TEMA 4: CRIPTOGRAFÍA

1. CIFRADO - CRIPTOGRAFÍA

Las tecnologías de seguridad mas importantes son los firewall (cortafuegos), la criptografía y los IDS (sistemas de detección de intrusiones)

La criptografía nos ayuda a mejorar la seguridad informática potenciando la confidencialidad, la integridad y la responsabilidad.

La mayoría de las herramientas y técnicas de seguridad informática se basan en la utilización de la criptografía o la utilizan en alguno de sus componentes.

El **cifrado** es simplemente la ofuscación de la información, de tal forma que quede oculta a los individuos no autorizados y permita verla a los individuos autorizados.
Los individuos se definen como autorizados si tienen la clave apropiada para descifrar la información.

NOTA: ofuscar.(Del lat. offuscāre).
1. tr. Deslumbrar, turbar la vista. U. t. c. prnl.
2. tr. Oscurecer y hacer sombra.
3. tr. Trastornar, conturbar o confundir las ideas, alucinar. U. t. c. prnl.

La criptografía surge de la necesidad de preservar la privacidad de la información en la transmisión de mensajes confidenciales entre el emisor y el receptor.

El concepto es simple, implementarlo ya es más complicado.

Implementación hardware – implementación software.

La intención de cualquier sistema de cifrado es hacer extremadamente difícil que un individuo no autorizado tenga acceso a la información, incluso si el individuo tiene la información cifrada.

A través del uso de la criptografía proporcionamos parte de los **servicios de la seguridad**:

- **Confidencialidad**: El cifrado puede ser utilizada para ocultar la información a los individuos no autorizados, ya sea en transito o almacenada.
- **Integridad**: El cifrado puede ser utilizada para identificar modificaciones a la información ya sea en transito o almacenada.
- **Responsabilidad**: El cifrado puede ser utilizada para autenticar el origen de la información e impedir que la fuente original de dicha información se niegue a aceptar que la información provino de ella.

Texto original (Plaintext): La información en su forma original. También se conoce como texto simple (**cleartext**).
Texto cifrado (Ciphertext): La información después que ha sido ofuscada por el algoritmo de cifrado.
Algoritmo: El método de manipulación utilizado para cambiar el texto original al texto cifrado.
Clave: Los datos de entrada en el algoritmo para que éste transforme ya sea el texto original en texto cifrado o el texto cifrado en texto original.
Cifrar: El proceso de realizar el cambio del texto original al texto cifrado.
Descifrar: El proceso de realizar el cambio del texto cifrado al texto original.

Criptografía: El arte de encubrir la información mediante el uso de cifrado.
Criptógrafo: Individuo que practica la criptografía.
Análisis criptográfico: Analizar algoritmos criptográficos con la intención de identificar debilidades.
Analista criptográfico: Individuo que utiliza el análisis criptográfico.

Ataques contra la criptografía: los sistemas de cifrado pueden ser atacados de tres maneras:

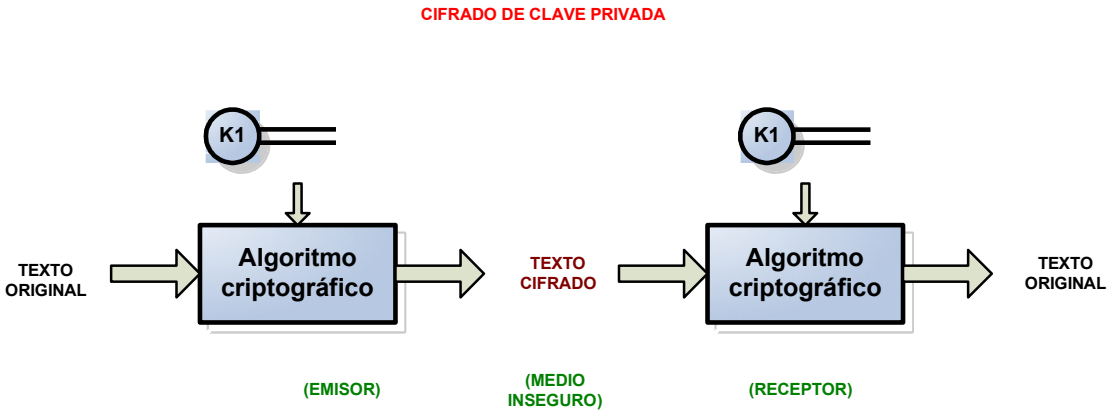
- A través de las debilidades en el algoritmo: estudiando debilidades en el algoritmo el texto puede ser recuperado sin necesidad de conocer la clave.
- Mediante la fuerza bruta en contra de la clave: intentos de usar toda clave posible sobre el texto cifrado para hallar el texto original. Un algoritmo se considera seguro en términos computacionales si el coste de adquirir la clave usando la fuerza bruta es mayor que el de la información que protege.
- Por medio de las debilidades en el sistema de entorno, por lo general es más fácil atacar al sistema de entorno que al algoritmo de cifrado. La elección del sistema de entorno es tan importante para la seguridad global de la cifrado como el algoritmo y la clave.

2. CIFRADO DE CLAVE PRIVADA O SIMÉTRICA

Existen dos tipos principales de cifrado: de clave privada y de clave pública.

El ***cifrado de clave privada o cifrado simétrico*** requiere que todas las partes que están autorizadas para leer la información tengan la misma clave. Esto reduce el problema de proteger la información a uno solo, proteger la clave. El cifrado de clave privada es el tipo de cifrado utilizado con mayor amplitud. Ésta proporciona la confidencialidad de la información y cierta garantía de que la información no pueda ser modificada mientras se encuentra en tránsito.

El cifrado de clave privada también se conoce como cifrado de clave simétrica, porque en ella se utiliza la misma clave tanto para cifrar la información como para descifrarla.



Tanto el remitente como el receptor de la información deben tener la misma clave.

El cifrado de clave privada mantiene la confidencialidad de la información mientras se encuentra cifrada. Solamente quienes conocen la clave pueden descifrar el mensaje. Cualquier cambio al mensaje mientras se encuentra en transito también será notificado en la medida que el descifrado no funcionará adecuadamente. El cifrado de clave privada no proporciona autenticación, en la medida que cualquier persona que tenga acceso a la clave puede crear, cifrar y enviar un mensaje valido.

Hablando en términos generales, el cifrado de clave privada es rápida y puede ser fácil de implementar tanto en hardware como en software.

2.1 CÓDIGOS DE SUSTITUCIÓN

El código de sustitución funciona sobre el texto original una letra a la vez. Mientras el remitente y el emisor del mensaje utilicen el mismo esquema de sustitución, el mensaje puede ser comprendido.

La clave para el código de sustitución es, o bien el número de letras que se desplazará el alfabeto, o bien un abecedario completamente reordenado.

2.2 LIBRETAS DE UN SOLO USU (One-Time Pads)

Las libretas de un solo uso (OTP) son el único sistema de cifrado teóricamente indescifrable.

Una OTP es una lista de números, en orden completamente aleatorio, que se utiliza para codificar un mensaje.

2.3 DES (Data Encryption Standard) - ESTANDAR DE CIFRADO DE DATOS

DES utiliza una clave de 56 bits. (8 bytes con un bit de paridad)

El DES es un cifrado en bloque que funciona sobre un bloque de 64 bits de texto original a la vez.

Existen 16 rondas de cifrado en el DES con una subclave diferente utilizada en cada ronda. La clave pasa a través de su propio algoritmo para derivar las 16 subclaves.

Existen cuatro modos de operación para el DES:

- Libro de código electrónico: una entrada idéntica proporciona una salida idéntica.
- Encadenamiento de bloques cifrados.
- Retroalimentación del cifrado.
- Retroalimentación de salida.

2.4 TDES (Triple DES)

En 1992, las investigaciones señalaron que DES podía ser empleado múltiples veces para crear un cifrado mas robusto.

TDES aplica DES tres veces seguidas con tres o dos claves distintas. La segunda operación es en realidad un descifrado.

TDES es un algoritmo relativamente rápido, todavía puede ser implementado en hardware.

2.5 CIFRADO DE CONTRASEÑA

El esquema de cifrado de contraseña estándar de UNIX es una variación de DES. (Una función de cifrado en un solo sentido).

La debilidad principal de este sistema reside en la elección de la contraseña.

2.6 AES (Advanced Encryption Standard) - RIJDAEL - CIFRADO ESTANDAR AVANZADO

A finales del 2000 se dio a conocer este algoritmo elegido sobre la base de su fortaleza, así como por su conveniencia para redes de alta velocidad y por su implementación en hardware.

Rijndael es un cifrado en bloque que utiliza claves y bloques de 128, 192 o 256 bits. Estas longitudes de clave hacen que los ataques por medio de fuerza bruta sean inverosímiles en este momento.

El algoritmo se compone de 10 a 14 rondas o series, dependiendo del tamaño del bloque de texto original y de las dimensiones de la clave.

Es una alternativa apropiada a TDES.

2.7 ALGORITMOS DE CLAVE PRIVADA

DES
TDES
AES
RC4
RC5
IDEA
Skipjack
Blowfish
Twofish
CAST-128
GOST

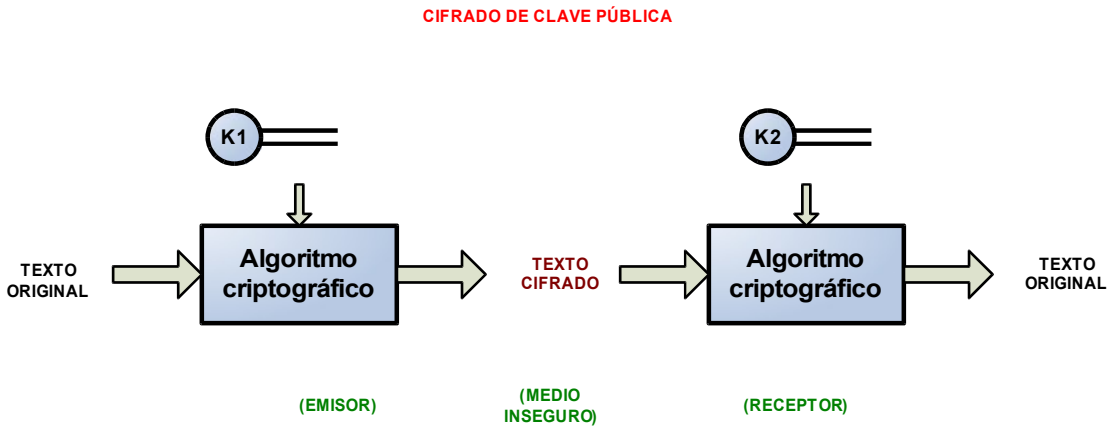
Cualquiera de estos algoritmos puede aparecer en productos de seguridad. Es probable que todos ellos sean lo suficientemente robustos para uso general.

3. CIFRADO DE CLAVE PÚBLICA O ASIMÉTRICA

El cifrado de clave pública es una invención más reciente que la de clave privada. La principal diferencia entre los dos tipos de cifrado es el número de claves utilizadas en la operación, el cifrado de clave pública utiliza dos claves, una clave es utilizada para cifrar y, posteriormente, se utiliza una clave diferente para descifrar la información.

En el ***cifrado de clave pública o asimétrica*** tanto el remitente como el receptor de la información deben tener una clave distinta.

Las claves están relacionadas entre si (par clave o key par) pero son diferentes. La relación entre las claves es tal que la información cifrada por K1 solamente puede ser descifrada por su par K2. Si K2 cifra la información, esta puede ser descifrada únicamente por K1.



En la práctica, una clave se conoce como la **clave privada** y la otra es denominada **clave pública**.

La clave privada se mantiene en secreto por el propietario del par clave.

La clave pública se divulga con información como quien es el propietario.

Otra propiedad del cifrado de clave pública es que si tenemos una de las claves del par, no podemos calcular la otra clave. Por eso es correcto divulgar la clave pública.

Si se desea **confidencialidad**, el cifrado se realizada con la clave pública. De esa manera solamente el propietario del par clave puede descifrar la información, puesto que la clave privada se mantiene en secreto por el propietario.

Si se desea **autenticación**, el propietario del par clave cifra la información con su clave privada. Solamente la clave pública correcta divulgada puede descifrar de modo acertado la información, de modo que solamente el propietario del par clave (el poseedor de la clave privada) podría haber enviado la información.

La **integridad** de la información en tránsito es protegida en cualquiera de las operaciones. La integridad de la información después de la recepción puede ser verificada si la información original fue cifrada con la clave privada del propietario.

La desventaja de los sistemas de cifrado de clave pública es que tienden a ser intensivos en términos computacionales, por lo que son mucho más lentos que los sistemas de clave privada.

Si combinamos el cifrado de clave pública con la de clave privada, obtenemos un sistema mucho más robusto.

El sistema de clave pública es utilizado para intercambiar claves y autenticar ambos extremos de la conexión. Posteriormente se utiliza el sistema de clave privada para cifrar el resto del tráfico.

3.1 INTERCAMBIO DE CLAVES DE DIFFIE-HELLMAN

El sistema Diffie-Hellman fue desarrollado (1976) para resolver el problema de la distribución de claves para los sistemas de cifrado de clave privada.

Diffie-Hellman no puede utilizarse para cifrar o descifrar información.

El intercambio de Diffie-Hellman es utilizado por muchos sistemas de seguridad para intercambiar claves secretas que se pueden utilizar con el trafico adicional.

La única debilidad en el sistema Diffie-Hellman es que es susceptible de un ataque desde una posición central (este ataque es poco probable en el mundo real).

http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/

3.2 RSA (Rivest – Shamir – Adleman)

En 1978, Ron Rivest, Adi Shamir y Len Adleman publicaron el algoritmo de clave pública Rivest-Shamir-Adleman RSA.

RSA puede ser utilizado tanto para el cifrado como para el descifrado.

Se supone que el propietario del par clave mantiene en secreto la clave privada, y que la clave pública es divulgada. Por tanto, si la información está cifrada por la clave pública, solamente el propietario puede descifrarla.

El algoritmo puede ser invertido para proporcionar la autenticación del remitente. Para la autenticación, el propietario cifra la información con su clave privada. Solamente el propietario podría hacer esto, pues la clave privada se mantiene en secreto. Todos pueden ahora descifrar la información utilizando su clave pública.

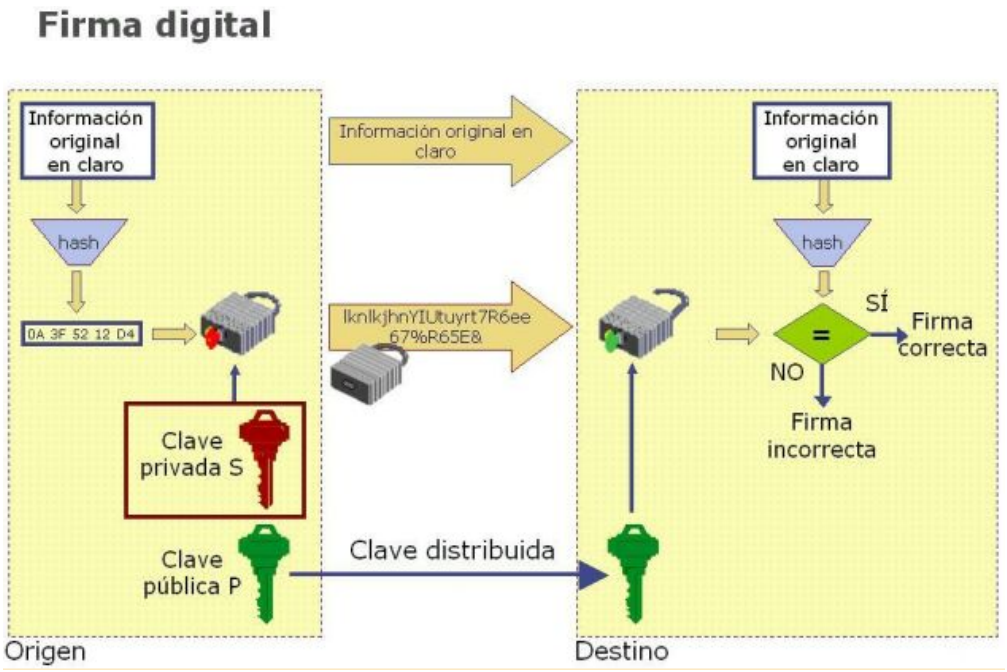
3.3 ALGORITMOS DE CLAVE PÚBLICA

DH
RSA
Elgamal
Algoritmo de firma digital (Digital Signature Algorithm, **DSA**)
Cifrado de curva elíptica **ECC**

4. FIRMA DIGITAL

La firma digital y la firma electrónica son conceptos distintos, solo la firma digital utiliza un certificado digital.

La firma digital sustituye a la manuscrita en el mundo de la informática. Si firmamos un documento de forma digital, no podemos decir que no lo hemos firmado nosotros y seremos responsables de lo que en el se diga.



Proceso de firma:

1. Se calcula un valor resumen del documento utilizando un algoritmo (Ej. SHA).
2. Ciframos el resumen con nuestra clave privada.
3. El resultado se añade al documento original como firma digital del documento.

Dos documentos distintos firmados con el mismo certificado digital tienen firmas distintas (porque los resúmenes son distintos); esto es una diferencia con respecto a la firma manuscrita (que no garantiza la integridad del documento original).

Proceso de comprobación de la firma:

1. La firma que nos llega junto al documento se descifra utilizando la clave pública del certificado del firmante. Necesitamos la clave pública del firmante.
2. Se obtiene (por otra parte) el valor resumen utilizando el documento y el mismo algoritmo que se utilizó para firma el documento.
3. Se comparan los dos resúmenes, si son iguales la firma es válida, si son distintos la firma es nula.

Con la firma digital se pretende proteger la información de modificaciones después de que haya sido recibida y descifrada.

En primer lugar, la información pasa por un resumen de mensaje con función de cálculo de dirección. Esta función crea una suma de verificación de la información.
Esta suma es cifrada entonces mediante la clave privada del usuario.
La información y la suma de verificación cifradas son enviadas al receptor de la información.

Cuando el receptor recibe la información, también puede pasarla por la misma función de cálculo de dirección. Descifra la suma de verificación que llega con el mensaje y compara las dos sumas de verificación. Si coinciden, la información no se ha modificado.

Al conservar la suma de verificación cifrada original con la información, esta siempre puede ser verificada para averiguar si ha sufrido modificaciones.

La seguridad y la utilidad de una firma digital dependen de dos elementos críticos:

- La protección de la clave privada del usuario.
- Una función segura de fragmentación.

4.1 FUNCIONES CONDENSADORAS SEGURAS – RESUMEN – HASH

Las funciones condensadoras seguras son necesarias para las firmas digitales. Una función condensadora puede ser llamada segura si:

- La función es de un solo sentido. La función crea la suma de verificación a partir de la información, pero no se puede crear la información a partir de la suma de verificación.
- Es muy difícil construir dos fragmentos de información que proporcionen la misma suma de verificación. Si se modifica un bit en la información cambiará una gran cantidad de bits en la suma de verificación.

Las funciones de cálculo de dirección seguras deben crear una suma de verificación de al menos 128 bits. Las dos funciones de cálculo de dirección seguras más comunes son MD5 que produce una suma de verificación de 128 bits y SHA, que produce una suma de verificación de 512 bits.

Las funciones resumen, condensadoras, hash son funciones que asocian a cada documento un valor numérico que tiene la propiedad de que conociendo el valor numérico, no se puede obtener el documento. Esta propiedad se conoce como funciones de un solo sentido.

MD5 genera un número de 128 bits
SHA (**SHA-0, SHA-1, SHA2**) genera un número de 160-512 bits

5. CERTIFICADO DIGITAL

Certificado digital:

- Documento que contiene información sobre una persona o entidad (Nombre, dirección,...), y una **clave pública** y una firma digital de un organismo de confianza (autoridad certificadora) que garantiza que la clave pública que contiene pertenece a dicha persona o entidad.
- **Clave privada** asociada a dicho certificado que la persona o entidad debe conservar y utilizar.

Existen muchas formas para los archivos que almacenan los certificados digitales. El mas conocido y utilizado en Internet es **X.509** donde podemos encontrar:

Versión, numero de serie.
Algoritmo de firma (utilizado para firmar el paquete X.509).
La autoridad certificadora (Emisor).
El periodo de validez (desde y hasta).
El propietario de la clave (asunto).
La clave pública.
La firma digital de la autoridad certificadora.
Huella digital.
Uso de la clave.
Dirección web de consulta.

6. PKI PUBLIC KEY INFRASTRUCTURE – INFRAESTRUCTURA DE CLAVE PÚBLICA

PKI Public Key Infrastructure – Infraestructura de clave pública

Todo lo necesario, tanto hardware como software, para comunicaciones seguras mediante el uso de certificados digitales y firmas digitales.

Objetivo: alcanzar los objetivos de seguridad: autenticidad, confidencialidad, integridad y no repudio.

La **PKI** están compuestas de:

- La **Autoridad de Certificación (CA – Certificate Authority)**, es la entidad de confianza encargada de emitir y revocar los certificados digitales. Ej. Fabrica Nacional de Moneda y Timbre.
- **Autoridad de Registro (RA – Registration Authority)** es la encargada de controlar la generación de certificados. Comprueba la identidad de los usuarios que solicitan los certificados. Ej. Seguridad Social, Agencia Tributaria, ...
- Las **Autoridades de los repositorios** donde se almacenan los certificados emitidos y aquellos que han sido revocados y han dejado de ser válidos.
- El **software** necesario para la utilización de los certificados digitales.
- La **Política de seguridad** definida para las comunicaciones.

6.1 ADMINISTRACION DE CLAVES

La administración de las claves es la ruina de todos los sistemas de cifrado.

Las claves son la información más valiosa de todo el sistema.

La administración de las claves no tiene que ver solo con la protección de las mismas mientras están en uso. También tiene que ver la creación de claves robustas, la distribución segura de claves de usuarios, la certificación de que estas sean correctas y la revocación de las mismas cuando hayan sido comprometidas o hayan caducado.

6.1.1 CREACION DE LA CLAVE

Ciertas claves tienen un rendimiento de seguridad deficiente respecto a ciertos algoritmos.

La mayor parte de los sistemas de cifrado tienen algún método para generar claves con las características adecuadas.

En algunos casos, se permite que los usuarios elijan la clave al seleccionar una contraseña. Debemos enseñar a los usuarios a elegir contraseñas robustas que incluyan números y caracteres especiales que dificultan la rotura de la clave por el método de fuerza bruta.

También hay que tener en cuenta la longitud de la clave; las más largas son más seguras.

Unas buenas recomendaciones para estos tiempos son emplear por lo menos claves de 80 bits para cifrado de clave privada, y claves al menos de 1024 bits para RSA y Diffie-Hellman. Las claves ECC de 160 bits también se consideran seguras.

6.1.2 DISTRIBUCIÓN DE LA CLAVE

Si la clave no se protege durante el tránsito, puede ser copiada o hurtada, y todo el sistema de cifrado quedará inseguro. Por tanto, el canal de distribución debe ser seguro por si mismo.

Podemos utilizar el intercambio de claves de Diffie-Hellman para crear y distribuir muchas claves de sesión (claves a corto plazo utilizadas para una sesión simple o una pequeña cantidad de tráfico). No es necesario viajar para transportar la clave.

Cualquier clave que sea utilizada por largos periodos de tiempo requerirá de mayor cuidado.

En el caso de pares de clave RSA, una clave debe mantenerse en secreto mientras que la otra puede ser publicada. La clave publicada debe divulgarse en una manera tal que impida su alteración (certificación de la clave).

Si los pares son generados por una autoridad central, la clave privada debe ser transmitida de manera segura hacia el propietario del par.

Si el propietario genera el par clave, la clave pública tiene que ser transmitida de manera segura hacia la autoridad central.

6.1.3 CERTIFICACIÓN DE LA CLAVE

Si las claves son transmitidas hacia un destino remoto por algún medio, deben ser verificadas una vez que lleguen, para asegurarse de que no han sido alteradas durante el tránsito. Esto puede ser un proceso manual o puede realizarse mediante algún tipo de firma digital.

Las claves públicas están destinadas a ser divulgadas o proporcionarse a otros usuarios, y también deben ser certificadas como pertenecientes al propietario del par clave. Esto puede hacerse a través de una autoridad central (autoridad de certificación CA). En este caso, la CA proporciona una firma digital en la clave pública y esto certifica que la CA considera que la clave pública pertenece al propietario del para clave.

6.1.4 PROTECCIÓN DE LA CLAVE

Las claves públicas de un par clave público no requieren la protección de la confidencialidad. Únicamente requieren la protección de la integridad proporcionada por su certificación. La clave privada de un par clave público debe ser protegida en todo momento. Por tanto, el archivo que contiene la clave debe quedar protegido igual que cualquier cinta de respaldo que pueda incluir el archivo. La mayor parte de los sistemas protegen la clave privada con una contraseña y evitando que el atacante obtenga el acceso al archivo.

Todas las claves para un sistema de clave privada deben ser protegidas. Si la clave se guarda en un archivo este debe ser protegido dondequiera que pueda residir (incluyendo cintas de respaldo, espacio de memoria, …)

6.1.5 REVOCACIÓN DE LA CLAVE

Las claves no tienen vidas infinitas.

Las claves de sesión solamente pueden existir para una sesión.

Algunas claves pueden ser certificadas para un periodo dado. Lo pares clave públicos son certificados para uno o dos años. La clave pública certificada identificará la fecha de caducidad, los sistemas no consideran válido el certificado después de esta fecha, por tanto, no es necesaria su revocación.

Las claves pueden perderse o ser comprometidas.

En el caso de la clave privada, su propietario debe avisar al los usuarios de la clave y cambiar de clave.

En el caso de los sistemas de cifrado de clave pública no hay forma de informar a todos los usuarios potenciales. Los usuarios de la clave pública deben visitar periódicamente el servidor de claves para averiguar si existe una revocación de la clave, y el propietario del par clave debe exponer la revocación a todos los servidores de clave potenciales. Los servidores de clave deben mantener la información de revocación por lo menos hasta el momento en el que el certificado original hubiera caducado.

6.2 CONFIANZA DEL SISTEMA

El concepto de confianza es el concepto subyacente en toda la seguridad y en el cifrado en particular. Para que el cifrado funcione se debe confiar en que la clave no está comprometida y que el algoritmo utilizado es un algoritmo robusto.

Para la autenticación y las firmas digitales se debe confiar también en que la clave pública pertenezca en realidad a la persona que la utiliza.

El mayor problema con la confianza es como establecerla y mantenerla. Existen dos modelos de confianza para el entrono de clave pública:

6.2.1 JERARQUICA

El modelo de confianza jerárquica es el mas sencillo de comprender, usted debe confiar en alguien debido a que alguien en una parte superior de la cadena le dice que debe confiar en él o ella.

La revocación de certificados puede ser un gran problema para las CA. La noticia de una revocación de clave debe estar disponible para cada entidad que pueda utilizar un certificado. Esto requerirá que cada entidad verifique con la CA antes de emplear un certificado.

6.2.2 WEB

Una red de confianza es un modelo de confianza alternativo. Este concepto fue utilizado primero por PGP (Pretty Good Privacy). El concepto es que cada usuario certifique su propio certificado y pase ese certificado a los asociados externos conocidos. Estos asociados pueden elegir firmar el certificado del otro usuario porque conocen a ese otro usuario.

Casa usuario es responsable de su propio certificado y de la verificación de otros.

Una organización puede escoger proveer un repositorio central para certificados y notas de revocación, pero no es necesario.

7. APLICACIONES DE LA CRIPTOGRAFÍA

Realiza un estudio sobre las aplicaciones de la criptografía indicando:

Herramienta o aplicación estudiada.
Plataformas que soportan dicha aplicación.
Tipo de cifrado que utiliza.
Algoritmos de cifrado que utiliza.
Utilidad de la herramienta.
Ejemplo de utilización.
Posibles ataques. Robustez de la herramienta.

Aplicaciones de cifrado de la información almacenada o de unidades de almacenamiento.

Firma digital y comprobación de la firma
Esteganográfía.
Utilización del cifrado para borrado seguro
Aplicaciones de cifrado de la instalación del sistema operativo.

Cifrado en el control de acceso y almacenamiento de contraseñas.

Cuentas locales
Active Directory – LDAP
VPN
RADIUS
KERBEROS
portal cautivo
servidor AAA

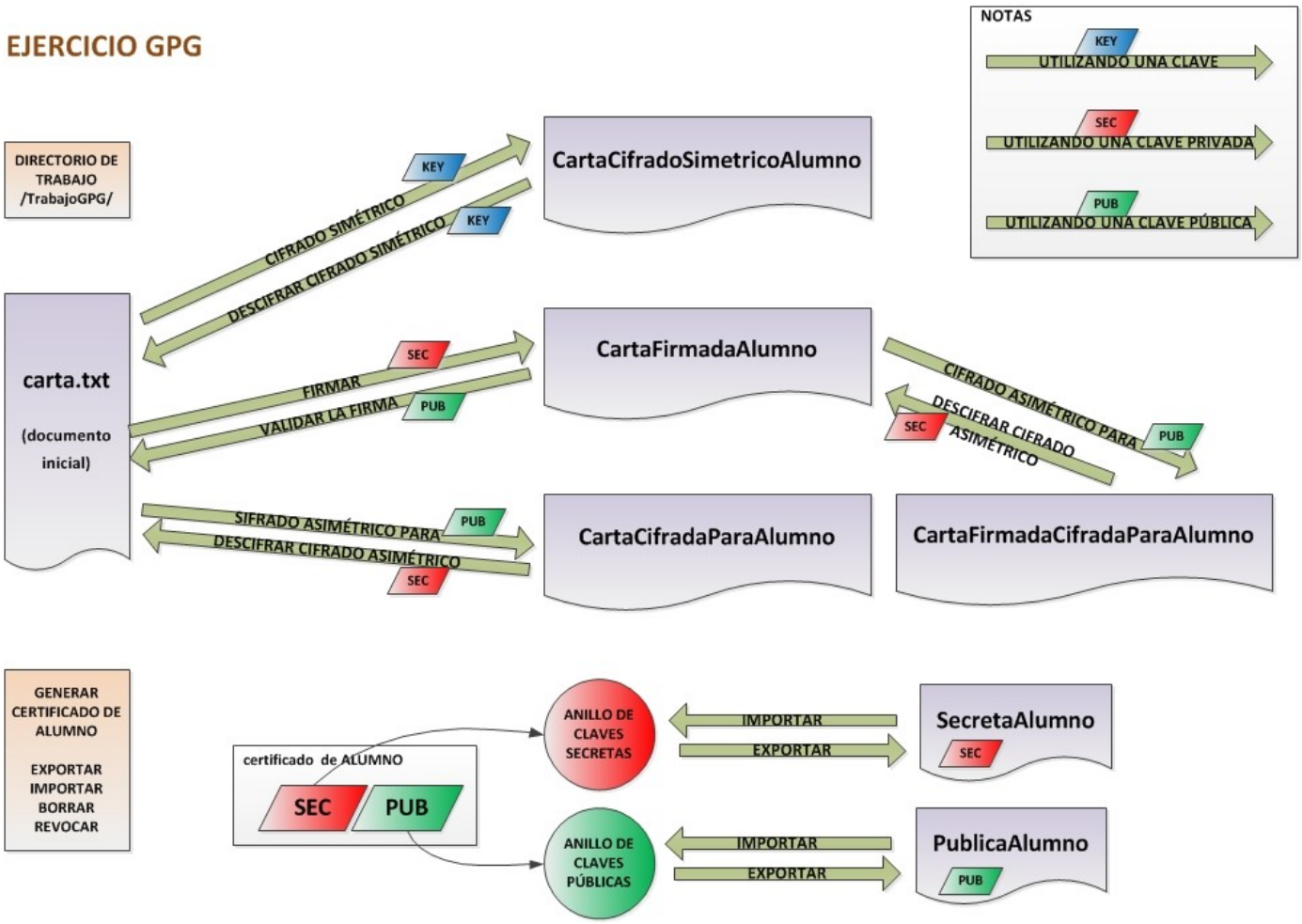
Gestión de certificados: generar, importar, exportar, revocar, borrar.

Autoridad de certificación.

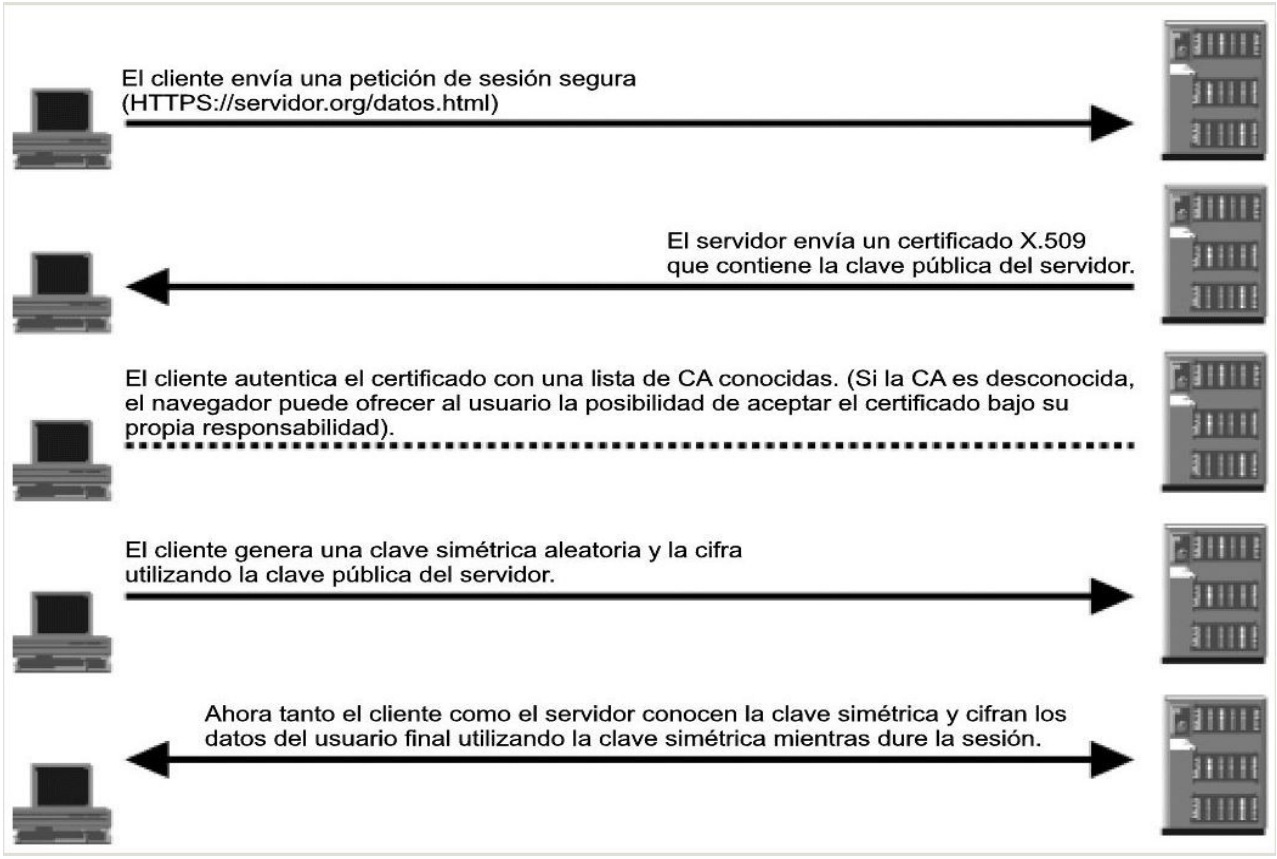
Cifrado en las comunicaciones:

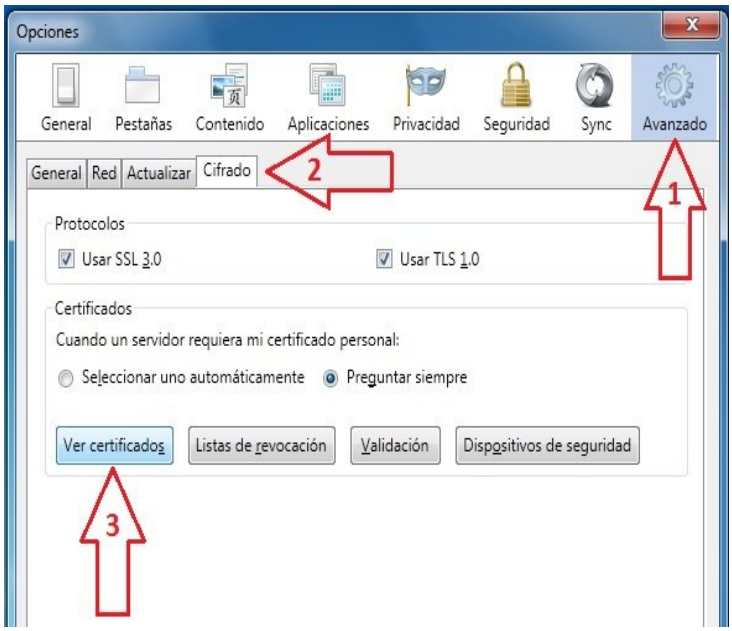
Capa de aplicación: **VPN**, **SSH, HTTPS, SFTP, FTPS,... (protocolos over SSL)**
Capa de transporte: **TLS/SSL** (sobre TCP), **DTLS**
¿como funciona SSL?
http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user277.htm
Capa de Internet: **IPsec**, **IPv6**
Capa de acceso a la red: **802.11 WI-FI** (**WEP**, **WPA**), **802.1Q** (**VLAN**)

7.1 CIFRADO DE DOCUMENTOS – FIRMA DE DOCUMENTOS

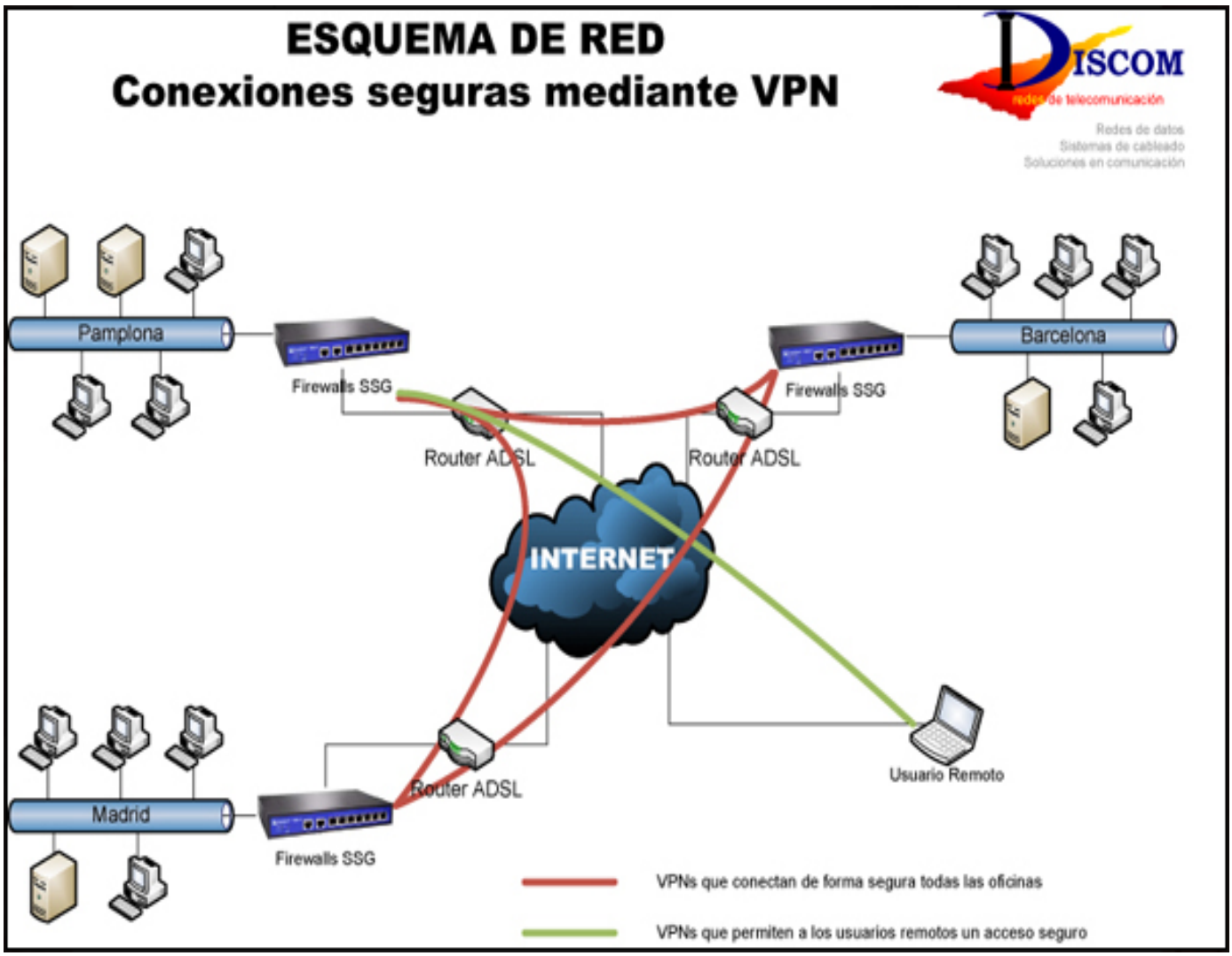


7.2 CONEXIÓN CIFRADA HTTPS

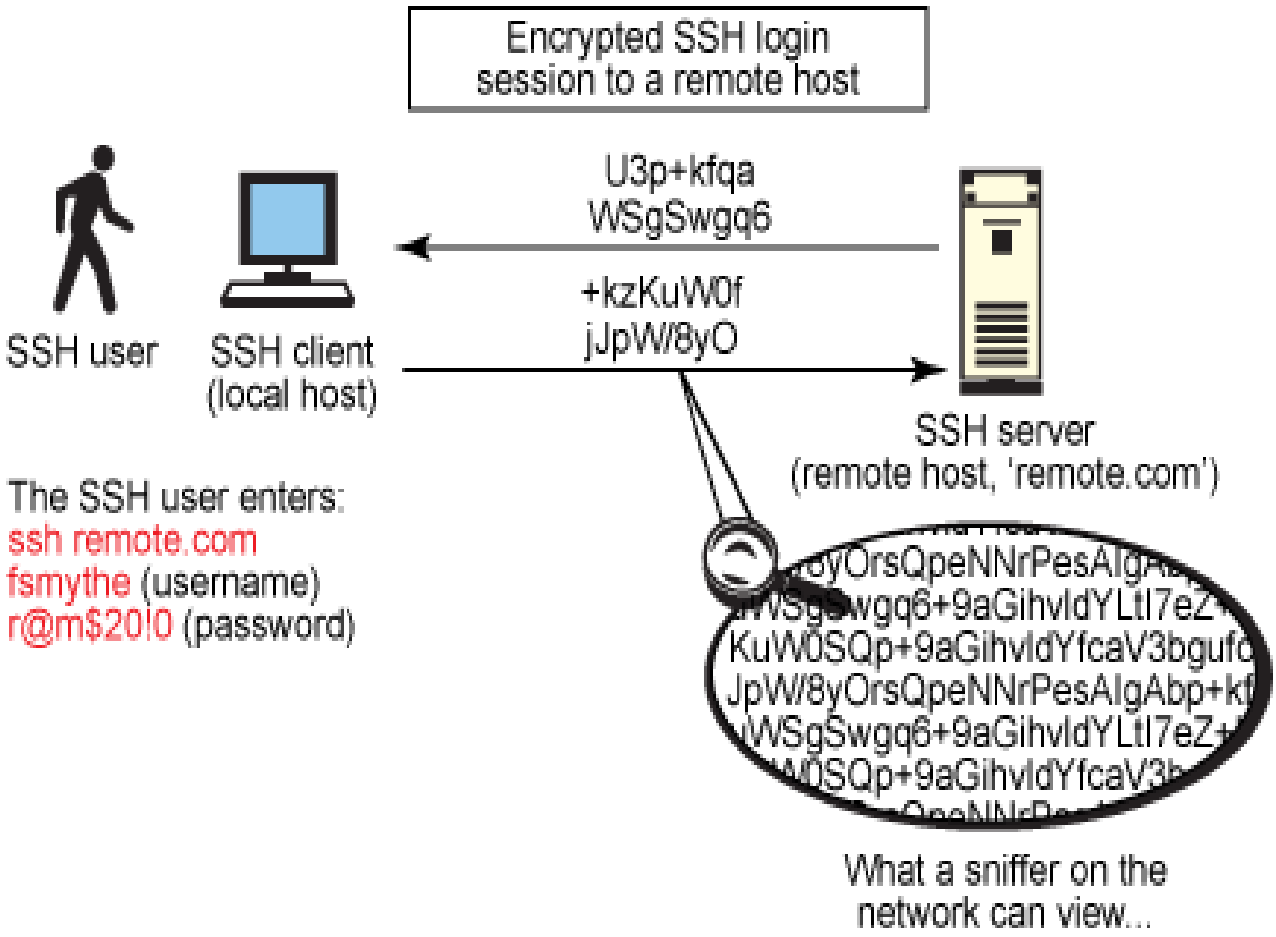




7.3 VPN


ESQUEMA DE RED
Conexiones seguras mediante VPN
DISCOM
redes de telecomunicación
Redes de datos
Sistemas de cableado
Soluciones en comunicación
Pamplona
Firewalls SSG
Router ADSL
Router ADSL
Firewalls SSG
Barcelona
INTERNET
Usuario Remoto
Madrid
Router ADSL
Firewalls SSG
VPNs que conectan de forma segura todas las oficinas
VPNs que permiten a los usuarios remotos un acceso seguro

7.4 ADMINISTRACIÓN REMOTA SEGURA – SSH



ENLACES INTERESANTES - BIBLIOGRAFÍA

Criptografía

Algoritmo criptográfico

Función hash **SHA** **SHA-2**

Criptografía simétrica **Esteganografía**

Criptografía asimétrica

Criptografía híbrida **GnuPG**

Firma digital **Firma electrónica**

Certificado digital **X.509**

Autoridad de certificación **PKI**

DNIe **CERES FNMT**

GnuPG

IZArc

Gpg4win

TinyCA

"Fundamentos de seguridad de redes" – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

"El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

"Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

EJERCICIOS

1. Explica los siguientes conceptos:
   - **Cifrado de clave privada o simétrica**
   - **Cifrado de clave pública o asimétrica**
   - **Función resumen**
   - **Certificado digital**
   - **PKI** (**Infraestructura de clave pública**)
   - **AC** (**Autoridad de certificación**)
2. Enumera los algoritmos de cifrado simétrico que conozcas.
3. Enumera los algoritmos de cifrado asimétrico que conozcas.
4. Enumera los algoritmos de función resumen que conozcas.
5. Enumera las **aplicaciones de la criptografía** que conozcas indicando que tipo de cifrado o algoritmo criptográfico utilizan y para que sirven.
6. Elegir distintas herramientas de **cifrado de archivos** y documentar:
   - Algoritmo que utiliza y características de seguridad.
   - Instalación y configuración.
   - Cifrado de documentos.
   - Descifrado de documentos.
7. Estudio de la herramienta **GnuPG** para Linux.

Avanzado

8. Estudia y define el concepto de **identificación digital**. Sistemas de identificación digitales.
9. Estudio: Sistemas de identificación: **firma electrónica, firma digital, certificados digitales** y otros.
10. Estudio: Política de contraseñas. Almacenamiento de contraseñas. **Cifrado de contraseñas**. (Sobre distintas plataformas). Técnicas para proteger las contraseñas almacenadas en el sistema.
11. Estudio: Métodos para asegurar la privacidad de la información transmitida: **SSL/TLS, SSH, HTTPS, IPSEC, RADIUS, KERBEROS**…
12. Estudio de la herramienta **gpg4win** para Windows.
13. Estudio de la herramienta **WinMD5** para el cálculo del valor resumen de un documento.
14. Estudio de la herramienta **OpenSSL**
15. Estudio sobre los certificados que utilizamos en los **navegadores**.
16. Estudio sobre las **autoridades de certificación** que utilizamos habitualmente. Ejemplos de certificados generados por dichas autoridades.
    Petición y retirada de certificados de una entidad emisora.
17. Creación de nuestros propios certificados. Herramienta **tynica2**. Valoración de otras herramientas de administración y generación de certificados.
    Instalación de una entidad emisora de certificados.
    Creación, distribución e instalación – utilización de los certificados creados.
18. Localiza y prueba una herramienta de **estaganografía**.
19. Creación y restauración de un script copia de seguridad para nuestro servidor Linux utilizando la herramienta **duplicity**. Comprimir y cifrar las copias. Almacenar la copia en un servidor FTP.
20. Implementación de una conexión remota segura: **SSH**.

21. Instalación y configuración de un servidor web seguro (**HTTPS, SSL/TLS**) (http://es.wikipedia.org/wiki/Ssl)
22. Estudio e implementación de una **VPN**.
23. Estudio sobre los algoritmos de cifrado de la comunicación **WI-FI.**
24. Estudio de la conexión segura a una red WI-FI.
25. Implantación de un servidor de correo seguro: **SMTP sobre SSL/TLS**
26. Implantación de un servidor de ficheros seguro: **SFTP** (FTP + SSH)
27. Implantación de un servidor **RADIUS**
28. Implantación de un servidor **KERBEROS**
29. Salida a Internet a través de un **portal cautivo.**