5

La ciberseguridad no es un enigma

Tema: Tecnología de la Información / Seguridad

La criptología

El procesamiento de información digitalizada y su comunicación masiva multiplican las posibilidades de incursiones indeseadas que atentan contra su integridad, confidencialidad y autenticidad. Esto es por demás importante en infinidad de procesos cotidianos, como cuando operamos a través del "home banking", o se transmiten por Internet datos personales, secretos tecnológicos o información relacionada a la seguridad de un país. Para proteger el intercambio de información se oculta el mensaje mediante una llave de acceso. Así surgieron dos metodologías que están contenidas dentro de la disciplina conocida como criptología. Una es la esteganografía, que consiste en ocultar un mensaje en un objeto portador (fotografía, video, audio), haciendo que el mensaje pase inadvertido. Este método es empleado más de lo que se piensa. La otra es la criptografía. En la antigüedad se consideraba a la criptografía el arte de hacer indescifrable un mensaje para todo aquel que no fuera su destinatario, lo cual era muy útil cuando un mensajero era capturado. A esto se lo denomina criptografía o cifrado clásicos, y dependía de operaciones realizadas con las letras de un alfabeto. La criptografía moderna es una ciencia relacionada con las computadoras, ya que el cifrado depende de operaciones matemáticas con bits o bytes, y se aplica en nuestros dispositivos portátiles o redes inalámbricas de comunicación segura. Hoy en día se puede pensar también en la criptografía cuántica, donde el cifrado está asociado a los qubits (bit cuántico), que son como "bits supercargados" pues tienen varios estados además del 1 y el 0.

Escítala espartana.
Fuentes de imágenes: Wiki commons.

Hitos de la criptografía

Si bien algunos textos hablan de los sumerios, como la primera sociedad (siglo IV a. C.) que comenzó a utilizar la criptografía, hay registros del 700 a. C. donde los espartanos utilizaban la escítala. Esta consistía en dos varas cilíndricas iguales (equivalente actual de la clave). Una vara se la quedaba el emisor del mensaje y la otra el receptor. El emisor enrollaba en forma de espiral una cinta de cuero sobre su vara, y escribía longitudinalmente un mensaje.
Al desenrollar la cinta el mensaje se hacía ilegible. Esta cinta luego era enviada al receptor, quien podía leer el mensaje oculto al enrollarla en su propia vara. El llamado cifrado César empleado en la Antigua Roma (58 a. C.) consistía en reemplazar cada letra del mensaje, por otra desplazada tres lugares hacia la derecha en un alfabeto. En la edad media encontramos el cifrado de Alberti, método que utilizaba dos discos concéntricos, con alfabetos en el borde; el inferior de mayor tamaño y fijo, y el superior giratorio. Emisor y receptor debían acordar la correspondencia entre ambos alfabetos, antes de intercambiar mensajes. En la edad moderna, el desarrollo de la tecnología generó grandes avances en criptografía. Durante la Segunda Guerra Mundial, Alemania empleó la máquina Enigma. Este sistema electromecánico que contaba con una serie de rotores, clavijas y un libro de claves, permitió generar infinidad de mensajes cifrados con órdenes militares. Cabe destacar al matemático inglés Alan Turing, por su trabajo destinado a descifrar sus códigos. Durante la misma época, EUA llegó a transmitir mensajes secretos por radio, entre locutores navajos, empleando su lengua nativa como clave.

Cifrado de Alberti.
Fuentes de imágenes: Wiki commons.

CONOCIENDO SOBRE CRIPTOLOGÍA Y CRIPTOGRAFÍA

La ciberseguridad no es un enigma

CIENCIA A GOTAS
FRD.UTN

Tema: Tecnología de la Información / Seguridad

Tipos de criptografía

Los conceptos matemáticos definidos por Claude Shannon (EUA – 1945), "el padre de la teoría de la información", permitieron desarrollar la criptografía moderna, al establecer dos operaciones claramente definidas para la realización del cifrado, la transposición y la sustitución que actualmente se aplican a los bits o bytes, operando con el código ASCII extendido. Conceptualmente se definen dos tipos de criptografía. La criptografía simétrica, donde se utiliza la misma llave para cifrar y descrifrar un mensaje. Este proceso es muy rápido, y adolece del problema de intercambio o distribución de claves. Por otro lado, en la criptografía asimétrica, cada usuario cuenta con un par de claves, la llave privada que no debe compartirse con nadie, y la llave pública que será conocida por todos los otros usuarios. Ambas llaves se generan automáticamente al emplearse por primera vez el cifrador y están relacionadas entre sí. En el caso de que alguien quiera enviar un mensaje seguro, solo es necesario conocer la llave pública del receptor y nadie podrá abrir el mensaje cifrado, excepto el que cuente con la llave privada del receptor. En cambio, para asegurar la autenticidad de una información, el emisor hace un digesto (también llamado resumen o hash) con su clave privada y lo envía con el documento. El receptor verifica la autenticidad de lo que recibe comparando ese digesto con la clave pública del emisor. Los sistemas actuales más seguros (por ejemplo, las transacciones bancarias) usan ambos métodos combinados.

Máquina ENIGMA que usaba Alemania para encriptar sus mensajes en la Segunda Guerra Mundial, y la máquina que inventó Alan Turing para descifrarlos en Bletchley Park - Gran Bretaña

Algoritmos

Entre los algoritmos de criptografía más importantes encontramos:
DES (Data Encryption Standard): Fue el primer algoritmo de cifrado simétrico aprobado como standard de uso nacional por la NBS - Oficina Nacional de Standards (EUA- 1976).
RSA (creado por Rivest, Shamir, Adleman): Fue el primer algoritmo de cifrado asimétrico (EUA - 1978). Su uso está tan extendido que se utiliza para brindarle seguridad a los certificados digitales de las páginas WEB.
AES (Advanced Encryption Standard): Es un algoritmo simétrico moderno (EUA - 2001) que reemplaza al viejo DES. En la actualidad se utiliza en gran cantidad de aplicaciones, incluyendo la seguridad de las redes inalámbricas.
BLOCKCHAIN: si bien su historia data de los años 80's y 90's, fue Satoshi Nakamoto (Japón – 2008) quién llevó la teoría a la práctica, permitiendo establecer cadenas de bloques no modificables y sellados para la realización de transacciones, a través de un libro de cuentas grupal. Así nacieron las criptomonedas.

Recomendaciones

Los sitios WEB seguros se identifican como https, e incluyen la imagen de un candadito. Antes de operar se debe hacer click en él, y verificar si muestra un certificado y si el mismo está vigente.

CARLOS ALFONSO HENSELER
Magister en Ciberseguridad (Universidad del Rey Juan Carlos – España)
Especialista en Criptografía y Seguridad Teleinformática
Jefe de Trabajos Prácticos de la Materia Seguridad en los Sistemas de Información (UTN-FRD)

Esta publicación es editada por la Secretaría de Ciencia, Tecnología y Posgrado - AÑO 2024