CRIPTOGRAFÍA Y CIFRADO

Por: Rohwinzon Urazán Bueno
José manuel Quintero Echeverri

Docente: Lina María Quintero

UNIVERSIDAD DEL QUINDÍO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
HERRAMIENTAS DE LA WEB 2.0 PARA EL DESEMPEÑO PROFESIONAL
Armenia 2011

CONTENIDO

1. DESCRIPCIÓN DEL TEMA

A lo largo de la historia el hombre ha tenido la necesidad de comunicarse, tanto a cortas como a grandes distancias. Esta comunicación en muchas ocasiones es privada y el riesgo de que pueda ser interceptada por un tercero induce la necesidad de ocultar de alguna manera la información confidencial.

Así nació el arte y la ciencia de la *criptografía*, que de manera sucinta puede definirse como la técnica de la escritura secreta. Etimológicamente, la palabra proviene de los vocablos griegos "*krypto*" y "*graphos*", que significan oculto y escritura, respectivamente.

La palabra encriptacion en el lenguaje español no existe aunque en muchos lugares ya es muy común, para referirse a este arte desde una perspectiva como ingenieros se debe nombrar "Cifrado".

El principio básico de la criptografía es mantener la privacidad de la comunicación entre dos o más personas, transformando o modificando de manera aparente la estructura y el contenido del mensaje original, de manera que sea incomprensible para una tercera persona.

La transformación del mensaje original, llamado también texto plano o claro, al mensaje ilegible se llama *encriptar* o *cifrar* y la operación inversa se denomina *desencriptar* o *descifrar*. El encriptado de un texto se realiza mediante un conjunto de reglas establecidas y predeterminadas entre el *emisor* i el *receptor*, que consisten, básicamente, en la aplicación al texto claro de un *algoritmo de cifrado*, en lo que se denomina *codificación*.

El objetivo de la criptografía no es, entonces, ocultar la existencia de un mensaje, sino ocultar su significado. Por tanto, la ventaja es que si una tercera persona intercepta una información cifrada, ésta será ininteligible hasta que no se descubra el protocolo codificador.

La búsqueda del protocolo para descifrar un mensaje es el fin mismo del *criptoanálisis*. El criptoanálisis es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta (clave), requerida para obtener este sentido normalmente. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código.

En términos generales, la *criptología* es el estudio de los criptosistemas, es decir, los sistemas que ofrecen medios seguros de comunicación en los que el emisor

cifra el mensaje antes de enviarlo para que sólo el receptor autorizado pueda descifrarlo. Sus principales áreas de interés son la *criptografía* y el *criptoanálisis.*

Para ilustrar el proceso criptográfico de manera sencilla, a continuación se muestra un antiguo modo de cifrado, atribuido a Julio César, quien lo diseñó para comunicarse con sus ejércitos aliados. Este método se conoce consecuentemente como *La cifra de César* y consiste en utilizar un nuevo alfabeto, denominado *alfabeto encriptado*, simplemente desplazando las letras tres espacios a la derecha, de tal manera que, por ejemplo, la letra A se transformaba en la D, la B en la E y así sucesivamente, con lo cual se obtenía la siguiente relación:

```
1-  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2-  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

1- (alfabeto original)
2- (alfabeto encriptado)

Así, el mensaje “uso de las herramientas de la web”, se encriptará de la manera siguiente:

```
USO DE LAS HERRAMIENTAS DE LA WEB
XVR GH ODV KHUUDPLHQWDV GH OD ZHE
```

Matemáticamente se entiende La cifra de César como un desplazamiento cíclico de las letras del alfabeto y se conoce como un algoritmo por sustitución monoalfabética simple. Este sistema de encriptación es uno de los más estudiados, ya que resulta de gran utilidad porque permite ilustrar los principios de la aritmética modular, uno de los pilares del estudio matemático de la escritura en clave.

Tal vez los sucesos históricos que más han incidido en el avance de la criptografía y el criptoanálisis han sido las guerras, debido a que durante éstas hay un gran flujo de información entre los diferentes frentes de batalla y los centros de comando, información que debe ser protegida para que el enemigo no pueda conocer las estrategias bélicas. Un ejemplo clásico de la lucha entre *criptógrafos* (encargados de diseñar y aplicar los métodos de cifrado) y *criptoanalistas* (interesados en romper los códigos), es el de la famosa *Máquina Enigma*, artefacto utilizado por los nazis durante la Segunda Guerra Mundial para encriptar los mensajes del ejército, cuyo código fue finalmente descifrado por los Aliados.

Comentario [1]: jmqdos:
Figura 1. Izquierda, máquina Enigma usada por la Kriegsmarine. Derecha, versión artística de la misma, fabricada por un aficionado.

Figura 1. Izquierda, máquina Enigma usada por la Kriegsmarine. Derecha, versión artística de la misma, fabricada por un aficionado.

Actualmente la ciencia de la criptografía ha adquirido una relevancia que envuelve prácticamente todas las esferas de la actividad humana en las cuales deba transferirse algún tipo de información a través de medios informáticos. El uso extendido de los computadores y de la internet ha supuesto un reto para criptógrafos y criptoanalistas, los primeros para proteger de intrusiones los sistemas y los datos y los segundos para descifrar los códigos de acceso. Hasta el momento parece que los criptógrafos pisan terreno firme y ganan la batalla, pues han desarrollado métodos que virtualmente inviolables; pero ¿hasta cuándo?

Hablando de cifrado pero en ingeniería tenemos que toda encriptación se encuentra basada en un Algoritmo, la función de este Algoritmo es básicamente codificar la información para que sea indescifrable a simple vista , de manera que una letra “A” pueda equivaler a :“5x5mBwE” o bien a “xQE9fq”, el trabajo del algoritmo es precisamente determinar cómo será transformada la información de su estado original a otro que sea muy difícil de descifrar.

Una vez que la información arribe a su destino final, se aplica el algoritmo al contenido codificado “5x5mBwE” o bien a “xQE9fq” y resulta en la letra “A” o según sea el caso, en otra letra. Hoy en día los algoritmos de encriptación son ampliamente conocidos,es por esto que para prevenir a otro usuario “no autorizado” descifrar información encriptada, el algoritmo utiliza lo que es denominado llave (“key”) para controlar la encriptación y decriptación de información. Algunos algoritmos son DES (algoritmo simétrico) AES que posiblemente suplantará a DES y uno de los más conocidos RSA (algoritmo asimétrico).

Figura 2. Los sistemas de pago por Internet se basan en la codificación SSL (Secure Socket layer)

Comentario [2]: jmqdos:
El SSL es un procedimiento de seguridad que prácticamente se ha estandarizado para pagos on-line. Éste transfiere datos del cliente al servidor después de codificarlos. La codificación SSL en las pàginas de Internet se reconoce por el candado en la barra de navegación.

2. JUSTIFICACIÓN

La criptografía ha pasado de ser una actividad reservada de las actividades estratégicas y militares a convertirse en una necesidad del mundo moderno. Con la introducción de los sistemas informáticos en las comunicaciones, el auge de la internet y la globalización económica y social, la criptografía se ha hecho indispensable en las comunicaciones. Las cuentas de correo electrónico, de las redes sociales, las transacciones bancarias por cajero electrónico o a través de internet, entre muchos otros, están protegidos por codificación electrónica. Es así como la criptografía, aún sin saberlo la mayoría de las personas, se ha convertido en una realidad del día a día.

Estas razones, sumadas a las características propias de esta ciencia, que conducen a un punto de encuentro entre la informática y las matemáticas, han incidido definitivamente sobre la selección de este tema para el trabajo conjunto en la asignatura Herramientas de la Web 2.0.

4. REFERENCIAS WEB

http://criptosec.unizar.es/ Página de la asignatura Criptografía y Seguridad en Redes de Comunicaciones de la Universidad de Zaragoza (España). Aquí se pueden consultar temas generales de criptografía clásica y moderna.

http://webpages.ull.es/users/cryptull/TallerCripto/Criptoanalisis.pdf Presentación de la propuesta de Edgar Alan Poe sobre criptoanálisis estadístico.

http://blog.intuicionlogica.com/la-maquina-enigma-y-la-seguridad-informatica/
Breve resumen sobre el funcionamiento y descifrado de la máquina Enigma y sus repercusiones en la criptología moderna.

http://www.shoptodate.es/shoptodate/funciones/codificacionssl.php Página que oferta software para ventas por internet y hace una corta decripción del sistema de codificación SSL.

http://solodecomputacion.blogspot.com/2009/12/tipos-de-cifrados-en-una-red-wifi.html Pagina que contiene información de las diferentes clases de cifrado y los medios por los cuales se realiza dicho procesamiento.

5. BIBLIOGRAFÍA

[1] SINGH, Simon. *Los códigos secretos*. 2 ed. Madrid: Editorial Debate, 2000. 382 p. ISBN: 978-8483062784.

[2] DE MIGUEL García, Roberto. *Criptografía clásica y moderna*. Oviedo: Septem Ediciones, 2008. 92 p. . ISBN: 849649179X

[3] ORTEGA, Jesús et al. *Introducción a criptografía. Historia y actualidad*. Cuenca: Ed. Universidad de Castilla- La Mancha, 2006. 128 p. ISBN: 84-8427—441-1

[4] GÓMEZ URGELLÉS, J. *Matemáticos, espías y piratas informáticos*. 1 Ed. Barcelona: Plaza Edición, 2010. 106 p. ISBN: 9788498678574