UNIVERSIDAD AUTÓNOMA

UNIVERSIDAD AUTONOMA GABRIEL RENÉ MORENO

"FACULTAD DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN Y TELECOMUNICACIONES"

"Autenticación y Firma Digital"

DOCENTE: ING. SHIRLEY

MATERIA: CRIPTOGRAFIA Y SEGURIDAD

ALUMNOS:

- COLQUEHUANCA VARGAS CARLOS DAVID 213074273
- FLORES TANTANI JULIETA 213007673
- LARA QUIROZ ELVIS 210207787

SEMESTRE: 2 – 2017

FECHA: 07/09/2017

Contenido

CONCEPTOS BASICOS

La autenticacion es un proceso de seguridad que empezo mucho antes que la era de la computacion. Solo para los de esta generación, uno lo relaciona con la seguridad digital.

Una definición acertada seria: “En contraste con la identificación que se refiere al acto de afirmar o indicar algo, la autenticación es, en realidad, el acto de **confirmar** dicha afirmación previa.”

Autorización. Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

Auditoría. Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

Etimologia: del griego: αὐθεντικός *authentikos*, "real, genuino", from αὐθέντης *authentes*, "autor"

Autenticacion digital: A partir de las ultima decada, se ha acunado un termino denominado *autenticación digital*, el cual se refiere a un conjunto de procesos donde la confidencialidad del usuario es establecida y presentada via electrónica.

Si bien esto representa un gran avance hacia la automatización, a su vez representa un problema ante el mercado del *hackeo*, como la vulnerabilidad del *MAN-IN-THE-MIDDLE-ATTACK,* en el cual una tercera persona se cuela en el canal de comunicación y pretende interceptar la información haciéndose pasar por ambas partes del proceso de la autenticación. Debido a esto, claramente se necesita factores de identificación adicionales para asegurar la identidad del usuario.

Es por eso que la *National Institute of Standards and Technology* (NIST) ha creado un modelo genérico para la autenticación digital que describe los procesos que se usaran para lograr una segura autenticación,

1. **INSCRIPCION.-** aquí un sujeto postula para un CSP (*credential service provider),* para iniciar un proceso de inscripción. Luego de proveer los datos necesarios, el CSP permite al usuario convertirse en un subscriptor.
2. **AUTENTICACION.-** Luego de subscribirse, el usuario recibe un autenticador (ej. Un token y credenciales como el *username*. Solo asi, el usuario será capaz de realizar transacciones via online con una autentica sesión del mismo en donde el usuario deberá probar que se trata en verdad de el/ella mismo. (ej. contraseña)
3. **MANTENIMIENTO.-** El CSP tiene la responsabilidad de mantener el credencial del usuario durante el curso de su vida, mientras que el usuario

tiene la tarea de mantener el token que lo acredita como el usuario verdadero.

FACTORES Y TIPOS DE AUTENTICACION

El uso de múltiples factores de autenticación para demostrar la identidad propia se basa en la premisa de que un tercero no autorizado probablemente no pueda ser capaz de suministrar los factores requeridos para el acceso. Si en un intento de autenticación al menos uno de los componentes falta o se suministra incorrectamente, la identidad del usuario no se valida y no puede acceder a los recursos —p. ej., un edificio o dato—.

Los factores de autenticación de un patrón de autenticación de múltiples factores podría incluir:

- **Factores físicos.-** Algún objeto físico en posesión del usuario, como una memoria USB con un identificador único, una tarjeta de crédito, una llave, etc.
- **Factores de conocimiento.-** Algún secreto conocido por el usuario, como una contraseña, un pin, etc.
- **Factores inherentes.-** Alguna característica biométrica propia del usuario, como una huella dactilar, iris, voz, velocidad de escritura, patrón en los intervalos de pulsación de teclas, etc.

Basados en los factores, existen diferentes tipos de autenticación que son:

- **Autenticacion Factor Simple.-** Hace uso de un solo factor, generalmente el físico, de autenticación.
- **Autenticacion Factor Doble.**- En caso de usarse dos factores para la autenticación, este tipo es utilizado. Un ejemplo: Las transacciones bancarias.
- **Autenticacion Multi-Factor.-** Es el mas utilizado ya que hace uso de los 3 factores, y en ocasiones, hasta mas de una vez. Se lo utiliza para aumentar la seguridad de la información que suele ser en estos casos, muy pero muy valiosa.

A su vez, existen otro par de términos como **Autenticacion Segura**, y la **Autenticacion Continua.**

El gobierno de los E.E.U.U define *Autenticacion Segura* al uso de de dos o mas factores de autenticación (autenticadores).

Algunos sistemas no se conforman con identificar al usuario al momento de loggearse, sino que analizan sus patrones de comportamiento en caso de sospechas para volver a pedirle una autenticación al usuario. Ej. Cambio de contraseña en Facebook. A esto se le conoce como *Autenticacion Continua.*

CONTROL DE ACCESO

Un sistema informático supuesto para ser utilizado solamente por aquellos autorizados, debe procurar detectar y excluir el desautorizado. El acceso a él por lo tanto es controlado generalmente insistiendo en un procedimiento de la autentificación para establecer con un cierto grado establecido de confianza la identidad del usuario, por lo tanto concediendo esos privilegios como puede ser autorizado a esa identidad. Los ejemplos comunes del control de acceso que implican la autenticación incluyen:

- Retirar de dinero de un cajero automático.
- Control de un computador remoto sin Internet.
- Uso de un sistema Internet banking.

Para intentar probar la identidad de un sujeto u objeto posible aplicar una o más pruebas que, si están pasadas, se han declarado previamente para ser suficientes proceder. El problema es determinarse qué pruebas son suficientes, y muchos tales son inadecuadas. Tienen sido muchos casos de tales pruebas que son spoofed con éxito; tienen por su falta demostrada, ineludible, ser inadecuadas. Mucha gente continúa mirando las pruebas -- y la decisión para mirar éxito en pasar -como aceptable, y para culpar su falta en “sloppiness” o “incompetencia” de parte alguien. El problema es que la prueba fue supuesta para trabajar en la práctica -- no bajo condiciones ideales de ningún sloppiness o incompetencia-y no. Es la prueba que ha fallado en tales casos. Considerar la caja muy común de un email de la confirmación a el cual deba ser contestado para activar una cuenta en línea de una cierta clase. Puesto que el email se puede arreglar fácilmente para ir a o para venir de direcciones falsas y untraceable, éste es justo sobre la menos autenticación robusta posible. El éxito en pasar esta prueba significa poco, sin consideración alguna hacia sloppiness o incompetencia

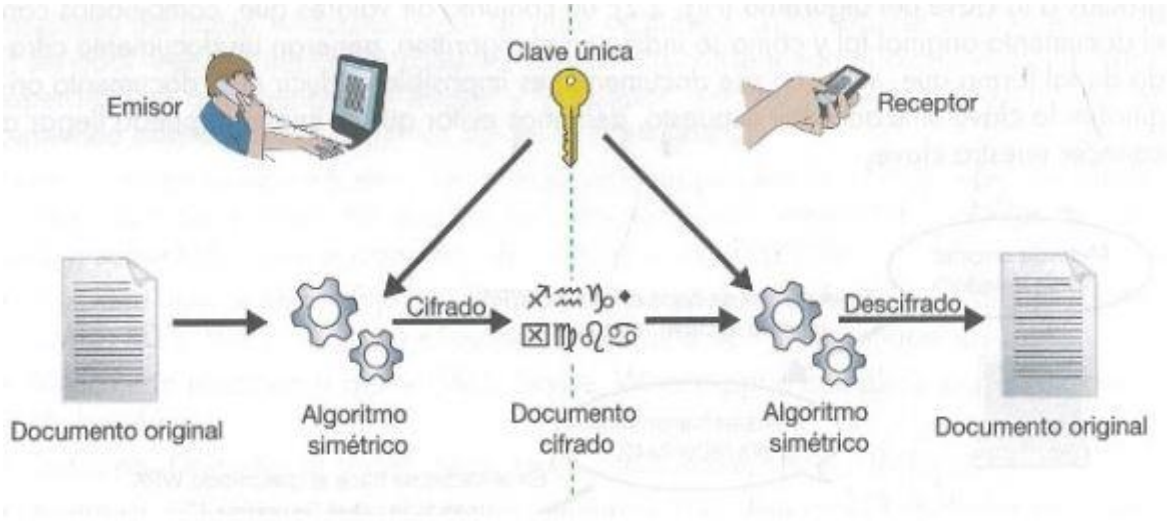
CRIPTOGRAFÍA SIMÉTRICA

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. Es importante que dicha clave sea muy difícil de adivinar ya que hoy en día los ordenadores pueden adivinar claves muy rápidamente. Debemos tener en cuenta que los algoritmos criptográficos son públicos, por lo que su fortaleza debe depender de su complejidad interna y de la longitud de la clave empleada para evitar los ataques de fuerza bruta.

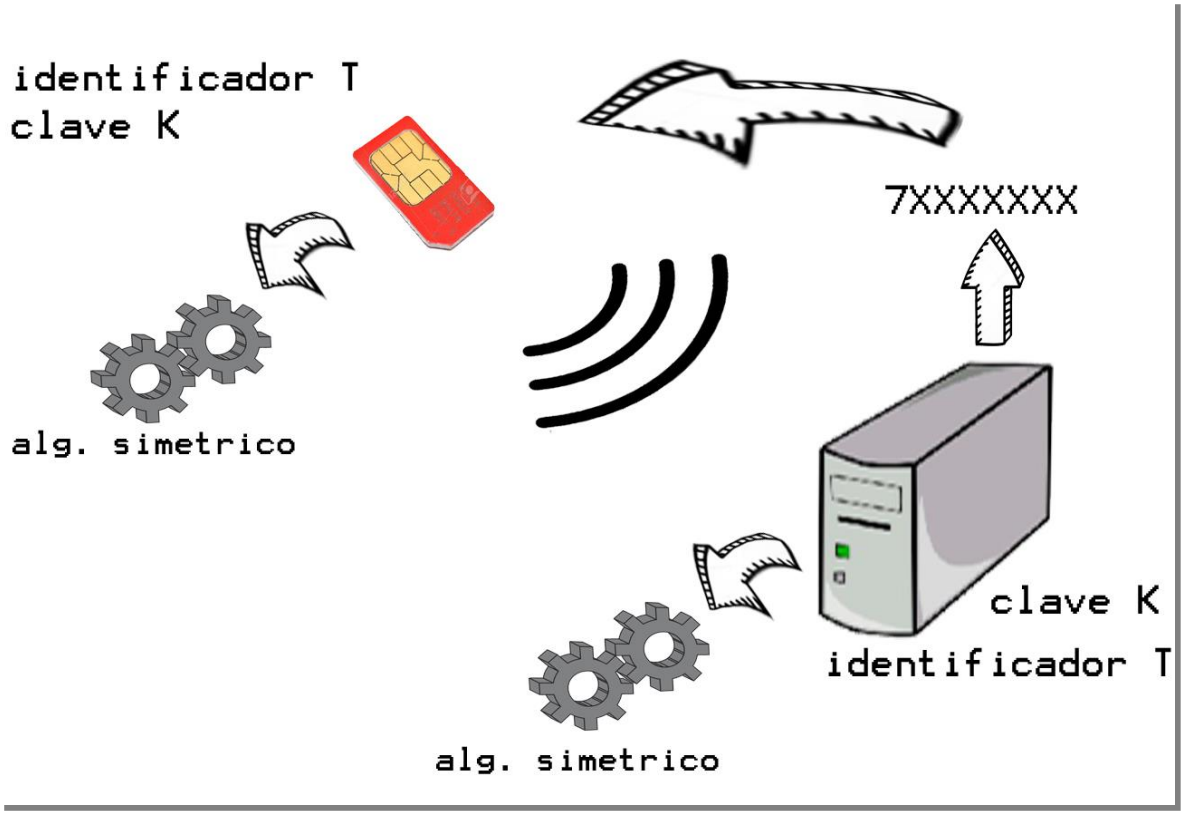
Por ejemplo el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles. Actualmente ya existen ordenadores especializados que son capaces de probar todas ellas en cuestión de horas. Hoy por hoy se están utilizando ya claves de 128 bits que aumentan el “espectro” de claves posibles (2 elevado a 128) de forma que aunque se uniesen todos los

ordenadores existentes en estos momentos no lo conseguirían en miles de millones de años.

El funcionamiento de la criptografía simétrica es el siguiente: el emisor quiere hacer llegar un documento al receptor. Toma ese documento y le aplica el algoritmo simétrico, usando la clave única que también conoce el receptor. El resultado es un documento cifrado que se puede ya enviar tranquilamente. Cuando el receptor recibe este documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar. Si el documento cifrado no ha sido alterado por el camino y la clave es la misma, se obtendrá el documento original.



Un ejemplo de criptografía simétrica es la “autenticación de un móvil GSM“: por qué sabe que es nuestro nº de teléfono aunque metamos la tarjeta SIM en otro teléfono. El mecanismo es el siguiente:



CRIPTOGRAFÍA ASIMÉTRICA VENTAJAS

La criptografía de clave simétrica tiene varios beneficios. Este tipo de cifrado es muy fácil de usar. Además, es muy útil para el cifrado de archivos de datos personales, ya que sólo se requiere de una clave. La criptografía de clave simétrica es rápida y utiliza menos recursos informáticos que otras formas de cifrado. Esta forma de cifrado también se puede utilizar para ayudar a prevenir riesgos en la seguridad. Si utilizas diferentes claves compartidas con diferentes personas, cuando una de las claves está en peligro, sólo una persona se ve afectada en lugar de todos.

CRIPTOGRAFÍA ASIMÉTRICA DESVENTAJAS

Hay varias desventajas en el uso de la criptografía de clave simétrica. 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. La criptografía de clave simétrica también es vulnerable a ataques de fuerza bruta y ataques de diccionario. Según la "Guía CWNA a las

LAN inalámbricas", los ataques de fuerza bruta se producen cuando un usuario intenta descifrar la clave mediante el uso de un programa que cambia sistemáticamente un carácter a la vez hasta que se consigue la llave correcta. Un ataque de diccionario es cuando un usuario codifica palabras del diccionario y luego las compara con el mensaje codificado. Esto se hace hasta que el atacante encuentra una coincidencia y conoce la palabra que conforma la contraseña.

CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica se basa en el uso de **dos claves**: **la pública** (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y **la privada** (que no debe de ser revelada nunca).

Cada participante en un sistema de claves públicas dispone de un par de claves. Una clave se designa como clave privada y se mantiene secreta. La otra clave se distribuye a quien lo desee; esta clave es la clave pública.

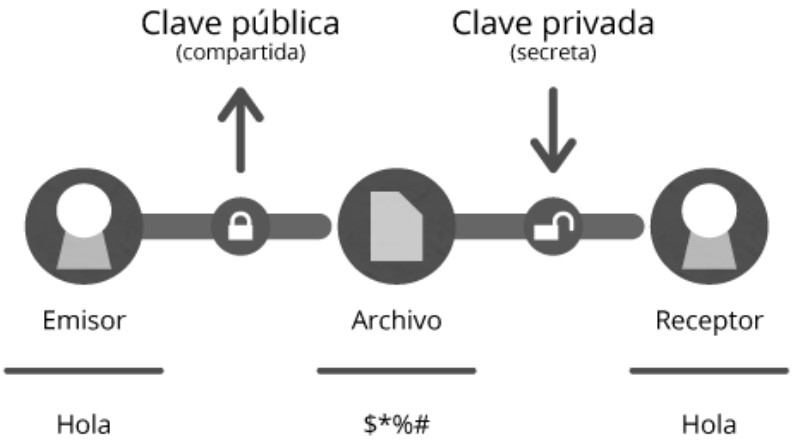
Cualquier usuario puede cifrar un mensaje utilizando su clave pública, pero sólo usted puede leerlo. Cuando recibe el mensaje, lo descifra utilizando la clave privada.

De forma parecida, puede cifrar un mensaje para cualquier otro utilizando su clave pública y, a continuación, descifrándola utilizando su clave privada.

Entonces podrá enviar el mensaje de forma segura a través de una conexión no segura.

Este tipo de cifrado tiene características que lo hacen muy adecuado para su uso general:

- El cifrado de clave pública sólo requiere dos claves por participante.
- La necesidad de mantener el secreto es más fácil de cumplir: únicamente debe mantenerse secreta la clave privada y puesto que no necesita compartirse, es menos vulnerable al robo en la transmisión que la clave compartida en un sistema de claves simétricas.
- Las claves públicas pueden publicarse, lo que elimina la necesidad de compartir previamente una clave secreta antes de la comunicación. Cualquiera que conozca la clave pública puede utilizarla para enviar un mensaje que sólo el usuario implicado puede leer.



DIFERENCIAS ENTRE EL SISTEMA SIMÉTRICA Y ASIMÉTRICA

- El sistema simétrico es más insegura ya que el hecho de pasar la clave es una gran vulnerabilidad
- El sistema simétrico puede cifrar y descifrar en menor tiempo del que tarda el sistema asimétrico.
- El cifrado simétrico usa mismo tipo de claves (secretas).
- El cifrado asimétrico usa distintos tipos de claves (privadas y públicas).

CERTIFICADOS DIGITALES

Para utilizar el cifrado asimétrico, debe haber una manera de descubrir otras claves públicas. La técnica típica es utilizar certificados digitales (también conocidos simplemente como certificados). Un certificado es un paquete de información que identifica a un usuario o un servidor y contiene información como el nombre de la organización, la organización que emitió el certificado, la dirección de correo electrónico y país y clave pública del usuario.

Cuando un servidor y un cliente requieren una comunicación cifrada segura, envían una consulta a través de la red a la otra parte, que devuelve una copia del certificado. Se pueden extraer la clave pública de la otra parte del certificado. Un certificado puede utilizarse también para identificar de forma exclusiva el titular.

FIRMA DIGITAL

Una firma digital es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.

Consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

* Vigencia del certificado digital del firmante.

* Revocación del certificado digital del firmante.

* Inclusión de sello de tiempo.