

Criptografía y Seguridad en Comunicaciones

Jordi Forné, José Luis Melús y Miguel Soriano
Departamento Matemática Aplicada y Telemática
Universitat Politècnica de Catalunya

1. INTRODUCCIÓN

Las redes de comunicaciones actuales permiten la conectividad de un gran número de usuarios que pueden estar situados en cualquier parte del mundo, tanto para transmisión de voz (red telefónica), imágenes (redes de distribución de televisión, TV via satélite) como para la transmisión de datos entre ordenadores (redes locales, metropolitanas, así como redes a nivel mundial, como por ejemplo Internet). La explosión de servicios ofrecidos por estas redes, especialmente las de datos, ha incrementado la dependencia de individuos y organizaciones de la transmisión de datos por estas redes. Esta dependencia ha despertado la conciencia de la necesidad de protección de la información y de garantizar la autenticidad de datos y mensajes.

En este artículo se presentan las amenazas a la seguridad en redes de transmisión de datos, así como los servicios de seguridad requeridos y los mecanismos necesarios para proveer estos servicios. Entre estos mecanismos destacan los criptográficos, tanto los sistemas convencionales (simétricos) como los de clave pública, concepto introducido en 1976 que produjo una revolución en el mundo de la criptología. Por último se introducen algunos de los algoritmos y aplicaciones criptográficas más extendidos en la actualidad o que de los que se prevee una mayor utilización en los próximos años.

2. AMENAZAS, MECANISMOS Y SERVICIOS DE SEGURIDAD

AMENAZAS

Las amenazas a la seguridad en una red de comunicaciones pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como pueda ser un fichero o usuario, a un destino, que pudiera ser otro fichero o usuario, tal como se muestra en la Figura 1. Los cuatro tipos genéricos de ataques a la seguridad son los siguientes:

- *Interrupción:* Una parte del sistema resulta destruida o no disponible en un momento dado. Ejemplos de este tipo de ataque pueden ser la destrucción de una parte del hardware o el corte de una línea de comunicación.
- *Intercepción:* Una entidad no autorizada accede a una parte de la información. La parte no autorizada puede ser una persona, una máquina o un programa. Ejemplos claros de este tipo de ataques son la escucha del canal, ya sea el típico "pinchazo" de la línea telefónica, la intercepción via radio de comunicaciones móviles o la copia ilícita de ficheros o programas transmitidos a través de redes de datos utilizando analizadores de redes.
- *Modificación:* Una entidad no autorizada no sólo accede a una parte de la información, sino que además es capaz de modificar su contenido. Ejemplos de estas modificaciones son la alteración de ficheros de datos, alteración de programas y modificación de mensajes mientras son transmitidos por la red.
- *Fabricación:* Una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo.

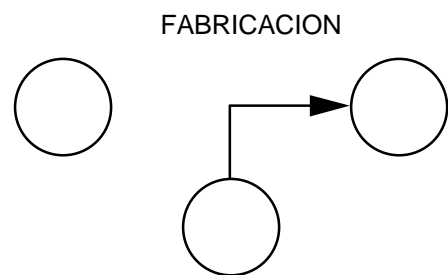
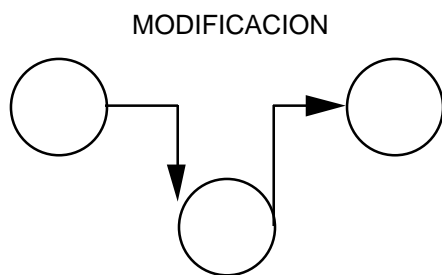
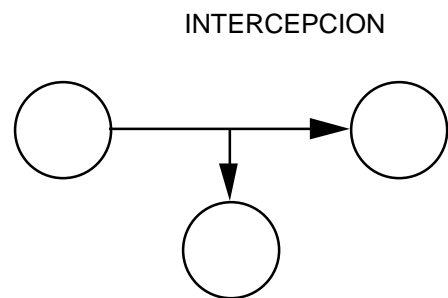
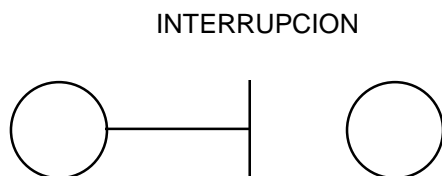
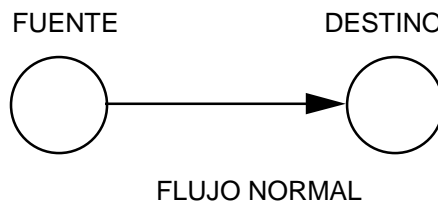


Figura 1. Amenazas a la seguridad

Otra clasificación útil es dividir los ataques en términos de pasivos y activos. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

En los ataques activos el atacante altera las comunicaciones. Pueden subdividirse en cuatro categorías: suplantación de identidad, donde el intruso se hace pasar por una entidad diferente; reactuación, donde uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no autorizado; modificación de mensajes, donde el intruso varía los datos transmitidos y degradación fraudulenta del servicio, donde el intruso intenta impedir que los entes dialogantes puedan realizar correctamente su función, mediante destrucción o retardo de mensajes o la introducción de mensajes espúreos con el fin de congestionar la red.

SERVICIOS DE SEGURIDAD

Para hacer frente a las amenazas a la seguridad del sistema, se definen una serie de servicios que realzan la seguridad de los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

- *Confidencialidad:* Requiere que la información sea accesible únicamente por las entidades autorizadas.
- *Autenticación:* Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa.
- *Integridad:* Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos.
- *No repudio:* Requiere que ni el emisor ni el receptor del mensaje puedan negar la transmisión.
- *Control de acceso:* Requiere que el acceso a la información sea controlado por el sistema destino.

-Ninguno de estos servicios anteriores fue concebido específicamente para entornos de comunicación de datos. Todos ellos tienen analogías no electrónicas, que emplean mecanismos familiares a cualquier persona, como se muestra en la siguiente tabla.

Servicio de seguridad	Ejemplo mecanismo no electrónico
Autenticación	Carné con identificación fotográfica. Huellas dactilares.
Control de acceso.	Llaves y cerrojos.
Confidencialidad	Tinta invisible. Carta lacrada.
Integridad.	Tinta indeleble.
No repudio	Firma notariada. Correo certificado.

MECANISMOS DE SEGURIDAD

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- *Intercambio de autenticación.* Corroborar que una entidad, ya sea origen o destino de la información, es la deseada.
- *Cifrado.* Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados.
- *Integridad de datos.* Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir. Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.
- *Firma digital.* Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía al receptor junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad.
- *Control de acceso.* Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.

- *Tráfico de relleno.* Consiste en enviar tráfico espúreo junto con los datos válidos para que el enemigo no sepa si se está enviando información, ni qué cantidad de datos útiles se está transfiriendo.
- *Control de encaminamiento.* Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

En la siguiente tabla se muestra una relación de los mecanismos de seguridad y los servicios de seguridad que hacen uso de ellos.

	Autenticación	Control de acceso	Confidencialidad	Integridad	No repudio
Intercambio de autenticación	S	N	N	N	N
Cifrado	S	N	S	S	N
Firma digital	S	N	N	S	S
Integridad de datos	N	N	N	S	S
Control de acceso	N	S	N	N	N
Tráfico de relleno	N	N	S	N	N
Control de encaminamiento	N	N	S	N	N

3. SISTEMAS CRIPTOGRAFICOS

Los sistemas de protección física son un mecanismo práctico para salvaguardar los equipos terminales de posibles ataques. Sin embargo, dada la dispersión geográfica de los sistemas de transmisión en redes, una protección de este tipo conllevaría un alto coste económico, haciéndolos totalmente desaconsejables en estos casos. Los sistemas criptográficos, por otra parte,

son muy útiles para la seguridad en redes de datos, ya que permiten paliar muchas de las posibles vulnerabilidades que estas presentan.

En Figura se presenta un esquema de la transmisión segura de un mensaje M entre dos entidades, a través de un canal inseguro.

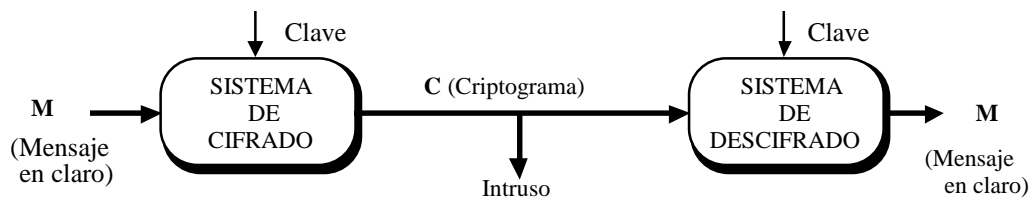


Figura 2. Esquema de transmisión segura de un mensaje

Los sistemas criptográficos de este esquema son los encargados de calcular el mensaje cifrado C, a partir del mensaje en claro M y de la "clave de cifrado"; y de realizar el proceso inverso, el descifrado, y así determinar M a partir del mensaje cifrado y la "clave de descifrado". Estas dos claves, como ya veremos más adelante, no tienen que ser necesariamente iguales.

Cuando un sistema criptográfico utiliza en el descifrado la misma clave que en el cifrado, se dice que utiliza un "cifrado simétrico". Por el contrario, si la clave de descifrado es distinta a la clave de cifrado el sistema estará empleando un "cifrado asimétrico".

Un sistema de criptografía simétrico es una familia de transformaciones inversibles (E_k) , donde emisor y receptor usan la misma clave k. La clave k ha tenido que ser puesta previamente en conocimiento de las dos partes mediante el uso de un canal secreto. Esta clave necesita, pues, ser distribuida con antelación a la comunicación. El coste y el retardo, impuestos por esta necesidad, son los principales obstáculos para la utilización de la criptografía de clave secreta en grandes redes.

Entre los algoritmos simétricos podemos destacar los de cifrado en bloque y los de cifrado de flujo. Estos últimos son los más indicados para entornos de alta velocidad de transmisión. Los algoritmos simétricos de cifrado en bloque son los más usados en redes de datos, y se pueden clasificar entre públicos y privados. El algoritmo simétrico público más utilizado en la práctica es el DES (*Data Encryption Standard*), aunque existen otros algoritmos secretos estandarizados por organismos americanos, europeos, etc.

En un sistema de clave pública, el cifrador utiliza una clave P , mientras que el descifrador utiliza una clave distinta S . La clave P es pública, y la clave S es privada e incalculable a partir de P en un tiempo prudente. El sistema asimétrico posibilita la comunicación en un sentido; para realizar la comunicación en sentido contrario se necesita otro par de claves secreta-pública. La principal característica que hace interesantes a estos métodos frente a los sistemas criptográficos simétricos, es que no necesita el intercambio de secretos entre los dos comunicantes. Los algoritmos de clave pública se basan en la teoría de números y de cuerpos finitos. Gracias a este fundamento matemático es posible demostrar la seguridad computacional de estos métodos.

Los algoritmos de clave pública sólo se utilizan para cifrar comunicaciones en los que la velocidad no sea un requisito crítico. Ésto se debe a la baja velocidad de cifrado que presentan las realizaciones de estos algoritmos. Por tanto, como en la distribución de claves la velocidad no es crítica, estos algoritmos son útiles para la transmisión de claves por medios inseguros entre sistemas que utilicen algoritmos simétricos. Uno de los algoritmos asimétricos más utilizados es el *RSA (Rivest-Shamir-Adleman)*.

3.1. Criptosistemas simétricos.

Los criptosistemas simétricos se caracterizan por el hecho que se emplea la misma clave en las transformaciones de cifrado y descifrado. Para proporcionar confidencialidad, un criptosistema simétrico actúa de la siguiente forma. Dos sistemas A y B desean comunicarse de forma segura, y mediante un proceso de distribución de claves, ambos comparten un conjunto de bits que será usado como clave. Esta clave será secreta para cualquier otro individuo, entidad,... distinto de A y de B. Así pues, cualquier mensaje intercambiado entre A y B irá cifrado usando dicha clave.

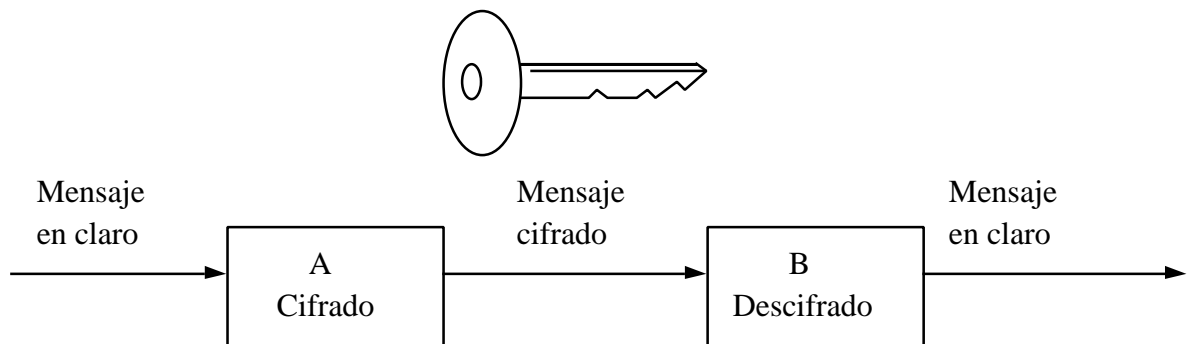


Figura 3. Criptosistema simétrico

Los criptosistemas simétricos han sido utilizados en redes comerciales desde el principio de los 70. El estándar americano DES (Data Encryption Standard) es el criptosistema de este tipo que mayor popularidad ha alcanzado.

Data Encryption Standard (DES).

Durante 1973 y 1974 hubo muchas solicitudes a la Oficina Nacional de Estandarización de Estados Unidos “National Bureau of Standards” para que se elaborase un algoritmo de cifrado estándar para su uso en agencias federales estadounidenses que tuviesen que manejar información sensible. De entre todas las propuestas, se eligió uno presentado por IBM y tras una serie de revisiones públicas, fue adoptado como estándar en 1977. El algoritmo se utilizó rápidamente para ofrecer confidencialidad en aplicaciones gubernamentales y para garantizar la integridad en la industria financiera.

El algoritmo DES emplea una clave de 56 bits y opera con bloques de datos de 64 bits. El proceso de cifrado ejecuta una permutación inicial al texto en claro, y aplica 16 veces una función que depende de la clave. Una de las controversias generadas con el DES es precisamente si la longitud de la clave es suficientemente grande o no. El algoritmo se basa en permutaciones, sustituciones y sumas módulo 2. Las permutaciones son de tres tipos.

- Directas: Reordenamiento de bits.
- Expandidas: Algunos bits se duplican y el conjunto se reordena.
- Selecciones permutadas: Algunos bits se desprecian y el resto se reordena.

Las sustituciones en el DES son conocidas como cajas S y están especificadas en ocho tablas diferentes. El algoritmo es el mismo para cifrar que para descifrar.

3.2. Criptosistemas de clave pública.

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman de la Universidad de Stanford en 1976. A diferencia de los criptosistemas simétricos, los algoritmos de clave pública utilizan pares de claves complementarias para separar los procesos de cifrado y descifrado. Una clave, la privada, se mantiene secreta, mientras que la clave pública puede ser conocida. El sistema tiene la propiedad que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Este enfoque con dos claves permite

simplificar la gestión de claves, minimizando el número de claves que deben ser gestionadas y permitiendo su distribución a través de sistemas no protegidos. En una red con n usuarios, si se usa cifrado de clave simétrica se precisan $n(n-1)/2$ claves, mientras que si se emplea cifrado de clave pública bastan $2n$ claves.

Potencialmente hay dos modos de uso de los criptosistemas de clave pública, dependiendo del uso que se haga de la clave privada (cifrado o descifrado). Por una parte cualquier usuario puede enviar un mensaje de forma confidencial a un receptor (p.e. B) cifrando su contenido con la clave pública del receptor, que será el único capaz de descifrarlo por ser el único concededor de la clave privada (en caso contrario la gestión de claves estaría mal hecha. Por otro lado cualquier usuario (p.e. A) puede autenticar el origen y contenido de un mensaje cifrandolo con su clave secreta, ya que prueba su identidad como único poseedor de esta clave. Cualquier receptor puede verificar la autenticidad del mensaje descifrándolo con la clave pública del emisor. La Figura 4 ilustra el proceso.

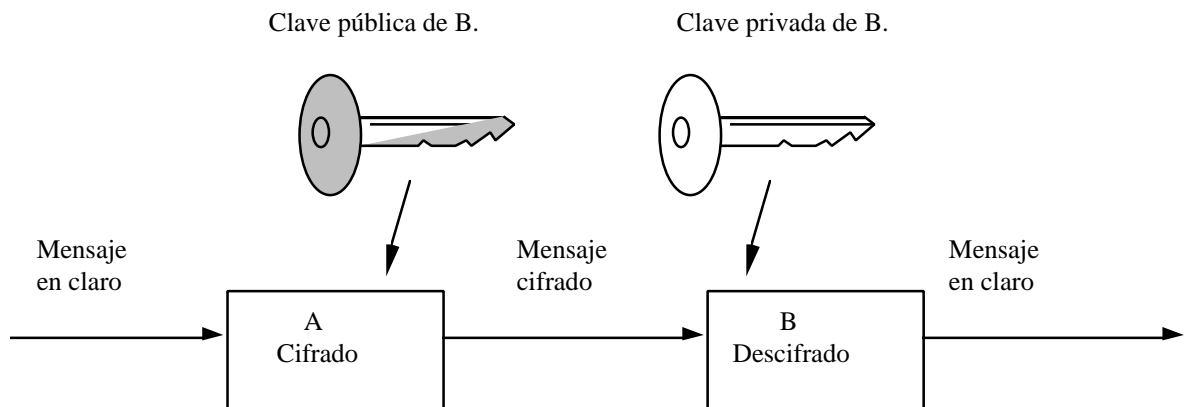


Figura 4a. Confidencialidad mediante criptografía de clave pública

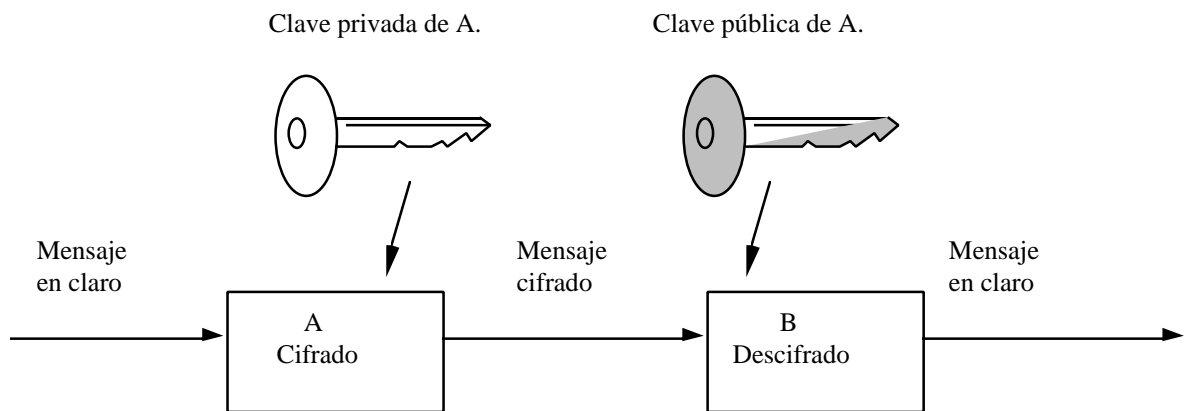


Figura 4b. Autenticación mediante criptografía de clave pública

Los criptosistemas de clave pública ofrecen muchas más posibilidades a los diseñadores que los de clave simétrica. La idea fundamental de los criptosistemas de clave pública consiste en utilizar funciones unidireccionales con trampa (trapdoor one-way function). Una función $y=f(x)$ se denomina unidireccional si:

- A cada valor de x le corresponde una y .
- Dado un valor de x es fácil calcular la y .
- Dado un valor de y es difícil calcular la x .

Se dice que un problema es “fácil” o “difícil” en función del coste de CPU que precise su resolución. Una función $y=f(x)$ se denomina unidireccional con trampa si:

- A cada valor de x le corresponde una y .
- Dado un valor de x es fácil calcular la y .
- Dado un valor de y es fácil calcular la x conociendo cierta información (clave) y difícil sin esta información.

Una de las primeras candidatas a función unidireccional con trampa fue el logaritmo discreto. El cálculo de la función exponencial discreta $y=a^x \text{ mod } p$, $1 < x < p$, es relativamente fácil de cálculo, incluso para valores grandes de x . En cambio, su función inversa, el logaritmo discreto $x=\log_a y \text{ mod } p$ es difícilmente calculable si p es primo y $p-1$ tiene un factor primo grande.

Algunos problemas que generan funciones unidireccionales, y algoritmos que hacen uso de ellos se presentan en la siguiente tabla:

BASADOS EN ...	ALGORITMO
Logaritmos discretos.	Diffie-Hellman Massey - Omura. ElGamal
Factorización	R.S.A.
Logaritmos elípticos	Miller.
Residuosidad cuadrática	Métodos probabilísticos

Algoritmo R.S.A.

Se trata de un criptosistema asimétrico basado en la dificultad de factorizar grandes números.

Construcción: Cada usuario se define de la siguiente forma:

- Halla dos primos p y q secretos.
- Calcula $n=p \cdot q$ y lo publica.
- Elige un número e aleatorio, co-primo con la función de Euler¹ $\phi(n)$ y lo publica.
- Calcula d , inverso de e modulo $\phi(n)$, y lo mantiene secreto.

¹ $\phi(n)$ indica el número de elementos del conjunto $(1, \dots, (n-1))$ coprimos con n



A desea enviar mensaje M a B de forma confidencial:

$$C = M^{e_B} \pmod{n_B} \longrightarrow C^{d_B} \pmod{n_B} = M$$

A desea enviar mensaje M a B de forma auténtica:

$$C = M^{d_A} \pmod{n_A} \longrightarrow C^{e_A} \pmod{n_A} = M$$

Fundamentos del método: El método se basa en la dificultad de obtener d a partir de e. d sólo se puede hallar a partir de $\phi(n)$, lo cual es fácil si se conocen p y q. Si no se conocen p y q, para hallar $\phi(n)$ se requiere la factorización de n (es una función trampa).

Consideraciones adicionales:

- p y q deben ser grandes (100 cifras decimales) y su tamaño debe diferir en algunas cifras.
- (p-1) y (q-1) deben contener un factor primo grande.
- El máximo común divisor de (p-1) y (q-1) debe ser pequeño.

Ejemplo:

$p = 47. \quad q = 59. \quad \implies \quad n = 2773.$
 $\phi(n) = 2668 \quad e = 17 \quad \implies \quad d = 157.$
 Cifrado $M = 920 \quad C = 920^{17} = 948.$
 Descifrado $M = 948^{157} = 920.$

4. ALGORITMOS Y APLICACIONES

Aparte del DES y el RSA, presentados anteriormente, los algoritmos criptográficos de los que se prevee una mayor utilización para ofrecer los servicios de confidencialidad y autenticidad en redes de datos son el IDEA (International Data Encryption Algorithm), desarrollado como esquema de cifrado convencional más seguro que el DES; el SKIPJACK, propuesto por la administración norteamericana y que se implementa en el polémico chip Clipper; y el LUC, un criptosistema de clave pública comparable al RSA en cuanto a seguridad y funcionalidad.

De todas las aplicaciones de red, el correo electrónico es la usada más ampliamente. Por ello existe una gran demanda de servicios de confidencialidad y autenticación para esta aplicación. Actualmente existen dos esquemas que probablemente alcanzarán una gran expansión en pocos años: PGP (Pretty Good Privacy) y PEM (Privacy-Enhanced Mail).

PGP es el esfuerzo de una única persona, Phil Zimmermann, y provee servicios de confidencialidad y autenticación que pueden ser usados por aplicaciones de correo electrónico y de archivo de ficheros. Esta disponible libremente a través de Internet para un gran número de plataformas, que incluyen DOS, Windows, UNIX y Macintosh entre otras. Además utiliza algoritmos que se han mostrado altamente seguros al examen público durante años. En concreto utiliza RSA para cifrado con clave pública, IDEA para cifrado simétrico y MD5 como función de hash.

Por otra parte, PEM es un borrador de estándar Internet que provee servicios de seguridad para aplicaciones de correo electrónico y posibilita varios esquemas de distribución de claves. Es un servicio extremo a extremo transparente a los distintos elementos intermedios de transmisión de correo. El diseño de PEM permite el empleo de distintos algoritmos criptográficos. Para ello los mensajes incluyen identificadores de los algoritmos usados. Para proporcionar integridad, se añade un código de hash calculado mediante MD2 o MD5. Se emplea cifrado asimétrico, el algoritmo usado es RSA y el código de hash constituye una firma digital. Si se emplea cifrado simétrico se utiliza el algoritmo DES. El servicio de confidencialidad se consigue siempre mediante cifrado simétrico utilizando el algoritmo DES.

5. CONCLUSIONES

Este artículo pretende ser una introducción al apasionante mundo de la criptografía y la seguridad en las comunicaciones. Lógicamente han quedado muchos temas sin abordar, como por

ejemplo el control de acceso mediante tarjetas inteligentes y los protocolos y algoritmos utilizados para autenticación. No conviene olvidar que, si bien la criptografía se inició para ofrecer el servicio de confidencialidad en entornos militares, hoy en día los servicios de integridad y confidencialidad tienen una gran importancia en entornos comerciales, ya que permiten transacciones electrónicas, confirmación de pedidos y reservas, y un largo número de operaciones sobre red que sin duda revolucionarán el mundo de los negocios en los próximos años.