UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 3: Anexo Historia

Fuente: "Criptografía y Seguridad en Computadoras", Manuel José Lucena López. Capitulo 1.2, Algunas notas sobre la Historia de la Criptografía

6. *Apéndices*.

Este texto no tiene necesariamente que ser leído capítulo por capítulo, aunque se ha organizado de manera que los contenidos más básicos aparezcan primero. La parte de fundamentos teóricos está orientada a personas con unos conocimientos mínimos sobre Álgebra y Programación, pero puede ser ignorada si el lector está dispuesto a prescindir de las justificaciones matemáticas de lo que encuentre en posteriores capítulos. La recomendación del autor en este sentido es clara: si es su primer contacto con la Criptografía, deje los fundamentos teóricos justo para el final, o correrá el riesgo de perderse entre conceptos que, si de una parte son necesarios para una comprensión profunda del tema, no son imprescindibles a la hora de empezar a adentrarse en este apasionante mundo.

Se ha pretendido que todos los conceptos queden suficientemente claros con la sola lectura de este libro, pero se recomienda vivamente que si el lector tiene interés por profundizar en cualquiera de los aspectos tratados aquí, consulte la bibliografía para ampliar sus conocimientos, pudiendo emplear como punto de partida las propias referencias que aparecen al final de este libro, aunque por desgracia, algunas de las más interesantes están en inglés.

1.2. Algunas notas sobre la Historia de la Criptografía

La Criptografía moderna nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un lugar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en el proyecto ULTRA tratando de descifrar los mensajes enviados por el ejército alemán con los más sofisticados ingenios de codificación ideados hasta entonces: la máquina ENIGMA y el cifrado *Lorenz*. Este grupo de científicos diseñó y utilizó el primer computador de la Historia, denominado *Colossus* —aunque esta información permaneció en secreto hasta mediados de los 70—.

Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayor parte de estos avances se mantenían —y se siguen manteniendo, según algunos— en secreto. Financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los EE.UU.), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares. Sin embargo, en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que la Criptografía sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de distribución de

contenidos multimedia. Esta dualidad civil–militar ha dado lugar a una curiosa *doble historia* de la Criptografía, en la que los mismos algoritmos eran descubiertos, con pocos años de diferencia, por equipos de anónimos militares y posteriormente por matemáticos civiles, alcanzando únicamente estos últimos el reconocimiento público por sus trabajos.

Muchas son las voces que claman por la disponibilidad pública de la Criptografía. La experiencia ha demostrado que la única manera de tener buenos algoritmos es que éstos sean accesibles, para que puedan ser sometidos al escrutinio de toda la comunidad científica. Existe una máxima en Criptografía que afirma que cualquier persona —o equipo— es capaz de desarrollar un algoritmo criptográfico que él mismo no sea capaz de romper. Si la seguridad de nuestro sistema se basa en que nadie conozca su funcionamiento tiene varias implicaciones perversas: por un lado, aquellos que quieran conocer su verdadera resistencia tendrán que confiar en nuestra palabra, y por otro, provoca una falsa sensación de seguridad, ya que si algún *enemigo* encuentra un agujero, es bastante probable que no lo publique. En consecuencia, el único secreto que debe tener un sistema criptográfico es la clave. Ejemplos a lo largo de la historia sobre fracasos de esta política de *seguridad basada en la oscuridad*, por desgracia, hay muchos, algunos de ellos en ámbitos tan delicados como el Voto Electrónico.

Salvo honrosas excepciones[1], la Criptografía llega hasta nosotros en forma de programas informáticos. Un programa mal diseñado puede echar por tierra la seguridad de un buen algoritmo criptográfico, por lo que es necesario conocer cómo está escrito el programa en cuestión, para poder detectar y eliminar los fallos que aparezcan en él. En este sentido, el *Sofware Libre*, cuyo código fuente está a disposición de los usuarios —a diferencia del *software* privativo, que mantiene el código fuente en secreto— quizás sea el que brinda mejores resultados, ya que permite a cualquiera, además de asegurarse de que no contiene *puertas traseras*, estudiar y eventualmente corregir el código si encuentra fallos en él. Actualmente, una de las mayores amenazas sobre el *software* libre es la pretensión de establecer sistemas de patentes sobre los programas informáticos, con un claro perjuicio tanto para los usuarios como para las pequeñas empresas frente al poder de las grandes corporaciones. Por desgracia, parece que a nuestros gobiernos les interesan más los beneficios de las multinacionales que los intereses de los ciudadanos.

Es imposible desligar la Criptografía moderna de todas las consideraciones políticas, filosóficas y morales que suscita. Hoy por hoy, tiene más poder quien más información controla, por lo que permitir que los ciudadanos empleen técnicas criptográficas para proteger su intimidad limita de forma efectiva ese poder. Con el pretexto de la seguridad se están aplicando medidas para ralentizar el acceso de los ciudadanos

[1]Como el algoritmo *Solitaire*, desarrollado por Bruce Schneier, para el que únicamente se necesita papel, lápiz, una baraja y algo de paciencia.

a la Criptografía *fuerte*, bien desprestigiando a quienes la usan, bien dificultando por distintos medios su adopción generalizada. Una de los frentes de debate más llamativos en este sentido es la intención de algunos gobiernos de almacenar todas las claves privadas de sus ciudadanos, necesarias para *firmar digitalmente*, y considerar ilegales aquellas que no estén registradas. Es como pedirnos a todos que le demos a la policía una copia de las llaves de nuestra casa. Esta corriente crea una situación extremadamente perversa: aquellos que quieren emplear la Criptografía para usos legítimos encuentran dificultades mientras que, por ejemplo, a un traficante de armas le tiene sin cuidado que sea ilegal usarla, con lo que no se frena su uso delictivo.

Existe un falaz argumento que algunos esgrimen en contra del uso privado de la Criptografía, proclamando que ellos nada tienen que ocultar. Estas personas insinúan que cualquiera que abogue por el uso libre de la Criptografía es poco menos que un delincuente, y que la necesita para encubrir sus crímenes. En ese caso, ¿por qué esas personas que *no tienen nada que ocultar* no envían todas sus cartas en tarjetas postales, para que todos leamos su contenido?, o ¿por qué se molestan si alguien escucha sus conversaciones telefónicas?. Defender el ámbito de lo privado es un derecho inalienable de la persona, que en mi opinión debe prevalecer sobre la obligación que tienen los estados de perseguir a los delincuentes. Démosle a los gobiernos poder para entrometerse en nuestras vidas, y acabarán haciéndolo, no les quepa duda.

Uno de los elementos más polémicos acerca de los ataques indiscriminados a la intimidad es la red *Echelon*. Básicamente se trata de una red, creada por la NSA en 1980 —sus *precursoras* datan de 1952— en colaboración con Gran Bretaña, Australia y Nueva Zelanda, para monitorizar prácticamente todas las comunicaciones electrónicas —teléfono, e-mail y fax principalmente— del planeta, y buscar de manera automática ciertas palabras clave. La información obtenida iría a la NSA, que luego podría a su vez brindársela a otros países. El pretexto es, nuevamente, la lucha contra el terrorismo, pero podría ser empleada tanto para espionaje industrial —como presuntamente ha hecho durante años el Gobierno Francés, poniendo a disposición de sus propias compañías secretos robados a empresas extranjeras—, como para el *control* de aquellas personas que pueden representar amenazas políticas a la *estabilidad* de la sociedad moderna. La Unión Europea reconoció la existencia de Echelon, pero hasta la fecha nadie ha exigido a ningún gobierno explicación alguna; es más, parece que los planes de la U.E. al respecto pasan por el despliegue de su propia red de vigilancia electrónica, llamada *Enfopol*. Si bien el proyecto se encuentra paralizado, es conveniente mantenerse en guardia, especialmente desde que los terribles atentados del 11 de septiembre de 2001 han propiciado una ola de limitación de las libertades civiles con el pretexto de la seguridad. Quizás algunos deberían recordar aquella famosa frase de Benjamin Franklin: *"Quienes son capaces de renunciar a la libertad esencial, a cambio de una seguridad transitoria, no son merecedores de la seguridad ni de la libertad."*

Uno de los logros más importantes de la sociedad humana es la libertad de expresión. Naturalmente, lo ideal sería que todos pudiéramos expresar nuestros pensamientos con total libertad, y que cada cual se hiciera responsable de sus palabras. Sin embargo, todos sabemos que hay situaciones, incluso en ámbitos en los que supuestamente se respeta la libertad de expresión, en los que ciertas afirmaciones *inconvenientes* o políticamente incorrectas pueden dar lugar a represalias. Es necesario, por tanto, para poder garantizar la libertad, poder garantizar también el anonimato. También es una cuestión de higiene otorgar menos crédito a aquellas cosas que se dicen bajo el paraguas del anonimato, pero sería peor no disponer de esa posibilidad. En este sentido la Criptografía, combinada con otras técnicas, es la única tecnología que puede permitirnos llegar a garantizar niveles razonables de anonimato. Después de todo, como dijo Thomas Jefferson, *"es preferible estar expuesto a los inconvenientes que surgen de un exceso de libertad que a los que provienen de una falta de ella."*

No cabe duda de que la información se está convirtiendo en la mayor fuente de poder que ha conocido la Humanidad, y que la Criptografía es una herramienta esencial para su control. Es necesario, pues, que los ciudadanos de a pie conozcan sus ventajas e inconvenientes, sus peligros y leyendas. Dicen que vivimos en Democracia pero, si a la gente no se le muestra toda la información relevante de manera honesta e imparcial, ¿cómo va a poder decidir su futuro? Esta obra pretende poner su pequeño granito de arena en ese sentido.

1.3. Números *Grandes*

Los algoritmos criptográficos emplean claves con un elevado número de bits, y usualmente se mide su calidad por la cantidad de esfuerzo que se necesita para romperlos. El tipo de ataque más simple es la *fuerza bruta*, que simplemente trata de ir probando una a una todas las claves. Por ejemplo, el algoritmo DES tiene 2^{56} posibles claves. ¿Cuánto tiempo nos llevaría probarlas todas si, pongamos por caso, dispusiéramos de un computador capaz de hacer un millón de operaciones por segundo? Tardaríamos... ¡más de 2200 años! Pero ¿y si la clave del ejemplo anterior tuviera 128 bits? El tiempo requerido sería de 10^{24} años.

Es interesante dedicar un apartado a tratar de fijar en nuestra imaginación la magnitud real de este tipo de números. En el cuadro 1.1 podemos observar algunos valores que nos ayudarán a comprender mejor la auténtica magnitud de muchos de los números que veremos en este texto. Observándola podremos apreciar que 10^{24} años es aproximadamente cien billones de veces la edad del universo (y eso con un ordenador capaz de ejecutar el algoritmo de codificación completo un millón de veces por segundo). Esto nos debería disuadir de emplear mecanismos basados en la