¿QUÉ ES LA CRIPTOGRAFÍA?

Ana María Peñas Díaz

La criptografía es una palabra de origen griego: «cripto» equivale a secreto y «grafía» a escritura, por lo que en su conjunto podemos definirla como la ciencia que estudia todo lo relativo a escritura secreta.

Si la criptografía trata de escribir mensajes de manera enigmática mediante claves secretas el criptoanálisis trata de descubrir dichas claves.

Ambas ciencias, criptografía y criptoanálisis, se engloban dentro del término de criptología o ciencia de lo secreto.

La criptografía es la ciencia que estudia todo lo relativo a escritura secreta.

Los sistemas criptográficos se denominan criptosistemas.

Desde principios de la humanidad el hombre se ha preocupado por cifrar, de acuerdo con los medios que poseía, los mensajes que deseaba transmitir para que sólo su destinatario fuese capaz de descifrarlos. Como ejemplo los egipcios y sus «complicados» jeroglíficos.

La criptografía ha ido avanzando conforme al tiempo; los algoritmos criptográficos son cada vez más complicados en el sentido de proporcionar mayor seguridad en todo aquello que se desea transmitir. Importa que un enemigo pueda violar la clave y descifrar el mensaje, pero más importa que de ocurrir ésto lo haga en un tiempo superior al periodo de validez del mensaje. Es decir si se manda un mensaje encriptado con la información: «Se atentará contra el primer ministro a las 15.00»; Si el emisor emitió el mensaje a las 00.00 horas se trataría de que el enemigo no pudiera descifrar el mensaje en un tiempo inferior a 15 horas. Si pasado este tiempo lo consiguiera ya no importaría pues el mensaje ya se habría «ejecutado».

Hoy en día los avances tecnológicos han permitido violar claves que en su día nadie creyó que pudieran ser descifrables. Era impensable que éso pudiera suceder. Ésto debieron pensar los creadores del sistema criptográfico RSA, Rivest, Shamir y Addleman, que en 1977 basaron la seguridad del mismo en la dificultad de factorizar un número «n» de 129 cifras, producto de dos números primos p y q.

Ellos pronosticaron, de acuerdo con los medios disponibles en su tiempo, que de ser posible su factorización ésta no se llevaría a cabo en menos de 40.000 billones de años. La sorpresa apareció el 13 de Octubre de 1993 cuando se anunció públicamente el conocimiento de los valores p y q, quedando por tanto rota la seguridad del sistema. Los descubridores del RSA no tuvieron en cuenta los avances tecnológicos que se avecinaban, entre ellos ordenadores más rápidos.

La criptografía es una ciencia realmente atractiva que vive en sintonía con el tiempo. El desarrollo de nuevas formas de transmitir la información como la telefonía móvil o Internet, la llamada superautopista de la información, hacen de ella un reto para encontrar nuevos algoritmos criptográficos que hagan frente a medios de transmisión cada vez más vulnerables.

El desarrollo de nuevas formas para transmitir la información como la telefonía móvil o internet hacen de ella un reto para encontrar nuevos algoritmos criptográficos que hagan frente a medios de transmisión cada vez más vulnerables.

Ya sabemos que los algoritmos criptográficos tratan de proporcionar seguridad en la información que se transmite. Si llamamos comunicación al intercambio de información entre comunicantes citemos cuáles son sus tres principios básicos:

ANA MARÍA PEÑAS DÍAZ *es proyectista en el Dpto de Matemática Aplicada y Telemática en la ETSETB (UPC).*

-.Privacidad: Se trata de que si alguien intercepta la comunicación no sepa descifrarla.

-.Autenticidad: Se ha de identificar de algún modo los interlocutores para evitar así intrusos.

-.Verificabilidad: Se ha de comprobar que la comunicación es auténtica, es decir no ha sido modificada por posibles intrusos, y además verificarlo.

Criptografía de clave pública/ privada.

Criptosistemas de clave privada:Sistemas en los que emisor y receptor se ponen de acuerdo respecto a una clave secreta.

Hasta los años 70 los criptosistemas más utilizados eran los llamados de **clave privada**. Sistemas en los que emisor y receptor se ponen de acuerdo respecto a una clave secreta. El emisor encripta la información y el receptor de manera reversible la descifra.

Siendo:

M : conjunto de mensajes

C : conjunto de mensajes encriptados

K : Conjunto de claves secretas

E : Función para encifrar

D : función para descifrar

Ek : M -> C

Dk : C -> M

El usuario A manda un mensaje m usando la clave secreta k : Ek(m)

El usuario B recibe Ek(m) y realiza la operación Dk(Ek(m))=m, obteniendo así el mensaje.

Este sistema presentaba varios problemas:

-.Si los dos usuarios van a utilizar una clave secreta común se han de poner de acuerdo en una primera transmisión por el canal. En dicha transmisión la información no va cifrada y puesto que el canal en sí es vulnerable frente a posibles intrusos podría ser captada. No parece un sistema 'muy' seguro.

-.Si cada par de usuarios tiene una clave secreta distinta, y el número de usuarios es elevado el número de claves aumenta considerablemente de manera que se hacen inmanejables. Para n usuarios se necesitarían n(n-1)/2 claves.

-.No es posible trabajar con firmas digitales (son firmas electrónicas equivalentes a las firmas manuales) ya que ambos usuarios utilizando la misma clave para cifrar y descifrar no podrían convencer a un tercero sobre quien de los dos había originado el mensaje.

Y a todo ésto hay que añadir lo ya dicho en el apartado anterior: Con los avances tecnológicos, entre ellos la aparición de ordenadores más rápidos, se podía descifrar mensajes en tiempos inferiores al margen de seguridad permitido.

Criptosistemas de clave pública:Cada usuario genera dos claves, una secreta y otra pública, ésta última a disposición de todos los usuarios.

En 1976, W.Diffie y M.Hellman, con el propósito de solventar los tres problemas anteriores crearon el sistema de **clave pública**. En este sistema cada usuario genera dos claves: una secreta y otra pública (por lo que está a disposición de todos los usuarios).

Un usuario A manda un mensaje al usuario B: Mediante la función F, llamada función trampa o Trapdoor, cifra el mensaje utilizando la clave pública generada por el usuario B. El usuario B obtendrá el mensaje haciendo la inversa de F utilizando la clave secreta por él generada. La función F presenta la propiedad de que su función inversa es prácticamente imposible de realizar si se desconoce la clave secreta. En caso contrario es fácil.

Siendo:

F : función trampa

K : listado de claves públicas {ka,kb,..}

T : función inversa de F

S : conjunto de claves privadas {sa,sb,..}

Para el caso explicado en que A manda mensaje a B:

Fkb : M -> C

Tsb : C -> M

El emisor A manda Fkb(m)=c. El receptor B crea Tsb y obtiene m=Tsb(c).

La función trampa siempre será la misma lo que variará será la clave secreta, además como sólo el usuario conoce su clave secreta sólo él podrá descifrar el mensaje. Por otra parte distinguiremos distintos sistemas criptográficos según la función trampa escogida de manera que cuanto más difícil sea hallar su función inversa más seguro será el sistema.

A diferencia del sistema anterior será posible la comunicación entre múltiples usuarios.

Análisis de sistemas criptográficos de clave pública

Entre los más conocidos tenemos:

1._ Basados en la factorización de números grandes en pocos factores primos.Ej:RSA.

Siendo x el mensaje:

2._ b=x^2 (mod n) --> x=sqrt(b) (mod n)

Ej : Tarjetas inteligentes (ver nota).

3._Logaritmos discretos

y=a^x (mod n) --> x

Ej : Criptografía con curvas elípticas.

Nota: Una tarjeta inteligente es una tarjeta plástica de dimensiones estándar que a diferencia de las tarjetas de banda magnética posee un micro-procesador además de la memoria (PRom,Rom,Ram).

El Dpto de Matemática Aplicada y Telemática trabaja con los tres. En lo que se refiere al último se está estudiando criptosistemas de clave pública basados en el logaritmo discreto sobre puntos de una curva elíptica definida sobre cuerpos finitos. El análisis de dichas curvas así como métodos de exponenciación que reduzcan el tiempo de cómputo en estos sistemas son tema de estudio en estos momentos.

Resumen

La criptografía es una ciencia que se renueva continuamente que te envuelve conforme la vas estudiando. No existe algoritmo seguro, todo está sujeto al paso del tiempo: Lo que hoy es seguro mañana puede no serlo. Dependerá de hasta donde pueda llegar el hombre con su inteligencia: El hombre crea la máquina y la máquina trabaja para el hombre.

Hoy en día, con los algoritmos criptográficos ya existentes los estudios se centran en analizar las ventajas e inconvenientes en cuanto al costo del hardware, la velocidad de cómputo, la seguridad del sistema y su propia aplicación. Las puertas a nuevos algoritmos siempre estarán abiertas.

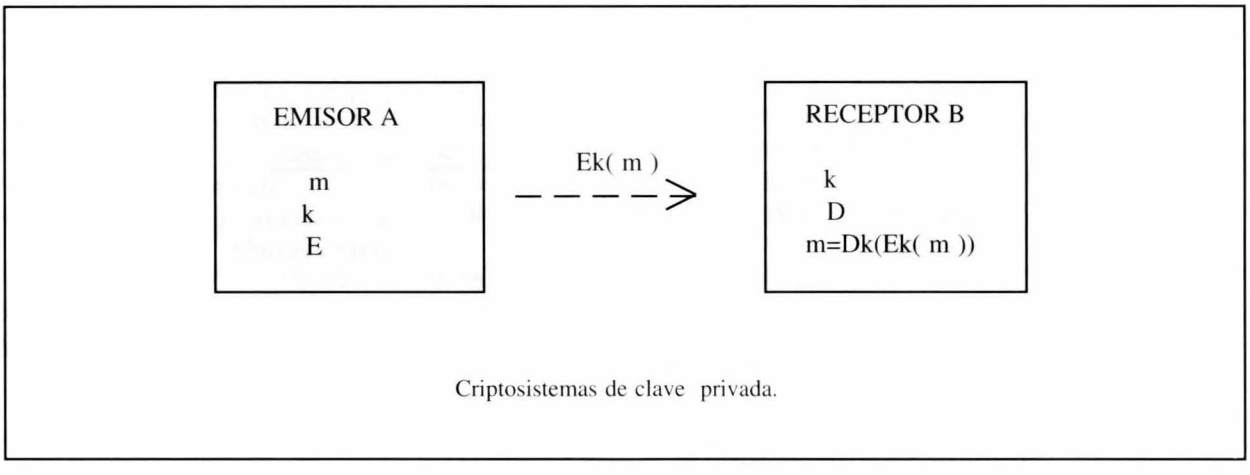
Bibliografía

A.J.MENEZES, *Elliptic Curve Public Key Criptosystems*

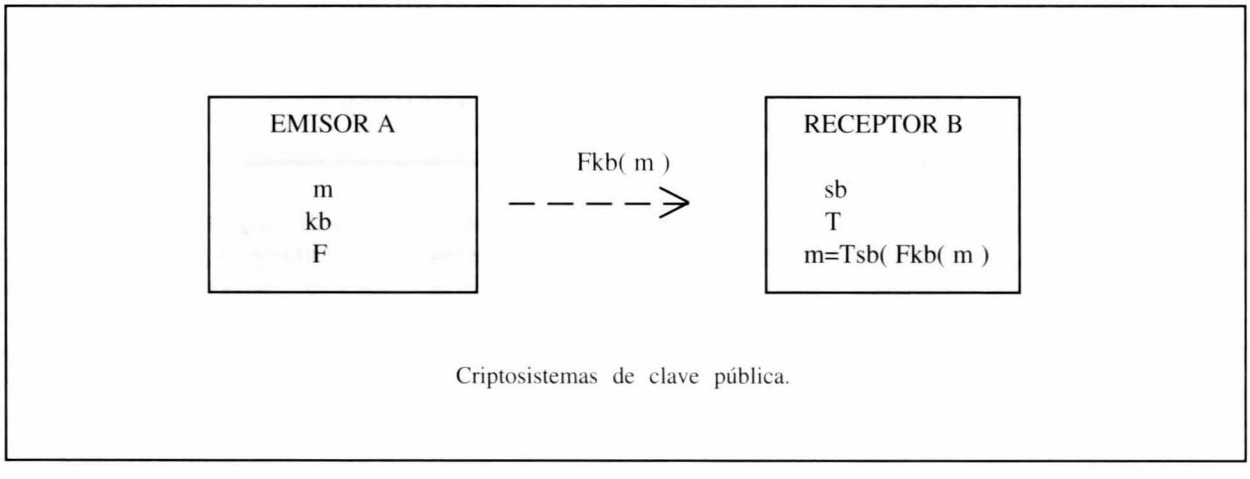
CHRISTIAN MARCOS GÓMEZ , P.F.C '*Curvas Elípticas en cuerpos de característica 2. Aplicaciones a la Criptografía de Clave Pública '1993.*

Biblioteca ETSETB:
512.742.72:514 Mar

Artículos y documentos del Dpto de Matemática Aplicada y Telemática.



Criptosistemas de clave privada.



Criptosistemas de clave pública.