe una clave CPrv de manera que

- para cada mensaje M: D(CPrv,E(CPub,M)) = M, y
- para cada cifrado C: E(CPub,D(CPrv,C)) = C.

En los esquemas de clave secreta, CPrv, coincide con la pública CPub, pero en los esquemas de clave pública obligadamente CPrv es distinta de CPub. Por un lado, fija la clave CPub, se quiere que el cifrar con esa clave, es decir, el cálculo de la transformación M a C=E(CPub,M), sea muy eficiente; y, por otro lado, que su transformación inversa C a M=D(CPrv,C) sea tan cara en cuanto a recursos de cómputo que en la práctica sea irrealizable. En términos técnicos, lo que se quiere es que la función de cifrado sea unidireccional (en inglés: trapdoor one-way function). La robustez de un sistema de clave pública radica en el hecho de que aun cuando sean conocidos los procedimientos de cifrado y descifrado, es decir, las funciones E y D, y una clave pública CPub, el cálculo de la correspondiente clave privada CPrv sea computacionalmente intratable.

Funciones unidireccionales

Como ejemplos de funciones unidireccionales están los siguientes:

- Productos y factorizaciones. Dados dos números primos p, q, el cálculo de su poducto n = p q es una operación muy sencilla de ser realizada. Recíprocamente, si se sabe que el entero n es el producto de dos primos p, q, calcular a estos últimos partiendo sólo de n es una tarea harto costosa. En efecto, supongamos que cada uno de los factores p, q se escribe con k dígitos (si los consideramos binarios hagamos b = 2 y si fuesen decimales hagamos b = 10), en otras palabras, que p, q son de tamaño k. Entonces n se escribe con 2k dígitos. El cálculo de n, dados p, q, se realiza con el más convencional de los procedimientos con k k operaciones dígito a dígito o bien con k log(k) de tales operaciones si se hace de una manera más inteligente (usando la llamada Transformada Rápida de Fourier). El producto es pues de costo menor que cuadrático en el tamaño de los factores. En cambio, dado n de tamaño 2k prácticamente la única manera de encontrar a los factores p, q es localizando a uno primero revisando si acaso n es divisible por cada uno de los primos menores que su raíz cuadrada. Por el Teorema de los Números Primos se tiene que hay del orden de n/log(n) de tales primos, es decir hay del orden de b a la potencia k, dividido entre k, candidatos. Factorizar es pues de costo exponencial con el tamaño, lo que es irrealizable para valores considerables de k. El producto de dos primos es una función unidireccional.

- Exponenciaciones y logaritmos. Sea x un número real positivo. La órbita de x en el conjunto de reales positivos consta de todas las potencias de x con exponente entero. Para determinar si acaso un real positivo y está o no en la órbita de x basta con calcular el logaritmo de y en base x: se tendrá que éste es entero si y sólo si y está en la órbita de x. El cálculo de logaritmos en los reales, siendo ésta una función analítica, es un problema muy sencillo, trivial en la práctica. Sin embargo, el problema cambia radicalmente cuando en vez de los reales consideramos grupos finitos. Si G es un tal grupo, su orden es su cardinalidad. Dado un elemento x en él, el orden de x es el número de elementos de su órbita. El Teorema de Lagrange establece que el orden de cualquier elemento es un divisor del orden del grupo. Hay grupos finitos en los que el problema de decidir cuándo un elemento y está en la órbita de un elemento x sólo puede hacerse de manera exhaustiva: una a una se van calculando las potencias de x y se detiene la primera vez que se obtiene y o la unidad del grupo. El cálculo de los llamados logaritmos discretos sólo puede hacerse de manera exhaustiva, lo que es irrealizable si el orden del generador x es grande. En cambio, el cálculo de las potencias se hace de manera muy eficiente. En grupos finitos, la exponenciación a potencias enteras es pues una función unidireccional.

- Elevación al cuadrado y raíz cuadrada. Aunque ambas operaciones son inmediatas en el grupo multiplicativo de los números reales positivos, la extracción de raíces en el grupo multiplicativo de residuos módulo un entero producto de dos primos es equivalente al problema de factorización de ese entero. Así, en tales grupos multiplicativos, la elevación al cuadrado es una función unidireccional.

- Reiteración de funciones. Supongamos dada una familia de funciones, cada una de las cuales se calcula eficientemente. Para un argumento dado y un criterio de selección de funciones, se reitera la aplicación sucesiva de funciones de acuerdo con el criterio de selección dado, partiendo del punto dado (la manera en la que actúan los autómatas celulares se adecúa a este esquema). La

10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

reiteración es una función unidireccional.

El esquema de cifrado RSA

El esquema de cifrado RSA (iniciales de sus autores: Ronald Rivest, Adi Shamir y Leonard Adleman), fue publicado en 1977 y es en la actualidad el más utilizado en aplicaciones criptográficas de clave pública. RSA se basa en la dificultad del problema de factorización. Sus fundamentos matemáticos son muy elementales, y el principal es el llamado Teorema Pequeño de Fermat (debido, evidentemente, a Pierre de Fermat (1601-1665)): Si n = p.q es el producto de dos primos, entonces para cualquier x no nulo, $x^{p-1} = 1 \bmod p$ y $x^{q-1} = 1 \bmod q$, luego $x^{(p-1)(q-1)} = 1 \bmod n$. Por tanto, si e y d son enteros tales que $e \cdot d = 1 \bmod [(p-1)(q-1)]$ entonces para todo x, $x^{e \cdot d} = x \bmod n$. Así, si x es un mensaje, su cifrado c ha de ser x elevado a la potencia e, y el mensaje x se descifrará como c elevado a la potencia d. La clave pública es la pareja (e, n) y la clave privada es la pareja (d, n). El cálculo de d sería inmediato conociendo e y la factorización de n. Como esto último es difícil, se tiene que el esquema RSA es seguro. Sorprende que hasta antes de la tercera cuarta parte del siglo XX no se haya concebido este sistema criptográfico, pero hay que tener en cuenta que, aunque las matemáticas involucradas son muy elementales y conocidas desde 300 años antes, los cálculos numéricos necesarios, propios de una aritmética de grandes números, sólo fueron accesibles a un segmento social amplio con las computadoras de esa época.

Existe también un esquema de clave pública basado en la dificultad de calcular logaritmos discretos, éste debido a Taher El-gamal en 1985, y esquemas similares en grupos de curvas elípticas fueron introducidos, unos por Victor Miller en 1985 y otros por Neal Koblitz en 1987. Desde los 90 se utilizan también grupos algebraicos propios de curvas hiperelípticas de género mayor. Así las matemáticas más sofisticadas de la Geometría Algebraica se han utilizado para desarrollar nuevos esquemas o para analizar la robustez de los de uso común en la actualidad, con el fin de prevenir a sus usuarios acerca de las debilidades descubiertas.[13]

Un caso controvertido

Las matemáticas han tenido una gran influencia en el desarrollo de la criptografía en las últimas cuatro décadas. Sin embargo, el trabajo de criptógrafos y el de matemáticos es muy distinto. En 2007, Neal Koblitz publicó en el Notices de la sociedad matemática norteamericana un artículo muy controvertido,[14] en donde apunta dos aspectos, que él considera indeseables, del efecto de la investigación matemática en criptografía. El primero se refiere a la tendencia en anunciar potenciales aplicaciones criptográficas de cualquier desarrollo en matemáticas, con el solo fin de obtener apoyos económicos, y estas supuestas aplicaciones criptográficas son inexistentes en los peores casos, o triviales y marginales en los mejores (en el caso estadunidense esta tendencia propicia además, según Koblitz, el surgimiento de actitudes chovinistas pues un patrocinador importante es la NSA (National Security Agency)). El segundo se refiere a que en criptografía se tiende a "matematizar" cualesquiera desarrollos, sobre todo cuando se pretende demostrar formalmente que éstos son robustos. Efectivamente, apuntaría yo, un enunciado de la forma "Tal protocolo es inmune a tales ataques" no puede equipararse a un enunciado "Tal teorema es válido ante tales hipótesis" pues en el primero ha de tenerse en cuenta que intervienen "atacantes pragmáticos", en tanto que el segundo es propio de la "epistemología matemática". Para cerrar su artículo, Koblitz cita a un

13 Un curso actual de criptografía es : Katz, J., AND LINDELL, Y. Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series). Chapman & Hall/CRC, 2007

14 Koblitz, N. "The uneasy relationship between mathematics and cryptography". Notices of the AMS 54, 8 (September 2007), 973-979.

criptógrafo de la NSA diciendo que en la criptografía de la vida real una falla de seguridad puede ocasionar pérdidas millonarias o de vidas humanas, en el caso de un enfrentamiento bélico, en tanto que en la criptografía de ambientes universitarios una falla puede significarle a sus autores la oportunidad de añadir más artículos a sus curricula. Uno de los autores de Introduction to Modern Cryptography (introducción a la criptografía moderna), Jonathan Katz de la Universidad de Maryland, responde[15] a Koblitz argumentando que las pruebas formales han transformado a la criptografía de un arte a una ciencia (y hace un reproche severo a los editores del Notices por haber publicado el artículo de Koblitz sin contraponerlo a una opinión opuesta).

Como lo mencioné al inicio de esta sección, las funciones unidireccionales son cruciales en los esquemas criptográficos, y en ellas, el cálculo de las funciones inversas debe ser "computacionalmente difícil". En la Teoría de la Complejidad hay diversas nociones de "dificultad". Hay problemas que de plano son irresolubles o no-computables (por ejemplo los llamados Problema de la Parada o Problema de Post de la Correspondencia) y también, fija una clase de problemas computables, se considera a aquellos a los cuales se reduce cualquier problema en esa clase mediante un procedimiento de conversión dentro de esa clase. Por ejemplo, la clase NP consta de los problemas tales que soluciones hipotéticas de ellas pueden verificarse como soluciones actuales de ellos por programas de computadora que corren en un tiempo polinomial en el tamaño de sus instancias. La clase P consta de los problemas cuyas soluciones son constructibles en tiempo polinomial. Naturalmente, P está contenida en NP, pero no se sabe en la actualidad si esa contención es propia. Uno de los problemas abiertos que se espera sean resueltos en el siglo XXI es decidir si P = NP. Un problema es difícil en la clase NP (o difícil-NP) si cualquier problema en NP se reduce a él en tiempo polinomial. Pues bien, es evidente que el problema de factorización de enteros y el problema del logaritmo discreto están en la clase NP (dadas soluciones hipotéticas se verifica sin esfuerzo alguno si éstas son en realidad soluciones verdaderas). Pero no se sabe a la fecha si acaso son difíciles-NP. Se conocen algoritmos de tiempo exponencial (o subexponencial pero superpolinomial) para resolverlos, pero ni se ha probado que cualquier problema en NP se reduce a ellos en tiempo polinomial, ni tampoco que no existan procedimientos polinomiales para resolverlos efectivamente (en el Cómputo Cuántico se ha diseñado algoritmos polinomiales para resolverlos, pero sus funciones primitivas entrañan una complejidad exponencial cuando se las quiere simular por esquemas clásicos).

Así que nos encontramos con que los esquemas criptográficos actuales son robustos de manera "condicional": Si hubiese un algoritmo polinomial para calcular las inversas de las funciones unidireccionales y éste se descubriese entonces los esquemas dejarían de ser robustos, mas si no hubiese tal algoritmo y esto se probase se habría demostrado que los esquemas son efectivamente robustos. A la fecha, ¡los esquemas usuales son seguros porque "creemos" que lo son!

Conclusiones

Las matemáticas se han aplicado en las comunicaciones electrónicas y en la seguridad de la información de manera esencial e impactante. Por un lado, el diseño de códigos que minimicen la aparición de errores y propicien velocidades aún mayores de transmisión, y la demostración de la robustez de sistemas criptográficos son áreas de contínua investigación actual, en la que se verán aplicaciones matemáticas aún más impactantes en las comunicaciones de la vida cotidiana.

15 MCCURLEY, K. The Koblitz "controversy". URL, 2008. http://www.sigcrap.org/2007/09/14/the-koblitz-controversy/.

10 de enero 2009 • Volumen 10 Número 1 • ISSN: 1067-6079

Bibliografía

Gobierno de España, Ministerio de Fomento. Documento nacional de identidad electrónico. URL, 2008. http://www.dnielectronico.es/.

Hardy, G. H. A Mathematician's Apology. Cambridge University Press, January 1992. Available at http://www.math.ualberta.ca/~mss/misc/A%20Mathematician's%20Apology.pdf

Hardy, G. H., and Wright, E. M. An Introduction to the Theory of Numbers. fifth ed. Oxford: Clarendon Press, 1979.

Huffman, W. C., AND PLESS, V. Fundamentals of error-correcting codes. Cambridge Univ. Press, 2003.

IETF Secretariat. Transport layer security (tls). Report, 2008. http://www.ietf.org/html.charters/tls-charter.html.

Katz, J., AND LINDELL, Y. Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series). Chapman & Hall/CRC, 2007.

Koblitz, N. "The uneasy relationship between mathematics and cryptography". Notices of the AMS 54, 8 (September 2007), 973-979.

Levinson, N. Coding theory: A counterexample to G. H. Hardy's conception of applied mathematics. American Mathematical Monthly 77, 3 (1970), 249-258.

Mccurley, K. The Koblitz "controversy". URL, 2008. http://www.sigcrap.org/2007/09/14/the-koblitz-controversy/.

Morales-Luna, G. Introducción a la teoría de códigos. Notas en desarrollo, 2008. http://delta.cs.cinvestav.mx/~gmorales/TeoriaDeCodigos/.

Muller, D. E. Application of Boolean algebra to switching circuit design and to error detection. IEEE Trans. on Electronic Computers 3 (1954), 6-12.

Reed, I. S. A class of multiple-error-correcting codes and the decoding scheme. IEEE Trans. on Information Theory 4 (1954), 38-49.

Reed, I. S., AND SOLOMON, G. Polynomial codes over certain finite fields. Journal of the Society for

Industrial and Applied Mathematics 8, 2 (1960), 300-304.

RSA Laboratories. Public-key cryptography standards (PKCS). Standards Initiatives, 991-2008. http://www.rsa.com/rsalabs/node.asp?id=2124.

Servicio de Administración Tributaria. Firma electrónica avanzada (fiel). URL, 2008. http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/.