Criptología

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

La palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático". Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que tratan sobre la protección de la información.

Es decir que la Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

Historia

En el año 500 a.C. los griegos utilizaron un cilindro llamado "*scytale*" alrededor del cual enrollaban una tira de cuero. Al escribir un mensaje sobre el cuero y desenrollarlo se veía una lista de letras sin sentido. El mensaje correcto sólo podía leerse al enrollar el cuero nuevamente en un cilindro de igual diámetro.

Durante el Imperio Romano, *Julio César* empleó un sistema de cifrado consistente en sustituir la letra a encriptar por otra letra distanciada a tres posiciones más adelante. Durante su reinado, los mensajes de *Julio César* nunca fueron desencriptados.

En el Siglo XII *Roger Bacon* y en el Siglo XV *León Batista Alberti* inventaron y publicaron sendos algoritmos de encriptación basados en modificaciones del método de *Julio César.*

Durante la segunda guerra mundial en un lugar llamado *Bletchley Park* (70 Km al norte de Londres) un grupo de científicos trabajaba en Enigma, la máquina encargada de cifrar los mensajes secretos alemanes.

En este grupo se encontraban tres matemáticos polacos llamados *Marian Rejewski, Jerzy Rozycki, Henryk Zygalski* y "un joven que se mordía siempre las pieles alrededor de las uñas, iba con ropa sin planchar y era más bien bajito" Este joven retraído se llamaba *Alan Turing* y había sido reclutado porque unos años antes había creado un ordenador binario. Probablemente poca gente en los servicios secretos ingleses sabía lo que era un ordenador (y mucho menos binario)... pero no cabía duda que sólo alguien realmente inteligente podía inventar algo así, cualquier cosa que eso fuese...

Era mucho más abstracto que todos sus antecesores y sólo utilizaba 0 y 1 como valores posibles de las variables de su álgebra." [*1].

Sería *Turing* el encargado de descifrar el primer mensaje de Enigma y cambiar el curso de la guerra, la historia y de... la Seguridad Informática actual.

Criptografía

La palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático" [*2].

Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica.

Es decir que la Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

El mensaje cifrado recibe el nombre Criptograma.

La importancia de la Criptografía radica en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática: "*mantener la Privacidad, Integridad, Autenticidad...*" y hacer cumplir con el No Rechazo, relacionado a no poder negar la autoría y recepción de un mensaje enviado.

Criptoanálisis

Es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.

Criptosistema

Un Criptosistema se define como la quíntupla *(m,C,K,E,D)* donde:

m representa el conjunto de todos los mensajes sin cifrar *(texto plano)* que pueden ser enviados.

C Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.

Continúa en página 180

Viene de página 176

K representa el conjunto de claves que se pueden emplear en el Criptosistema.

E 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 . Existe una transformación diferente E_k para cada valor posible de la *clave K*.

D es el conjunto de transformaciones de descifrado, análogo a *E*.

Todo Criptosistema cumple la condición $D_k(E_k(m))=m$ es decir, que si se tiene un mensaje m , se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m.*3

Existen dos tipos fundamentales de Criptosistemas utilizados para cifrar datos e información digital y ser enviados posteriormente después por medios de transmisión libre.

• **Simétricos o de clave privada:** se emplea la misma *clave K* para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave. El mayor inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.

• **Asimétricos o de llave pública:** se emplea una doble clave conocidas como K_p *(clave privada)* y K_P *(clave Pública)*. Una de ellas es utilizada para la transformación *E* de cifrado y la otra para el descifrado *D*. En muchos de los sistemas existentes estas clave son intercambiables, es decir que si empleamos una para cifrar se utiliza la otra para descifrar y viceversa.

Los sistemas asimétricos deben cumplir con la condición que la clave Pública *(al ser conocida y sólo utilizada para cifrar)* no debe permitir calcular la privada. Como puede observarse este sistema permite intercambiar claves en un canal inseguro de transmisión ya que lo único que se envía es la clave pública.

Los algoritmos asimétricos emplean claves de longitud mayor a los simétricos. Así, por ejemplo, suele considerarse segura una clave de 128 bits para estos últimos pero se recomienda claves de 1024 bits (como mínimo) para los algoritmos asimétricos. Esto permite que los algoritmos simétricos sean considerablemente más rápidos que los asimétricos.

En la práctica actualmente se emplea una combinación de ambos sistemas ya que los asimétricos son computacionalmente más costosos (mayor tiempo de cifrado). Para realizar dicha combinación se cifra el mensaje m con un sistema simétrico y luego se encripta la *clave K* utilizada en el algoritmo simétrico (generalmente más corta que el mensaje) con un sistema asimétrico.

Después de estos Criptosistemas modernos podemos encontrar otros no menos importantes utilizados desde siempre para cifrar mensajes de menos importancia o domésticos, y que han ido perdiendo su eficacia por ser fácilmente criptoanalizables y por tanto "*reventables*". Cada uno de los algoritmos clásicos descriptos a continuación utilizan la misma *clave K* para cifrar y descifrar el mensaje.

• **Transposición:** Son aquellos que alteran el orden de los caracteres dentro del mensaje a cifrar. El algoritmo de transposición más común consiste en colocar el texto en una tabla de n columnas. El texto cifrado serán los caracteres dados por columna (de arriba hacia abajo) con una *clave K* consistente en el orden en que se leen las columnas.

• **Cifrados Monoalfabéticos:** Sin desordenar los símbolos del lenguaje, se establece una correspondencia única para todos ellos en todo el mensaje. Es decir que si al carácter A le corresponde carácter D, este correspondencia se mantiene durante todo el mensaje.

Si el algoritmo de cifrado es:

```
A B C D E F G H I...
D E F G H I J K L...
```

Entonces el mensaje cifrado será:

```
S E G U R I D A D...
V H J X U L G D G...
```

Autentificación

Se entiende por Autentificación cualquier método que permita garantizar alguna característica sobre un objeto dado. Interesa comprobar la autentificación de:

Un Mensaje mediante una firma: se debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se lo conoce como *Firma Digital* y consiste en asegurar que el mensaje m proviene del emisor E y no de otro.

Un Usuario mediante una contraseña: se debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta.

Un Dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo una llave electrónica.

PGP (Pretty Good Privacy)

Este proyecto de "*Seguridad Bastante Buena*" pertenece a *Phill Zimmerman* quien decidió crearlo en 1991 "*por falta de herramientas criptográficas sencillas, potentes, baratas y al alcance del usuario común. Es personal. Es privado. Y no es de interés para nadie más que no sea usted... Existe una necesidad social en crecimiento para esto. Es por eso que lo creé.*" *4

Actualmente PGP es la herramienta más popular y fiable para mantener la seguridad y privacidad en las comunicaciones tanto para pequeños usuarios como para grandes empresas.

Esteganografía

Consiste en ocultar en el interior de información aparentemente inocua, otro tipo de información (cifrada o no). El texto se envía como texto plano, pero entremezclado con mucha cantidad de "*basura*" que sirve de camuflaje al mensaje enviado. El método de recuperación y lectura sólo es conocido por el destinatario del mensaje y se conoce como "*separar el grano de la paja*".

Los mensajes suelen ir ocultos entre archivos de sonido o imágenes y ser enormemente grandes por la cantidad extra de información enviada (a comparación del mensaje original). ☒

1 Extraído de http://www.kriptopolis.org

2 LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. http://www.kriptopolis.org - Capítulo 2, Página 23.

3 LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. http://www.kriptopolis.org. Capítulo 2, Página 24.

4 "Porqué escribí PGP". Declaraciones de Phill Zimmerman. http://www.pgpi.com - http://pgp.org

Fuente: www.segu-info.com.ar