Criptografía

¿Para que sirve la criptografía?

Los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos informáticos y calculadoras.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la Web. Las transacciones que se realizan a través de la red pueden ser interceptadas y, sobretodo, porque actualmente resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse: éste es el papel de la criptografía.

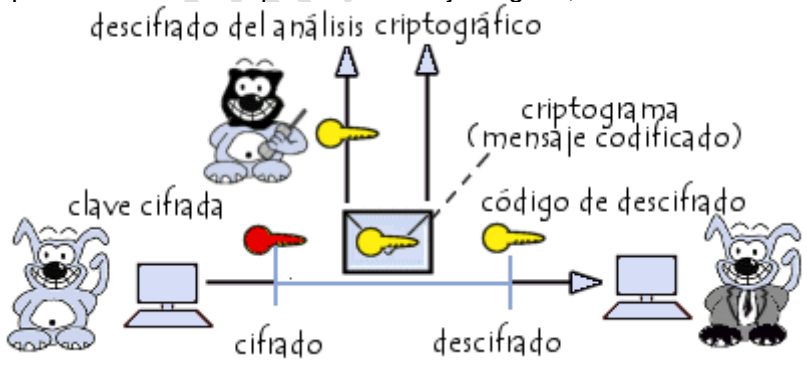
¿Qué es la criptografía?

La palabra **criptografía** es un término genérico que describe todas las técnicas que permiten **cifrar** mensajes o hacerlos ininteligibles sin recurrir a una acción específica. El verbo asociado es **cifrar**.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama **texto cifrado**, en contraste con el mensaje inicial, llamado **texto simple**.
- asegurarse de que el receptor pueda descifrarlos.

El hecho de codificar un mensaje para que sea secreto se llama *cifrado*. El método inverso, que consiste en recuperar el mensaje original, se llama *descifrado*.



El cifrado normalmente se realiza mediante una *clave de cifrado* y el descifrado requiere una *clave de descifrado*. Las claves generalmente se dividen en dos tipos:

- *Las claves simétricas*: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.

Versión de Revisión y Edición

- *Las claves asimétricas*: son las claves que se usan en el caso del cifrado asimétrico (también llamado *cifrado con clave pública*). En este caso, se usa una clave para el cifrado y otra para el descifrado.

En inglés, el término *decryption* (descifrado) también se refiere al acto de intentar *descifrar en forma ilegítima* el mensaje (ya conozca o no el *atacante* la clave de descifrado). Cuando el atacante no conoce la clave de descifrado, hablamos de **criptanálisis** o **criptoanálisis**(también se usa el término *decodificación*).

La **criptología** es la ciencia que estudia los aspectos científicos de estas técnicas, es decir, combina la criptografía y el criptoanálisis.

Las funciones de la criptografía

La criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

Criptoanálisis

El **criptoanálisis** consiste en la reconstrucción de un mensaje cifrado en texto simple utilizando métodos matemáticos. Por lo tanto, todos los criptosistemas deben ser resistentes a los métodos de criptoanálisis. Cuando un método de criptoanálisis permite descifrar un mensaje cifrado mediante el uso de un criptosistema, decimos que el algoritmo de cifrado ha sido decodificado.

Generalmente, se distinguen cuatro métodos de criptoanálisis:

- Un **ataque de sólo texto cifrado** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados;
- Un **ataque de texto simple conocido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados conociendo el texto correspondiente;
- Un **ataque de texto simple elegido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de textos simples;
- Un **ataque de texto cifrado elegido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de los textos simples.

Referencias:
http://es.ccm.net/

Versión de Revisión y Edición