INTRODUCCIÓN Y ANTECEDENTES:

El cifrado es ocultar o enmascarar un mensaje, el cifrado se traduce como la escritura de mensajes ocultos, permite ocultar la identidad de un mensaje. En la antigüedad ya se empleaban métodos de criptografía para ocultar mensajes en tiempo de guerra para evitar que personas no autorizadas supieran el contenido del mensaje, de forma que aunque el mensajero fuera interceptado por el enemigo, el contenido del mensaje estaba a salvo.

Hablamos con nuestros amigos, reservamos nuestras vacaciones, damos en número de nuestra tarjeta de crédito, ofrecemos nuestros datos personales… y todo ello mediante:

- Voz telefónica
- Mensajería breve por ejemplo SMS, WhatsApp.
- Información que se trasmite por internet.

La criptografía es una necesidad derivada de realizar comunicaciones por escrito (en su origen) creada para preservar la privacidad de la información que se transmite, garantizando que una persona que no esté autorizada no pueda leer el contenido del mensaje.

A lo largo de la evolución hemos tenido multitud de ejemplos de como cifrar mensajes como los métodos espartanos de hace 2.500 años.

En la computación se izó un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes.

OBJETIVOS.

El objetivo de la criptografía es:

- Diseñar.
- Implementar.
- Implantar.
- Hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad.

La Criptografía es el método para proteger la información haciendo uso del cifrado o codificación para alterar cualquier representación lingüística legible o inteligible a una representación lingüística no legible y no comprensible.

- La criptografía se encarga de proteger la integridad de la información como al mismo tiempo protege la confidencialidad, dos procesos que se encuentran integrados en los pilares de la seguridad informática:
  - Integridad.
  - Confidencialidad.
  - Disponibilidad.

La criptografía actualmente se encarga del estudio de:

- Algoritmos.
- Protocolos.
- Sistemas que se utilizan para dotar de seguridad a las comunicaciones a la información y a las entidades que se comunican.

Por tanto el tipo de propiedades de las que se ocupa la criptografía son:

- **Confidencialidad.** Es decir garantiza que la información está accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.
- **Integridad.** Es decir garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de motorización electrónica.
- **Vinculación:** Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado.

- **Autenticación.** Es decir proporciona mecanismos que permiten verificar la identidad del comunicador.
- Soluciones a problemas de la falta de simultaneidad en la telefirma digital de contratos.
- Un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.

CHECKLIST.

Criptografía simétrica.

Los algoritmos de criptografía simétrica utilizan la misma clave para los dos procesos: cifrar y descifrar. Suelen ser sencillos de utilizar y bastante eficientes.

El emisor quiere enviar un documento al receptor, para ello le aplica al documento un algoritmo simétrico con una clave que también conoce el receptor. Cuando el receptor recibe el mensaje le aplica el mismo algoritmo (inverso) con la misma clave. Si el documento no ha sido modificado en la transmisión, el resultado será el documento original.

Lo que afecta la criptografía.

El mayor inconveniente es la necesidad de comunicar la clave compartida. Esto debe hacerse con mucho cuidado para asegurarse de que la clave no sea revelada a usuarios no autorizados. También puede haber un problema con el número de claves utilizadas. Cuando se tiene un gran número de claves, puede llegar a ser difícil de gestionar.

Funciones Hash.

Una herramienta fundamental en la criptografía, son las funciones hash, son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen. Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la

función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

Comercio electrónico.

Hoy en día, gran parte de la actividad comercial ha podido transformarse gracias a redes de conexión por ordenadores como Internet, esta transformación facilita hacer transacciones en cualquier momento, de cualquier lugar del mundo.

PUNTOS DE APLICACIÓN.

Para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Para ello se usan técnicas como el cifrado negable.

En el campo de la criptografía muchas veces se agrupan conjuntos de funcionalidades que tienen alguna característica común y a ese conjunto lo denominan 'Criptografía de' la característica que comparten. Veamos algunos ejemplos:

- **Criptografía simétrica.** Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de una sola clave.
- **Criptografía de clave pública o Criptografía asimétrica**. Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de parejas de claves compuesta por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar.
- **Criptografía con umbral.** Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de un umbral de participantes a partir del cual se puede realizar la acción.
- **Criptografía basada en identidad.** Es un tipo de Criptografía asimétrica que se basa en el uso de identidades.
- **Criptografía basada en certificados.**
- **Criptografía sin certificados.**
- **Criptografía de clave aislada.**

Criptografía simétrica.

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave.

Desventaja.

- La distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.
- La seguridad en clave simétrica reside en la propia clave secreta, y por tanto el principal problema es la distribución de esta clave a los distintos usuarios para cifrar y descifrar la información.

Criptografía asimétrica.

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje.

La criptografía asimétrica resuelve las dos desventajas principales de la simétrica:

A. No se necesita canales seguros para mandar la clave. La distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario.
B. No hay desbordamiento en el tratamiento de claves y canales.

Criptografía híbrida.

Este sistema es la unión de las ventajas de los dos anteriores, ya que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento.

Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico.

Caso FBI vs Apple.

Hace unas cuantas semanas llamó mi atención esta nota en particular, relacionada al caso de la matanza en San Bernardino cuando en un hecho trágico un asesino victimó a una multitud de inocentes, para luego ultimarse a sí mismo, pero más allá de este trágico y lamentable incidente, lo que me gustaría puntualizar, es que el hecho sin precedentes en el que el FBI exigió a Apple, a través de una corte, que otorgara acceso al teléfono encontrado del asesino, ya que éste, como todos los iPhones, se encontraba encriptado y la policía no podía tener acceso a su contenido sin correr el riesgo de perder para siempre dicha información. Cabe señalar que este sencillo sistema de encriptación y seguridad de Apple, puso en un gran dilema al FBI, ya que después de 10 intentos fallidos al introducir la contraseña de 4 dígitos de forma errónea, borra todo el contenido del teléfono.

INFORMACIÓN Y ELEMENTOS ADICIONAL

- Steven Levy, Cripto. Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital, Madrid, Alianza, 2002.
- David Kahn, The Codebreakers, New York, Macmillan, 1967.
- Cnet News staff (11 de enero de 1996). Feds drop charges in encryption case. CNet News (en inglés). Consultado el 7 de noviembre de 2014.
- https://criptografiafirmasdigitales.wordpress.com/2014/09/26/ventajas-y-desventajas-de-la-criptografia/
- http://instintologico.com/introduccion-a-la-criptografia-es-necesario-cifrar-criptografia-simetrica-y-asimetrica/