Índice

Alejandro García y Jaime Garzón: Documentación y fundamentos teoriocos.
Artur Kayda: Obtención de certificado
Lara Urbina, Hao Zhe Chen: Uso de certificado
Mario López-Gasco: Autofirma
Gabriel Revilla: Apartado gráfico

1. Privacidad de la información

Desde que el hombre es capaz de comunicarse por escrito, ha tenido la necesidad de preservar la privacidad de la información en la transmisión de mensajes confidenciales entre el emisor y el receptor.
Surge la necesidad de garantizar la confidencialidad de la información, por eso se han desarrollado diversas técnicas de enmascaramiento u ocultación de la información, siendo en la actualidad uno de los principales objetivos que persigue la seguridad informática.

2. Historia de la criptografía.

La palabra criptografía proviene de dos palabras del griego, cripto, que significa escondido, y grafía, que quiere decir escritura.
Los tres tipos de encriptación, son la Escítala, Polybios, y la famosa maquina Enigma.

El Escítala aparece en el siglo V A.C. utilizada por los espartanos para cifrar los mensajes de guerra. Consistia de una cinta enrollada al rededor de un bastón, y se escribía el mensaje. Se desenrollaba y el texto estaría encriptado, que solo se podria ver el mensaje usando un bastos del mismo ancho.

Polybios aparece en el siglo II antes de cristo, desarollado por los griegos, el nombre se dice que proviene del que lo invento

Enigma era una maquina que disponia un mecanismo de cifrato rotatorio, que servia para cifrar y descifrar mensajes utilizada por los nazis en la segunda guerra mundial.

3. ¿Qué se quiere conseguir?. Autenticación, confidencialidad, integridad, no repudio.

Confidencialidad: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información.

Autenticidad: garantiza que el emisor es realmente quien dice ser.

Integridad: diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización.

No repudio: este objetivo garantiza la participación de las partes en una comunicación.

4. Criptografía simétrica, asimétrica e híbrida.

Criptografía Simétrica

El emisor y el receptor previamente se ponen de acuerdo que clave van a utilizar.
En este cifrado se utiliza la misma clave para cifrar y para descifrar.
Este tipo de cifrado no es del todo seguro dado que la clave tiene que viajar, hasta el receptor. Si son interceptadas la clave y el mensaje se podría descifrar el mensaje.

Criptografía Asimétrica

Consiste en que cada una de las partes involucradas en una comunicación segura tienen una pareja de claves. Una de ellas, pública, que deberá intercambiar con cada una de las entidades con las que quiera comunicarse mensajes secretos, y otra de ellas privada, y que por tanto, jamás debe comunicar a nadie.

Para cifrar un mensaje, el emisor utilizará la clave pública del receptor, y a su vez, el receptor descifrará este mensaje haciendo uso de su clave privada.

Criptografía híbrida:

Dado que la criptografía de clave publica el proceso de cifrado y descifrado es lento. Además el gran tamaño de la información cifrada con la clave publica en comparación a la cifrada con la clave privada.
Entonces lo ideal seria utilizar criptografía de clave privada para intercambiar mensajes, pues estos son más pequeños y además el proceso es rápido, y utilizar criptografía de clave pública para el intercambio de las claves privadas.

5. **Algoritmos, Kertchoff, Función resumen**

Un algoritmo es un conjunto de instrucciones ordenadas y finitas que permite llevar a cabo una actividad. Un ejemplo de esto son los manuales de instrucciones.

Los principios o principio de Kerckhoffs: Son seis propiedades desesables en un sistema criptográfico y son las siguientes:

1º:Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.

2º:La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
Significa que todo el mundo puede saber como ha sido diseñado pero no por ello debe ser ineficiente

3º:La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas. Esto reduciría la eficacia del sistema porque alguien podría robar o extraviar la clave

4º:Los criptogramas deberán dar resultados de letras y números. Utilizar distintos caracteres aumenta la fuerza y la seguridad de la clave.

5º:El sistema debe ser operable por una única persona.

6º:El sistema debe ser fácil de utilizar.

Los hash o funciones resumen son algoritmos que crean una salida alfanumérica de una longitud generalmente fija a partir de una entrada. Estas funciones sirven para asegurar que un archivo no ha sido modificado, hacer ilegible una contraseña o para firmar digitalmente un contenido. En la actualidad se utilizan para en criptar contraseñas y que no aparezcan en texto plano.

6. Firma digital. Autenticidad, integridad, no repudio

La firma electrónica es **un conjunto de datos electrónicos** que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

Identificar al firmante de manera inequívoca porque el es el único que puede emitir ese conjunto de datos. (autenticidad)

Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación. Para ello se utilizan funciones Hash (integridad)

No repudio. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico.

Dni Electónico

El certificado electrónico o el DNI electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación. Estos proveedores pueden ser tanto organismos públicos como la Fábrica Nacional de Moneda y Timbre o FNMT para abreviar, u organismos privados como Camerfirma.

7.Certificados digitales. Autenticidad,confidencialidad, Firma electrónica

El Certificado FNMT de Persona Física, que se emite sin coste a cualquier ciudadano que esté en posesión de su DNI o NIE, es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor con unos Datos de verificación de Firma y confirma su identidad personal.

Este certificado le **permitirá identificarse de forma telemática y firmar o cifrar documentos electrónicos.**

8.PKI;FNMT,Camerfirma.

PKI son las siglas en inglés de infraestuctura de clave pública. Permite a los usuarios autenticarse ante otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes o firmar digitalmente información con lo que ello conlleva

FNMT y Camerfirma son ejemplos de entidades certificadoras que pueden emitir y revocar certificados, así como de verificar la identidad del solicitante del certificado.

9.DNI ELECTRÓNICO

a. ¿Qué es el DNI Electrónico?

El DNI electrónico es un documento emitido por la Dirección General de la Policía (Ministerio del Interior). Además de acreditar físicamente la identidad personal de su titular permite:

- **Acreditar electrónicamente** y de forma inequívoca su identidad.
- **Firmar digitalmente** documentos electrónicos, otorgándoles una **validez jurídica** equivalente a la que les proporciona la firma manuscrita.

El DNI electrónico incorpora un pequeño circuito integrado (**chip**), que contiene los mismos datos que aparecen impresos en la tarjeta (datos

personales, fotografía, firma digitalizada y huella dactilar digitalizada) junto con los **certificados de Autenticación** y de **Firma Electrónica**.

De esta forma, cualquier persona podrá realizar múltiples gestiones online de forma segura con las Administraciones Públicas, con empresas públicas y privadas, y con otros ciudadanos, a cualquier hora y sin tener que desplazarse ni hacer colas.

Certificados Electrónicos en el DNIe

Con el DNI electrónico se obtienen dos certificados:

> **Certificado de Autenticación**: Garantiza electrónicamente la identidad del ciudadano al realizar una transacción telemática. Este Certificado asegura que la comunicación electrónica se realiza con la persona que dice ser, con el certificado de identidad y la clave privada asociada al mismo.
>
> **Certificado de Firma**: Permite la firma de trámites o documentos, sustituyendo a la firma manuscrita. Por tanto, garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma.

AUTOFIRMA

Autofirma es un software que firma con certificado electróncio que es como una firma real, esto sirve para identificar al emisor de forma inequívoca , asegura que el documento firmado es el mismo que el original y el no repudio que significa que no se puede decir que no has firmado el correo.
Este software se podrá descargar de este enlace:
http://firmaelectronica.gob.es/Home/Descargas.html
Será importante seleccionar que versión nos vale(x86 o x64) normalmente los ordenadores modernos son de x64.
Antes de instalar este software deberemos tener importado nuestro certificado en el navegador de internet explorer o firefox o importarlo despues de la instalación.
Dentro de la aplicación le daremos a seleccionar fichero a firmar y por último firmar fichero.

BIBLIOGRAFÍA

Esta documentación la podeis encontrar en:

http://villaverdesmr.es/certificados-digitales

Documentación sobre criptografía, páginas de FNMT:

https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-android

http://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-asimetrica/cifrado-de-clave-publica