Criptología

JESÚS Mª MINGUET MELIÁN

Prof. Titular Universidad UNED

> Lo que permite al soberano saber y al buen general intuir, esperar y anticiparse, aquello que sobrepasa los límites del común de los mortales, es el conocimiento previo

Podemos definir **información** como el resultado de conocer hechos, sus causas y sus consecuencias. Adquirimos información cuando conocemos algo que antes no conocíamos. es decir, cuando pasamos del desconocimiento de algo a su conocimiento.

Poseer información es sinónimo de poder. La información puede ser o no útil en un momento determinado, pero casi siempre se considera como algo valioso. Esto ha sido así desde el principio de la historia de la Humanidad, como confirma la frase que inicia este trabajo tomada del libro *El arte de la guerra*, escrito en el siglo V antes de Cristo por el chino Sun Tse.
Si la posesión de información privilegiada siempre ha sido una ventaja competitiva, en la época actual, en la era de la información se ha convertido en algo imprescindible.

Las tecnologías de la información y las telecomunicaciones han permitido la constitución de grandes sistemas de almacenamiento, proceso y transmisión de datos e información. No es concebible ninguna organización, pública o privada, con o sin fines lucrativos, que no disponga de un sistema imformático más o menos grande. De hecho la situación es en muchos casos irreversible. ¿Podemos pensar en una sociedad sin cajeros electrónicos, tarjetas de crédito, despacho automático de billetes de avión o

tren? De hecho las estadísticas demuestran que la mayor parte de las empresas que sufren algún daño grave en su sistema informático, y que no tienen planes de contingencia o de recuperación de negocios, quiebran en el plazo máximo de un año.

EL SISTEMA DE INFORMACIÓN

De hecho el **Sistema de Información** desempeña cada vez un papel más importante en el funcionamiento de las organizaciones, las cuales llegan casi a depender totalmente de ellos. Un Sistema de Información está compuesto por los **Recursos Informáticos** (soporte informático tanto **físicos** como **lógicos**), **Activos de Información** (datos o información) y **Personas** (usuarios informáticos o usuarios finales).

Pero a la vez que los sistemas informáticos se han ido haciendo más complejos, aparecen
más y más puntos vulnerables. El número de posibles atacantes a los sistemas de información crece día a día y con las más variadas motivaciones (beneficios económicos, espionaje, venganza, terrorismo, reto personal, etc. Simultáneamente los medios técnicos pasa intentar vulnerar un sistema informático son muy sofisticados y de su mismo nivel tecnológico.
de ahí que sea imprescindible el pensar en proteger los sistemas de información. Es necesario el practicar la **Seguridad Informática**.

LA SEGURIDAD INFORMÁTICA

Resulta en general muy difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro sería necesario identificar todas las amenazas a las que puede verse sometido. Por ello quizás sea más apropiado hablar de **vulnerabilidad**.

Según el profesor Valentín San Caja la **vulnerabilidad de un sistema informático** es *la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseados, de recibir algún daño o perjuicio en cualesquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.*

Análogamente define la **seguridad de un sistema informático** como *el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos.*

Actualmente se está tendiendo por los responsables de la seguridad de las empresas con grandes sistemas de información a una normalización de la terminología de seguridad informática. Según la Comisión de Seguridad de SEDISI se distinguen los siguientes componentes en un **Análisis de riesgos**:

. **Sistema de información.** Son los Recursos Informáticos y Activos de Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

. **Amenaza.** Cualquier evento que pueda provocar daño en los Sistemas de información, produciendo a la empresa pérdidas materiales o financieras.

. **Vulnerabilidad.** Cualquier debilidad en los SI que pueda permitir a las amenazas causarles daño y producir pérdidas a la empresa.

. **Impacto.** Es la medición y valoración del daño que podría producir a la empresa la materialización de una amenaza sobre los SIs. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

. **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del SI, causando un impacto en la empresa.

. **Defensa.** Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.

AMENAZAS

Podemos dividir las amenazas que se ciernen sobre los recursos informáticos, los activos informáticos y el personal informático en cuatro clases: **Intercepción, Modificación, Interrupción** y **Generación**.

La **Intercepción** se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es la más difícil de detectar, ya que generalmente no produce una alteración en el sistema.

La **Modificación** intenta, además de la intercepción, cambiar en todo e en parte el funcionamiento del sistema. Es quizás el tipo de amenaza más peligroso.

La **Interrupción** puede ser temporal o permanente e incluye la posibilidad de destrucción de recursos y activos. Es la más sencilla de detectar y la que presenta mayor dificultad para luchar contra ella.

Por último, la **Generación** se refiere a la adición de campos o registros en los activos, en la adición de líneas de código a los recursos lógicos, o en la introducción en el sistema de programas completos (virus, gusanos, caballos de Troya, bombas lógicas, etc.).

Evidentemente, la mayoría de las amenazas participan de las características de más de uno de los grupos estudiados.

EL ACTIVO INFORMACIÓN

El activo información puede adoptar muchos formatos, tanto dentro de los sistemas como fuera de ellos. Así podemos clasificar la información en:

. **Impresa**. Escrita en papel:
. **Almacenada**. En los sistemas o en medios portables;
. **Transmitida**. A través de redes o entre sistemas;
. **Hablada**. En conversaciones.

Pero independientemente de su formato, la clasificación que más nos interesa es la que se relaciona con el valor que la información tiene para la organización. Según este criterio podemos dividir las informaciones en **clasificadas** y **no clasificadas**.

Las **informaciones no clasificadas** son aquellas que su divulgación o uso no autorizado no ocasionan pérdidas significativas para la organización. A su vez se subdividen en: de **Uso general** (información que puede ser conocida y utilizada sin autorización por cualquier persona de la empresa o ajena a ella) y de **Uso interno** (información que no puede ser publicada, pero que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podrían originar pérdidas leves y asumibles por la organización).

Los **activos clasificados** se subdividen en: **Confidencial** (información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesitan para

realizar su trabajo, y cuya divulgación o uso no autorizado podría ocasionar pérdidas significativas, materiales o de imagen) y **Secreta o Reservada** información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y que su divulgación o uso no autorizados podrían ocasionar graves pérdidas materiales o de imagen).

Cada nivel de información debe tener defensas o prevenciones en función de la gravedad del impacto que produciría su vulnerabilidad.

LA SEGURIDAD DEL ACTIVO INFORMACIÓN

Según el *Libro Naranja de los E.E.U.U.* (normas del Truster Computer System Evaluation Criteria) y el **ITSEC** (Information Technology Security Evaluation Criteria) al establecer la seguridad de la información hay que tener en cuenta tres criterios fundamentales: **confidencialidad, integridad y disponibilidad**.

La **confidencialidad** (secreto) protege a los activos de información contra acceso o divulgación no autorizados.

La **integridad** garantiza la exactitud de los activos contra alteraciones, pérdida o destrucción, ya sea accidental o intencionada.

Por último, la **disponibilidad** asegura que los recursos y activos informáticos pueden ser utilizados en la forma y el momento requeridos. También incluye a su posible recuperación en caso de desastre.

La transmisión de datos a través de redes de computadores han creado nuevos problemas de seguridad, por lo que las normas ISO y CCITT añaden dos nuevas características: la **autenticidad** y la **imposibilidad de rechazo**.

La **autenticidad** asegura el origen y el destino de la información.

La **imposibilidad de rechazo** o **no repudio** asegura que cualquiera que envíe o reciba un activo no información no puede alegar ante terceros que no la envió o la recibió.

DEFENSA DE LOS ACTIVOS DE INFORMACIÓN

Las defensas o medidas de seguridad a establecer en un sistema de información se agrupan en cuatro tipos: legales, administrativas u organizativas, físicas y lógicas.

Los informáticos deben conocer la **legislación** vigente, pues a veces imponen obligaciones de seguridad, para conocer que tipos de amenazas deben ser prevenidas especialmente y que tipos de impactos pueden ser perseguidos legalmente. En algunos casos la referencia es a modo de recomendación. En otros la norma es un imperativo legal. Esto es especialmente importante cuando los activos a proteger contienen datos de carácter personal, los que afectan al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 de la vigente Constitución Española).

En desarrollo del mandato constitucional se ha promulgado la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal). Otras normativas vigentes que afectan que afectan a la seguridad informática son la Ley de Facturación Telemática (arts. 4.2.f, 5.2.d, 6.1 y 7.b), la LOT (Ley de Ordenación de las Telecomunicaciones, arts. 5.4 y 24) y el nuevo Código Penal (arts. 197, 256, 264.2, 278 y 400).

Una primera forma de defensa y aplicación de la legislación vigente son las medidas de carácter **administrativo u organizativo**, como la creación de una infraestructura de seguridad informática en los distintos niveles (Comité de Dirección, Comité de Seguridad Informática, Responsable de Seguridad, etc.), normativas de seguridad y planes de seguridad y contingencias.

El siguiente nivel de protección es el **físico.** Sin entrar en detalles este nivel abarca la construcción y control de acceso a los Centros de Proceso de Datos, las medidas de protección contra fuegos, fallos de energía eléctrica o falta de aire acondicionado, los armario de almacenamiento de la cintas de back-up, la protección durante el transporte de los soportes de almacenamiento, las llaves de disqueteras, etc.

En el nivel más cercano a los activos de información se encuentran las medidas de protección **lógicas**: identificación, autorización y autentificación de usuarios, contraseñas (password), claves, cortafuegos (firewalls), cifrado, etc.

Por fin hemos situado en el entorno de la seguridad el tema objeto de este trabajo, la Criptología, la ciencia que permite el cifrado de la información.

CRIPTOGRAFÍA Y CRIPTOANÁLISIS

El ataque a los **datos** ha sido siempre el más sencillo de realizar ya que no es necesaria ninguna especialización para ello. Interceptado el mensaje (o el mensajero) o alcanzada la información el atacante logra su objetivo. Por ello, desde la más remota antigüedad, los que poseían información valiosa (estadistas, militares, diplomáticos, etc.) intentaron hacerla **ininteligible** a toda persona no autorizada mediante su cifrado.

La **Criptografía** (del griego *Kriptos*, secreto u oculto, y *Graphos*, escrito) es *la ciencia que estudia la escritura secreta*, la forma de ocultar el significado de una información.

Pero como el conocimiento de la información puede proporcionar beneficios siempre ha habido personas dispuestas a atacar una información, aunque se encuentre cifrada, por encargo de gobiernos (espías), empresas (espías industriales) o para su propio beneficio (chantajistas, estafadores o ladrones informáticos). Surge entonces la ciencia contraria, el **Criptoanálisis**. Podemos definir el Criptoanálisis como *la ciencia que estudia como esclarecer la escritura secreta u oculta.*

Aunque durante mucho tiempo ambas ciencias se han considerado un arte, no cabe duda que hoy día constituyen conjuntamente una ciencia bien estructurada llamada **Criptología**. Se puede definir la Criptología como *la ciencia que estudia como cifrar y descifrar información.*

Hemos obviado intencionadamente el término información escrita puesto que en estos momentos se está trabajando en la denominada Criptografía visual que permite el cifrado de información gráfica, que por supuesto puede ser un documento escrito. También se utiliza desde hace tiempo el cifrado de los mensajes de voz en teléfonos móviles o líneas especiales, mediante procedimientos digitales o distorsión de ondas. Por lo tanto la Criptología permite el cifrado de todo tipo de información (escrita, sonora y gráfica), aunque principalmente se dedica a la información escrita.

FUNDAMENTOS TEÓRICOS DE LA CRIPTOLOGÍA

Aunque Bauer en su trabajo ha demostrado que todos los algoritmos criptográficos de la historia obedecen a los principios de la ciencia criptográfica, se

considera que el nacimiento, como verdadera ciencia, de la criptografía se basa en dos hechos recientes:

- Los estudios de Shannon sobre los fundamentos matemáticos de la teoría de la comunicación (1948) y su aplicación a los sistemas criptográficos (1949).

- La publicación de Diffie sobre las bases teóricas de la criptografía de clave pública en 1976.

La ciencia criptológica se basa en aspectos de la **Teoría de la Información y de la Codificación,** de la **Teoría de números,** de la **Teoría de la Complejidad Algorítmica** y de la **Teoría de la Probabilidad.**

Dentro de la **Teoría de la información** los aspectos mas fundamentales son los conceptos de entropía, entropía condicional, secreto perfecto, distancia de unicidad, confusión y difusión.

De la **Teoría de números** destacaremos la aritmética modular, los logaritmos discretos, el cálculo de inversos, la función de Euler, el teorema chino del resto y el cálculo aritmético en campos de Galois.

La **Teoría de la complejidad algorítmica** trata de la clasificación de los problemas en función de que se conozca o no un algoritmo para su resolución y del tipo de estos algoritmo en función de su tiempo de computación. Es de destacar que la evolución de la tecnología en el campo de la velocidad de cómputo hace que problemas que eran intratables o computacionalmente incalculables años atrás sean hoy día totalmente resolubles en tiempo y costo admisibles.

Por último, la **Teoría de la probabilidad**, aunque importante para algunos aspectos de la Criptografía. es básica para la práctica del Criptoanálisis.

CRIPTOSISTEMAS

Un **criptosistema** o sistema criptográfico está formado por cinco elementos:

1.- **Espacio de mensajes**. Generalmente denominado **M,** es el conjunto de todos los posibles mensajes $\{m_1, m_2, m_3,...\}$ en claro, es decir inteligibles, formados con caracteres de un cierto alfabeto A, siguiendo sus reglas sintácticas y semánticas.

2.- **Espacio de cifrados**. Denominado **C**, está formado por los mensajes cifrados $\{c_1, c_2, c_3,...\}$ utilizando un alfabeto B que puede o no coincidir con A.

3.- **Espacio de claves**. Denominado K y formado por el conjunto $\{k_1, k_2, k_3,...\}$ de las claves utilizadas para el cifrado.

4.- **Familia de transformaciones de cifrado**. Una transformación E_k aplicada a un mensaje del conjunto **M** obtiene un mensaje cifrado dentro del conjunto **C** dependiendo de la clave k empleada.

5.- **Familia de transformaciones de descifrado**. Una transformación D_k utiliza el parámetro k del conjunto **K** para pasar del mensaje cifrado al mensaje en claro.

Durante mucho tiempo las claves de cifrado y descifrado eran las mismas y las transformaciones para descifrar eran las inversas de las transformaciones de cifrado. Esto no tiene por qué ser así; de hecho lo único que tiene que cumplirse es $E_k(D_k(c))=c$.

Pueden existir infinitos sistemas de cifrado pero para que realmente sea útil en la práctica y resistente a los ataques de los criptoanalistas debe cumplir los siguientes requisitos:

1º Las transformaciones de cifrado y descifrado deben ser, para todo el espacio de claves, computacionalmente eficaces y eficientes.

2º La seguridad del sistema debe depender en exclusiva del secreto de las claves y no del secreto de las transformaciones.

De hecho debe desconfiarse de los sistemas de cifrados propietario de firmas de software que mantienen secreto el algoritmo utilizado. Con gran probabilidad son algoritmos débiles que no resistirán un ataque bien organizado de criptoanalistas expertos. Aunque el algoritmo sea de dominio público, la fortaleza del criptosistema se basa en la imposibilidad de inferir la clave de cifrado de la de descifrado, o al revés.

Se distinguen dos tipos de criptosistemas: de **clave privada** y de **clave pública**.

Los **criptosistemas de clave privada**, también llamados simétricos o de clave única, la fortaleza del sistema está en el secreto de la clave k. La pareja emisor-receptor del mensaje comparten el secreto de la clave. El sistema será útil siempre que sea computacionalmente imposible determinar la clave mediante una ataque sistemático aún conociendo las funciones de cifrado y descifrado. Es de advertir que los avances de las tecnologías de los computadores hace que el concepto de incomputabilidad varíe continuamente.

Los criptosistemas de clave privada proporcionan simultáneamente el secreto y la autenticidad de los mensajes; sabemos que su contenido no ha sido modificado ni conocido por persona no autorizada.

Los **criptosistemas de clave pública**, llamados también asimétricos o de dos claves, disponen de dos claves para cada usuario U (la clave **pública** ub y la clave **privada** uv), siendo computacionalmente imposible obtener una de otra. Las Funciones de transformación E y D son conocidas. Quién quiere mandar un mensaje a U lo hace cifrando con la transformación E_{ub}. U descifra el mensaje con la transformación D_{uv}.

En este tipo de criptosistema se proporciona el secreto con la clave ub, pero no puede garantizar la autenticidad, que necesitaría el cifrado mediante la transformación D_{uv}, que sólo conoce el propietario de la clave uv. De todas maneras establecer las dos propiedades simultáneamente mediante la adición de algunos requisitos.

CRIPTOANÁLISIS

Si queremos comprobar la seguridad de un criptosistema hemos de considerar todos los posibles ataques que puede sufrir los mensajes cifrados por parte de personas que no poseen la clave. De hecho en los congresos internacionales no se admite ningún trabajo sobre un nuevo algoritmo que no vaya acompañado del correspondiente criptoanálisis, y no olvidemos que hoy día el criptoanalista posee uno medios muy poderosos de cómputo.

Una de las técnicas más utilizadas es el análisis estadístico de los mensajes cifrados para determinar la frecuencia de aparición de los diferentes símbolos, el tamaño de las palabras, las palabras más comunes, etc.. Por todo ello los criptosistemas que proporcionan una correspondencia uno a uno entre los símbolos de los alfabetos del mensaje y del cifrado son muy vulnerables al criptoanálisis.

Existen principalmente tres métodos de atacar a los criptosistemas: **ataques a partir sólo del texto cifrado, ataques a partir de algún mensaje conocido** y **ataques por elección del mensaje**.

El ataque por elección del mensaje se produce cuando el criptoanalista tiene acceso al sistema informático para introducir mensajes y observado el resultado privado. Por ejemplo el atacante podría introducir un registro apropiado en una base de datos criptografiada y obtener como se ha cifrado la información. Insistimos por tanto en la aplicación conjunta de diversas defensas o medidas de seguridad (control de acceso, autentificación de usuarios, etc) además de las criptológicas.

También es importante para que los criptoanalistas, aunque lleguen a consumar su ataque y obtengan las claves, estas les sean inútiles, el recordar que la fortaleza de los criptosistemas reside en el secreto de las claves. Por ello aparece un problema que suele traer de cabeza a los responsables de seguridad y administradores de sistemas de información: la **generación, administración y distribución de claves**.

CRIPTOGRAFÍA CLÁSICA

El procedimiento más antiguo para cifrar que se conoce es la **escítala lacedemónica**, que usaban los *éforos* de Esparta para comunicarse con sus generales. Consistía en un cilindro de madera de un diámetro determinado en el se enrollaba una cinta de pergamino, en donde se escribía el mensaje a lo largo de la generatriz. Al desarrollar la cinta el mensaje quedaba cifrado, y solamente quedaba en claro si se enrollaba en otro cilindro del mismo diámetro. Los generales espartanos jamás abandonaban su bastón. Hoy día, aunque desconozcan su uso, los altos cargos militares siguen usando la *escítala*: su bastón de mando.

A través de los tiempos se han empleado diversos métodos para cifrar la información, siendo quizás los más curiosos los cifrarios que fueron muy populares entre los siglos XV y XVII.

El método de **sustitución simple monoalfabeto** consiste en sustituir cada letra del texto en claro por otra letra del alfabeto que forma parte del texto cifrado. El método inventado por Julio César es de este tipo y consistía en sustituir cada letra del alfabeto por la situada tres lugares a la derecha (por supuesto cuando se llegaba a la z

se continuaba con la a). En general los diferentes métodos se expresan mediante la transformación:

$$E(m) = (am + b) \bmod n$$

En la **sustitución homofónica** cada letra del alfabeto se sustituye por uno de un conjunto de símbolos llamados homofónicos, siendo estos distintos para cada símbolo del alfabeto inicial. El objetivo es evitar que siempre se cambie un símbolo por el mismo, destruyendo la frecuencia de caracteres típica de un idioma. Por ejemplo a la letra A se le hace corresponder el conjunto de homófonos {13, 25, 34, 50, 95}; cada vez que se vaya a cifrar la A se toma uno de esos números de una forma aleatoria. El más conocido es el Thomas J. Beale en el que los números homofónicos indicaban la posición de una palabra en la *Declaración de Independencia de los Estados Unidos* cuya primera letra es la que corresponde cifrar.

La **sustitución polialfabeto** utiliza una palabra clave cuyas letras definen los desplazamientos que se aplican al mensaje en claro. Veamos un ejemplo con la clave SOL:

Mensaje P	L	A	N	T	A	
Clave	S	O	L	S	O	L
Cifrado I	Z	L	F	I	L	

Los más conocidos métodos de sustitución polialfabeto son los del disco del Leon Battista Alberti (siglo XV), cuadro de Vignére (siglo XVI), cifrado de Beaufort y Autoclave.

Los **cifrados tipo Vernam** se desarrollaron a partir del método diseñado por Gilbert Vernam de AT&T en 1917. El método consiste en combinar una secuencia aleatoria de números no repetitiva con el mensaje en claro, utilizando la secuencia una sola vez. La operación empleada cuando los mensajes estaban en bits para combinar las secuencias era el "O exclusivo".

La **sustitución poligráfica**, en vez de sustituir una letra por otra, sustituye digramas, trigramas, tetragramas, etc. de letras. De esta forma se destruye la frecuencia de los monogramas. Los métodos más famosos de este tipo son los de Playfair (1854) y Hill (1929).

La **transposición** es un método que no efectúa ninguna sustitución de caracteres; lo que hace es cambiar su posición dentro del mensaje. Por ejemplo la escítala lacedemónica corresponde a este tipo. Otros métodos son la permutación por grupos, el posicionamiento en zig-zag y la distribución en figuras geométricas.

Otros tipos utilizado se basan en **métodos aritméticos** (adición y sustracción, multiplicación y división, cambio de base del sistema de numeración), **transformaciones lógicas booleanas** (solo con aquellas que poseen inversa), **transformaciones matriciales** (se pasan los mensajes a bits y se forman matrices de ceros y unos con las que se operan).

No podemos abandonar este paseo por la historia de la criptografía sin mencionar las máquinas de cifrar que pretendían facilitar la labor de los criptógrafos a la hora de cifrar sus mensajes. Por no hace demasiado larga la lista sólo citaremos la famosa máquina de cifrar alemana de la Segunda Guerra Mundial: la **Enigma**. Por cierto, que los británicos lograron luchar contra ella mediante una máquina para criptoanalizar: el **Colossus**.

CRIPTOGRAFÍA DE CLAVE PRIVADA

La característica de los criptosistemas de clave privada o secreta es utilizar la misma clave para el cifrado y el descifrado, por lo que también se llaman simétricos. Como indicamos anteriormente proporcionan secreto y autenticidad. El secreto quedará garantizado si los comunicantes mantienen la clave común en secreto. La autenticidad se consigue al emplear ambos la misma clave y, por lo tanto, sólo el emisor legitimado puede enviar un mensaje cifrado que al descifrarse quede en claro. El principal problema de estos sistemas es el intercambio seguro de las claves, aunque existen algunos protocolos, como el de Diffie-Hellman, que lo facilitan y añaden seguridad. También hay que limitar el número de corresponsales ya que el número de claves aumenta con el cuadrado del número de nodos. Además casi todos los algoritmos de este tipo han sido vulnerados.

Existen dos esquemas principales de cifrado: el **cifrado en flujo** (se cifra cada uno de los bits del mensaje) y el **cifrado en bloque** (se cifran conjuntos de bits).

El más utilizado actualmente de los cifradores en bloque es el DES (Data Encryption Standard) desarrollado por IBM y estándar del NIST (National Institute of Standards and Technology) para las aplicaciones no clasificadas del Gobierno de USA. Aunque parece ser que todavía no ha sido vulnerado, ha sufrido numerosas críticas

por la escasa longitud de su clave (64 bits). De todas formas ISO considera a este algoritmo como una posible norma bajo del nombre de DEA1 (Data Encryption Algoritm 1).

El algoritmo cifra un bloque de 64 bits de texto en claro en un bloque de 64 bits de texto cifrado usando una clave de 8 octetos (64 bits). El último bit de cada octeto de la clave es un bit de paridad impar. El algoritmo consta de 16 iteraciones en las que se usan las operaciones "O exclusivo", permutaciones y sustituciones.

La única forma conocida de ataque es probar las 72.057.594.037.927.936 (2^{56}) claves distintas, lo que para un ordenador que pudiera probar un millón de claves por segundo supondría unos 2.285 años. Este tiempo se reduciría de forma considerable utilizando supercomputadores con muchos procesadores en paralelo (hasta unas pocas horas) y que sólo están al alcance de ciertas organizaciones.

CRIPTOGRAFÍA DE CLAVE PÚBLICA

Se caracterizan por el uso de dos claves por cada miembro del sistema: la **pública** (que sirve para que el resto de los miembros puedan cifrar los mensajes que quieran dirigirle) y la **privada** (que evidentemente es secreta y sirve para recuperar la información).

Se basan en las llamadas **funciones unidireccionales con trampa**. Una función unidireccional es aquella que es *fácil* de calcular mientras que su inversa es *difícil* de computar por su elevada complejidad. Se denomina función unidireccional con trampa a aquellas funciones unidireccionales que pueden ser invertidas fácilmente si se conoce alguna información adicional extra (**trampa**).

Los **cifrados exponenciales** se basan en el uso de la operación de exponenciación sobre campos finitos. Los más conocidos son el de **Pohling-Hellman** y el **RSA**.

El algoritmo debido a Pohling y Hellman en 1978 se basa en el problema NP-completo de la mochila y opera con un número primo p muy grande, realizándose toda la aritmética en el campo de Galois CG(p) o en el campo de Galois CG(2^n), siendo 2^n-1 un número primo muy grande (número de Mersenne).

Para una clave de 200 bits el número de pasos que necesitaría un atacante para violar el sistema sería de 2,7 x 10^{11}, que a un microsegundo por paso supondría

varios días. Si la clave sube a 664 bits (200 dígitos decimales) el número de pasos asciende a $1{,}2 \times 10^{23}$, lo que supondría actualmente 10^{12} años.

El algoritmo debido a Rivest, Shamir y Adleman (1977) se basa en la factorización de un número resultado de multiplicar dos números primos de gran número de cifras. El método proporciona diferentes niveles de seguridad en función de la longitud e la clave, lo que puede ser muy útil para cifrar en función del nivel de secreto del activo.

De los posibles procedimientos de ataque criptoanálitico el más sencillo es el de factorización del número n. Utilizando el algoritmo de Schroeppel se obtienen los siguientes datos en función de la longitud del número a factorizar y suponiendo que cada paso supone 1 microsegundo de computación:

Dígitos	Nº de pasos	Tiempo
50	$1{,}4 \times 10^{10}$	3,9 horas
100	$2{,}3 \times 10^{15}$	74 años
200	$1{,}2 \times 10^{23}$	$3{,}8 \times 10^{9}$ años
500	$1{,}3 \times 10^{39}$	$4{,}2 \times 10^{25}$ años

APLICACIONES CRIPTOGRÁFICAS

La criptología permite realizar con seguridad muchas aplicaciones informáticas en redes de computadores que están revolucionando la sociedad actual y lo harán mucho más en el futuro cuando se regulen legalmente. Entre ellas destacaremos la **firma digital**, las **elecciones electrónicas**, la **autenticidad, integridad y reutilización** de mensajes, la **certificación y notaría electrónicas**, la **firma de contratos**, demostrar el **conocimiento de secretos** sin proporcionar ninguna información de ellos, la **transferencia electrónica de fondos**, el manejo de **tarjetas inteligentes** en cajeros automáticos, etc.

Para la resolución de estos problemas se emplean los algoritmos de clave pública y privada existentes siguiendo protocolos de funcionamiento bien determinado. Un **protocolo** es una secuencia ordenada de pasos a realizar por dos o más entidades para completar una tarea. Entre todos los casos enumerados elegiremos los más llamativos.

Los cifrados de clave pública permiten generar **firmas digitales** que permiten asegurar que un mensaje proviene de quien dice enviarlo, evitando la suplantación de

usuarios. La firma digital electrónica, que no tiene nada que ver con la digitalización de firmas que se realiza cuando se envían fax directamente generados por un computador, es imposible de falsificar. También se garantiza simultáneamente que el mensaje no ha sido alterado, es decir, se garantiza su integridad. La firma digital se añade al mensaje o puede aplicarse a un mensaje completo. Los sistemas más empleados son la firma digital RSA, la firma digital de El Gamal y la firma DSS (Digital Signature Standard).

El **esquema electoral** permite que muchas personas puedan emitir sus votos en una red de computadores de modo que éstos sean contabilizados, que se mantenga el secreto y que el votante pueda verificar que su voto ha sido atribuido correctamente. Las condiciones para el proceso electoral electrónico son:

1º Existe una mesa que legitima el censo de votantes (L) y otra mesa que hace público el resultado (M).
2º Sólo pueden votar los electores censados.
3º Los votos son secretos.
4º Sólo se puede votar una vez.
5º Cada votante podrá verificar su voto.

El protocolo de votación en una red de computadores sería:

1º El votante A envía un mensaje a la mesa L identificándose.
2º L comprueba si A está censado y si es así le envía un número de identificación i(A) y le borra de la lista de votantes.
3º A elige una identificación secreta s(A), una de las opciones a votar v(A) y envía a M su número de identificación, su voto y su identificación secreta.
4º M localiza si i(A) está en el conjunto de los números de identificación de votantes. Si es así, M elimina i(A) de dicho conjunto y añade s(A) al conjunto de electores que votaron por la opción v(A).
5º Finalizado el proceso electoral, M pública en la red el resultado de la votación y las listas de las identificaciones secretas que votaron por cada una de las opciones.

CONCLUSIONES

Como punto de vista personal, después de todo lo expuesto, termino esta ponencia con las siguientes conclusiones:

1º La Criptografía permite prácticamente impedir la comisión del delito.

2º Algunas asignaturas de los estudios de Informática deben de adaptar sus contenidos a las nuevas necesidades. (Por ejemplo, las Matemáticas deben incluir las teorías en las que se basa la Criptología).

3º Los planes de estudios de las titulaciones informáticas deben incluir asignaturas como los Aspectos Legales de la Informática, Seguridad en Entornos Informáticos, Criptología, etc.

4º Implantación de una Política Criptográfica Nacional por los Organismos correspondientes (Defensa, Agencia de Protección de Datos, Justicia, etc.).

5º La creación por el Estado de Notarías Electrónicas u Organismos de Certificación Electrónica.

BIBLIOGRAFÍA

Bauer, F.L. **Decrypted Secrets,** Ed. Springer, Berlin, 1997.

Caballero, P. **Introducción a la Criptografía.** Ed. Ra-ma, Madrid, 1996.

Comisión de Seguridad de Sedisi. **Guía de Seguridad Informática.** SEDISI, Madrid 1997.

Menezes, van Oorschot, Vanstone. **Handbook od Applied Cryptpgraphy.** CRC Press, N. York, 1997

Morant, Ribagorda y Sancho. **Seguridad y Protección de la Información.** Ed. CERASA, Madrid, 1994.

Nombela, J.J. **Seguridad Informática.** Ed. Paraninfo, Madrid 1997.