SOLEMNE ACTO DE APERTURA DEL CURSO ACADÉMICO 2011-2012

UNIVERSIDAD CARLOS III DE MADRID

Lección Inaugural:

LA ESCRITURA SECRETA. Una historia de 4.000 años

Prof. Arturo Ribagorda Garnacho

Sr. Rector Magnífico, Autoridades, queridos compañeros y alumnos, señoras y señores.

En la primavera de 1974, dos investigadores de la universidad de Stanford comenzaron a estudiar un problema criptográfico irresuelto: la distribución de claves, que había dificultado notablemente el uso de la criptografía durante toda la historia. En efecto, las técnicas de cifrado usadas desde la Antigüedad conllevaban el uso de una clave, con la que el emisor de un mensaje, antes de transmitirlo por un canal inseguro, lo cifraba, descifrándolo el receptor con la reiterada clave. Ello conllevaba que el emisor debía hacer llegar previamente dicha clave al receptor, obviamente por un canal seguro, y por tanto distinto del empleado para transmitir el mensaje. Encontrar dicho canal alternativo y seguro había planteado formidables dificultades. Por ejemplo, en la II Guerra Mundial, los submarinos alemanes debían atracar mensualmente en sus puertos, independientemente de que no

necesitasen repostar ni reponer sus torpedos, pues precisaban conocer la clave para cada uno de los siguientes treinta días.

Tras dos años de trabajos, Whitfield Diffie y Martin Hellman –los protagonistas de esta historia– encontraron la solución en las funciones unidireccionales, aquellas cuya inversa es, o bien matemática o bien computacionalmente, imposible de obtener. Cada interlocutor elige un número muy grande al que aplica una cierta función de este tipo, tras ello intercambian los resultados (incluso por un canal inseguro), llegando ambos a obtener –independiente y sorprendentemente–, un mismo número: la clave deseada. Y todo ello sin que un atacante pueda obtener ese número, ni siquiera interceptando el trueque citado. Este intercambio se denomina en su honor "intercambio de Diffie-Hellman".

La función unidireccional que encontraron fue la exponencial operada módulo un cierto número primo excepcionalmente grande. Esta función es simple de calcular, pero el cálculo de su inversa –necesario para romper el modelo propuesto– supone la resolución del problema del logaritmo discreto, incluido en la clase de problemas denominada NP-completos, de enorme dificultad matemática.

Con todo, mayor relevancia tuvo otra idea: la criptografía de clave pública o asimétrica. Los autores conjeturaron que podían existir funciones criptográficas que permitiesen sistemas con claves de cifrado y descifrado distintas –aunque vinculadas–, pero tal que su relación fuese tan compleja que resultase computacionalmente imposible obtener una conocida la otra. Con este sistema, si yo

poseyese un par de tales claves podría hacer una de público conocimiento (denominada clave pública) manteniendo la otra a buen recaudo (clave privada). Cualquiera podría remitirme un mensaje cifrado con mi clave pública, en la seguridad de que sólo yo (único conocedor de la correspondiente privada) podría descifrarlo.

Pero además, también demostraron que estos sistemas, de existir, podrían usarse para firmar documentos digitales, de modo que el firmante no pudiese renegar de su autoría y, más importante aún, nadie pudiese alterarlo tras la firma, lo que obviamente no sucede con la firma manuscrita que no es garante de la inalterabilidad del documento firmado.

Las funciones que aventuraron podrían ser usadas fueron las funciones unidireccionales con trampa, que a diferencia de las unidireccionales pueden invertirse, pero sólo por el conocedor de una cierta información: la trampa. Sin embargo, no encontraron ningún ejemplo de tales funciones.

Estos resultados se publicaron en 1977 en un artículo de título "*New dirección in cryptography*", que espoleó a numerosos criptólogos deseosos de encontrar un ejemplo de tales funciones.

Un grupo de éstos se asentaba en el MIT y lo constituían tres jóvenes investigadores, Leonard Adleman, Ronald Rivest y Adi Shamir, que tras seis meses encontraron un ejemplo de estas funciones, las exponenciales operadas con un módulo muy grande producto de dos primos enormes. Para que un conocedor de mi clave pública fuese capaz de hallar mi privada debería descomponer dicho número gigantesco en sus dos factores primos,

lo que constituye un problema irresuelto desde hace más de 2000 años y cuya solución es generalmente reputada como inexistente.

El artículo que describe su descubrimiento apareció en 1978 bajo el título: "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*, y desde entonces este algoritmo se conoce como RSA (iniciales de sus inventores). Hoy lo llevamos en nuestro Documento Nacional de Identidad electrónico, lo usamos cuando nos conectamos a un banco por internet, a la Agencia Tributaria o al ayuntamiento para pagar un impuesto, a la DGT para ver si tenemos alguna sanción, etc.

Lo contado hubiese sido la verdad histórica hace quince años; hoy sin embargo se sabe que esta historia es más antigua y sorprendente.

En los sesenta del pasado siglo, el ejército británico estaba convencido que más pronto que tarde sus soldados llevarían en su equipamiento dispositivos comunicación con posibilidades de cifrado. Empero, para evitar el disparate de que todos dispusieran de la misma clave, debería hallarse un sistema diferente de cualquiera conocido hasta entonces.

Para encontrarlo, en 1969, el *Communications Electronics Security Group*, del servicio de inteligencia del Ejército comisionó a uno de sus criptógrafos, James Ellis. Éste tuvo rápidamente una idea de cómo resolver el problema, aunque fue incapaz de materializarla en un algoritmo. Afortunadamente, en 1973 se incorporó a este servicio Clifford Cocks, quien en pocos días dio la misma solución que Rivest, Shamir y Adleman, sólo que cuatro años antes. Meses más tarde, otro joven, que también acababa de desembarcar en el

grupo, Malcolm Williamson, obtuvo la misma solución que Diffie y Hellman hallarían tres años después al intercambio de claves.

Estos descubrimientos se mantuvieron clasificados hasta 1997 cuando ya eran “vox populi” entre la comunidad criptológica. Es difícil imaginar un mayor suplicio para un investigador, que hacer un avance sustancial y observar cómo son otros los que se llevan el reconocimiento. Sin embargo, la criptografía (y en general la seguridad) ofrece abundantes ejemplos de esto, cuando se trabaja en, o para, los servicios de inteligencia.

En el presente, sistemas como los descritos son de uso cotidiano: cada vez que usamos un teléfono móvil, introducimos una contraseña en un ordenador, hacemos una operación con una tarjeta de débito o de crédito, nos conectamos con un servidor (y aparece https en vez de http), vemos un canal de televisión de pago, etc. Empero, estos tan universalmente empleados tienen una longeva vida

El primer escrito cifrado fue hallado en la tumba de de Khnumhotep, nomarca del Faraón Amenemhet II, de la XII dinastía del Antiguo Egipto, aproximadamente 2.000 años a. C. En dicha tumba se localizaron numerosos epitafios con jeroglifos inusuales –pero legibles con un plus de atención–, cuyo propósito es objeto de controversia entre los egiptólogos. Quizás despertar el interés por lo escrito, o bien ensalzar la figura del difunto o, lo más probable, encumbrar al propio escriba. Está tónica deliberada de confundir ciertos jeroglifos se mantuvo hasta el fin del Imperio egipcio.

Por su parte, la civilización mesopotámica, aunque inventó la escritura casi 300 años antes que Egipto (*c.a* 3.300 a.C.), nos ha

dejado vestigios más tardíos de escritura secreta, pues los más antiguos hallados datan del 1.500 a.C. Se trata de pequeñas tablillas, de 2 × 3 pulgadas, que describen en escritura cuneiforme sistemáticamente modificada la fabricación de cerámica, conocimiento muy valorado por aquel entonces.

A partir de este momento, los métodos de encubrimiento se enmarcaron en dos grandes grupos: aquellos que ocultan el texto o aquellos que lo alteran para imposibilitar su entendimiento. Los primeros, aquellos que hacen el mensaje imperceptible, se denominan esteganográficos y la disciplina que los estudia esteganografía. Los segundos, los que hacen el texto incomprensible, se denominan métodos de cifrado y la disciplina correspondiente criptografía. Por el contrario, la ciencia y técnica que trata de hallar el texto original a partir del cifrado se denomina criptoanálisis y criptoanalistas sus practicantes. El conjunto de criptografía y criptoanálisis se conoce como criptología.

En nuestro país, la primera referencia al cifrado la encontramos en una joya de nuestra Edad de Oro: “Tesoro de la lengua castellana o española”, escrita por Sebastián de Covarrubias y publicada en 1611. En esta obra la voz cifra aparece definida como:

> “Escritura enigmática, o con caracteres peregrinos o los nuestros trocados uno por otros en valor o lugar.”

Y sigue nuestro eminente lexicógrafo:

> “Tengo escrito un tratado de cifras, al cual remito lo que dellas se podía aquí decir, porque hará un volumen entero, y para lo

> que yo pretendo para el trabajo de las etimologías, pienso se ha cumplido con lo dicho."

Lamentablemente, este tratado se tiene por perdido.

También recoge la voz el primer diccionario de nuestra Real Academia, el diccionario de Autoridades de 1729:

> "Cifra: Modo u arte de escribir dificultoso de comprender sus cláusulas sino es teniendo la clave: el cual puede ser usando de caracteres inventados, o trocando las letras, eligiendo unas en lugar de otras …".

Dos siglos después, el diccionario de 1925 refleja el lema Criptografía como: "Arte de escribir con clave secreta o de un modo enigmático."

Es lamentable, que poseyendo palabras patrimoniales recurramos a barbarismos, por supuesto inexistentes, como "encriptar" (del inglés *to encrypt*) y sus derivados, lo que sólo puede explicarse por el desconocimiento, o peor el esnobismo, tan enraizado en algunos.

Por su parte, ejemplos de esteganografía se encuentran en los más notables historiadores griegos. Así, Heródoto, el padre de la Historia, o Jenofonte o Tucídides nos han dejado numerosos testimonios de su uso. A modo de ejemplo, el primero de ellos cuenta en el VII libro de su obra magna "Los nueve libros de la Historia", cómo los griegos fueron alertados del ataque del Rey de Reyes persa, Jerjes, que dio origen a la II Guerra Médica. En Susa (Persia) vivía Demarato, un espartano que, enterado de las intenciones de Jerjes, resolvió avisar a sus compatriotas. La cuestión era cómo enviar un mensajero que recorriese el Asia

Menor y cruzase el estrecho de los Dardanelos sin ser descubierto por los guardias persas. Para resolverlo, en palabras de Heródoto:

> "Tomó un cuadernillo de dos tablillas; rayó bien la cera que las cubría, y en la madera grabó con letras la resolución del rey. Hecho esto, volvió a cubrir con cera las letras grabadas, para que el portador del cuadernillo no fuera molestado por los guardas de los caminos."

El mismo Heródoto nos relata, ahora en su libro V de la misma obra, otra peripecia similar, aunque anterior, con el griego Histaeio de protagonista. Deseando éste que Aristágoras, tirano de Mileto, se rebelase contra Dario I de Persia (padre del aludido Jerjes), rapó el pelo a un esclavo y le tatuó en el cuero cabelludo un mensaje instando a Aristágoras a levantarse. Luego de crecerle el pelo, le envió a su destino sin temor a que se descubriese el aviso.

Estos métodos esteganográficos se han usado en todas las civilizaciones. Por ejemplo, los chinos escribían en un retal de seda, que se envolvía en cera formando una bolita que era engullida por el portador.

Más cercanas en el tiempo, se empiezan a usar las tintas simpáticas, definidas así en nuestro diccionario:

> "Composición líquida que tiene la propiedad de que no se conozca lo escrito con ella hasta que se le aplica el reactivo conveniente."

Una curiosa tinta simpática fue ideada por el criptógrafo napolitano Giovanni della Porta y usada en esa República durante el s. XVI. Se cuece un huevo, a continuación se disuelve piedra de alumbre en

vinagre formando una tinta con la que se escribe sobre la cáscara del huevo duro que, al ser porosa, absorbe la tinta sin dejar rastro de la misma. Basta con descascarillar el huevo para que en la clara aparezca el mensaje.

En todo caso, en el presente los métodos más empleados son los criptográficos, cuyo antecedente histórico fue un instrumento usado por los espartanos (*c.a* 400 a. C.), según cuenta el historiador griego Plutarco en sus “Vidas Paralelas: Lisandro-Sila”. El dispositivo, conocido como escítala lacedemonia, consistía en un bastón de determinado diámetro que se vendaba con una estrecha tira de piel, sobre la que se escribía un mensaje siguiendo el sentido longitudinal del bastón así vendado. Tras ello, bastaba con desenrollar la tira para que las letras quedasen desordenadas, haciendo el mensaje ilegible. Sólo si el receptor poseía un bastón del mismo grosor podía volver a enrollarlo con la tira y recuperar el mensaje. Este parece ser el origen del llamado bastón de mando de los jefes militares.

Pero debemos esperar al siglo I a. C., para que Julio César nos legue el primer método sistemático de cifrado. Como explica el historiador Suetonio en su obra “Doce Césares”, consistía en sustituir cada letra del mensaje por aquella otra situada tres posiciones por detrás de ella en el alfabeto (es decir, la A por D, la B por E y hasta las X, Y y Z cambiadas respectivamente por las, A, B y C). El método se puede expresar fácilmente mediante la aritmética modular y es el primero que admite una formulación matemática.

Estos métodos se denominan de sustitución monoalfabeto, pues sustituyen cada letra por otra o por un símbolo cualquiera. Su éxito fue enorme, pues durante mil años no se conoció la forma de vulnerarlos, si bien gran parte de estos años coincidieron con la oscuridad cultural de la Alta Edad Media Occidental.

En claro contraste con estas tinieblas culturales, en los dos últimos siglos del primer milenio, durante el califato abasí, Bagdad se convirtió en la capital cultural y política del mundo. En particular, las escuelas coránicas estaban muy interesadas en los estudios lingüísticos, para saber qué suras o aleyas del Corán eran del tiempo de Mahoma y cuales posteriores. De resultas, descubrieron que todas las lenguas tienen frecuencias característica de aparición de sus letras. Por ejemplo, la “e” es la letra más frecuente en español –figurando en torno a un 12% en un texto suficientemente largo–, seguida de la “a” –sobre un 11%–, etc.

De esta suerte, basta con contar el número de veces que aparecen los distintos símbolos –letras o no– de un texto cifrado, para deducir que el más frecuente será una e, aunque su grafía no se corresponda con esta letra, y así sucesivamente. Se había roto el cifrado de sustitución monoalfabeto. El descubrimiento fue publicado por uno de los sabios árabes más relevantes, Al-Kindi, en su obra “Sobre el desciframiento de mensajes criptográficos”. Con justicia, está considerado el “padre” del criptoanálisis.

A partir de Al-Kindi los criptoanalistas tomaron ventaja sobre los criptógrafos, situación que se prolongó hasta el Renacimiento con la creación de los Estados Modernos, que conllevaron el establecimiento de embajadas permanentes, la formación de

ejércitos estables y profesionales, y el asentamiento de las Cortes –principalmente ambulantes hasta entonces–. Todo ello, provocó un renovado interés en el, por entonces llamado, “arte de la escritura secreta” (ars occulta scribendi).

Esta escritura se impulsó, en primer lugar, en las ciudades-estado italianas y fueron los estados pontificios los primeros de dotarse de secretarios de cifra. Es Gabrieli di Lavinde, al servicio del antipapa Clemente VII en Avignon, el primer criptógrafo relevante de este renacer de la criptografía. Pero casi todas las ciudades italianas se dotan de notables expertos, autores de nuevos métodos de cifrado. Así, Simeone de Crema, al servicio de los Duques de Mantua, Giovanni Soro a las órdenes de los dogos de Venecia (y por extensión del Consejo de los Diez), Francesco Simonetta a disposición de los Sforza en Milán y, sobre todo, Leon Batista Alberti, en la Florencia de los Medicis, que inventó el primer dispositivo de cifrado, consistente en un disco sobre el que gira concéntricamente una corona circular, precursor remoto de la máquina Enigma.

Ellos idearon numerosos sistemas de cifrado, que de nuevo confirieron la primacía a los criptógrafos sobre los criptoanalistas. Por ejemplo, inventaron el nomenclátor, lista de nombres frecuentes, como reyes, países, ciudades, etc., en el que cada uno aparece asociado a unas letras o grupo de símbolos. También los silabarios, catálogo de sílabas en el que cada una se asocia a un símbolo. Igualmente los nulos, letras o símbolos sin significado y cuyo único objeto es desorientar al criptoanalista. Pero sus inventos fundamentales son las sustituciones polialfabéticas (en las que una misma letra se puede sustituir otra de entre varias según su

posición en el texto en claro) y homofónicas (en las que una letra tiene varios símbolos equivalentes que se van eligiendo al azar). Obviamente, todos ellos invalidan el análisis de frecuencias.

En España, hay constancia del uso esporádico del cifrado en la Corona de Aragón, con los trastámara Alfonso V el Magnánimo y Juan II, aunque es bajo el reinado de los Reyes Católicos, cuando su uso se generaliza. El principal responsable de esto es Miguel Pérez de Almazán quien en la década de 1480 comienza a emplear esta técnica en la correspondencia diplomática y universaliza su empleo a partir de 1493, cuando es nombrado Primer Secretario de los Reyes Católicos.

Pero hay que esperar medio siglo para que las técnicas de ocultación alcancen su mayor esplendor en España y el resto de Europa. En nuestro país, Felipe II, él mismo muy aficionado a la criptografía, renueva todo el sistema de cifras heredado de Carlos I y, adelantándose a su tiempo, establece un sistema de claves (en realidad un sistema de cifrados) diferentes para cada necesidad, que denomina clave general y particular. La primera es compartida por el Monarca, los Secretarios de Estado y de la Guerra, los virreyes, gobernadores generales y embajadores, mientras que la particular es distinta para cada uno de los anteriores dignatarios y sólo conocida por el interesado y el Rey. En palabras de Felipe II, recogidas de su misiva del 19 de junio de 1581 al Duque de Medina Sidonia:

> “Algunas veces ofrécense negocios tan graves e importantes y de tanto secreto que no será bueno escribirlos en cifra

general, se os envía para este caso una particular en la cual no podéis escribir a los demás ministros, si no sólo a mí."

Tanto en el caso de la particular como en el de la general, los cifrados eran de gran complejidad, estando compuestos de nomenclátores, silabarios, sustituciones homofónicas y nulos.

Además, la general se cambia tras un tiempo prudencial, o bien cuando hay indicios de que ha caído en manos enemigas. Así, se cambió en los años, 1556, 1562, 1564, 1567, etc., lo que dice mucho de los espías de nuestros enemigos y de la negligencia de algunos de nuestros diplomáticos, por más que algunos aficionados a la criptografía hayan especulado, con más ligereza que argumentos, que estos cambios obedecían a que eran rotas fácilmente por los criptoanalistas extranjeros, singularmente el matemático Francois Viète, al servicio de Enrique III de Navarra (posteriormente Enrique IV de Francia) o Thomas Phelippes, Secretario de cifra de Francis Walsingham, Ministro de Isabel I de Inglaterra.

Igualmente, es Felipe II el primer rey de la Corona española que establece la figura del Secretario de Cifra, alto cargo de la Corte que dirige un gabinete encargado de crear nuevas claves y descifrar la correspondencia intervenida. De estos secretarios el más famoso fue D. Luis Valle de la Cierva (fenómeno de la cifra, dice de él el Dr. Marañón en su libro sobre Antonio Pérez), que trabajó al servicio del Secretario de Estado D. Juan de Idiáquez.

Aunque en los siglos siguientes los desarrollos criptográficos siguieron acelerándose y su uso extendiéndose, el siguiente salto cualitativo se da en la 2ª Guerra Mundial, con el uso generalizado

de las máquinas de cifra. Es la época de la mítica Enigma, de la más sofisticada y robusta Lorenz, usada en las comunicaciones entre Hitler y su Estado Mayor, de las japonesas Jade y Púrpura, de la americana Sigaba, la británica Tipex, etc.

Pero es la Enigma la que siempre ha concitado el mayor interés. Fue ideada por Arthur Scherbius y patentada en 1918. La Wechmart la adoptó en 1923, comenzando su fabricación en serie en 1925. A lo largo de la Guerra las fuerzas armadas alemanas compraron más de treinta mil.

Es de destacar que unas veinte Enigma fueron cedidas al bando rebelde para ser probadas en nuestra Guerra Civil. Hoy, excepto una que se expone en el Museo de Ejército, duermen, lamentablemente, el sueño de los justos en el Cuartel General del Ejército de Tierra.

La máquina, en su versión más segura, constaba de 5 rotores, elegibles por el operador de entre 8, que giraban independientemente sobre un eje. Cada rotor tenía en sus dos caras 26 conectores (las letras del alfabeto alemán) y un cableado establecía un contacto entre pares de conectores de los rotores contiguos. La señal que salía de los conectores del quinto rotor se reflejaba en un reflector volviendo a pasar, y cifrarse por segunda vez, por los cinco rotores. Además, un teclado se unía por cables intercambiables a un clavijero, que hacía contacto con los conectores del primer rotor. Finalmente, un visor mostraba el texto cifrado.

Como el operador podía elegir los rotores de entre varios, colocarlos en cualquier orden, conectar los cables del teclado en

cualquier posición del clavijero, etc., el número de configuraciones posible (es decir de claves) superaba, para las máquinas menos potentes, los 1000 billones.

El desciframiento de estos mensajes fue una aventura titánica y apasionante, en la que intervinieron criptoanalistas polacos –singularmente Marian Rejewski–, eminentes matemáticos por ejemplo, Alan Turing– y grandes recursos. El centro de todo fue una mansión victoriana, Bletchley Park, a 80 km. al norte de Londres y que se mantuvo incomprensiblemente ignorada por los servicios de inteligencia germanos.

Para acelerar el descifrado, se mejoraron unas máquinas creada por los criptoanalistas polacos denominada *bombas*, convirtiéndose en voluminosos equipos de 1 tonelada, de los que llegó a haber 200 en Bletchley Park.

Pero no menos interés tiene el criptoanálisis de la Lorenz. Era ésta una máquina más compleja y robusta que la Enigma, que requirió de equipos mucho más sofisticados. Fueron los matemáticos de Bletchley, Newman y Flowers, quienes basándose en la máquina universal de Turing, diseñaron un aparato capaz de adaptarse a los cambiantes problemas que planteaba la Lorenz, es decir diseñaron lo que después se denominaría ordenador programable, que fue construido a base de válvulas en 1943 y bautizado como Colossus. Tras la contienda, Bletchley Park fue desmantelado y su información clasificada, por lo que estos hallazgos, permanecieron ignorados hasta recientemente. En particular, aunque Colossus fue anterior en dos años al tradicionalmente considerado primer

ordenador, el ENIAC, ni su nombre ni el de sus inventores, han obtenido el crédito merecido.

El eminente criptólogo Gustavus Simmons denomina al periodo de 4.000 años esbozado era de la criptografía precientífica, pues carece de fundamentos teóricos globales. Esto cambió en tan solo dos años, 1948 y 1949, cuando el ingeniero Claude Shannon publicó dos magistrales artículos: "*A mathematical theory of communication"*, y "*Communication Theory of Secrecy Systems*."

En el primero, Shannon sentó las bases matemáticas de la teoría de la información, postulando las leyes que han de satisfacer los símbolos para ser portadores de información, y relacionó las propiedades de estos símbolos con las cantidades de información que pueden transportar. Para ello, comenzó midiendo la cantidad de información ganada al recibir un mensaje por la incertidumbre que sobre el mismo se tenía antes de recibirlo.

Seguidamente definió entropía de una fuente a la cantidad promedio de información transportada por un mensaje de la misma. En el caso de tener dos fuentes de mensajes entre las que existe alguna relación, la aparición de un mensaje de la primera fuente disminuye la incertidumbre en la aparición de otro mensaje de la segunda. La medida de esta incertidumbre tiene importancia criptológica, pues da una pista sobre un cierto texto en claro cuando se conoce su correspondiente cifrado.

En el segundo de los artículos (*Communication Theory of Secrecy Systems*), Shannon propuso una métrica para evaluar el secreto de un cifrador, basándose en la incertidumbre que sobre el texto en claro tiene un criptoanalista que intercepte el texto cifrado

correspondiente. Si la incertidumbre es infinita jamás, podrá recuperar el texto en claro, salvo, naturalmente, que conozca el algoritmo y la clave.

Todos los cifradores, con una excepción, filtran alguna información del texto en claro al texto cifrado. Además, según la longitud del cifrado crece también aumenta la información filtrada, hasta que la incertidumbre sobre el texto en claro es cero. En este momento, el cifrador es matemáticamente vulnerable.

En todo caso, matemáticamente vulnerable no significa inseguro, pues el volumen de cálculo preciso puede ser inabordable. Surge así el concepto de cifrador computacionalmente seguro, como aquel que es hoy en día inquebrantable, aunque pueda ser roto con la potencia de los ordenadores del futuro.

Desde estos artículos de Shannon– y siguiendo al citado Simmons– se afirma que comienza la era de la criptografía científica, que se extiende hasta el 1977, con la publicación de Diffie y Hellman –con la que hemos comenzado esta lección–, que marca el comienzo de la era de la criptografía de clave pública.

De esta suerte, esta longeva disciplina, está jugando, y aún jugará más, un papel crucial en la era de la información, que requiere de la confianza de la sociedad para su consolidación y progreso, confianza que sólo puede venir de la mano de la seguridad cuya componente más importante es hoy, como hace 4000 años, la criptografía y la esteganografía, es decir las técnicas de ocultación de la información.

Leganés, Madrid, 27 de septiembre de 2011