Introducción a la criptografía

Josep Domingo Ferrer

P05/75024/00985
Módulo 1

UOC
Universitat Oberta de Catalunya

Índice

Introducción 5

Objetivos 6

1. Terminología 7
1.1. Criptosistemas elementales 7
1.2. Resistencia de los criptosistemas 8
1.3. Ataques criptoanalíticos 8
1.4. Ataques a los sistemas de comunicación y a los sistemas informáticos 9

2. Evolución histórica 12
2.1. La criptografía como arte 12
2.2. La criptografía como ciencia moderna 12

3. Aplicaciones de la criptografía 14
3.1. Seguridad de las comunicaciones 14
3.2. Votaciones y contratos electrónicos 15
3.3. Comercio electrónico 16

Resumen 17

Actividades 19

Glosario 19

Bibliografía 19

Introducción

Criptografía es un término de origen griego que proviene de las palabras *krypto* ('esconder') y *grapho* ('escribir'). Podemos decir que la criptografía es la ciencia y el estudio de la escritura secreta.

Inicialmente, la criptografía apareció para resolver la necesidad de comunicarse en presencia de un adversario (normalmente en un contexto militar o diplomático). Actualmente, incluye muchos otros problemas. Por citar sólo algunos, podemos hablar de cifrado, autenticación, distribución de claves, etc.

La criptografía moderna proporciona los cimientos teóricos necesarios para poder:

- Entender exactamente los problemas que acabamos de enumerar.
- Evaluar los protocolos que en teoría pueden resolver estos problemas.
- Construir protocolos en cuya seguridad podamos confiar.

Los protocolos que resuelven los problemas básicos mencionados se pueden utilizar como base para resolver otros problemas más complejos, como los sistemas de pago electrónico seguro, usados en el comercio electrónico, que se valen de protocolos de autenticación y de cifrado.

Objetivos

En los materiales didácticos de este módulo el estudiante encontrará los contenidos necesarios para alcanzar los objetivos siguientes:

1. Conocer la terminología básica utilizada en criptografía.

2. Disponer de una visión histórica de la criptografía.

3. Tomar conciencia de la omnipresencia de la criptografía en el mundo actual.

1. Terminología

Tu as tes procédés d'information que je ne pénètre point.
Guy de Maupassant

Una **cifra** o **criptosistema** es un método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado*. El proceso de transformar texto en claro en texto cifrado se llama *cifrado*, mientras que el proceso inverso, transformar texto cifrado en texto en claro, se denomina *descifrado*. Tanto el cifrado como el descifrado son controlados por una o más claves criptográficas.

* A veces llamado *criptograma*.

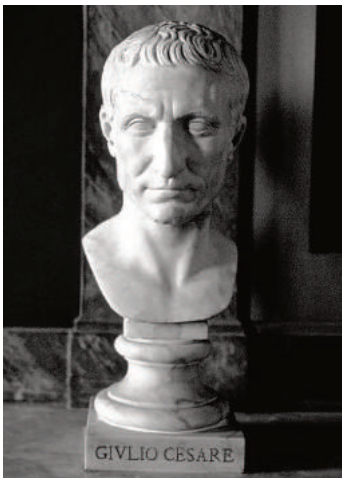
La **criptografía** y una disciplina complementaria denominada **criptoanálisis** se conocen conjuntamente con el nombre de **criptología**. La criptografía se ocupa del diseño del diseño de cifras. El criptoanálisis se ocupa de romper cifras. La motivación del criptoanalista puede ser el interés intrínseco de descubrir el texto en claro cifrado y/o la clave empleada, o bien ser de corte científico-técnico (verificación de la seguridad de la cifra). La vertiente científicotécnica del criptoanálisis es esencial para la depuración de las cifras y resulta muy útil para el progreso de la criptografía.

La necesidad del criptoanálisis...

... está menos reconocida socialmente que la de la criptografía. "Los caballeros no leen el correo de los demás", respondió en 1929 H.L. Stimson, el secretario de estado norteamericano, al enterarse de que su departamento rompía sistemáticamente los telegramas diplomáticos cifrados de diversos países.

1.1. Criptosistemas elementales

Hay dos tipos básicos de cifras: las transposiciones y las sustituciones. A continuación describimos e ilustramos brevemente cada una de estas cifras:



Los secretos de César

La cifra de sustitución del ejemplo se suele llamar cifra de César, porque Julio César la utilizaba con $k = 3$ para comunicarse con Cicerón y otros amigos suyos.

1) Una **cifra de transposición** reordena los bits o los caracteres del texto en claro; la clave de la cifra es el criterio de reordenación utilizado.

Ejemplo de criptosistema de transposición

Considerad la cifra que divide el texto en claro en grupos de k letras e invierte el orden de las letras dentro de cada grupo para obtener el texto cifrado. La clave en este caso es k. Tomando el texto en claro siguiente:

NO HAY MAL QUE POR BIEN NO VENGA

si utilizamos $k = 5$ y descuidamos los espacios en blanco, obtenemos el texto cifrado siguiente:

YAHONUQLAMBROPEONNEIAGNEV

2) Una **cifra de sustitución** cambia bits, caracteres o bloques de caracteres por sustitutos; la clave es el criterio de sustitución utilizado.

Ejemplo de criptosistema de sustitución

Considerad la cifra que desplaza cada letra del alfabeto *k* posiciones adelante (la letra Z se desplaza cíclicamente al inicio del alfabeto). La clave es *k*. Tomando el texto en claro siguiente:

NO HAY MAL QUE POR BIEN NO VENGA

si utilizamos *k* y descuidamos los espacios en blanco, obtenemos el texto cifrado que presentamos a continuación:

RSLECQEPUYITSVFMIRRSZIRKE

1.2. Resistencia de los criptosistemas

Según la resistencia que tengan a los ataques de los criptoanalistas, las cifras, o criptosistemas, se pueden clasificar de la manera siguiente:

a) Cifras rompibles o débiles: cifras para las que el criptoanalista tiene bastantes recursos de cálculo a fin de determinar el texto en claro o la clave a partir del texto cifrado, o para determinar la clave a partir de parejas de texto en claro/texto cifrado.

b) Cifras computacionalmente seguras o fuertes: cifras que no pueden ser rotas a partir de un análisis sistemático con los recursos de que dispone el criptoanalista.

c) Cifras incondicionalmente seguras: una cifra lo es si, independientemente de la cantidad de texto cifrado interceptada por el criptoanalista, el texto cifrado no ofrece información suficiente para determinar el texto en claro de manera única.

De hecho, tan sólo hay una cifra incondicionalmente segura y veremos que en muchas situaciones no es práctica. El resto de cifras conocidas se pueden romper si los recursos de cálculo del enemigo son ilimitados. Por lo tanto, es más interesante hablar de cifras computacionalmente seguras.

Podéis ver la cifra incondicionalmente segura en el subapartado 3.1 del módulo "Fundamentos de criptografía" de esta asignatura.

1.3. Ataques criptoanalíticos

Existen cuatro métodos básicos de ataque criptoanalítico:

1) En un **ataque con sólo texto cifrado**, el criptoanalista tiene que encontrar la clave basándose sólo en el texto cifrado que ha podido interceptar. Se puede suponer que el método de cifrado, la lengua en la que está escrito el texto en claro y algunas palabras probables son conocidas.

Para hallar la clave...

... de un texto que se sabe que en claro es una orden financiera, el criptoanalista explotará el hecho de que probablemente incluirá palabras como "comprar", "vender", "euro", etc.

2) En un **ataque con texto en claro conocido**, el criptoanalista sabe unas cuantas parejas de texto en claro/texto cifrado e intenta deducir su clave o algún texto en claro de que no conoce.

Ejemplos de ataque con texto en claro conocido

Supongamos que utilizamos cifrado en nuestras sesiones *telnet* contra un sistema Unix. Un espía que intercepte nuestros mensajes sabe que en una determinada posición aparecerá la forma cifrada de la palabra *login* y en otra, la forma cifrada de *password*. Además, sabe que es probable que más adelante aparezca la forma cifrada de algunos mandatos como *ls*, *pwd*, *whoami*, etc.

Los programas (código fuente) cifrados son otro ejemplo vulnerable a ataques con texto en claro conocido. En efecto, el criptoanalista sabe que buena parte del texto cifrado corresponde a palabras reservadas del lenguaje.

3) En un ataque **con texto en claro escogido**, el criptoanalista que intenta deducir la clave es capaz de adquirir el texto cifrado correspondiente a un texto en claro escogido por él mismo. Este ataque constituye la situación más favorable para el criptoanalista, y es, por lo tanto, el más peligroso. Las bases de datos que guardan la información en forma cifrada se prestan a este tipo de ataques si el enemigo puede insertar registros en claro y observar los cambios en el texto cifrado almacenado.

4) Un **ataque con texto cifrado escogido** sólo tiene sentido en criptosistemas de clave pública, en los que una de las dos transformaciones de cifrado/descifrado son públicas. En esta modalidad de ataque, el criptoanalista es capaz de adquirir el texto en claro correspondiente a un texto cifrado escogido por él mismo. Aunque es poco probable que el texto en claro que ha obtenido sea inteligible, puede ayudar a deducir la clave.

Podéis ver los criptosistemas de clave pública en el apartado 4 del módulo "Criptosistemas de clave pública" de esta asignatura.

Actualmente se considera que una cifra ofrece una seguridad aceptable sólo si puede resistir un ataque con texto en claro conocido en que el criptoanalista tiene un número arbitrario de pares texto en claro/texto cifrado.

1.4. Ataques a los sistemas de comunicación y a los sistemas informáticos

Los ataques criptoanalíticos intentan romper el algoritmo de cifrado suponiendo el conocimiento de una determinada información. Ahora bien, normalmente se necesita un ataque de tipo informático para obtener la información necesaria a la hora de montar un ataque criptoanalítico. De hecho, si el ataque informático es lo bastante hábil, puede ser que no haya que recurrir al criptoanálisis. Imaginemos que un pirata informático consigue entrar en nuestro ordenador y leer el fichero donde guardamos la clave de nuestra cifra.

Para preparar un ataque criptoanalítico, suele ser necesario montar conjuntamente un ataque informático.

La criptografía protege datos enviados por un medio de comunicación o guardados en un sistema informático. La protección tiene dos vertientes:

- El **secreto** o la **privacidad**, que permite preservar la confidencialidad de los datos, es decir, impedir cualquier revelación no autorizada.

- La **integridad** o **autenticidad**, que impide la modificación no autorizada de los datos.

Los **ataques a los sistemas de comunicación** por donde circulan datos cifrados consisten en escuchas y se pueden distinguir dos tipos:

1) Los **ataques contra el secreto**, que consisten en la llamada **escucha pasiva***. El enemigo se limita a interceptar el texto cifrado, normalmente sin ser detectado, con la finalidad de deducir su clave o el texto en claro. El uso de buenos métodos de cifrado puede impedir este tipo de ataques.

*** En inglés, *eavesdropping*.**

2) Los **ataques contra la autenticidad**, que consisten en la llamada **escucha activa***. El enemigo se dedica a modificar mensajes interceptados o a insertar otros completamente inventados, con la finalidad de que el receptor acepte como buenos los mensajes modificados o inventados. La criptografía no puede impedir que el enemigo haga este tipo de ataques (por ejemplo, que vuelva a insertar un texto cifrado anterior), pero permite que el receptor los detecte.

*** En inglés, *tampering*.**

Los **ataques a un sistema informático** en que se guardan datos cifrados también atentan contra el secreto y la autenticidad:

1) Los **ataques contra el secreto** pueden ser de tres tipos diferentes:

a) El **barrido de memoria**, que hace referencia a la busca de información confidencial en el almacenaje primario (memoria) o secundario (disco).

b) La **filtración**, que es la transmisión de datos confidenciales a usuarios no autorizados por parte de procesos con acceso legítimo a los datos en claro.

c) El **ataque de inferencia**, que intenta deducir información confidencial sobre un individuo a partir de la correlación de estadísticas publicadas sobre grupos de individuos.

Un ataque de inferencia...

... puede servir para deducir el sueldo de un analista de sistemas concreto a partir del sueldo medio de los analistas de sistemas de la empresa.

2) Los **ataques contra la autenticidad** incluyen los dos tipos siguientes:

a) La **falsificación**, que consiste en modificar, insertar o borrar datos.

b) La **destrucción accidental**, que hace referencia al borrado o la sobrescritura no intencionada de datos.

3) Los **ataques mixtos**, que básicamente se reducen al llamado **enmascaramiento**. Si un usuario consigue entrar al sistema con la cuenta de otro usuario, puede acceder a información confidencial del otro usuario (ataque contra el secreto) y hacerse pasar por el otro usuario ante terceros (ataque contra la autenticidad). El almacenamiento de las contraseñas en forma cifrada contribuye a dificultar el enmascaramiento, pero hay que tomar precauciones suplementarias.

Mientras que la falsificación puede ser detectada (no impedida) por técnicas criptográficas, la destrucción accidental puede pasarnos inadvertida incluso si utilizamos la criptografía.

La criptografía puede hacer estéril el barrido de memoria, pero no puede combatir por sí sola la filtración y la inferencia.

Las técnicas criptográficas son suficientes ante los ataques contra los sistemas de comunicación. En cambio, necesitan ser complementadas por controles de acceso para contrarrestar los ataques contra los sistemas informáticos.

2. Evolución histórica

Desde la antigüedad hasta la aparición de los ordenadores, la criptografía fue más un arte que una ciencia. La aparición del ordenador forzó la revolución científica de las técnicas criptográficas.

2.1. La criptografía como arte

El periodo que va desde la antigüedad hasta el año 1949 se puede denominar *era de la criptografía precientífica*. Se trataba más de un arte que de una ciencia, lo cual no significa que careciera de interés. Ya hemos comentado que Julio César usaba una cifra de sustitución. No hay pruebas que demuestren que Bruto hubiera roto esta cifra, pero es obvio que ahora cualquier chiquillo con nociones de latín no tendría problema para desarrollar un ataque con sólo texto cifrado sobre unas cuantas frases cifradas. De hecho, durante casi dos mil años después de César, los criptoanalistas se desenvolvían mejor que los criptógrafos.

Ataque a la cifra del César

Para romper la cifra de César, sólo hay que comparar las frecuencias de las letras en el texto cifrado con las frecuencias de las letras en latín clásico; entonces se sabe a qué letra corresponde la A, la B, etc.

En 1926, un ingeniero de la compañía norteamericana AT&T llamado G.S. Vernam publicó una cifra destacable para ser usada con el código binario de Baudot. Como la de César, la **cifra o criptosistema de Vernam** consiste en sumar una clave K aleatoria al texto en claro M para obtener el texto cifrado C. La diferencia es que M, C y K adoptan valores en $\{0, 1\}$ y que la suma es módulo 2 (es decir, una *o exclusiva*):

$$C = M \oplus K.$$

La innovación fundamental introducida por Vernam consistió en utilizar la clave sólo una vez, es decir, cifrar cada bit de texto en claro con un nuevo bit de clave escogido al azar. Eso requiere la transferencia segura (con mensajeros armados, por ejemplo) de emisor a receptor de tantos bits de clave como texto en claro deseemos cifrar más tarde. A pesar de este inconveniente, veremos que ésta es la única cifra incondicionalmente segura*.

*** Esta propiedad fue intuida, pero no demostrada, por Vernam.**

Durante la Segunda Guerra Mundial, momento en que el uso de la criptografía se generalizó, empezó a reconocerse que las matemáticas podían ser útiles en criptografía y en criptoanálisis.

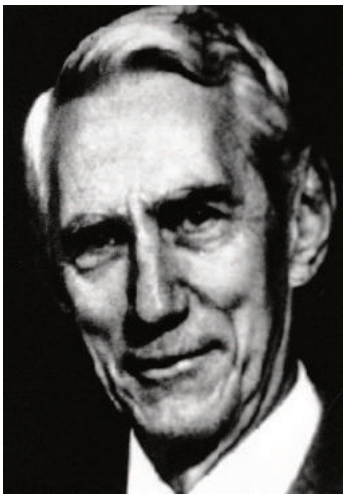
Turing y el Enigma

Durante la Segunda Guerra Mundial, un equipo de matemáticos encabezado por el inglés A.M. Turing (inventor de la máquina que lleva su nombre) fue el encargado de romper la cifra alemana basada en las máquinas de rotores Enigma.

2.2. La criptografía como ciencia moderna

La publicación el año 1949 por parte de C.E. Shannon del artículo "Communication Theory of Secrecy Systems" inauguró la **era de la criptología**

científica de clave compartida. Shannon, que era ingeniero y matemático, elaboró una teoría de los sistemas secretos casi tan completa como la teoría de las comunicaciones que había publicado el año anterior. Entre otras cosas, el artículo de 1949 demostraba la seguridad incondicional de la cifra de Vernam. Pero a diferencia del artículo sobre comunicaciones de 1948, que hizo nacer la teoría de la información como disciplina, el artículo de 1949 no supuso un impulso similar para la investigación criptográfica.



Claude Elwood Shannon (1916-2001), matemático norteamericano.

La eclosión real de la criptografía se produce con la publicación en 1976 por parte de W. Diffie y M.E. Hellman del artículo "New Directions in Cryptography". Diffie y Hellman mostraron por primera vez que era posible una comunicación secreta sin ninguna transferencia de clave secreta entre el emisor y el receptor, lo cual inició la **época de la criptografía de clave pública** en la que nos encontramos actualmente.

3. Aplicaciones de la criptografía

Actualmente, la criptografía está omnipresente en la vida cotidiana, aunque de una manera silenciosa. Desarrollos de una actualidad tan candente como la telefonía móvil, la televisión de pago o el comercio electrónico no serían viables sin las técnicas criptográficas. En particular, el desarrollo de sistemas de comercio electrónico seguro es una actividad que absorbe en estos momentos una buena cantidad de mano de obra informática.

En este apartado pretendemos dar una visión rápida y estimulante de algunas de las aplicaciones más vistosas de la criptografía. Confiamos en que eso estimulará al alumno a seguir adelante con la asignatura.

3.1. Seguridad de las comunicaciones

El objetivo primordial de la criptografía consiste en proporcionar seguridad en las comunicaciones y, en la medida de lo posible, seguridad en los sistemas informáticos. A continuación vemos algunos campos concretos donde hay que aplicarla:

1) En una red de **paquetes conmutados** como IP o X.25, la seguridad de la información transmitida se puede conseguir con un cifrado de enlace (al nivel de enlace de la jerarquía OSI) o bien extremo a extremo (en los niveles altos de la jerarquía OSI). En el caso de un cifrado de enlace se necesitan equipos de cifrado en cada nodo de la red. En el caso de un cifrado extremo a extremo, los equipos terminales son los encargados de hacer el cifrado y el descifrado.

El correo electrónico seguro...

... implementado por paquetes tan conocidos como *Pretty Good Privacy* (PGP) o *Privacy Enhanced Mail* (PEM), es un ejemplo de cifrado extremo a extremo en el nivel de aplicación.

2) La **telefonía móvil** es otra gran consumidora de criptografía. Los primeros sistemas de telefonía móvil no utilizaban ningún tipo de cifrado, a semejanza de la telefonía fija. La diferencia, sin embargo, entre ambos sistemas es que una llamada de un teléfono móvil puede ser escuchada sin necesidad de pinchar ningún cable: basta con un equipo sintonizador. Actualmente, las distintas tecnologías de teléfonos móviles (GPS, GPRS, 3G, etc.) utilizan algoritmos de cifrado en flujo que permiten cifrar y descifrar la comunicación en tiempo real.

Los peligros de los móviles

En su día, fue muy comentada la interceptación de conversaciones comprometedoras mantenidas por dirigentes socialistas españoles con teléfonos móviles sin cifrado.

3) La **televisión de pago** es una aplicación de la criptografía que se puede ver tanto desde el punto de vista de la seguridad de las comunicaciones como desde el punto de vista del comercio electrónico. En efecto, es preciso proteger los contenidos televisivos respecto a los espectadores que no están abonados. Los descodificadores habituales son en realidad dispositivos descifradores. Al igual que en el caso de la telefonía móvil, se utiliza una cifra en flujo que permite cifrar y descifrar las imágenes en tiempo real.

3.2. Votaciones y contratos electrónicos

Una **votación electrónica** es una votación en la cual el votante no se desplaza físicamente a un colegio electoral para votar, sino que vota por medio de su terminal, que está conectada a una red. Los problemas de seguridad que plantea la votación electrónica son complejos:

1) Sólo a los votantes autorizados se les tendría que permitir votar y éstos sólo podrían hacerlo una sola vez. En un colegio electoral, el votante presenta un documento acreditativo, se comprueba si aparece en la lista del censo y, en caso afirmativo, se hace constar. Realizar este procedimiento de manera electrónica requiere proporcionar una credencial electrónica al votante y mantener la integridad del censo. Las técnicas criptográficas pueden satisfacer estos requerimientos.

2) El voto ha de ser secreto. En un colegio electoral, el votante deposita su voto en un sobre cerrado antes de meterlo en la urna. La criptografía puede ayudar a mantener el secreto del voto en un entorno electrónico.

3) No debería ser posible duplicar ningún voto. A diferencia de los votos de papel en una urna, la copia de votos electrónicos es trivial si no se utiliza la criptografía.

4) El votante tiene que poder comprobar que su voto se ha tenido en cuenta. Cuando depositamos un voto de papel en la urna, sabemos que los interventores y la mesa no permitirán que se descarte nuestro voto. En un entorno electrónico, tendríamos que tener la misma tranquilidad.

La **firma electrónica de contratos** plantea unos problemas similares a los de la votación electrónica. En efecto, firmar un contrato sobre papel de manera

presencial es trivial: dos partes A y B se reúnen en una sala; A no deja marcharse B hasta que A no obtiene una copia del contrato firmada por B; igualmente, B no deja marcharse A hasta que B no obtiene una copia del contrato firmada por A.

Veremos que hay técnicas criptográficas que permiten firmar documentos en formato electrónico. Ahora bien, sin la presencia física de las dos partes interesadas en la misma sala, ¿cuál osará firmar en primer lugar el contrato electrónico? Si no se recurre a una tercera parte de confianza (notario electrónico), podría suceder que B obtuviera una copia del contrato firmado por A, y que A, en cambio, se quedara sin nada. Para resolver este problema, existen protocolos criptográficos que aseguran que ambas partes se encuentran en igualdad de condiciones durante todo el proceso de firma del contrato.

3.3. Comercio electrónico

Al igual que las votaciones y los contratos electrónicos, el comercio electrónico es otro paso hacia la informatización de las relaciones socioeconómicas. Ya hemos visto que la pérdida de presencia física en las relaciones humanas genera problemas de seguridad complejos. El comercio electrónico no es una excepción y tampoco sería viable sin la criptografía.

El problema básico del comercio electrónico es el pago: ¿cómo se puede pagar por medio de una red? La manera usual de hacer transacciones monetarias por Internet es, hoy día, enviando el número de la tarjeta de crédito. Eso tiene inconvenientes si lo comparamos con el pago en efectivo: por una parte, nos pueden cobrar más de lo que queríamos pagar; por la otra, el pago no es anónimo: el cliente se identifica cada vez que hace una compra y por lo tanto el vendedor sabe quién compra qué. En su artículo "Untraceable electronic mail, return addresses, and digital pseudonyms", D. Chaum sugirió un protocolo criptográfico para obtener **dinero electrónico** que no supusiera ningún inconveniente respeto al dinero convencional.

Cuando la mercancía objeto de comercio electrónico es información en formato digital (música, libros, películas, etc.) aparece otro problema, el de la **protección del *copyright***. En efecto, si fotocopiar papel ya es fácil, copiar información en formato digital es trivial, barato y está al alcance de cualquiera. La criptografía difícilmente puede impedir la piratería informática, pero puede ayudar a identificar a los piratas.

La supresión de la presencia física en las relaciones socioeconómicas sería inviable por razones de seguridad sin la existencia de la criptografía.

Resumen

Con la aparición de los primeros ordenadores, la criptografía deja de ser un arte milenario y se convierte en una ciencia cuyo objetivo básico consiste en permitir la comunicación y el almacenamiento seguro de información en presencia de un adversario. Junto con este **objetivo básico de secreto o privacidad**, la criptografía moderna permite resolver el **problema de la autenticidad o integridad de la información**.

Una **cifra** o **criptosistema** transforma un texto en claro en un texto cifrado o criptograma. Los procesos de cifrado y de descifrado son controlados por una o más claves, que suelen ser secretas. Las cifras elementales se basan en transposiciones y en sustituciones.

En función de la seguridad, las cifras se pueden clasificar en débiles, fuertes e incondicionalmente seguras. El **criptoanálisis** tiene como objetivo romper una cifra determinando su clave a partir del texto en claro y del texto cifrado; según el conocimiento que se supone tiene el criptoanalista, hay diversos **tipos de ataque criptoanalítico**.

Aparte de los ataques criptoanalíticos, es preciso considerar los **ataques a los sistemas informáticos y de comunicaciones**. A diferencia de los ataques criptoanalíticos, esta modalidad de ataques no se basa en la explotación de las debilidades de los algoritmos de cifrado. La idea es aprovechar debilidades de los sistemas informáticos o de las comunicaciones para recuperar la clave o el texto en claro.

Las **aplicaciones de la criptografía moderna** van mucho más allá de la seguridad de las comunicaciones militares y diplomáticas. Con respecto a comunicaciones seguras, la criptografía permite garantizar la seguridad de las redes abiertas, del correo electrónico y de la telefonía móvil. Procesos como las votaciones, la firma de contratos, etc., también pueden realizarse de manera electrónica y sin coincidencia física de las partes mediante técnicas criptográficas.

Actividades

1. Identificad en vuestro entorno algún dispositivo que utilice el cifrado.

2. ¿Los piratas informáticos se valen de ataques criptoanalíticos o de ataques a los sistemas informáticos y de comunicaciones?

3. Buscad en Internet información sobre los programas analizadores de tráfico (en inglés, *sniffers*), que permiten al usuario de una estación que está conectada a una red local rescuchar el tráfico que circula por dicha red.

4. ¿Qué problemas de seguridad plantea efectuar una votación de manera electrónica? ¿Cómo se resuelven estos problemas en las votaciones convencionales?

Glosario

ataque *m* Estrategia o método que tiene por objetivo descubrir la clave de cifrado o bien el texto en claro. Los ataques criptoanalíticos explotan las debilidades de los algoritmos de cifrado. Los ataques a los sistemas informáticos y de comunicaciones explotan la vulnerabilidad de estos sistemas.

autenticidad *f* Propiedad de encontrarse, en relación con la información, en el mismo estado en que fue producida, sin modificaciones no autorizadas. Es sinónimo de integridad.

autenticación *f* Comprobación de la autenticidad.

cifra *f* Método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado.
sin: criptosistema

cifra de sustitución *f* Cifra basada en cambiar los bits o los caracteres del texto en claro por sustitutos.

cifra de transposición *f* Cifra basada en reordenar los bits o los caracteres del texto en claro.

cifrado *m* Proceso de transformación de un texto en claro en un texto cifrado.

clave *f* Parámetro, normalmente secreto, que controla los procesos de cifrado y/o de descifrado.

criptoanálisis *m* Ciencia que se ocupa de romper cifras, es decir, de descubrir la clave o el texto en claro usados como entradas de la cifra.

criptografía *f* Ciencia y estudio de la escritura secreta.

criptograma *m* Texto cifrado.

criptología *f* Denominación conjunta de la criptografía y del criptoanálisis.

criptosistema *m* Cifra.

descifrado *m* Proceso de transformación del texto cifrado en texto en claro.

integridad *f* Propiedad de no haber sufrido, en relación con la información, modificaciones ni supresiones parciales no autorizadas.

privacidad *f* Derecho de las personas a salvaguardar su intimidad, especialmente con respecto a los datos de que disponen las entidades públicas o privadas.

Bibliografía

Denning, D. E. (1982). *Cryptography and data security*. Reading: Addison-Wesley.

Fuster, A.; de la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. (1997). *Técnicas criptográficas de protección de datos*. Madrid: Ra-ma.

Simmons, G. J. (1992). *Contemporary cryptology: the science of information integrity*. Nueva York: IEEE Press.