ÍNDICE

Página

I. INTRODUCCIÓN

Seguridad informática en el Ciberespacio

La criptografía responde a la necesidad de codificar mensajes que sólo pueda descifrar el destinatario y se ha aplicado tanto a defensa, como a secretos industriales y, en los últimos años, sobre todo, al comercio electrónico. Esto es así porque actualmente la seguridad de los sistemas informáticos se ve debilitada por el fuerte crecimiento de las redes y cuando se trata este tema hay que tener en cuenta un aspecto tan importante como la privacidad e integridad de los datos.

El motivo de la existencia de numerosas barreras para la aceptación generalizada del comercio electrónico en el mundo de hoy es que muchas de las grandes ventajas de la banca y la compra en el ciberespacio representan también obstáculos potenciales que es necesario superar.

En primer lugar, el reciente aumento del uso de la Red Internet ha dirigido la atención del mundo entero a un problema crucial que ya mencionábamos antes: la privacidad. Hasta el momento, no ha existido una protección real que garantice que los mensajes que enviamos o recibimos no son interceptados, leídos o incluso alterados por algún desconocido, ya que, en realidad, nadie controla Internet. Puede parecer que esto ocurra únicamente en las películas de guerra fría o las novelas de espionaje, pero no es así: también nos afecta a nosotros. Hace escasos meses se conoció la noticia de que el FBI había desarrollado un programa informático, el Carnivore, que filtraba los correos electrónicos sospechosos para controlar el tráfico de información y correo peligroso; su revisión ha sido solicitada por numerosas universidades norteamericanas, pero parece que todavía existen demasiados secretos alrededor de este programa censurador. Después de esto resulta comprensible que el objetivo de muchas de esas novelas a las que nos referíamos sea el de advertirnos para que protejamos nuestra identidad; éste es el caso, por ejemplo, de *Database Nation (The death of the privacy in the 21st century)*, de Simson Garfinkel, recientemente publicado. Si tenemos en cuenta la cantidad de datos almacenados en bases de datos informatizadas o la utilización cada vez mayor del correo electrónico, se comprende la necesidad de encontrar sistemas lo más seguros posible que garanticen la confidencialidad de datos y comunicaciones.

En segundo lugar, en el mundo del ciberespacio la posibilidad de que el fraude o la estafa existan es mucho mayor. La capacidad de tener acceso a información las 24 horas del día, desde cualquier lugar del mundo, es para muchos un beneficio que brinda la Red Internet. Sin embargo, esto plantea algunos inconvenientes prácticos. Las redes y sistemas informáticos se han convertido en un nuevo escenario para el delito: interceptar comunicaciones electrónicas entre dos personas, introducirse en los sistemas informáticos de empresas, difundir y vender ciertos datos industriales, destruir, modificar o alterar datos, programas o documentos electrónicos.

Los ***hackers*** o piratas informáticos son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección utilizando diferentes tipos de programas (*gusanos*, *troyanos*, *bombas*...). Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. La NASA es uno de los objetivos prioritarios de los *hackers*, soportando medio millón de ataques al año. El incidente más grave ocurrió en 1997, cuando un pirata informático bloqueó las comunicaciones del trasbordador Atlantis justo cuando iba a acoplarse a la estación Mir. Además, a finales de octubre del año

pasado la compañía Microsoft reconoció que un grupo de piratas informáticos había tenido acceso a su más íntimo secreto, el código de programación que hace funcionar Windows y los otros programas de la empresa, utilizados por casi el 90% de los usuarios de ordenadores. Esto deja claro que no existe un lugar seguro, ya que si han podido colarse en Microsoft es que pueden entrar en cualquier sitio, incluso en el portal de la compañía Yahoo!, que en febrero fue puesto fuera de combate durante tres horas tras un asalto en el los servidores de Yahoo! fueron bombardeados con mensajes falsos. Sin embargo, aunque los casos de jóvenes sumergiéndose en los potentes ordenadores de la NASA, el Pentágono o los grandes portales han sido constantemente aireados por la prensa, los episodios más relevantes han gozado de mucha menos publicidad y, en la mayoría de los casos, todavía siguen siendo desconocidos. El principal de los pocos que alcanzaron la luz pública es el del ciberataque contra el Citibank en 1994, cuando un delincuente que actuaba con un modesto equipo desde San Petersburgo transfirió unos 10 millones de dólares a diferentes cuentas. En este caso la conexión a la entidad bancaria no fue a través de Internet, sino utilizando la línea telefónica convencional de un país que, como es el caso de Rusia, no está precisamente desarrollada en este aspecto. Sin embargo, Internet, con sus grandes facilidades de conectividad, permite a los *hackers* intentar el acceso remoto a cualquier máquina conectada de forma anónima. Los expertos en crimen electrónico afirman que el fraude existe, pero no amenaza tanto a usuarios individuales como a las empresas punto com, las que hacen negocios en y con Internet. Las principales víctimas potenciales son los que venden en Internet los llamados bienes digitales, es decir, todo aquello que está hecho de bits, por ejemplo programas informáticos, acceso a servicios *on line* (subscripciones, juegos de pago) o documentos en formato digital (archivos en Word y otros). También aquellos que venden productos de alto valor a través de la Red, como coche y joyas, se encuentran entre los principales candidatos a ser atacados.

Una de las principales causas de que todavía no se den estos delitos es la escasa cuantía que supone actualmente el comercio electrónico, ya que las transacciones en Internet representan sólo un 2% del total de operaciones realizadas con tarjeta de crédito, lo que las convierte en un segmento poco interesante para delincuentes e investigadores. Difícilmente la policía va a poder dedicar muchos medios a delitos que alcancen poca cuantía, por lo que cada organización debe estar bien preparada para no encontrarse luego con sorpresas desagradables.

Cuando el cliente es sólo alguien al otro lado de la pantalla, ¿cómo saber si esa persona tiene efectivamente una cuenta válida? O, desde el punto de vista del consumidor, ¿por qué confiar en un comerciante al que nunca hemos visto o en una empresa que no conocemos? Después de todo, es posible que la "tienda" del comerciante exista sólo en el disco duro de la computadora de alguien con pocos escrúpulos dispuesto a obtener beneficios fáciles, el llamado **ciberdelincuente**.

El pasado verano, sin ir más lejos, nos sorprendió la publicación en la Red de una supuesta lista, que contenía las contraseñas de acceso a Internet de miles de usuarios de una conocida compañía. Al parecer, la empresa responsable de mantener la confidencialidad de esa información tenía conocimiento de la fuga desde hacía tiempo, y no había avisado a sus clientes para no alarmarles. Cuando la noticia trascendió se vio obligada a corregir la situación de forma precipitada, deshabilitando sin previo aviso las cuentas de los afectados, que contemplaban con perplejidad el espectáculo.

Después de este ejemplo, resulta obvio que para que el comercio electrónico cobre verdadero auge, cada una de las entidades que participan necesita contar con una manera de verificar la identidad de la otra para establecer un nivel de confianza.

La necesidad de una legislación seria que proteja a los consumidores de nuevas tecnologías del abuso de las compañías es apremiante, ya que actualmente, en España, a pesar de disponer de los mismos productos o servicios que en el comercio tradicional a unos precios mucho más ventajosos tan sólo un 2% de los consumidores ha comprado alguna vez por Internet.

Algunas empresas ya están tomando medidas para ofrecer al usuario un elevado nivel de seguridad en lo que

se refiere al almacenamiento y protección de su identidad. Éste es el caso de la empresa española ipsCA, que ha anunciado recientemente la inminente comercialización de sus tarjetas criptográficas −ipsCards− con sus respectivos lectores. De esta manera, y gracias al Certificado Digital que alberga (reconocido por Microsoft en sus navegadores y programas de correo electrónico) será posible asegurar la confidencialidad de las operaciones electrónicas.

Una técnica para proteger la confidencialidad es el cifrado. La información puede cifrarse y descifrarse empleando ecuaciones matemáticas y un código secreto denominado **clave**. Generalmente se emplean dos claves, una para codificar la información y otra para descodificarla. La clave que codifica la información, llamada clave privada, sólo es conocida por el emisor. La clave que descodifica los datos, llamada clave pública, puede ser conocida por varios receptores. Ambas claves se modifican periódicamente, lo que complica todavía más el acceso no autorizado y hace muy difícil descodificar o falsificar la información cifrada. Estas técnicas son imprescindibles si se pretende transmitir información confidencial a través de un medio no seguro como puede ser Internet. Las técnicas de firma electrónica permiten autentificar los datos enviados de forma que se pueda garantizar la procedencia de los mismos (imprescindible, por ejemplo, a la hora de enviar una orden de pago).

Otro sistema de seguridad es el formado por la especificación SET, Secure Electronic Transactions, que está diseñada con el propósito de asegurar y verificar la identidad de los participantes en las compras abonadas con tarjetas de pago en cualquier tipo de red en línea, incluyendo la Red Internet. SET fue desarrollada por Visa y MasterCard, con la participación de Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems, VeriSign y otras empresas líderes en tecnología. Al emplear sofisticadas técnicas criptográficas, SET convertirá el ciberespacio en un lugar más seguro para efectuar negocios, y con su implementación se espera estimular la confianza del consumidor en el comercio electrónico. El objetivo primordial de SET es mantener el carácter estrictamente confidencial de la información, garantizar la integridad del mensaje y autenticar la legitimidad de las entidades o personas que participan en una transacción.

Quizá el punto más importante en toda transacción comercial electrónica segura es el **certificado digital**, que brinda una forma conveniente y fácil de asegurar que las dos partes implicadas puedan confiar el uno en el otro. Esta confianza se establece a través de un tercero, en este caso Visa. Por ejemplo, Visa suministrará certificados digitales a las instituciones financieras emisoras de tarjetas, y cada institución, a su vez, ofrecerá un certificado digital al titular de la tarjeta. El proceso será similar en el caso de los comercios.

En el momento en que se efectúa la transacción, el software que cumple las normas de SET de cada entidad participante en la transacción, verifica y confirma la identidad del comercio y del propietario de la tarjeta antes de que se intercambie ningún tipo de información. Esta confirmación se realiza revisando los certificados digitales emitidos por una tercera parte autorizada y fiable.

Un mensaje puede pasar por un proceso de conversión o de encriptación, que lo transforma en código usando una clave, es decir, un medio de traducir los signos de un mensaje a otro sistema de signos cuya lectura no tenga ningún sentido para un desconocido que los intercepte. Esto se conoce como el proceso de encriptación de un mensaje. Así, para descifrar el mensaje o revertir la encriptación, el que lo recibe necesita conocer la clave secreta.

La gente se refiere a cosas muy dispares cuando habla de criptografía. Los niños juegan con cifras y lenguajes secretos. Sin embargo, esto tiene muy poco que ver con la seguridad real y el cifrado. Un sistema fuerte de encriptación puede ser usado para proteger información valiosa frente a delincuentes organizados, corporaciones multinacionales y poderosos gobiernos. Los sistemas más robustos de encriptación solían usarse únicamente en el sector militar, pero en la sociedad de la información se ha convertido en una de las herramientas principales para resguardar nuestra privacidad, realizar el control de acceso, los pagos electrónicos...

El espionaje

Si bien este término se puede emplear en referencia a los ámbitos militar, económico o político, en general suele relacionarse con la política exterior y de defensa. Fue hace más de 2000 años cuando se reconoció la información como una herramienta vital para el Estado, tanto para la diplomacia como para la guerra. Sin embargo, los estados modernos no crearon departamentos permanentes de espionaje hasta finales del siglo XIX.

La Segunda Guerra mundial fue el incentivo definitivo para los servicios de inteligencia en todo el mundo. Las modernas tecnologías militares y de comunicaciones hicieron imprescindible la información precisa y rápida. Algunas de las grandes batallas de esta guerra se entablaron entre los servicios de espionaje y contraespionaje. Por ejemplo, mientras Alemania realizaba sus transmisiones secretas, sobre todo submarinas, usando el cifrado **Enigma** (que era un aparato de apariencia similar a las máquinas de escribir portátiles, con un teclado convencional y tres ruedas transversales en el sitio en que las máquinas de escribir llevaban los tipos que golpeaban la cinta), los británicos y sus aliados consiguieron descubrir el código secreto alemán y llegaron a interceptar las comunicaciones de sus enemigos y decodificarlas en tan solo unas horas.

El ataque por sorpresa de Japón a Pearl Harbor el 7 de diciembre de 1941 supuso un gran éxito de los servicios de inteligencia japoneses y un gran fallo para los estadounidenses. Aquel fallo estimuló el respaldo a la ampliación de un enorme aparato de inteligencia en Estados Unidos después de la guerra. Antes de la II Guerra Mundial, Estados Unidos no tenía en la práctica ningún servicio de inteligencia, pero después de la guerra la CIA adquirió renombre en todo el mundo por su omnipresente vigilancia internacional.

La mayor parte de las corporaciones modernas tienen secciones de planificación estratégica que requieren servicios de inteligencia.

En Estados Unidos, la Agencia Central de Inteligencia (**CIA**) sigue siendo el eje de un elaborado sistema formado por una docena de organizaciones diferentes, donde cada una tiene un papel específico y un determinado ámbito de operaciones. El director central de Inteligencia es también el máximo dirigente de la CIA y el principal asesor del presidente en estas cuestiones.

En contraste con el sistema estadounidense, la estructura de los servicios de inteligencia de los antiguos países comunistas está muy centralizada. En la Unión Soviética el poder del Comité de Seguridad del Estado (**KGB**) invadía todos los aspectos de la vida nacional y poseía dos secciones principales. La primera se ocupaba de obtener información en el extranjero. La segunda tenía como principales responsabilidades el contraespionaje para proteger al régimen y el reclutamiento de agentes extranjeros para la Unión Soviética.

Un tercer modelo de servicios de inteligencia es el británico: consiste en un conjunto de oficinas coordinadas por un subcomité del gabinete ministerial. Sus dos principales departamentos son el Servicio Secreto de Inteligencia (también llamado MI6) y el Servicio de Seguridad (conocido como MI5). Estos nombres reflejan el origen militar de estos departamentos. El MI6 es similar a la CIA y al KGB y se ocupa del espionaje, el contraespionaje y de misiones secretas en el extranjero. El MI5 se ocupa del contraespionaje interno y de la seguridad interna. Scotland Yard posee una sección especial que funciona como el brazo visible del servicio de seguridad: detiene a sospechosos y proporciona pruebas en casos de espionaje, mientras que los agentes del MI5 se mantienen ocultos. También existen cierto número de unidades especializadas que operan en el ámbito de la comunidad de la Inteligencia británica. Los servicios de inteligencia de Francia, Israel, Italia y de los países de la Commonwealth han tomado como modelo la organización del sistema británico con algunas variantes nacionales.

En España, los servicios de inteligencia del Estado están a cargo del Centro Superior de Información para la Defensa (**CESID**), que cuenta con ocho divisiones responsables de su funcionamiento: Seguridad,

Contrainteligencia, Inteligencia Interior, Inteligencia Exterior, Apoyo Técnico, Apoyo Operativo, Economía y Tecnología, y Personal, Administración y Servicios.

Existe además, el llamado espionaje industrial: las empresas en competencia tienen un inusitado interés por los planes de sus rivales, apoyando sus técnicas de espionaje en las cada vez más eficientes tecnologías de las comunicaciones y en dispositivos de medida y cálculo. Y aquí es donde entra en juego la Criptografía.

Algoritmos básicos de criptografía

La Criptografía es la ciencia que se ocupa del cifrado seguro de mensajes y está estrechamente relacionada con las Matemáticas y, en particular, con los números primos, como veremos más adelante.

Existen dos tipos principales de criptografía de uso común hoy día. La más antigua (usada hasta los años 70) y simple se conoce como **criptografía de clave sencilla o de clave secreta** (criptografía simétrica), que resulta útil en muchos casos, aunque tiene limitaciones significativas. Los algoritmos simétricos, o de clave secreta, se caracterizan por ser altamente eficientes (en relación al tamaño de su clave) y robustos. Se les llama así porque se emplean la misma clave para cifrar y para descifrar. Se basan en el uso de claves secretas que previamente hay que intercambiar mediante canales seguros, con los riesgos que ello supone. Todas las partes deben conocerse y confiar totalmente la una en la otra. Cada una de ellas debe poseer una copia de la clave que haya sido protegida y mantenida fuera del alcance de los demás. Además, dichas claves no se deben utilizar para varios mensajes, ya que si se interceptaran algunos de ellos, se podrían encontrar métodos para descodificarlos. Por sí solo, este tipo de encriptación no es suficiente para desarrollar el pleno potencial del comercio electrónico, el cual debe vincular a un número ilimitado de compradores y vendedores de todas partes del mundo. De un lado, resulta poco práctico que una gran corporación intercambie claves con miles o incluso millones de clientes o, peor todavía, con posibles clientes con los que nunca ha tratado.

La solución a la seguridad en toda red abierta es una forma de codificación más novedosa y sofisticada, desarrollada por los matemáticos de MIT en los años setenta, y conocida como **clave pública o criptografía asimétrica**. Al contrario que los anteriores, los algoritmos asimétricos tienen claves distintas para cifrado y descifrado. Por ello, también se les llama algoritmos de clave pública. Permiten eliminar el gran inconveniente de cómo hacer llegar al remitente la clave de cifrado. En el caso de los algoritmos asimétricos se usan una clave pública (para cifrar) y una secreta (para descifrar). La primera se publica en un tipo de directorio al que el público en general tiene acceso (una especie de guía telefónica), mientras que la privada se mantiene en secreto. Las dos claves funcionan conjuntamente como un curioso dúo. De esa manera, una intercepción de la clave pública es inútil para descifrar un mensaje, puesto que para ello se requiere la clave secreta. Cualquier tipo de datos o información que una de las claves cierre, sólo podrá abrirse con la otra. De forma que, por ejemplo, si queremos enviar a un amigo un mensaje sin que ningún intruso lo lea buscamos la clave pública del amigo y la utilizamos para realizar la encriptación del texto. Luego, cuando él lo recibe, utilizamos su clave privada para revertir la encriptación del mensaje en la pantalla de su computadora y aparece el mensaje en forma de texto normal y corriente. Si un extraño interceptara este mensaje, no podría descifrarlo porque no tendría de la clave privada de ese amigo nuestro.

Como desventaja, las claves han de ser de mayor tamaño para ofrecer una seguridad comparable a la de los algoritmos simétricos. También resultan más lentos y producen mensajes cifrados de mayor tamaño.

Para que existan sistemas de clave pública es necesario encontrar funciones de dirección única, es decir, funciones fáciles de calcular (que se utilizarán para cifrar), pero cuya inversa (que se usa para descifrar) es prácticamente imposible de calcular a no ser que se conozca la clave secreta.

Además los algoritmos simétricos se pueden dividir en los de cifrado en flujo y los de cifrado en bloque. Los primeros cifran el mensaje original bit a bit, mientras que los segundos toman un número de bits (típicamente 64 bits en los algoritmos modernos) y los cifran como si se tratara de una sola unidad.

Generalmente, los algoritmos simétricos ejecutados en ordenadores son más rápidos que los asimétricos. En la práctica se suelen usar juntos, de modo que el algoritmo de clave pública se emplea para cifrar una clave generada, y éste se emplea para cifrar el mensaje usando un algoritmo simétrico. Esto es lo que se conoce como cifrado híbrido.

Las claves consisten en una serie de señales electrónicas guardadas en las unidades de disco de los PCs, o transmitidas como datos a través de las líneas telefónicas siguiendo lo especificado en los estándares de la industria. El complejo proceso matemático de encriptación del texto y su opuesto lo realiza el propio ordenador, de modo que nosotros no debemos preocuparnos de nada más.

Además, los bancos, los comercios y otros participantes en el nuevo mundo del comercio electrónico podrán ajustar las características más importantes del software para satisfacer las necesidades específicas de sus clientes. En este tipo de software se incluirá un nivel de código que se ajuste al nuevo estándar de la industria. Este nivel emplea la encriptación de clave pública para asegurar que los mensajes que contengan números de tarjetas bancarias y otro tipo de información similar se mantengan en el más estricto carácter confidencial. Este código también da lugar a otra revolución en el campo de las transacciones seguras en el ciberespacio: las firmas digitales.

Nos podemos plantear la siguiente pregunta: cuándo ese amigo al que habíamos mandado un mensaje nos responde con otro, ¿cómo sabemos que lo envió realmente él y no alguien que se hace pasar por él?

El sistema de clave pública puede resolver este problema en una forma sencilla pero eficaz. Si estamos hablando con nuestro banco en la red y queremos probar nuestra identidad sólo tenemos que guardar un mensaje con nuestra clave privada. Entonces el banco puede abrir el texto con nuestra clave pública, tomada de nuestro certificado digital, lo cual prueba que somos la única persona que ha podido haber cifrado ese mensaje en primer lugar.

Niveles de seguridad

En teoría, un buen algoritmo criptográfico debería ser invulnerable. Pero, en general, es muy difícil diseñar cifradores que no puedan ser vulnerados en la práctica usando distintos métodos. Y la experiencia nos ha mostrado que la gran mayoría de los algoritmos secretos que después han pasado al conocimiento público eran en realidad sorprendentemente vulnerables.

Un buen diseñador no debe descuidar ningún aspecto de su sistema, pues la seguridad de un sistema criptográfico está directamente relacionada con su elemento más débil. Dentro de esta seguridad podemos hablar de dos tipos:

La **de los operadores**, que se viola cuando se descubre la clave del sistema. En función de la dificultad de conseguir esa clave tendremos distintos niveles de seguridad: incondicional (cuando el cifrado no aporta ninguna información acerca de la clave), computacional (cuando no existe capacidad suficiente de cálculo para obtener la clave), probable (cuando no han sido violados a pesar de no estar basados en principios matemáticos de seguridad demostrable) y condicional (cuando la dificultad de vulneración es mucho mayor que la capacidad de cálculo del posible atacante). El sistema RSA es ofrece una seguridad computacional, mientras que la del cifrado Vernam es incondicional y la del sistema DES es probable.

La **de los protocolos**, que provoca vulneraciones del sistema debidas a posibles debilidades del mismo, sin necesidad de conocer su clave.

Criptoanálisis y ataques a sistemas criptográficos

El criptoanálisis es el arte de descodificar comunicaciones cifradas sin conocer las claves de las mismas. Existen multitud de técnicas, algunas de las cuales se citan a continuación:

Ataque a partir del cifrado: Ésta es la situación en la cual el atacante desconoce el contenido del mensaje y trabaja únicamente sobre el texto cifrado. Por ejemplo, clásicamente se realizaba un análisis estadístico de las frecuencias de los símbolos en los distintos idiomas, aunque los sistemas modernos no son vulnerables a este tipo de ataques.

Ataque a partir del texto en claro: El atacante conoce o puede conocer el texto en claro correspondiente a algunas partes del texto cifrado. El objetivo es descifrar el resto de los bloques del texto usando esta información, lo cual suele hacerse averiguando la clave usada para cifrar los datos.

Ataque a partir del texto en claro elegido: El atacante puede elegir un texto en claro y obtener su cifrado correspondiente.

Ataque a partir de la clave: El atacante intenta determinar la clave actual a partir de claves que conoce y han sido utilizadas en cifrados previos.

Suplantación de identidad: El atacante asuma la identidad de uno de los participantes en la comunicación.

Ataque mediante intromisión: El atacante se introduce en medio de la línea de comunicación, de modo que mientras ambas partes piensan que están manteniendo una comunicación segura él está interceptando todo.

Búsqueda exhaustiva: El atacante genera aleatoriamente todos los valores posibles de las claves de acceso y las transforma hasta que encontrar aquella que coincida con la previamente interceptada.

II. CIFRADO EN FLUJO

Cifrado síncrono y autosincronizante

En el cifrado síncrono la secuencia pseudoaleatoria (clave) generada para cifrar y descifrar un mensaje es independiente de éste, mientras que en los cifradores de flujo autosincronizantes la secuencia de cifrado sí es función del mensaje. Así, en el cifrado síncrono, el emisor y el receptor deben usar la misma clave (que, además, debe estar sincronizada) para poder establecer la comunicación; por este motivo utilizan señales de sincronización, que no son necesarias en el cifrado autosincronizante, ya que al tener una realimentación, en caso de pérdida de sincronismo, éste puede recuperarse transcurrido un tiempo.

Cifrado Vernam

El cifrado Vernam fue desarrollado en los Estados Unidos y recibe el nombre del que fuera su creador en 1917.Originalmente se usó en circuitos teletipo, siendo su diseño para el cifrado en tiempo real y el descifrado de señales teletipo.

El cifrado Vernam hace uso de la función OR−exclusiva (XOR) para cifrar un mensaje dado con una clave determinada. Es un proceso simétrico, pues usa la misma clave para el proceso de cifrado y el de descifrado.

Las versiones más recientes de cifradores Vernam usan claves generadas electrónicamente, que son infinitamente largas y de naturaleza aleatoria, en principio, aunque por supuesto cada usuario del sistema debe ser capaz de generar la misma secuencia usada como clave. Sin embargo, no existen secuencias completamente aleatorias, sino secuencias periódicas con periodo muy elevado, conocidas como secuencias pseudoaleatorias o, en inglés, **Pseudo Random Binary Sequence (PRBS)**. Existen diferentes métodos de generar estas secuencias, pero el más habitual es el que usa registros de desplazamiento (shift registers).

Es un sistema incondicionalmente seguro siempre que la clave sea realmente aleatoria, lo cual es imposible en la práctica. Actualmente un área de investigación importante se centra en encontrar funciones generadoras de secuencias pseudoaleatorias que sean criptográficamente seguras.

Sincronización y ataques activos

Ya hemos dicho que existen dos tipos básicos de cifradores en flujo: los síncronos y los autosincronizantes. En los últimos, la secuencia pseudoaleatoria utilizada para cifrar y descifrar es función del mensaje a través del cifrado, mientras que en los síncronos es independiente de éste.

Los métodos síncronos son inmunes a los ataques activos de inserción de mensajes extraños, puesto que al destruir la sincronización que estos sistemas requieren (entre el emisor y el receptor) son fácilmente detectables. Sin embargo, los métodos autosincronizantes sí están expuestos a ataques activos de repetición de mensajes, pues no siempre se pueden diferenciar de posibles errores de transmisión en el canal. Un procedimiento para reducir la probabilidad de un eventual ataque consiste en realizar un cifrado doble, con lo que se requiere otra clave de cifrado. La idea en la que se basa este procedimiento, que sirve también para controlar la propagación de un posible error introducido por el canal, es la que utilizan los códigos convolucionales de coerción de errores, en los que por cada bit de información se transmiten varios.

El cifrador lineal perfecto

Este cifrador fue introducido por Massey y Rueppel y es semejante al estándar utilizado para el cifrado de la televisión en la European Broadcasting Universe.

III. CIFRADO EN BLOQUE

DES

Para la transmisión de datos confidenciales entre ordenadores se desarrolló a principios de la década de 1970 LUCIFER, un sistema de cifrado basado tanto en la sustitución como en la transposición, y en 1976 se elaboró la norma de cifrado de datos o DES (Data Encryption Standard) sobre la base del primero. Fue, y todavía es, ampliamente usado, sobre todo, en el campo financiero. El DES transforma segmentos de mensaje de 64 bits en otros equivalentes de texto cifrado, empleando una clave de 56 bits. Cada usuario elige una clave al azar, que sólo comunica a aquellas personas autorizadas a conocer los datos protegidos. El mensaje real se codifica y descodifica automáticamente mediante equipos electrónicos incorporados a las computadoras emisoras y receptoras. Como existen más de 70.000 billones de combinaciones de 56 bits, la probabilidad de descubrir la clave aleatoria parece mínima. Así, es un método de cifrado altamente resistente frente a ataques criptoanalíticos diferenciales. Sin embargo, algunos expertos han criticado la técnica DES por su vulnerabilidad frente a los potentes métodos de descodificación posibles para los grandes ordenadores y no lo han considerado apropiado para las aplicaciones recientemente realizadas. Y es que, por desgracia, el tamaño de su clave (56 bits) lo hace vulnerable a ataques de fuerza bruta. Un reciente ataque contra un mensaje con cifrado DES requirió el uso de cientos de ordenadores durante 140 días. Pero hay diseños de máquinas que, con un costo de un millón de dólares, podrían descifrar mensajes DES en cuestión de minutos. Quizá por eso el gobierno de EEUU lo utiliza solamente para cifrar datos no clasificados. En la actualidad ofrece protección contra el pirata informático habitual, pero no contra un esfuerzo masivo por parte de un usuario con grandes recursos.

Una variantes de DES, Triple−DES (3DES), basado en el uso de DES tres veces (normalmente en una secuencia de cifrado−descifrado−cifrado con tres claves diferentes y no relacionadas entre sí). El sistema 3DES es bastante más seguro que el Des (simple), aunque presenta el inconveniente de ser considerablemente más lento que los modernos sistemas de cifrado en bloque.

A pesar de que DES parece ser de escaso interés para aplicaciones de hoy en día existen numerosas razones para considerarlo todavía importante. Fue el primer sistema de cifrado en bloque que se extendió al sector público, por lo que ha desempeñado un importante papel en hacer asequible la criptografía segura al gran público.

Además, su diseño era excepcionalmente bueno para un sistema de cifrado pensado para tener un uso de tan sólo unos años. Demostró ser un sistema fuerte y soportó una década de ataques, hasta que llegaron los procedimientos más potentes de criptoanálisis diferencial y lineal (ataques a partir del texto en claro escogido). En la etapa de introducción del DES su filosofía de diseño se mantuvo en secreto, pero actualmente ya se conoce gran cantidad de información sobre su diseño, y uno de sus diseñadores, Don Coppersmith, ha comentado que ya se descubrieron ideas similares a las del criptoanálisis diferencial cuando estaban diseñando DES allá en 1974; así pues, sólo era cuestión de tiempo el que estas ideas fundamental fueran `redescubiertas'.

Aún actualmente, cuando DES ya no se considera una solución práctica, es usado a menudo para describir nuevas técnicas de criptoanálisis. Es importante destacar que incluso hoy, no existe ninguna técnica de criptoanálisis que pueda vulnerar completamente DES de un modo estructural; de hecho, la única debilidad de DES es el pequeño tamaño de la clave (y quizá el pequeño tamaño del bloque)

Claves: Para todos los cifradores en bloque existen claves que se deben evitar debido a la escasa complejidad del cifrado al que dan lugar. Estas claves son aquellas para las que la misma sub−clave es generada en más de una iteración e incluyen: **Claves débiles**: La misma sub−clave es generada en cada iteración. DES tiene 4 claves débiles.

Claves semi−débiles: Sólo dos sub−claves se generan en iteraciones alternadas. DES tiene 12 claves de estas (en 6 pares).

Modos de cifrado de DES: DES cifra bloques de datos de 64 bits usando una clave de 56 bits. Normalmente tenemos una cantidad de información arbitraria para cifrar y necesitamos una forma de especificar cómo realizamos ese cifrado. La manera en que usamos un cifrador en bloque se denomina **modo de uso** y para DES se han definido cuatro por el estándar ANSI.

En bloque:

Electronic Codebook Book (ECB): El mensaje se divide en bloques independientes de 64 bits y el cifrado se efectúa bloque a bloque.

C(i) = DES(K1) (P(i))

Cipher Block Chaining (CBC):De nuevo el mensaje se divide en bloques de 64 bits, pero estos se unen en el cifrado mediante un vector de inicialización IV.

C(i) = DES(K1) (P(i)(+)C(i−1)), con C(−1)=IV

En flujo:

Cipher FeedBack (CFB): Los bits del mensaje son añadidos a la salida del DES, y el resultado se lleva al siguiente bloque. Requiere también de un vector de inicialización.

C(i) = P(i)(+) DES(K1) (C_(i−1)), con C_(−1)=IV

Output FeedBack (OFB): Es igual que el anterior pero sin realimentación.

C(i) = P(i)(+) O(i) O(i) = DES(K1)(O(i−1)), con O(−1)=IV

Cada modo presenta sus ventajas y sus desventajas.

RSA

Se han propuesto diferentes alternativas, como el criptosistema de clave pública (PKC), que utiliza una clave pública y otra secreta. El PKC, basado en un enfoque matemático, elimina el problema de la distribución de claves pero no resulta tan eficaz, desde el punto de vista informático, como el DES. En 1978 apareció el denominado algoritmo RSA, ideado por Rivest, Shamir y Adleman, que utiliza números primos y la aritmética modular, que trabaja con subconjuntos finitos de números enteros: los conjuntos de todos los números enteros que tienen el mismo resto al dividirlos entre n. Por ejemplo, la aritmética módulo 7 viene dada por el conjunto {0,1,2,3,4,5,6}, y para representar cualquier número entero en este conjunto, bastará con tomar su resto después de dividirlo por 7. Así, por ejemplo, el número 64 corresponderá al 1 módulo 7, ya que si dividimos 64 entre 7, nos queda como resto 1. En otras palabras, podemos poner 64=k*7+1, donde k será un número entero cuyo valor no nos va a importar. Análogamente, 17=k*7+3 (luego 17 corresponde a 3 módulo 7), 57=k*7+1 (57, al igual que 64, corresponde a 1 módulo 7), etc.

Pues bien, dentro de estos conjuntos se pueden definir fácilmente las operaciones aritméticas suma, resta y multiplicación: bastará con sumar, restar o multiplicar y luego tomar el módulo correspondiente. Siguiendo con nuestro ejemplo, el producto de 3 por 5 módulo 7 es precisamente 1 (ya que 3*5 = 15, y al dividir por 7 nos queda como resto 1). Al igual que con los números reales, si el producto de dos números vale 1, diremos que uno es la inversa de otro, por lo que 3 es la inversa de 5 módulo 7. Una vez que tenemos la noción de inversa de un número en aritmética modular, podemos definir la operación división a/b como el producto de a por la inversa de *b*. Por ejemplo, 4/3 será igual a 4*5 = 20 = 6 módulo 7.

Existe una propiedad muy interesante, y es que un número *a* tiene inversa módulo *n* siempre y cuando no exista ningún número menor que *a* y *n* que los divida de forma exacta a los dos, es decir, *a* y *n* sean primos relativos. Fijándose un poco, en el ejemplo anterior, el módulo empleado es un número primo, por lo que podemos concluir que todos los números (excepto el cero) tienen inversa módulo 7. En general, se define la función (n) (Totient de Euler) como la cantidad de números que tienen inversa módulo n. En particular, si *n* puede descomponerse en dos números primos *p* y *q*, (n)= (p−1)*(q−1).

La última propiedad que nos interesa es que si multiplicamos un número a (distinto de cero) por sí mismo (n) veces, obtenemos 1 módulo *n*, y en esto es precisamente en lo que se apoya RSA.

Para poder emplear el algoritmo RSA tenemos que escoger un número entero n que sea producto de dos números primos *p* y *q* muy grandes. Escogemos luego un número *e* aleatoriamente, que sea primo relativo con (n), y calculamos su inversa módulo (n), que denominaremos *d*. El par (n,e) será nuestra clave pública, y *d* será la clave privada. Para cifrar un número *m* calcularemos me módulo *n* (*m* elevado a *e* módulo *n*, o bien m multiplicado por sí mismo *e* veces).

La parte más complicada viene al intentar descifrar un número: hay que elevarlo a *d*. Como d*e = 1 modulo (n), elevar *m* a *e* y luego a *d* será equivalente a multiplicar *m* por sí mismo d*e(o sea, k* (n)+1) veces. Esto es equivalente a calcular *m* elevado a (n), multiplicarlo por sí mismo *k* veces, y luego multiplicar por *m* una vez más. Como *m* elevado a (n) es igual a 1, será como multiplicar 1 por sí mismo *k* veces y luego multiplicar por *m*, con lo que nos queda de nuevo *m*.

Para ayudar a comprenderlo, vamos a poner un ejemplo: supongamos que n=5*11=55, entonces (n)=4*10=40. Sea e=7, cuya inversa módulo 40 es 23, ya que 7*23=161=1 módulo 40. Nuestra clave pública será (55,7), y nuestra clave privada será 23. Para cifrar ahora el número 2 bastará con calcular 27=128=18 módulo 55. Si luego elevamos 18 a 23 módulo 55 nos queda de nuevo 2.

El `truco' de RSA está precisamente en que si conocemos los factores de *n* podemos calcular fácilmente el valor de (n), por lo que un atacante tendrá que factorizar *n* si quiere calcular nuestra clave privada *d*, lo cual resulta prácticamente imposible si *n* es lo suficientemente grande. En la práctica, encontrar esta factorización para números grandes requiere mucho tiempo de trabajo de un potente ordenador. La factorización de un número en producto de primos esconde en sí misma dos problemas matemáticos: reconocer si un número es primo o no y encontrar la factorización. Si queremos factorizar un número de 300 dígitos que es producto de dos primos de gran tamaño, con los métodos actuales necesitaríamos alrededor de un siglo. Por ello este tipo de sistemas son útiles y poco menos que invulnerables ya que, dentro de un siglo, ¿qué puede importarnos ya que alguien descubra el contenido de un mensaje nuestro?

Un detalle, no obstante, debe tenerse en cuenta. La dificultad intrínseca de factorizar grandes números es un tema abierto. Actualmente el método de factorización más rápido conocido es la Criba Numérica Especial de Campo (Special Number Field Sieve), pero no está demostrado que no haya otro mejor. Si se descubre un método de tiempo polinómico (esto es, cuyo tiempo de ejecución dependa del número N de cifras como Na), cualquier producto de números primos podrá factorizarse con relativa facilidad. No obstante, desde1978 se han estudiado muchas variantes de este tipo de claves y parece ser que RSA continúa siendo el sistema más eficaz y seguro.

Aplicación práctica. PÓKER CON RSA:

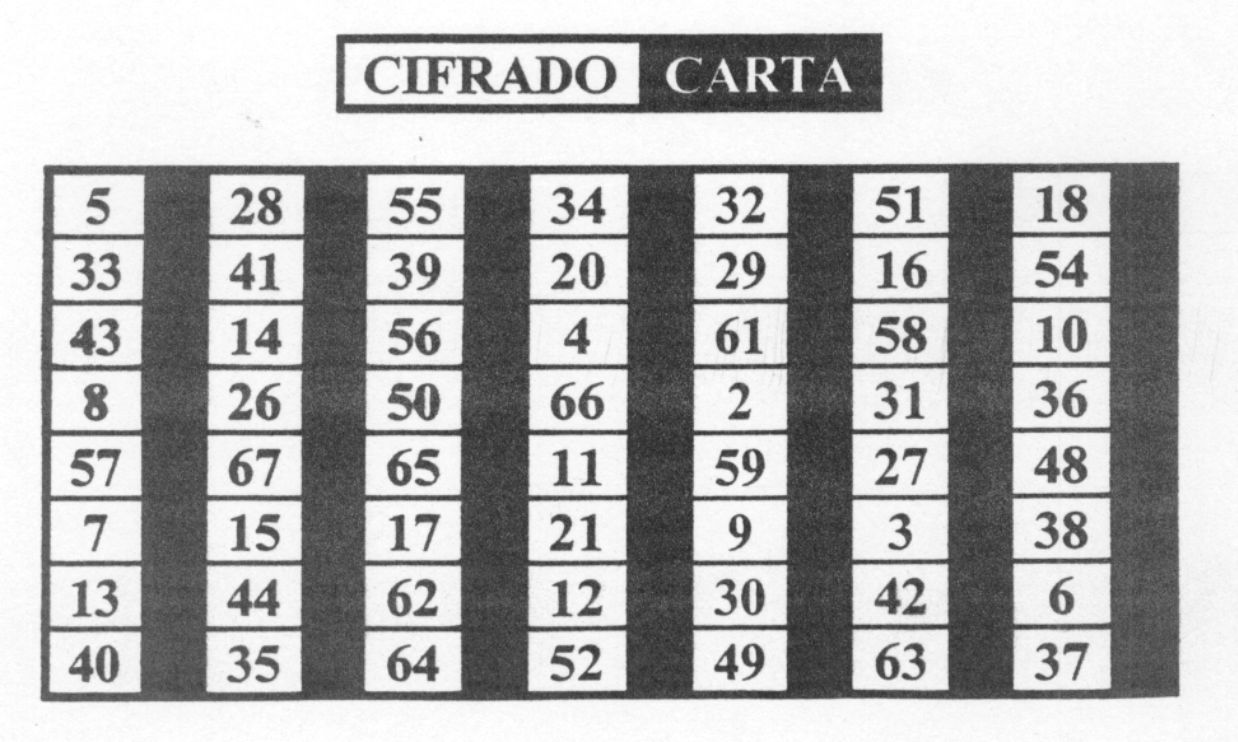
Se nos propone jugar a este famoso juego de cartas contra un adversario sin utilizar baraja y empleando, en su lugar, el algoritmo RSA. Se trata de codificar el mazo de cartas según dicho algoritmo, de modo que a cada carta le corresponderá un código distinto. La codificación se realiza mediante dos claves secretas, cada una de las cuales sólo es conocida por el jugador que la ha elegido, y una clave pública común N conocida por ambos.

Para el caso de N = 69 (producto de los números primos 3 y 23), el mazo de las 56 cartas queda:

	A	2	3	4	5	6	7	8	9	10	J	Q	K	
♥	2	3	4	5	6	7	8	9	10	11	12	13	14	15
♣	16	17	18	19	20	21	25	26	27	28	29	30	31	32
♦	33	34	35	36	37	38	39	40	41	42	43	44	48	49
♠	50	51	52	53	54	55	56	57	58	59	60	61	62	63

Para jugar hay que elegir de entre el mazo cifrado una carta para cada jugador y, una vez intercambiados los cifrados, obtener las respectivas manos descifrando cada uno con su clave. A continuación se hace la apuesta y se intercambian las claves de los dos jugadores para comprobar quién ha sido el ganador del juego.

Veamos el mazo cifrado y barajado con clave:



Rijndael

Actualmente el algoritmo DES está obsoleto y, para sustituirlo, el NIST (National Institute of Standards and Technology) propuso una competición para desarrollar el estándar AES, hasta cuya resolución ha adoptado el sistema Triple−DES como una solución temporal.

Los cinco algoritmos finalistas para AES, elegidos entre un total de quince, fueron MARS, RC6, Rijndael, Serpent y Twofish. Así, Rijndael es un cifrador en bloque diseñado por John Daemen y Vincent Rijmen como algoritmo candidato al AES (Advanced Encryption Standard). Su diseño estuvo fuertemente influenciado por el de un cifrador (block cipher Square), que también fue creado por John Daemen y Vincent Rijmen y se centraba en el estudio de la resistencia al criptoanálisis diferencial y lineal. El nombre del algoritmo es una combinación de los nombres de sus dos creadores

El cifrador tiene longitudes de bloque y de clave variables y puede ser implementado de forma muy eficiente en una amplia gama de procesadores y mediante hardware. Como todos los candidatos del AES es muy seguro y hasta la fecha no se le han encontrado puntos débiles.

La longitud de la clave de Rijndael, si bien es variable, debe ser de 128, 192 o 256 bits, según los requisitos establecidos para el AES. Asimismo, la longitud del bloque puede variar entre 128, 192 o 256 bits. Todas las posibles combinaciones (nueve en total) entre longitudes de clave y bloque son válidas, aunque la longitud oficial de bloque para AES es de 128 bits. Las longitudes de la clave y el bloque pueden ser fácilmente ampliadas a múltiplos de 32 bits. El número de iteraciones del algoritmo principal puede variar de 10 a 14 y depende del tamaño del bloque y de la longitud de la clave. Una de las críticas más habituales de Rijndael es el escaso número de iteraciones, pero esto no supone un problema, pues el coste operacional puede aumentarse sin más que incrementar el tamaño del bloque y la longitud de la clave.

La implementación Stealth de Rijndael usa una clave de 256 bits y un bloque de 128 bits de tamaño. Usando la mayor longitud posible de clave conseguimos la máxima seguridad para el usuario. La filosofía de este diseño concedería pues mayor importancia a la seguridad que a la velocidad. Si el usuario proporciona una clave de menor longitud Stealth la transforma de una forma especial, casi

aleatoriamente, para hacerla de 256 bits. Y aunque acepta tamaños de bloque mayores que 128 bits, no existe ninguna razón para usarlos siendo que este número de bits ha sido elegido como tamaño estándar.

ElGamal

Propuesto por T. ElGamal, este sistema de clave pública está basado en un procedimiento de cifrado que usa dos valores públicos: un número primo *p* de aproximadamente 200 dígitos y un entero *g* tal que sus potencias generan todos los elementos del grupo. Así, la clave secreta del firmante es un entero aleatorio *x* elegido por el mismo tal que $1 < x < p-1$, y la clave pública asociada *y* se obtiene como sigue: $y = g^x \pmod p$

El cifrado de un mensaje en claro M tal que $1 < M < p$, se lleva a cabo eligiendo un valor entero aleatorio *k* con $1 < k < p-1$ y *k* relativamente primo con *p*. Si los valores de *k* elegidos para la computación de un mismo mensaje en claro son distintos los cifrados resultantes también lo serán.

Un inconveniente importante de este sistema de cifrado es la capacidad de almacenamiento necesaria, al ser la longitud del mensaje cifrado el doble que la del mensaje en claro.

La ruptura de este sistema pasa por la resolución de un problema de logaritmo discreto, lo cual resulta complicado cuando se trabaja con números suficientemente grandes. Sin embargo, en ocasiones el cálculo del logaritmo discreto resulta viable incluso para valores de *p* de gran tamaño, lo cual se debe a la existencia de números primos con características debilitantes para el sistema, esto es, números a partir de los que resulta posible obtener la clave secreta *x* a partir de la pública *y*, que deberemos evitar.

Es el predecesor del DSS (Digital Signature Standard) y su uso está bastante extendido a pesar de que no se ha creado ningún estándar conocido para ello.

Criptografía y números primos

Una de las mejores definiciones para la palabra Criptografía, viene a decir que es el conjunto de técnicas que permiten transformar un trozo de información, de tal forma que quienes deseen recuperarlo sin estar en posesión de otra pieza de información (clave), se enfrentarán a un problema intratable. Conviene recordar que "intratable" no significa lo mismo que "irresoluble"; puesto que el número de posibles claves ha de ser finito, la fuerza bruta siempre nos permitirá recuperar el mensaje original, al margen de que seamos luego incapaces de reconocerlo. En cualquier caso, desde un punto de vista práctico la casualidad debe ser descartada, ya que las probabilidades de que se descifre por la fuerza bruta un mensaje en tiempo razonable es ínfima.

Pero, ¿qué es exactamente un problema intratable? Sencillamente aquel que para ser resuelto de forma satisfactoria requiere una cantidad de recursos computacionales (tiempo y memoria) más allá de las posibilidades del atacante. Sin embargo, existe un último e inquietante detalle para tener en cuenta: para ser operativa esta definición necesita que el contrincante carezca de "atajos" para resolver nuestro problema en teoría intratable. Por desgracia, prácticamente para ninguno de los problemas que plantean los algoritmos criptográficos actuales se ha demostrado que no pueda existir algún atajo.

Multiplicación y factorización: Supongamos dos números enteros cualesquiera *a* y *b*. Recordemos que el número de operaciones elementales que requiere un algoritmo sencillo para obtener su producto no depende directamente del valor de *a* y *b*, sino del número de dígitos que éstos posean (o sea, de su logaritmo). Esta propiedad permite que podamos multiplicar números muy muy grandes en un número de pasos razonablemente pequeño. Por ejemplo, dos números de siete cifras (del orden del millón) requieren menos de sesenta operaciones elementales para ser multiplicados.

Pero analicemos ahora la operación inversa: supongamos que tenemos un número *n* y queremos conocer sus dos factores *a* y *b*. En la actualidad existen algoritmos relativamente eficientes para llevar a cabo esta operación, pero siguen requiriendo un número de operaciones que se vuelve astronómico cuando *a* y *b* son lo suficientemente grandes. Normalmente el caso más desfavorable se da cuando *a* y *b* son números primos, puesto que entonces son los únicos factores de *n*.

Esta dificultad es aprovechada por muchos algoritmos de clave privada, como es RSA, que en principio basa su fuerza en el problema de la factorización. Sin embargo, aunque es conocido que si dicho problema fuera resuelto el algoritmo caería, nadie ha demostrado que no exista un método para descifrar un mensaje RSA sin factorizar el módulo.

En fin, parece bastante claro que la investigación dentro de estos ámbitos matemáticos es fundamental, ya que permitirá constatar (o refutar en su caso) la capacidad que tienen muchos algoritmos de proteger nuestros datos.

Test de primalidad: Una vez conocida la importancia de los números primos, hay que buscar un método para identificarlos. Y aquí es donde surge la primera paradoja aparente: un número es primo si no se puede factorizar, pero intentar factorizarlo es una tarea impracticable si el número es lo suficientemente grande. Por suerte, existen técnicas probabilísticas para tener un grado de certeza aceptable acerca de la primalidad de un número concreto.

Las técnicas arriba mencionadas se basan en escoger un número aleatorio x y efectuar una serie de operaciones entre x y n. Si se cumplen ciertas propiedades, sabremos con un grado de certeza determinado que n puede ser primo. Repitiendo este test muchas veces con diferentes valores de x, podemos aumentar nuestra confianza en la primalidad de n tanto como queramos.

Conclusiones: Los números primos son una de las entidades matemáticas más apasionantes y útiles que existen. De hecho, Carl Sagan, en su novela "Contact", contaba cómo los extraterrestres escogían una secuencia de primos para identificarse frente a la Raza Humana. Y ese interés y utilidad con toda seguridad va a continuar durante bastantes años.

El estudio dedicado a los números primos centra gran parte de su esfuerzo en el descubrimiento de números lo más grandes posibles (primos, se entiende). En junio de 1999, Nayan Hajratwala encontró el todavía actual record, 26972593. En enero de 1998, Roland Clarkson encontró el que fuera el primo con el anterior record, 23021377. En agosto de 1997, Gordon Spence descubrió el primo 22976221. Y en noviembre de 1996, Joel Armengaud encontró el 21398269. ¿Cuál será el próximo?

Criptografia cuántica: Como vemos, los números primos son de suma importancia en la criptografía y, en la actualidad, tan sólo la **computación cuántica** representa una amenaza para ellos. La mecánica cuántica permite hacer cosas que son imposibles con la mecánica clásica y si alguna vez llegamos a tener computadores cuánticos, que son aquellos que hacen uso de las leyes cuánticas para funcionar, el problema de la factorización habrá sido resuelto, y habrá que buscar algún otro modelo matemático para construir nuestros algoritmos asimétricos. Por el momento sólo se está ensayando con la criptografía cuántica, que nos permitirá enviar mensajes que no podrán ser descifrados y detectar con total seguridad si éstos han sido interceptados. En cuanto a los ordenadores cuánticos, se han logrado desarrollar modelos simples. De todas formas, aunque algunas de las ideas desarrolladas entorno al diseño y funcionamiento de los ordenadores cuánticos (como la comunicación por un canal cuántico a través de una fibra óptica) ya encuentran aplicaciones prácticas en el presente, parece bastante seguro que pasarán algunos años antes de tener computadores de este tipo en nuestros hogares, pues el estudio de estos sistemas requiere mucho esfuerzo y presupuesto.

IV. Criptografía con curvas elípticas

Son los criptosistemas más recientes dentro del campo de los sistemas de clave pública y representan sólo otra forma de implementar métodos de logaritmo discreto. Las curvas elípticas en criptografía son básicamente un conjunto de puntos que cumplen la y2 = x3 + ax + b siempre que sean considerados en un cuerpo finito de característica *p* (con p > *3*). Para características del cuerpo p = 2 y p = *3* se requiere una ecuación ligeramente diferente.

Los puntos de una curva elíptica forman una estructura llamada **grupo** (concretamente son un grupo abeliano). Esto significa que podemos realizar las operaciones aritméticas de suma y resta con ellos del mismo modo que lo hacemos con los enteros.

Además de presentar algunas ventajas teóricas son muy prácticas. No existe ningún algoritmo rápido de cálculo de un logaritmo, lo cual supone que el tamaño de la clave, así como las firmas digitales y mensajes cifrados obtenidos son pequeños. De hecho, los criptosistemas basados en curvas elípticas proporcionan la misma seguridad que los basados en factorización o logaritmo discreto reduciendo considerablemente el número de dígitos.

Las curvas elípticas pueden ser implementadas con gran eficiencia en hardware y software, y son capaces de competir en velocidad con sistemas como RSA y DSS. En general se cree que son bastante seguros, pero no ha sido demostrado. Sí se sabe que existe un tipo de curvas que recientemente se ha revelado extremadamente vulnerable, por lo que éstas no deben usarse en criptografía. Y de entre los demás tipos de curvas se deberá examinar cuidadosamente antes de elegir uno concreto para comprobar su idoneidad como base para un código de cifrado de datos.

La seguridad de los sistemas de criptografía con curvas elípticas es buena a priori y, pese al esfuerzo realizado para intentar atacarlos, hasta el momento no ha habido ninguna sorpresa.

El algoritmo XTR introducido recientemente Lenstra y Verheul podría convertirse en una competencia importante para las curvas elípticas. Sin embargo, las curvas elípticas parecen funcionar ligeramente mejor en la práctica y presentan una ventaja definitiva en cuanto al tamaño de la clave.

Hay varios intentos de estandarización para los criptosistemas de curvas elípticas (como por ejemplo ECDSA por ANSI). Actualmente las curvas elípticas son sobradamente conocidas, pero no su uso en la práctica no está muy extendido.

Comparación de las curvas elípticas con el sistemas RSA

A continuación se comparan los métodos criptográficos de RSA y curvas elípticas a nivel de seguridad y eficiencia:

Nº dígitos	Sistema criptográfico	Nº operaciones (cifrado/descifrado)	Nº operaciones (ruptura clave)	Tiempo (ruptura clave con ordena. de 10^9 FLOPS)
30	*RSA* Curvas elípticas	9.0 E 02 2.7 E 04	2.7 E 07 1.0 E 15	0.3 segundos 11 días
35	*RSA* Curvas elípticas	1.2 E 03 4.2 E 04	1.4 E 08 3.0 E 17	1.2 segundos 9.1 días
40	*RSA* Curvas elípticas	1.6 E 03 6.4 E 04	7.3 E 08 1.0 E 20	6.0 segundos 3.0 E 03 años
50	*RSA* Curvas elípticas	2.5 E 03 1.2 E 05	1.4 E 10 1.0 E 25	2.0 minutos 3.0 E 06 años
85	*RSA* Curvas elípticas	7.2 E 03 6.1 E 05	9.0 E 13 3.0 E 42	1 día ---
100	*RSA* Curvas elípticas	1.0 E 04 1.0 E 05	2.3 E 15 1.0 E 50	28 días ---
200	*RSA* Curvas elípticas	4.0 E 04 8.0 E 05	1.2 E 23 1.0 E 100	3.8 E 6 años ---

Podemos observar que las diferencias son significativas, siempre muy a favor de las curvas elípticas. Esto es así porque el logaritmo elíptico puede ser una función mucho más segura que el logaritmo discreto o la factorización cuando se trabaja con números enteros de una determinada dimensión.

V. Firmas digitales

Una firma digital es un bloque de caracteres que acompaña a un documento o fichero acreditando quién es su autor (**autenticación**) y que no ha existido ninguna manipulación posterior de los datos (**integridad**).

Una buena firma digital debe ser: Única.

Infalsificable, o lo que es lo mismo, computacionalmente segura.

Verificable por el receptor de la misma.

Viable, es decir, fácil de generar.

Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación). De esta forma, el autor queda vinculado al documento que firma.

Una firma digital ofrece una forma de asociar un mensaje con la entidad que lo envía, y es la forma en la que podemos "firmar" (de forma similar a la que firmamos tradicionalmente sobre un papel) al efectuar una compra en el ciberespacio. De esta manera se evitan fraudes y falsificaciones, ya que, por ejemplo, sólo nosotros podremos utilizar nuestra cuenta de tarjeta Visa en la Red de Internet.

Cualquier persona puede verificar la validez de una firma si dispone de la clave pública del autor.

Para realizar una firma digital el software del firmante aplica de forma transparente al usuario un algoritmo hash (los más usados son MD5 o SHA−1) sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje (un mínimo cambio en el mensaje produce un extracto completamente diferente). Este extracto, cuya longitud oscila entre 128 y 160 bits (en función del algoritmo

utilizado), se somete a continuación a cifrado mediante la clave secreta del autor, previa petición de contraseña.

El algoritmo utilizado para cifrar el extracto puede ser el mismo RSA o una clave específica para firmar tipo DSS. El extracto cifrado constituye la firma y se añade al final del mensaje o en un fichero adherido a él.

Para comprobar la validez de una firma digital se necesita disponer de la clave pública del firmante para poder verificar su firma.

El software del receptor descifra el extracto cifrado que constituye la firma digital (de forma transparente al usuario), utilizando para ello la clave pública del remitente y obtiene como resultado un bloque de caracteres. A continuación, calcula el extracto hash que corresponde al texto del mensaje. Si el resultado coincide exactamente con el bloque de caracteres obtenido en la operación anterior, la firma se considera válida. Si existe la menor diferencia, la firma se considera no válida.

Para que este esquema tenga éxito, es preciso una función hash que elija fragmentos adecuados del texto a cifrar. Evidentemente, no sirve cifrar las cuatro primeras palabras del mensaje, ya que podría usarse esa firma en otro mensaje cuyas tres primeras palabras sean iguales. Por otro lado, puede cifrarse todo el mensaje, pero este procedimiento podría doblar fácilmente el tamaño del mismo, lo cual no resulta conveniente ni aconsejable: el ataque principal contra el sistema de cifrado RSA consiste en firmar un mensaje cuidadosamente escrito por el atacante; eso puede permitirle averiguar la clave secreta del firmante.

Lo que se ha de firmar es un "resumen" o "revoltillo" (hash) representativo del mensaje particular, que solamente pueda generarse mediante la clave secreta del firmante y mediante el mensaje, y que no sea de longitud excesiva. Así que no sirven sistemas que puedan generar firmas iguales para mensajes distintos. Tampoco puede admitirse un hash que filtre información sobre el mensaje; si se puede reconstruir el mensaje a partir del hash se podría obtener un segundo mensaje con el mismo hash.

El sistema tiene un punto débil, que es consustancial a los criptosistemas de clave pública.

Efectivamente, la firma digital nos permite comprobar la relación entre un mensaje y la clave utilizada pero no podemos estar seguros de que esa clave corresponde realmente a la persona o entidad que dice poseerla. Este problema requiere la intervención de una tercera parte fiable, en la que confíen las dos partes implicadas. Es lo que se llama **Autoridad de Certificación**. Y es esa tercera parte fiable la que acredita, actuando como una especie de notario que extiende un certificado de claves (firmado con su propia clave), la ligazón entre una determinada clave y su propietario real.

Algunos programas, como PGP, no utilizan autoridades de certificación externas, sino que delegan en el propio usuario la responsabilidad de certificar claves conforma a su criterio, estableciendo lo que se denomina una red de confianza (Web of Trust) totalmente descentralizada, pero con el apoyo de una red de servidores de claves.

Los servidores de certificados son aplicaciones destinadas a crear, firmar y administrar certificados de claves, y que permiten a una empresa u organización constituirse en autoridad de certificación para subvenir sus propias necesidades.

La relevancia del firmado digital, pese a que no se suele pensar mucho en él cuando se estudia la seguridad global de un protocolo criptográfico, es grande: si bien pocas veces nos vemos en la necesidad de cifrar nuestros datos, sí es importante autentificarlos.

Al hacer un pedido a una cibertienda por correo electrónico, importa relativamente poco que los datos vayan cifrados (a no ser que incluyamos información sensible como números de cuenta corriente); pero es

imprescindible tener un medio de certificar que ese mensaje ha sido enviado. Si compro la tostadora de 5.000 ptas. y el vendedor se empeña en que mi mensaje pedía el televisor de 50.000 pts, ¿cómo puedo demostrar lo contrario? Y al revés, si yo soy el vendedor, ¿cómo sé que el comprador no se va a echar atrás alegando que jamás envió ese mensaje? Las cabeceras de los mensajes son demasiado fáciles de falsificar o alterar, por lo que no constituyen ninguna prueba.

En algunos estados norteamericanos, la firma digital se acepta como elemento de prueba en iguales términos que la firma autografiada en papel. En España se acepta un fax como documento vinculante, a pesar de que resulta un juego de niños digitalizar una firma (o fotocopiarla) y adosarla a otro documento, de manera que ¿por qué no aceptar firmas digitales sin están convenientemente construidas? Por desgracia, no podremos efectuar tal cosa hasta que dispongamos de un procedimiento seguro de creación de firmas digitales. Y sin un algoritmo hash adecuado la situación resulta algo complicada.

Estos son los principales algoritmos hash que existen:

MD2 (Message Digest 2). Se diseñó para ordenadores con procesador de 8 bits, y hoy apenas se utiliza. Se conocen ataques a versiones parciales de MD2.

MD4 (Message Digest 4). Fue desarrollado por Ron Rivest, de RSA Data Security. Su diseño es la base de otros hash, aunque se le considera inseguro. Un ataque desarrollado por Hans Dobbertin permite generar colisiones (mensajes aleatorios con los mismos valores de hash) en cuestión de minutos para cualquier PC. Por ese motivo, está en desuso.

Función SHA−1

SHA (Secure Hash Algorithm) fue desarrollado como parte del estándar hash seguro (Secure Hash Standard, SHS) y el estándar de cifrado digital (Digital Signature Standard, DSS) por la Agencia de Seguridad Nacional norteamericana (NSA). Aparentemente se trata de un algoritmo seguro y sin fisuras, al menos por ahora. La primera versión, conocida como SHA, fue mejorada como protección ante un tipo de ataque que nunca fue revelado. El documento FIPS (Federal Information Processing Standard) que oficialmente lo describe afirma que los principios subyacentes al SHA−1 son similares a los del MD4 de Rivest. Su implementación puede estar cubierta por patentes en Estados Unidos y fuera de ellos. A falta de ataques ulteriores, se le puede considerar seguro. Es el algoritmo de firmado utilizado por el programa PGP en sus nuevas claves DH/DSS (que significa: cifrado mediante clave Diffie−Hellman y firmado mediante función hash/ Digital Signature Standard).

Para la generación de otro tipo de firmas digitales suelen usarse algoritmos basados en criptografía de clave pública, sobre todo RSA y DSS.

VI. PROTOCOLOS CRIPTOGRÁFICOS

A estas alturas deberíamos saber que uno de los objetivos principales de la criptografía es asegurar la seguridad de las comunicaciones. Cualquier sistema de cifrado de datos tiene puntos débiles, y los modernos (RSA, Diffie−Hellman, PGP, criptografía de curva elíptica...) no se escapan a esta regla. En ocasiones un sistema es mal implementado en la práctica, de modo que las posibles ventajas quedan anuladas por el mal hacer de un programador descuidado. Por ejemplo, casi todos los códigos actuales requieren cadenas de dígitos elegidos aleatoriamente, para lo cual se utilizan generadores de números aleatorios o pseudoaleatorios. Pero si dichos números no son realmente aleatorios, las claves así generadas son vulnerables. Un fallo de implementación de dicho tipo hizo que las comunicaciones "seguras" utilizando el navegador Netscape Navigator 1.1 pudiesen ser leídas en segundos: el sofisticado protocolo SSL resultaba en la práctica inútil porque utilizaba números no tan aleatorios. Cualquier programa de cifrado de datos es susceptible a mil y una fallas de seguridad.

Incluso un protocolo criptográfico bien implementado puede contener imperfecciones que permitan un ataque más eficiente que el de fuerza bruta. Sistemas tan popularizados como el Estándar de Cifrado de Datos (DES) están basados en los viejos métodos de trasposición, sustitución y similares. Resulta muy difícil diseñar un algoritmo de cifrado de datos que resulte realmente robusto, esto es, que no pueda violentarse más que mediante un ataque de "fuerza bruta". Sutiles detalles pueden hacer, por ejemplo, que algunas claves sean más probables que otras, lo que permitiría montar un ataque estadístico con ciertas garantías de éxito sin necesidad de probar todas las posibles claves. Por ejemplo: el código de cifrado conocido como LOKI tiene una clave de 64 bits de longitud, lo que hace un número total de 264 claves, pero un criptoanálisis diferencial ha demostrado que solamente hace falta probar 256 claves.

La situación suele empeorar si el atacante tiene acceso a mensajes cifrados y/o sin cifrar, al igual que en los viejos tiempos de la criptografía sin ordenadores. Al mismo tiempo, la creciente potencia de los ordenadores hace cada vez más vulnerables los ataques de fuerza bruta contra sistemas con claves pequeñas. DES, utilizado desde los años setenta, es uno de los protocolos de cifrado más usados y a la vez más resistentes a ataques criptoanalíticos, pero su clave de sólo 56 bits la hace vulnerable a ataques de fuerza bruta.

El problema principal con un sistema de cifrado es que no hay manera de probar de antemano si es robusto y fiable. Como los castillos medievales, parecen fuertes desde fuera, pero sólo mediante repetidos ataques podrán exponer puntos débiles. Un protocolo descubierto hoy puede que sea fiable o puede que no, pero no se sabrá hasta que se haya "ganado los galones" ante la comunidad criptográfica. Desafortunadamente, algunos de los algoritmos más fiables han resultado no serlo tanto.

VII. CURIOSIDADES

Esteganografía

Muy a menudo la criptografía resulta insuficiente para cubrir nuestras necesidades de protección de información. Pensemos, por ejemplo, en un malintencionado servicio de espionaje que intercepta e inspecciona todo el tráfico que circula por la red: normalmente, basta con que la correspondencia aparezca codificada para despertar las sospechas de estos entrometidos, lo cual podría inducirlos a destruir nuestros preciosos mensajes para que jamás alcancen su destino, al margen de que puedan o no descifrarlos.

Una interesante posibilidad, empleada prácticamente desde que existe la escritura, es lo que se conoce como esteganografía. Esta técnica se basa en ocultar la verdadera información dentro de algo que parezca del todo inofensivo, pero que tenga sentido por sí solo, de forma que no despierte las sospechas de nuestros "enemigos". Quizás el caso más conocido de esteganografía en lengua castellana sea el poema que aparece al principio de "La Celestina", en el que Fernando de Rojas "codificó" su nombre y lugar de nacimiento empleando las letras iniciales de cada verso.

Parece que la Humanidad lleva introduciendo mensajes ocultos en sus escritos desde mucho antes del nacimiento de las computadoras. La Informática moderna nos está permitiendo alcanzar niveles de complejidad absolutamente impensables hace poco tiempo a la hora de camuflar información, y quizás algún día nos ayude a extraer alguno de esos mensajes que con toda seguridad permanecen aún escondidos en nuestros textos antiguos. Tanto la Literatura en lengua castellana como la universal están plagadas de casos más o menos conocidos de esteganografía, la mayoría de las veces porque el autor trataba de ocultar su identidad. No hay que olvidar que cierto tipo de obras podía despertar las iras de la Inquisición, mientras que otras podían suponer un desprestigio para quien las escribía, por considerarse frívolas y poco dignas.

La Esteganografía es, en un 99%, ingenio. Y si no que se lo digan a Ron Rivest −la "R" de RSA−, cuando en 1998 desarrolló un sistema de "cifrado sin cifrar", basado en técnicas esteganográficas, que permitía enviar de forma segura mensajes en claro, intercalándoles tal cantidad de basura que un atacante se veía incapaz de separar el "grano" de la "paja" −no en vano el método fue bautizado como "Chaffing and winnowing"−.

También podemos mencionar el ejemplo del archivo de gráficos trucado, en el que los bits menos significativos de cada píxel son sustituidos por el mensaje que deseemos ocultar dentro de la imagen. Usando una técnica parecida se podrían emplear también los archivos de sonido para menesteres similares, e incluso nada nos impediría grabarnos un CD de audio con unos 40 MB de información clandestina sin despertar la más mínima sospecha.

¿Paranoia o realidad?

¿Existe un borrador codificado del futuro? Son muchos los que piensan que sí y, en consecuencia, se afanan en completar un gigantesco puzzle de infinitas piezas con sólo unas pocas de ellas en la mano. Por citar un caso mencionaré *El Código de la Biblia*, de Michael Drosnin, que, presentado como un juego pseudocientífico, ha conseguido un inesperado éxito en cuantos países se ha publicado. En él se afirma que hay un código secreto en la Biblia y que en un gran número de dramáticos casos ha servido para anunciar hechos que ocurrieron tal y como se habían predicho. Quizá pueda parecer descabellado, pero debo reconocer que el libro trata todos los asuntos que describe con mucho rigor. El autor dice haber empleado cinco años para verificar la información y no haber dado nada por hecho sin haberlo contrastado antes. Además, cada hallazgo del código bíblico ha sido confirmado mediante un ordenador a través de dos programas distintos e independientes.

Recordemos que ya Newton estaba convencido de que la Biblia y el Universo entero eran un criptograma pergeñado por el Todopoderoso, mediante el cual se podía conocer el futuro. Y que siglos más tarde un matemático israelí, Eliyahu Rips, descubrió que la tecnología informática y la física cuántica podían resolver el enigma.

En este libro se muestra cómo las palabras en la Biblia suelen formar una matriz de crucigrama, lo cual permite identificar bloques homogéneos de información. Y se explica que gracias a ese código se pronosticó la Guerra del Golfo, la colisión de un cometa con Júpiter y el asesinato de Itzhak Rabin, entre otros. Al igual que se codificó con exactitud la fecha de otros acontecimientos, así como las circunstancias que sirvieron de detonante en varios conflictos como Hiroshima, el Holocausto...

Sin embargo, también fallan determinadas profecías, pues, por ejemplo, el año 2000 aparece con el mensaje holocausto atómico. Así que, ¿quién sabe?, tal vez se trate sólo de simples coincidencias...

¿Imposible de descifrar?

En la Librería Beinecke, perteneciente a la Universidad de Yale, se haya uno de los más misteriosos e interesantes desafíos que la Historia ha legado a la criptografía. Se trata de un manuscrito de 235 páginas, donado en 1969 por H.P Kraus, que en 1912 había sido adquirido por Wilfrid M. Voynich a un colegio jesuita de Villa Mondragone, cerca de Roma. Este libro fue escrito por un autor desconocido (aunque algunos lo atribuyen a Roger Bacon, uno de los personajes del S.XIII con un pensamiento científico más avanzado), y constituye en sí mismo todo un enigma, ya que está escrito en un lenguaje desconocido, con unos caracteres desconocidos, y hasta la fecha nadie ha logrado descifrarlo.

La primera noticia fiable que se tiene del **Manuscrito Voynich** data de principios del S.XVII, cuando el emperador Rodolfo II de Bohemia lo compró por una cifra desorbitada. Luego pasó por varias manos hasta llegar en 1666 a las de Atanasio Kircher, un sacerdote jesuita, pero desde ese momento hasta 1912, nadie sabe a ciencia cierta qué le ocurrió al libro.

Para cualquier criptógrafo y estudioso de los lenguajes este libro constituye un estimulante reto, ya que ni siquiera se sabe con seguridad cuál es el tema que trata. Sus numerosas ilustraciones parecen indicar que es un tratado de alquimia cuyo auténtico contenido se quiso mantener en secreto, pero esto no son más que especulaciones. Posee diferentes secciones, que parecen tratar los siguientes temas tan dispares como

Botánica, Astronomía, Biología, Cosmología y Farmacia; y al final se incluye lo que parece un recetario.

Además, el texto del manuscrito cumple con las propiedades estadísticas principales de los lenguajes naturales, aunque presenta alguna peculiaridad, que puede deberse a la presencia de abreviaturas; el libro posee numeración de páginas, algunas anotaciones en alemán, otras en algún alfabeto desconocido, y una anotación en la última página en caracteres tradicionales que parece representar una clave para descifrar el texto. No obstante, ni siquiera sabemos a ciencia cierta si el texto está cifrado o no.

A partir de las vestimentas de los personajes dibujados, podría decirse que el manuscrito fue escrito en Europa durante el S.XIII, aunque una de las ilustraciones se parece a un girasol, lo cual sugiere que parte de él fue escrita después del Descubrimiento de América. De todas formas, tampoco está descartado que el libro sea un simple engaño hecho para estafar a alguno de sus poseedores, ya que en ocasiones se han pagado fuertes sumas por él.

Hasta la fecha se han llevado a cabo multitud de estudios sobre el Manuscrito Voynich, e incluso en más de una ocasión ha habido personas que aseguran haberlo traducido, pero todavía ninguna de las traducciones ha sido reconocida por la comunidad. Gracias a Internet, que está permitiendo dar a conocer este misterio, en los últimos años hayan surgido varios estudios interesantes y se han elaborado herramientas para apoyar las investigaciones.

La dificultad principal es que no sabemos apenas nada sobre el posible significado real del libro, por lo que decidir cómo dar por válida una posible solución constituye un problema en sí mismo. Parece evidente que la traducción debería cumplir una serie de condiciones mínimas: ser criptológicamente coherente, no permitir soluciones alternativas, cubrir todo el manuscrito, ser factible con los medios de la época, dar un significado coherente al libro, etc.

El proyecto EVMT (European Voynich Manuscript Transcription) pretende recoger y aglutinar todo lo que en la actualidad se sabe acerca del libro, y elaborar una trascripción completa en formato electrónico. Cuando esta versión esté finalizada, probablemente permita efectuar análisis numéricos más precisos que corroboren o refuten algunas de las teorías expuestas hasta la fecha. En la página "web" del proyecto, podremos encontrar entre otras muchas cosas varias trascripciones diferentes, herramientas para visualizarlas y convertirlas, programas de análisis del texto...

Todavía quedan muchas cuestiones abiertas y sin duda el Manuscrito Voynich constituye una gran incógnita en el panorama criptográfico actual: cuando muchos algoritmos de cifrado son abandonados por presentar fisuras en su estructura matemática, seguimos teniendo un texto codificado a mano que se resiste a las poderosas técnicas de criptoanálisis.

Bibliografía y referencias: PASTOR FRANCO, J. ; SARASA LÓPEZ, M.A. *Criptografía digital.*

Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. *Handbook of applied cryptography*.

Menezes, A. J. *Eliptic curve cryptosystems.*

SCHNEIER, B. *Applied cryptography.*

GIMPS (The Great Internet Mersenne Prime Search)

http://www.kriptopolis.com

SSH Communications Security

1