Ingeniería 1 (2): 69-76, 1991 San José Costa Rica

CRIPTOSISTEMAS

Geovanny A. Delgado C. *

Resumen

Este trabajo presenta los principales aspectos de la seguridad en las comunicaciones haciendo uso de sistemas de encubrimiento de datos, comunmente conocidos como criptosistemas.

Inicialmente se presentan algunas definiciones importantes de los criptosistemas, además de varios conceptos básicos para el cifrado de datos. Se analizan dos esquemas criptográficos: el convencional y el de llave pública.

En la última parte se analiza un método de encripción en cada esquema: el DES para criptografía convencional y el RSA para criptografía con llave pública. El análisis de estos métodos se enriquece con un ejemplo particular en cada uno de ellos.

Summary

This article presents the main aspects involved in comunications security using data encription systems, comonly know as criptosystems.

In first place, we examine some basic definitions in criptosystems, as well as several basic concepts in data encription. We study in particular two criptographic systems: a basic or standard scheme, and the public key system.

Later, we present in some details a encription method: The DES metohd for the basic criptography, and the RSA method for the public key criptography. The analysis in each case is enhanced with an example.

1. ENCRIPCION: DEFINICION Y CONCEPTOS BASICOS

La encripción de datos se puede definir como el método de encubrir alguna información con el objetivo de mantenerla asegurada contra agentes ajenos, que puedan apropiarse de ella, utilizarla o alterarla. Este "encubrimiento" se lleva a cabo mediante la definición de alguna codificación o llave. El criptoanálisis es, por lo tanto, el estudio de los datos con el objeto de descubrir la técnica de codificación del mensaje utilizada.

Históricamente la encripción se ha utilizado como una poderosa herramienta en la seguridad de sistemas de información. De ahí que, con el avance tecnológico, han sido desarrollados complejos sistemas de seguridad de datos, tal como los equipos de seguridad criptográfico [1] y tarjetas de encripción para computadores personales. Paralelo al advenimiento de estos equipos se han desarrollado sofisticados métodos de encripción, tal como los criptosistemas de llave pública [2].

La encripción de datos es un tema muy antiguo en el problema de la transmisión secreta de mensajes. Generalmente el objetivo fundamental de la encripción es desarrollar una clave fácil de implementar pero segura. Un ejemplo simple e interesante es el caso de la clave malespín utilizada por un revolucionario salvadoreño que luchó en una revuelta en Nicaragua, esta clave debía ser recordada fácilmente por los seguidores del general Malespín y se propuso las siguientes reglas simples: 1) La letra **a** debía ser cambiada por el letra **e** y viceversa. 2) La letra **i** debía ser cambiada por la letra **o** y viceversa. 3) La letra **b** debía ser cambiada por la letra **t** y viceversa. 4) La letra **m** debía ser cambiada por la letra **p** y vicersa. De esta histórica y sencilla clave militar a los costarricenses sólo nos queda el legado de las palabras buenos y malos, que en malespín se diría tuanis y pelis.

En principio es necesario establecer una base linguística para la definición de algunos términos de uso común en la práctica de la encripción de datos. Se define el cifrador (del inglés "cipher") como un algoritmo que se implementa, con una base de ejecución símbolo por símbolo, sobre un conjunto de datos. Los términos "encriframiento" y "encripción" se refieren a la aplicación de un cifrador a una base de datos. Un algoritmo de

* Profesor de la Escuela de Ingeniería Eléctrica Universida de Costa Rica.

encripción es cualquier algoritmo que implementa un cifrador. La entrada a un algoritmo de encripción se conoce como texto normal, mientras que su salida se conoce como texto encriptado o texto cifrado.

2. ESQUEMAS PARA ENCRIPCION DE DATOS

2.1 Esquema Criptográfico Convencional

En un esquema de comunicaciones se tiene, en general, una arquitectura en la que participa un TRANSMISOR, un CANAL y un RECEPTOR. El emisor contará con algún medio de encripción de datos para asegurar la integridad de su mensaje ante la presencia de posibles intrusos en el canal de comunicaciones. Consecuentemente el receptor debe contar con un medio para descifrar la información recibida.

La arquitectura básica de un sistema de comunicaciones que utiliza alguna técnica de encripción de datos se presenta en la *Figura No.1.*

El transmisor genera un mensaje en texto no cifrado T, el cual será comunicado a un receptor legítimo por medio de un canal de comunicaciones no seguro, monitoreado por algún intruso. Para evitar que el intruso se apodere de la información transmitida, el transmisor encripta T con una transformación revertible E_K para generar un mensaje encriptado o texto cifrado $C = E_K\{T\}$. El receptor legítimo puede recuperar el mensaje transmitido mediante una transformación inversa D_K. La transformación E_K es elegida de una familia de transformaciones $\{ E_K \}$ indexadas por el parámetro K conocido como LLAVE. La familia de transformaciones puede ser generada a partir de algún algoritmo o partir de una circuitería especialmente diseñada para tal efecto; consecuentemente la llave se elige como variable cargada por un programa o mediante la configuración de un circuito por medio de un conjunto de microinterruptores mecánicos.

La seguridad de todo el sistema de comunicaciones reside en mantener la privacidad de la llave. Para ello la llave debe hacerse llegar a los usuarios por algún medio protegido tal como correo certificado o courier. Debe notarse que en el esquema presentado en la *Figura No. 1* el intruso es PASIVO, en virtud de que no altera la información, únicamente la monitorea.

Mientras que el sistema de CRIPTOGRAFIA descrito es muy importante para proveer seguridad, en las aplicaciones comerciales [3] la AUTENTICACION es más importante. En la *Figura No. 2* se presenta el esquema básico de un sistema de AUTENTICACION CRIPTOGRAFICA, en este caso el intruso presente en el canal de comunicaciones no solo está en capacidad de interceptar el mensaje transmitido, sino que además puede alterarlo. A este tipo de intruso se le conoce como intruso ACTIVO. El receptor podrá recuperar el mensaje transmitido por medio de un decifrador el cual recibe el texto encriptado más algunas modificaciones o inclusiones de información por parte del intruso activo. A la salida del decifrador

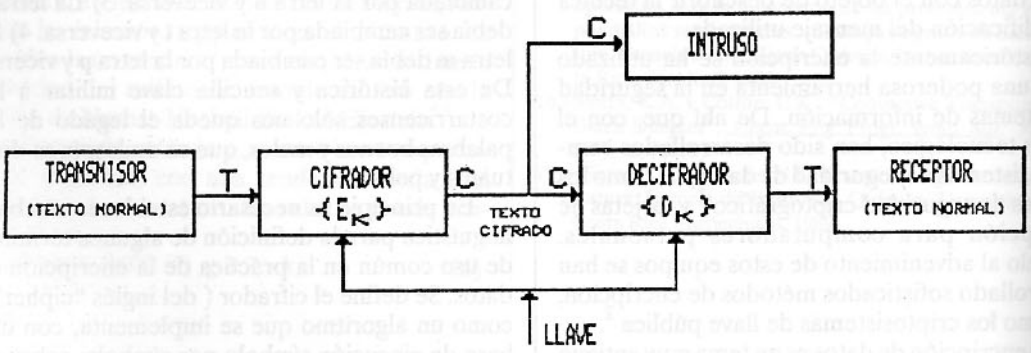

FIGURA No. 1. Esquema básico de un sistema de comunicaciones que utiliza alguna técnica convencional de encripción de datos.

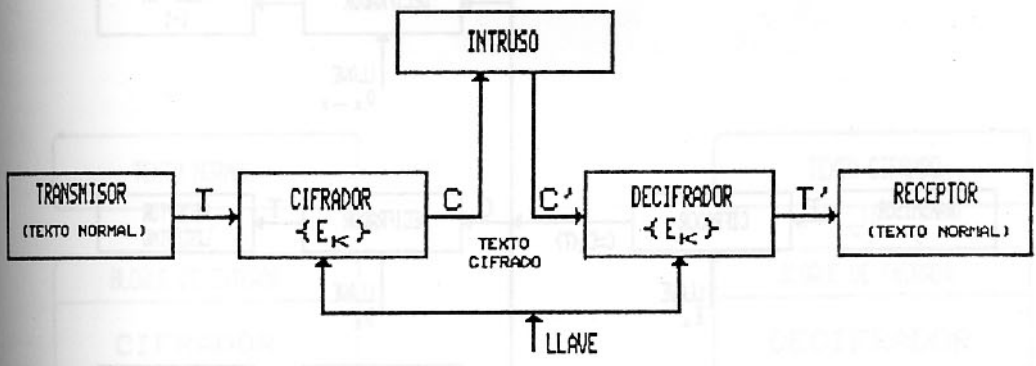

FIGURA No. 2 Esquema básico de un sistema de comunicaciones que utiliza alguna técnica convencional de Autenticación de datos.

se recupera solo aquella información que se logró convertir en texto puro por medio de algún método de decifrado.

Existen varias técnicas de encripción por métodos convencionales, entre las que se destacan la técnica de sustitución, la técnica de trasposición y principalmente el estándar de encripción DES (Data Encryption Standar).

2.2 ESQUEMA CRIPTOGRAFICO DE LLAVE PUBLICA

En el sistema de encripción convencional el transmisor utiliza la misma llave para cifrar que el receptor para decifrar; el éxito en la seguridad del método de transmición depende de la privacidad de esta llave, además tanto el transmisor como el receptor deben conocerla. Un inconveniente importante en este método de cifrado se presenta cuando la llave debe ser modificada frecuentemente, por razones de seguridad, ya que, los costos y retardos en la distribución de la nueva llave se hacen inmanejables.

La solución al problema del cifrado convencional la presentaron Diffie y Hellman [4] en 1976, quienes propusieron el uso del Sistema de LLave Pública, el cual utiliza dos llaves, una pública y otra secreta. En este sistema la habilidad de cifrar mensajes por medio de una llave pública es independiente de la habilidad de decifrar mensajes por medio de otra llave secreta.

El Sistema de LLave Pública, entonces, se implementa con la utilización de dos llaves E_K y D_K, para cada usuario, cada una de las cuales es la inversa de la otra, pero ninguna de las cuales es derivable a partir de la otra. La llave pública E_K es utilizada por los usuarios transmisores para encriptar datos y enviarlos por el canal de comunicaciones inseguro, mientras la llave secreta D_k es utilizada por el usuario destinatario para decifrar los mensajes enviados hacia él.

Un esquema de comunicaciones que utiliza el Sistema de LLave Pública se presenta en la *Figura No. 3*. Sobre el canal de comunicaciones, cualquier transmisor j puede enviar un mensaje T cifrado en la llave pública Ei, donde $C = Ei\{T\}$, sin embargo, solo el destinatario legítimo está en capacidad de decifrar este mensaje utilizando la llave secreta Di, ya que, $T = Di\{C\} = Di\{Ei\{T\}\}$.

Nótese que cualquier usuario puede encriptar mensajes T de la forma: $C = Ei(T)$ y enviarlos por el canal de comunicaciones, sin embargo, solo el destinatario legítimo puede decifrarlos; esto trae consigo privacidad pero no autenticación, en virtud de que cualquier usuario conoce Ei. De esta forma, la ventaja fundamental de este método sobre la encripción convencional es que se hace innecesario el envio de las llaves por un canal privado.

Si se considera ahora que un texto normal T es cifrado con la llave secreta Di, entonces $C = Di\{T\}$ y se tiene un sistema de firma digital: solo el transmisor puede enviar mensajes encriptados con la llave privada Di; esto genera autenticación pero no privacidad, pues todos los usuarios conocen como decifrar el mensaje (Ei). En este caso cualquier usuario puede reconocer la firma pero

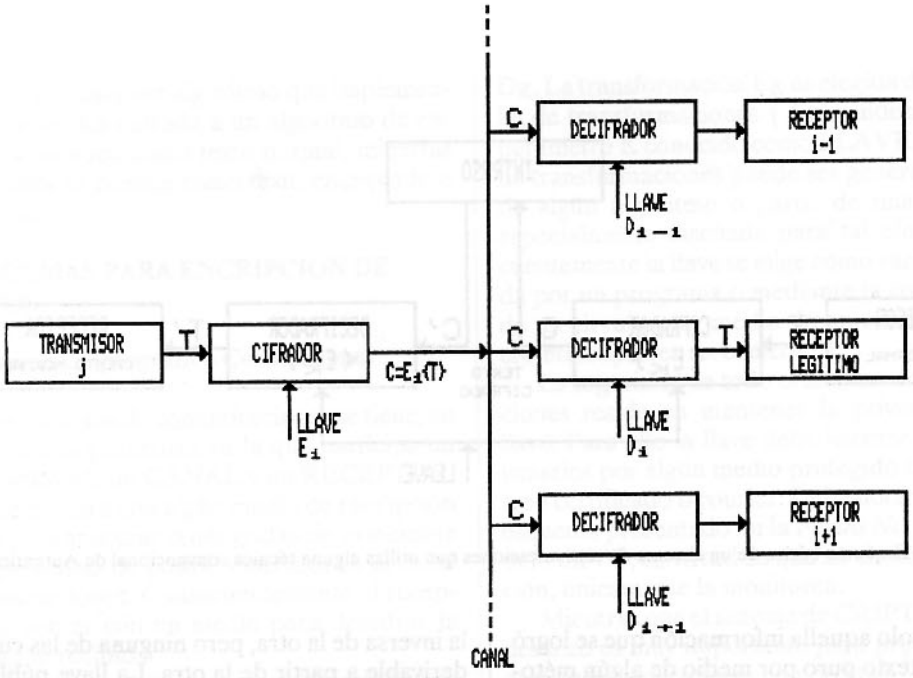

FIGURA No. 3. Esquema general de un criptosistema de llave publica

solo el dueño de la llave puede consignar un mensaje. En este modo el sistema opera como una firma escrita: solo una persona puede poner su firma, pero cualquiera puede reconocerla.

En última instancia se puede presentar un esquema en el que se satisfaga tanto la privacidad como la autenticidad. Supóngase que se desea enviar un mensaje privado y protegido a un usuario j desde un emisor i, entonces el emisor i encripta el mensaje T con su firma digital (Di{T}) y lo transmite con la llave pública del usuario j, o sea, C = Ej{Di{T}}. El usuario j puede encontrar qué persona realizó el envío, con la utilización de su llave privada, es decir, C' = Dj{C} = Dj{Ej{Di{T}}} = Di{T}, este mensaje C' puede ser almacenado como prueba de autenticidad; adicionalmente el usuario j puede recuperar el mensaje original transmitido con la llave pública de i, o sea, C" = Ei{C'} = Ei{Di{T}} = T.

Cuando se utiliza un criptosistema de llave pública, la llave Ei puede ser publicada en un directorio, similar al directorio telefónico, mientras que la llave secreta es privada. Para generar las llaves en este sistema existen varias técnicas tales como la técnica de Elementos Idempotentes, el método de Diffie-Hellman, el método de Rabin o la popular técnica RSA (Rivest-Shamir-Adleman) .

3. METODOS PARA LA CRIPTOGRAFIA DE DATOS

3.1 El Estandar de Encripción de datos (DES)

En 1977 la Oficina Nacional de Estándares de los Estados Unidos de Norteamérica (NBS) adoptó un estándar para la encripción de datos desarrollado originalmente por IBM; este estándar se llamó DES (del inglés " Data Encryption standard "). El DES es la elección más popular para la encripción de datos utilizada en equipo comercial de seguridad [5]. Este algoritmo de criptografía fue aceptado también por ANSI en 198[6]

Existen varios modos de operación de este estándar, desarrollados en función de lograr diferentes grados de dificultad para la ruptura de sus llaves y considerando su posible implementación por medio de circuitería. Sin embargo, todos coinciden en su estructura básica; el DES es una compleja sucesión de permutaciones y sustituciones aplicadas a bloques de 8 bytes (64 bits), bajo el control de llaves variables de 64 bits, de los cuales los 54 bits menos significativos son la llave y los restantes son bits de control de paridad. En el algoritmo DES el cifrado y decifrado de los

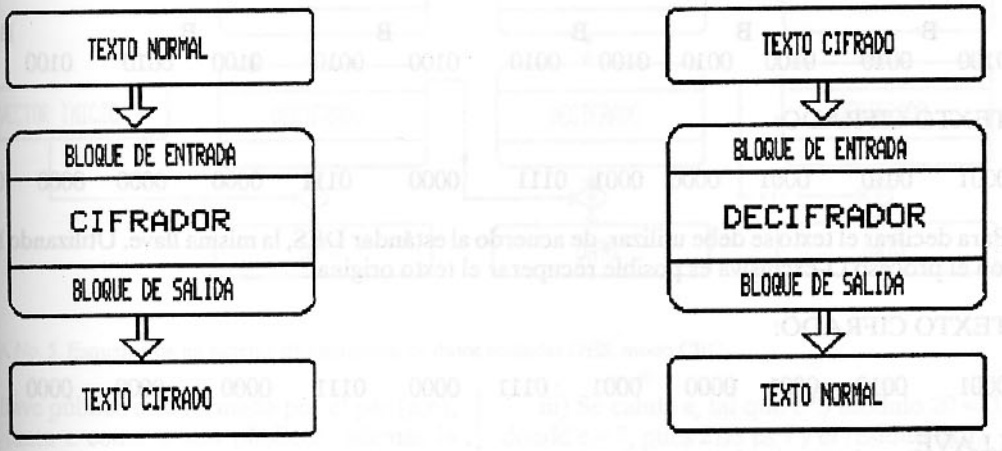

FIGURA No. 4. Esquema de un sistema de encripción de datos estándar DES, modo ECB.

datos se realiza con una sola llave, es decir es un esquema convencional de encripción de datos.

El primer modo de operación del estándar DES es el más sencillo, comunmente conocido como "Libro Electrónico de Códigos (ECB)". En este modo de operación el bloque de texto normal es cargado en un registro de entrada del DES, al cual se le aplica la llave de 64 bits para producir un texto cifrado en un registro de salida; esta operación se muestra en la *Figura No. 4.* Un mismo texto normal produce el mismo texto cifrado a una llave dada. La posible complejidad del método de cifrado de la llave incrementa la probabilidad de error en la transmisión del bloque cifrado, de igual forma si uno de los 54 bits menos significativos de la llave es erróneo, este error se propagará por el bloque completo, sin embargo, no afectará a los otros bloques de datos a transmitir. Para ello se requiere que las fronteras de los distintos bloques de datos a cifrar sean claramente delimitadas, lo que trae como consecuencia rígidos protocolos de control y formatos de mensaje.

Para suprimir la necesidad de fronteras rígidas en los bloques de datos, se desarrolló otro modo de operación, dentro del estándar DES, conocido como "Cifrado por Cadena de Bloques (CBC)". En este modo de operación el texto normal es aplicado a una operación lógica de O-exclusiva con el texto cifrado del bloque anterior, como se muestra en la *Figura No.5.* Nótese, sin embargo, que en este caso un error en un bit se propagará a lo largo del mensaje; la consecuencia inmediata es un incremento de la tasa de error, que, en muchas aplicaciones, no es aceptable.

Otros modos de operación dentro del estándar DES utilizan métodos de encripción por fila [7], tales como el el método " Encripción Realimentada (CFB)", ó " Salida Realimentada (OFB)".

Un aspecto final del análisis del estándar DES es la implementación de la llave, para ello considérese el esquema básico de encripción, del modo de operación ECB, el cual consiste en un sencillo sumador módulo 2, o sea una operación lógica O-exclusiva con la llave.

Supóngase que se cuenta con una simple llave de un caracter: B (lo cual, evidentemente, no es una llave del estándar DES), cuya representación hexadecimal del código ASCII es 0100 0010. Utilizando esta llave es posible encriptar, por medio de una operación O-exclusiva, con el texto normal. A continuación se presenta la encripción del mensaje PRUEBA con la llave B:

TEXTO NORMAL:

P		R		U		E		B		A	
0101	0000	0101	0010	0101	0101	0100	0101	0100	0010	0100	0000

LLAVE:

B		B		B		B		B		B	
0100	0010	0100	0010	0100	0010	0100	0010	0100	0010	0100	0010

TEXTO CIFRADO:

0001	0010	0001	0000	0001	0111	0000	0111	0000	0000	0000	0010

Para decifrar el texto se debe utilizar, de acuerdo al estándar DES, la misma llave. Utilizando la llave B, con el proceso O-exclusiva es posible recuperar el texto original:

TEXTO CIFRADO:

0001	0010	0001	0000	0001	0111	0000	0111	0000	0000	0000	0010

LLAVE:

B		B		B		B		B		B	
0100	0010	0100	0010	0100	0010	0100	0010	0100	0010	0100	0010

TEXTO NORMAL:

P	R	U	E	B	A						
0101	0000	0101	0010	0101	0101	0100	0101	0100	0010	0100	0000

Debe notarse que el uso de estos métodos no asegura completamente el mensaje, en virtud de que un criptoanálisis estadístico del mensaje puede dar rapidamente con la llave. Este análisis estadístico se basa en la estructura del lenguaje, de acuerdo a patrones conocidos como el "qu","ión", ect, así como la probabilidad de ocurrencia de las letras. En un esquema tan sencillo como el presentado, un criptoanalista puede dar con la llave con un método "violento", ya que, solo existen 256 llaves posibles.

3.2 METODO DE ENCRIPCION DE LLAVE PUBLICA RSA

El RSA es un método que se hizo muy popular desde su propuesta por Rivest, Shamir y Adleman en 1978. En este método el objetivo es cifrar y descifrar de acuerdo a dos llaves: una pública, que se denotará como (e,n), y otra privada, que se denotará por (d,n). Además se requiere un método de implementación criptográfica a partir de estas llaves.

Para la determinación de estas llaves, el RSA parte de la elección aleatoria de dos números primos muy grandes, denotados por p y q; a partir de los cuales se calcula "n", como el producto de los mismos, es decir:

$$n = p*q$$

Partiendo de p y q se elige aleatoriamente un número grande d, tal que d sea relativamente primo a (p-1)*(q-1), es decir que el máximo común divisor de d y (p-1)*(q-1) sea 1.

Finalmente para la determinación de las llaves se determina "e", tal que: e*d módulo ((p-1)*(q-1)) = 1. La notación "x módulo y" es igual al residuo de dividir x por y, utilizando división entera. Por ejemplo, 22 módulo 4 = 2, 6 30 módulo 6 = 0.

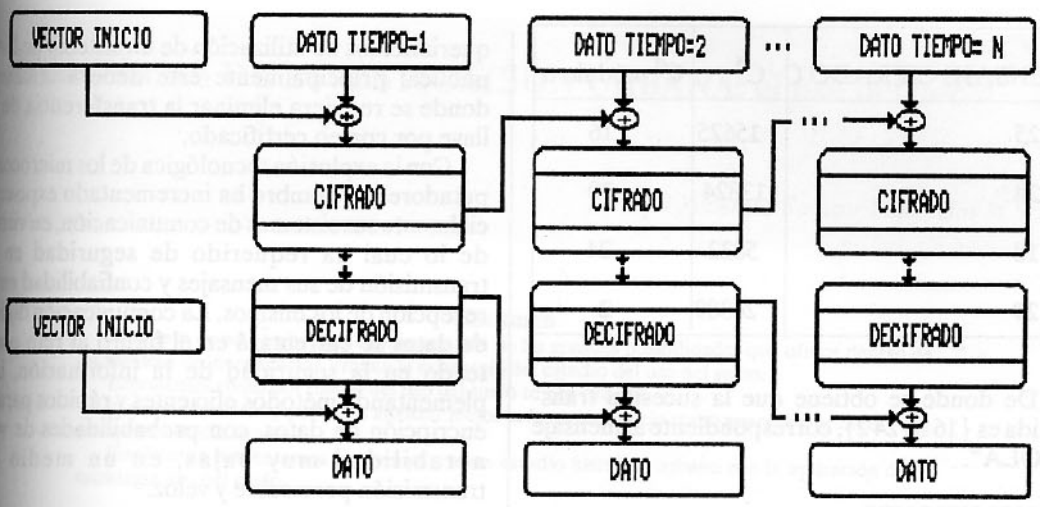

FIGURA No. 5. Esquema de un sistema de encripción de datos estándar DES, modo CBC.

La llave pública está formada por el par (e,n), donde tanto **e** como **n** son públicos; además la llave privada está formada por el par (d,n). La seguridad del método consiste en que no es fácil determinar **d**, a partir de **e** y **n**, pues no existen métodos eficientes de factorización de números grandes. Por tal motivo, se recomienda[8] que tanto p como q sean números muy grandes, de al menos 100 dígitos, para asegurar que **n** es grande, de al menos 200 dígitos.

El método de encripción RSA, a partir de las llaves, se inicia descomponiendo el texto normal en bloques que se puedan representar como números enteros entre 0 y (n-1), denotados por **P**. Luego se encripta el bloque elevando su número entero correspondiente a la potencia "**e**" en módulo "**n**", es decir:

$C = P^e$ módulo n

Donde C es el texto cifrado.

Para decifrar el texto encriptado, este se eleva a la potencia "**d**" en módulo **n**, es decir:

$P = C^d$ módulo n.

Donde P es la representación por números enteros del mensaje.

Para aclarar estos conceptos considérese el siguiente ejemplo:

i) Supóngase que se eligen los números primos: p= 11 y q= 3, entonces el número n=p*q, es n=33.

ii) Dado que (p-1)*(q-1) = 20, se elije arbitariamente d=3, pues 3 es relativamente primo a 20.

iii) Se calula **e**, tal que e*3 módulo 20= 1, de donde e=7, pues 21/3 es 7 y el residuo es 1.

iv) Finalmente la llave pública es (7,33) y la llave privada es (3,33).

Para realizar la encripción de los datos se asignan números enteros a los caracteres a transmitir, por ejemplo, si se asigna la sucesión ascendente de números pares dada por {2 4 6 8 .... 50} a la sucesión de las letras del alfabeto { A B C D ... Z}, el mensaje "HOLA" se representa por la sucesión { 16 30 24 2}. La codificación de este mensaje con las llaves determinadas en el esquema RSA, se presenta en la siguiente tabla:

MENSAJE P	P^e	P^e módulo n
16	268435456	25
30	21870000000	24
24	4586471424	18
2	128	29

La sucesión del texto cifrado es {25 24 18 29}. En este caso la sucesión es simple debido al uso de números pequeños. El texto normal se obtiene de acuerdo al algoritmo RSA, como aparece en la siguiente tabla:

MENSAJE CIFRADO C	C^d	C^d módulo n
25	15625	16
24	13824	30
18	5832	24
29	24389	2

De donde se obtiene que la sucesión transmitida es {16 30 24 2}, correspondiente al mensaje "HOLA".

CONCLUSIONES

Los métodos de encripción o cifrado de datos convencionales han sido históricamente los más utilizados; desde la clave del César (un método convencional por sustitución simple), hasta el estándar DES estos métodos proveen seguridad en la comunicación de datos.

Paralelo al desarrollo de la criptografía y, más aún, con el reconocimiento del estándar DES, los métodos convencionales han sido implementados, tanto por programa como por circuitería, en una gran cantidad de criptosistemas de seguridad.

Una opción más versátil, aunque más costosa la representan los criptosistemas de llave pública, ofreciendo ventajas importantes en la autenticación de mensajes transmitidos. Dentro de los métodos modernos de criptografía se destacan los esquemas de llave pública al representar una alternativa menos rígida en los protocolos de comunicación y más rica en opciones.

Los sistemas de llave pública ofrecen una variedad de características que los hacen versátiles y robustos para un amplio horizonte de aplicaciones. Sin embargo, estos sistemas no son inherentemente más seguros que los sistemas criptográficos convencionales. En general, los sistemas de llave pública son más difíciles de implementar, tanto por sus algoritmos, como su principio de operación, en contraste con un sistema criptográfico convencional. En una aplicación particular deben considerarse los requerimientos de utilización de un sistema de llave pública; principalmente este deberá utilizarse donde se requiera eliminar la transferencia de la llave por correo certificado.

Con la explosión tecnológica de los microcomputadores, el hombre ha incrementado exponencialmente sus sistemas de comunicación, en virtud de lo cual ha requerido de seguridad en la transmisión de sus mensajes y confiabilidad en la recepción de los mismos. La comunicación digital de datos se enfrentará en el futuro al reto planteado en la seguridad de la información, implementando métodos eficientes y rápidos para la encripción de datos, con probabilidades de vulnerabilidad muy bajas, en un medio de transmisión permeable y veloz.

BIBLIOGRAFIA

1. S.C. Serpell. "Crytographic Equipment Security". COMPUTER AND SECURITY. Volumen 4. Número 1. Marzo 1985. Pag 47 a 64.
2. Jozef Pieprzyk y Dominik Rutkewski. "Desing of public key Cryptosystems Using Idempotent Elements". COMPUTER AND SECURITY. Volumen 4. Número 4. Diciembre 1985. Pag. 297 a 308.
3. Rvanden Assen y W.J. Vanelk. "A chosen Paintext Attack on the Microsoft Basic Protection". COMPUTER AND SECURITY. Volumen 5. Número 1. Marzo 1986. Pag 36 a 45.
4. Harold Josept Highland. "Advanced Microcomputer Security System". COMPUTERS AND SECURITY. Volumen 5. Número 4. Diciembre 1986.
5. Martin Hellman. "Comercial Encryption". IEEE NETWORK. Volumen 1. Número 2. Abril 1987.
6. Martin Kochanski. "How Safe Is It". BYTE. Volumen 14. Número 6. Junio 1989.
7. Asael Dror. "Secrets Codes". BYTE. Volúmen 14. Número 9. Junio 1989.
8. Steve Ciarcia. "Build a Hardware Data Encrytor". BYTE. Volumen 11. Número 9. Setiembre 1986. Pag 97 a 111.
9. C.R. Abbruscato. "Data Encryption Equipment". IEEE COMMUNICATIONS. Volumen 22. Número 9. Setiembre 1984. Pag 15 a 21.
10. Victor Voydock y Stephen Kent. "Security in High Level Network Protocols". IEEE COMMUNICATIONS. Volumen 23. Número 7. Julio 1985.
11. Joseph Tardo. "Standardizing Cryptographic Services at OSI Higher Layers". IEEE COMMUNICATIONS. Volumen 23. Número 7. Julio 1985.