TEORIA DE NUMEROS Y CRIPTOGRAFIA

Karina Yazan (karinna_dc@yahoo.es) Udenar

Diana Lasso (dialas-21@hotmail.com) Udenar

Históricamente el desarrollo matemático de la criptografía se puede situar alrededor del año 1948 cuando Shannon establece las bases matemáticas de la teoría de la información al publicar "Communication Theory of Secrecy Systems" en donde expone un algoritmo cifrado irrompible. En los años 1973-1975 Ellis, Cocks y Williamson desarrollan un algoritmo de cifrado de clave pública para el gobierno británico. Posteriormente, en 1976 Whitfield Diffie y Martin Hellman publican "New Directions in Cryptography" que introduce un nuevo método de distribución de claves criptográficas, lo que era hasta la fecha uno de los problemas fundamentales de la criptografía. En 1977 es publicado el algoritmo RSA, llamado así por sus creadores, Ronald Rivest, Adi Shamir y Leonard Adleman, éste algoritmo es el primer criptosistema de clave pública utilizado en la práctica y basa su seguridad en el Problema de Factorización Entera (PFE), sin embargo dado que la longitud de la clave era grande y el tiempo empleado en la trasmisión del mensaje se hacía extenso no tardaron en crearse nuevos criptosistemas que fueran más eficientes, basados en el PLD. Fue así como en 1986 Neal Koblitz y Víctor Miller trabajando de forma independiente proponen usar el PLD en el grupo de puntos de una curva elíptica sobre un campo finito, lo cual permitió desarrollar criptosistemas más seguros y eficientes. Debido al desarrollo de los criptosistemas basados en Problema del Logaritmo Discreto en Curvas Elípticas (PLDCE).

Encontrar métodos que permitan cifrar información es un campo de estudio que en la actualidad ha adquirido mucha importancia, a estos métodos se les conoce como criptosistemas, los cuales son una colección de transformaciones que permiten cambiar un texto en un texto cifrado y viceversa, dichas transformaciones son definidas generalmente por un algoritmo matemático.

La utilidad de los criptosistemas tanto en el campo comercial como el académico ha sido determinante en el desarrollo de investigaciones acerca de la implementación de algoritmos cada vez mas seguros que permitan cifrar mensajes. Los criptosistemas como el RSA y

ELGAMAL se basaron en el PFE y en el PLD, sin embargo se ha podido demostrar mayor seguridad y eficiencia en aquellos algoritmos que se basan en el PLD en curvas elípticas.

Por otro lado, el criptoanálisis es el estudio de los métodos que permiten obtener el sentido de una información cifrada, sin acceso a la información secreta, es decir, obtener la clave secreta. El creciente desarrollo del criptoanálisis ha originado la necesidad de construir criptosistemas cada vez más seguros, en general fundamentados en la teoría de números y el álgebra de campos finitos; que pretenden disminuir al máximo la posibilidad de que el criptoanálisis tenga un éxito ilimitado al romper los códigos generados por estos criptosistemas.

En este sentido, el Problema de Logaritmo Discreto (PLD) ha permitido implementar criptosistemas con mayores ventajas que las que ofrecen otros criptosistemas basados en problemas matemáticos diferentes. En general el PLD es difícil, en verdad no existe un algoritmo en tiempo polinomial que lo solucione, por esta razón los criptosistemas basados en el PLD disminuyen la posibilidad de que el criptoanálisis tenga éxito sobre ellos. Sin embargo la eficacia del PLD depende en gran parte del grupo cíclico sobre el cual se trabaje. En la actualidad, se ha logrado la construcción de criptosistemas cada vez más seguros recurriendo al PLD sobre la estructura de grupo que tiene un conjunto de puntos en una curva elíptica definida sobre un campo finito.

REFERENTES TEÓRICOS

Etimológicamente la palabra criptografía proviene del griego Kryptos que significa esconder y Graphos escribir; es decir escritura oculta.La criptografía es una ciencia en la que se diseñan métodos que proporcionan seguridad en la comunicación. cifrar o encriptar un mensaje es ocultarlo, es convertirlo en algo que no tenga sentido (texto cifrado) , para un receptor al cual no se le haya enviado el mensaje. Descifrar o desencriptar es el proceso que permite leer un mensaje cifrado.

Los problemas de seguridad que la criptografía abarca son la confidencialidad, la integridad, la autenticación y el no rechazo.

- La confidencialidad consiste en otorgar una característica a la información con la cual esta solo puede ser revelada a usuarios autorizados.
- La integridad se refiere a que la información no puede ser alterada (de forma accidental o fraudulenta)en el transcurso de ser enviada.
- La autenticación es el procedimiento de comprobación de la identidad de un usuario.Mediante el procedimiento se garantiza que es usuario es quien dice ser. Por lo general los sistemas de autenticación están basados en el cifrado mediante una clave privada y secreta.
- El no rechazo se refiere a que no se pueda negar la autoría de un mensaje enviado.

Cuando se diseña un sistema de seguridad, una gran cantidad de problemas pueden ser evitados si se puede comprobar la autenticidad, asegurar integridad y el no rechazo del mensaje.

FUNDAMENTOS

Definición 1: Criptosistema

Un criptosistema es una quíntupla (M, C, Y, T, D), donde las siguientes condiciones se satisfacen:

1) M es un conjunto finito de todos los mensajes sin cifrar que pueden ser enviados. Sus componentes pueden ser bits, signos, caracteres, etc.,

2) $M = \{m1, m2, \ldots, mn\}$

3) C es el conjunto finito de todos los mensajes cifrados. Normalmente el alfabetoes el mismo que el utilizado para crear un mensaje.

$$C = \{c1, c2, \ldots, cn\}$$

4) Y es el conjunto finito de todas las claves que puede emplear un sistema criptográfico. Se supone que es un conjunto altamente aleatorio de caracteres, palabras, bits, etc.,

$$Y = \{k1, k2, \ldots, kn\}$$

5) T es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C.

$$ek : M \rightarrow C \text{ con } k \in Y$$

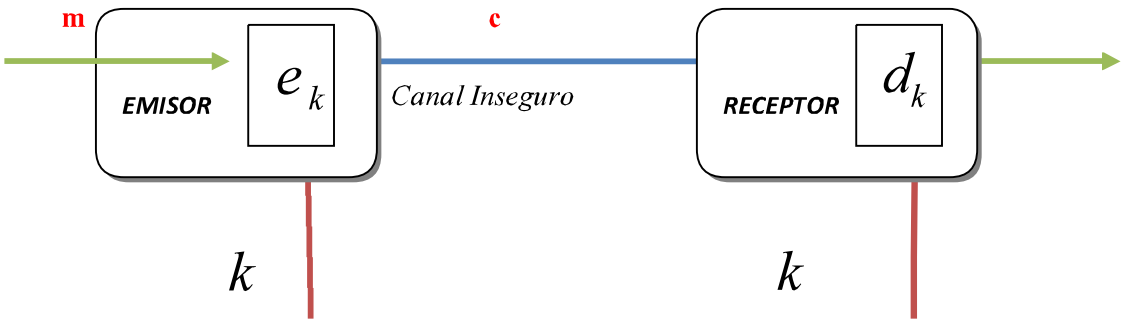
6) D es el conjunto de transformaciones de descifrado, análogo a T. En este caso dk es una aplicación con clave k € Y de C en M.

$$dk: C \rightarrow M \text{ con } k \in Y$$

Definicion 2: Criptografía Simétrica

Un sistema de cifrado simétrico o de clave privada, es un tipo de cifrado que usa una misma clave tanto para cifrar como para descifrar. En la *Gráfica 1.1* se muestra como las dos partes, emisor y receptor, que se comunican mediante el cifrado simétrico deben primero estar de acuerdo en la clave k, una vez de acuerdo, el emisor cifra un mensaje m usando la clave, es decir, aplica una función (o algoritmo) de encriptación ( ) = , que transforma el mensaje m en un mensaje encriptado c, bajo la acción de la clave . Al recibir c, el receptor aplica la función para desencriptar, ( ) = , recuperando m.

Gráfica 1.1: ***Sistema de Cifrado Simétrico***



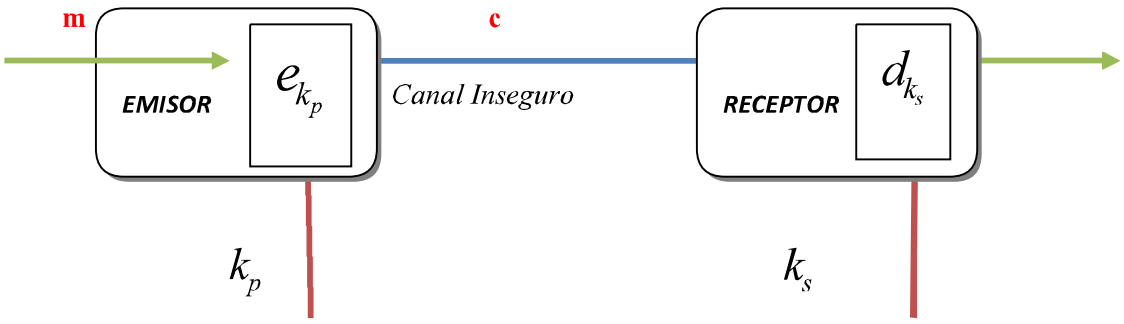
Los sistemas simétricos tienen el inconveniente de que para ser empleados, la clave k debe ser conocida tanto por el emisor como por el receptor, lo cual plantea el problemade comunicarse la clave de forma segura.

Definicion 3: Criptografía Asimétrica

La criptografía asimétrica o criptografía de clave pública, inventada en el año de 1976 por Whitfield. Diffie y MartinHellman, se creo con el fin de evitar el problema que surgía en el intercambio de claves en la criptografía simétrica.

En la criptografía de clave pública cada usuario tiene dos claves, (,), de las cuales una es pública y la otra privada, en la *Gráfica 1.2* se mira como el emisor cifra un mensaje mcon la clave pública del receptor , aplicando la función de encriptación y obteniendo c, ( ) = , éste envía el mensaje cifrado al receptor y como solamente él conoce su clave privada , nadie más que él va ha poder descifrar el mensaje encriptado que le fue enviado, así sólo aplicando la función de descifrado recupera el mensaje, ( ) = .

Gráfica 1.2: ***Sistema de Cifrado Asimétrico***



En este sistema toda persona tiene acceso a la clave de cifrado, solo el receptor tiene la clave para descifrar el mensaje, puesto que conocer la clave pública, no implica encontrar la privada sin haber invertido una gran cantidad de tiempo. Ejemplos de criptosistemas asimétricos son: el RSA, ElGamal, el Massey–Omura en curvas elípticas y ElGamal en curvas elípticas.