

# Privacidad, confidencialidad

Álvaro González Sotillo

30 de marzo de 2018

## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Autenticación.</b>	<b>2</b>
<b>3. Criptografía.</b>	<b>6</b>
3.1. Terminología. . . . .	6
3.2. Utilización . . . . .	7
<b>4. Criptografía simétrica</b>	<b>7</b>
4.1. Características principales: . . . . .	7
4.2. Algoritmos simétricos comunmente usados: . . . . .	9
<b>5. Criptografía asimétrica</b>	<b>10</b>
5.1. Características principales: . . . . .	10
5.2. El desafío/respuesta criptográfico. . . . .	12
<b>6. Criptografía híbrida</b>	<b>12</b>
<b>7. Firma digital</b>	<b>13</b>
7.1. Algoritmos de resumen criptográficos. . . . .	13
7.2. El mecanismo de la firma digital. . . . .	14
<b>8. Sistemas de confianza e intercambio de claves: la PKI y PGP</b>	<b>14</b>
8.1. PGP (Pretty Good Privacy) . . . . .	15
<b>9. x509 y la Public Key Infrastructure (PKI)</b>	<b>15</b>
<b>10. Aplicaciones</b>	<b>16</b>
10.1. Cifrado/descifrado en información almacenada . . . . .	16
10.2. Cifrado/descifrado en la red . . . . .	21
<b>11. El nivel de red/transporte: TLS y SSL</b>	<b>23</b>
<b>12. El nivel de aplicación</b>	<b>23</b>
12.1. Ejemplo: HTTPS . . . . .	24

---

<b>13.Firma digital</b>	<b>24</b>
13.1. FNMT . . . . .	24
13.2. DNIe . . . . .	24
<b>14.Referencias</b>	<b>25</b>

## 1. Introducción

Ya hemos estudiado muchas medidas de seguridad que ayudan a proteger la confidencialidad como propiedad segura importante que es, aunque en general, casi todas las medidas que hemos visto y que ayudaban a proteger la confidencialidad, también contribuían en mayor o menor medida al mantenimiento de las otras dos propiedades seguras: la disponibilidad y la integridad.

En éste tema, ahondaremos en algunas medidas y sistemas cuyo objetivo primordial es la confidencialidad.

- Hablaremos de la autenticación, el procedimiento por el cual una máquina puede reconocer al legítimo usuario de una determinada información.
- Hablaremos de la criptografía, la ciencia y los procedimientos para enviar y recibir información cifrada. Además de sus fundamentos, también hablaremos de la técnica del

desafío/respuesta, para evitar que las contraseñas viajen, y de los algoritmos de resumen criptográfico, que son la base de la firma digital.

- Hablaremos de la firma digital o electrónica, un procedimiento por el que se verifica el emisor de una información, y que contribuye al no repudio.
- Por último, hablaremos de algunas aplicaciones comunes en el mundo real de la criptografía en:
  - Los almacenamientos
  - Las comunicaciones

## 2. Autenticación.

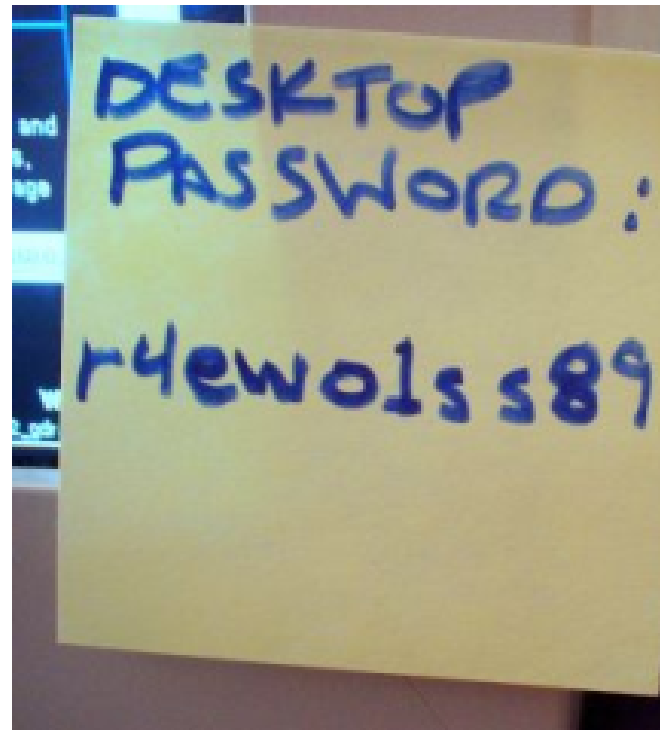
La confidencialidad es la propiedad que nos asegura que la información llega sólo a sus usuarios legítimos. Para ello, un punto clave suele ser autenticar a éstos usuarios legítimos. Aunque autenticación e identificación son palabras que en el uso común pueden confundirse, en nuestro mundillo tienen significados diferentes. Identificar es decir quién eres... y autenticarse es demostrarlo. Por ejemplo, para meterte en la página de la asignatura, te has identificado con un nombre de usuario, pero el sistema te ha autenticado con la contraseña.

La identificación no es significativa desde el punto de vista de la Seguridad.

Hay muchas formas de autenticar a un usuario frente a una máquina, pero desde el punto de vista de la Seguridad Informática, todas caen en tres grandes categorías:

1. Saber algo: El usuario sabe una contraseña, o PIN, que introduce para que el sistema lo autentique

Cuadro 1: Ejemplo de contraseña y PIN



2. Tener algo El usuario posee algún objeto que tiene grabado en su interior una contraseña, y que el sistema es capaz de leer. (Por ejemplo, tarjetas con banda magnética, Tarjetas Smartcard con chip, Llaveros de radiofrecuencia)

Cuadro 2: Llave RFID y tarjeta magnética





Figura 1: En esa imagen hay un tipo que se identifica como Eduardo Punset. ¿Realmente es quien dice ser?

3. Exhibir algún rasgo o característica física intransferible.

Cuadro 3: Diferentes medidas biométricas



Aunque todavía es una tecnología emergente y no demasiado precisa, la biometría es la tercera vía para autenticar a un usuario: que el sistema reconozca alguna característica física, como la huella dactilar, el iris o la retina, o los movimiento y la presión en el gesto de firmar sobre una tableta.

En este caso, el sistema almacena un indicador estadístico de cada usuario, tomado previo a la autenticación.

Observa que:

- saber algo y tener algo, no pueden garantizar la identidad de una persona. . . así pues, lo que autentican es una credencial: es decir, la máquina puede autenticar que la persona tiene las credenciales de quien dice ser. Por contra, la biometría, al basarse en indicadores intransferibles, puede autenticar que

alguien es quien dice ser. . . por supuesto, todo esto con matices.

- Saber algo y tener algo siempre pasan por ser algún tipo de clave o contraseña que tarde o temprano se representa como bits, y por lo tanto, puede participar en criptografía.

---

La biometría, por el momento, se basa en técnicas estadísticas, no hay ningún número fijo que alguien tenga escrito en ningún rasgo físico... así que, en general, no puede participar en criptografía de manera directa.

### 3. Criptografía.

La criptografía es la ciencia (una rama de las matemáticas y la estadística) que se encarga de ocultar la información, para que sólo sea accesible para sus usuarios legítimos. Aunque se utiliza desde hace muchos siglos, en el mundo actual en el que la información es digital, la criptografía también se ha hecho digital.

La idea es que un usuario de la información, utilizando alguna clave secreta numérica (“la clave”), y algún método matemático (“el algoritmo de cifrado”), transforma los bytes que componen la información original (“en claro”) en otros bytes (“cifrados, encriptados”), que no tienen sentido para nadie que los intercepte. Un usuario legítimo de la información original (quizá el mismo que la encriptó o quizá otro) puede volver a restaurar la información original a partir de la cifrada (“descifrar, desenscriptar”), a costa de poseer la claves que lo permita y utilizando el algoritmo adecuado.

#### 3.1. Terminología.

Concepto	Significado
En claro (texto, información o mensaje)	Se refiere al texto, a la información o a un mensaje original, antes de cifrar.
Cifrar, encriptar	Los consideramos sinónimos... Es el acto de transformar la información en claro a información cifrada, sin sentido para cualquiera que no sea usuario legítimo
Descifrar, desenscriptar	Pues obtener la información en claro a partir de la cifrada
Algoritmo criptográfico	El método que transforma la información en claro en información cifrada o al revés.
Clave	Es un valor (contraseña) que se proporciona al algoritmo, y que sirve para cifrar o para descifrar.
Tamaño de clave	Número de dígitos (binarios) necesarios para expresar la clave. La dificultad para encontrar por fuerza bruta dicha clave crece exponencialmente con el número de bits. Por ejemplo, una clave de 256 bits es una entre $2^{256}$ posibilidades, algo así como 115.792 .089.237 .316.195 .423.570 .985.008 .687.907 .853.269 .984.665 .640.564 .039.457 .584.007 .913.129 .639.936
Criptoanálisis	La rama de las matemáticas que analiza mensajes cifrados, intentando descubrir sus claves, sus algoritmos y en última instancia, la información en claro

Continúa en la siguiente página

---

Continúa de la página anterior

Concepto	Significado
Hash, huella digital (resumen)	Información de pequeño tamaño generada por un algoritmo de <i>un solo sentido</i> a partir de otra información. Es fácil conseguir el resumen de una información, pero es muy difícil encontrar la información a partir del resumen
Codificar	Aunque en el lenguaje coloquial lo utilizamos a menudo como sinónimo de cifrado, en la informática no lo es. codificar es utilizar un código público (como el código ASCII) para representar información. No hay clave, ni intención de encriptar.

### 3.2. Utilización

La criptografía se usa en distintas aplicaciones, pero las principales formas de utilizarla caen en alguno de estos grupos:

1. Cifrado de información almacenada: es decir, se guardan datos cifrados en almacenamientos de memoria secundaria (discos, pendrives, archivos comprimidos, copias de seguridad, e incluso bases de datos). Posteriormente son descifradas cuando se van a utilizar... por la misma persona que cifró la información o por cualquier otra autorizada.
2. Cifrado de información en movimiento a través de redes de comunicaciones. Es decir, la información va a viajar de un lugar a otro por un medio electrónico y se envía cifrada para evitar que un posible intruso que intercepte la comunicación pueda tener acceso a ella. Éste cifrado suele hacerse en tres puntos muy concretos, y según el ámbito de aplicación:
  - En el nivel físico/enlace, para evitar pérdidas de confidencialidad en LAN
  - En el nivel de red/transporte, cuando la información atraviesa varias redes
  - En el nivel de aplicación: teniendo en cuenta la comunicación de extremo a extremo
3. Desafío/respuesta: Una forma de evitar que las contraseñas que utilizamos a menudo para autenticarnos viajen de un lugar a otro, pudiendo ser interceptadas.
4. Firma digital: la criptografía, mediante el mecanismo de firma digital puede servir para garantizar cualquiera de estas tres cosas acerca de una pieza de información:
  - Que no ha sido alterada durante su almacenamiento o transporte (integridad)
  - Que el emisor de la información es quien realmente dice ser (autenticación)
  - Que el emisor de una información no puede negar que él es el emisor original (no repudio, una de las propiedades seguras adicionales)

## 4. Criptografía simétrica

### 4.1. Características principales:

- Para cifrar y descifrar se utiliza una única clave, que debe permanecer en secreto.

- Dicha clave, debe ser conocida por quien cifra y por quien descifra... así que deben comunicársela previamente utilizando un **canal seguro**.
- Se utiliza un algoritmo que utiliza de una forma la clave para cifrar, y de forma contraria la clave para descifrar.

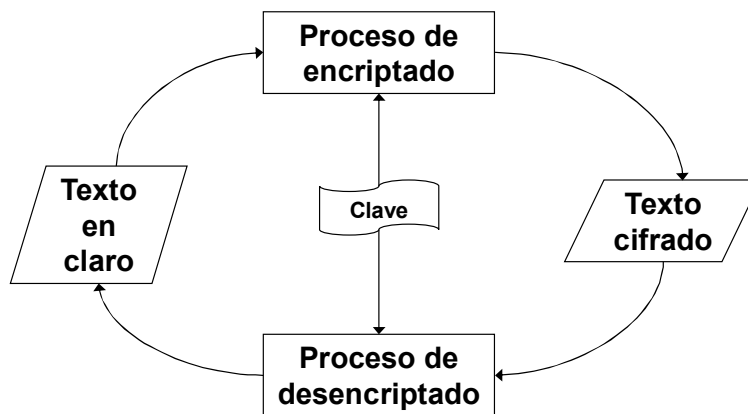


Figura 2: Cifrado simétrico

- Antiguamente, el algoritmo se mantenía en secreto. Hoy en día se considera inseguro confiar en un algoritmo secreto. Los algoritmos de cifrado son conocidos, y para aumentar la seguridad se eligen claves suficientemente grandes.
- Es el tipo de cifrado basado en los métodos tradicionales, ya que suelen necesitar poca capacidad de cálculo.
- Casi todos los algoritmos de cifrado simétrico tienen debilidades, o se pueden atacar utilizando criptoanálisis, aunque si el algoritmo es bueno y la clave secreta es grande, se puede requerir muchísimo esfuerzo y tiempo.
- A lo largo de la historia se conocen muchos algoritmos de cifrado simétrico, pero hoy en día, en la práctica, sólo se utilizan unos pocos de manera habitual.

#### 4.1.1. Cifrado del César

Cada letra del alfabeto se reemplaza por la que se encuentra varias posiciones más a la derecha. Es un cifrado por sustitución, y puede atacarse criptográficamente con medios muy básicos. Originalmente se desplazaban dos posiciones, y posteriormente la **clave** se acordaba previamente como el número de posiciones a desplazar

Texto en claro	Texto cifrado
En el parque a las cinco	Hq ho sdu tx d odv flqfr



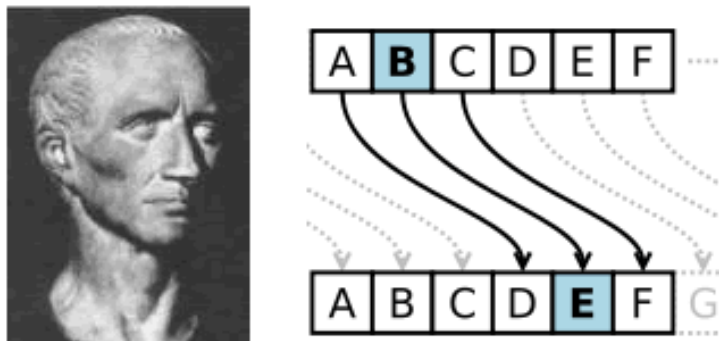


Figura 3: Cifrado del César (3 posiciones)

#### 4.1.2. Cifrado por sustitución

Es una evolución del cifrado del César. La tabla de sustitución ya no se calcula a partir del alfabeto y un desplazamiento, sino que es la propia clave

alfabeto:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
V	X	B	G	J	C	Q	L	N	E	F	P	T

---

Texto en claro: **COMUNIDAD MYGNET**

---

Texto cifrado: **MQCESGXVX CPISUZ**

Figura 4: Posible clave en cifrado por sustitución

#### 4.2. Algoritmos simétricos comunmente usados:

- DES (Data Encryption Standard) 1976: Escogido por el gobierno de los EEUU como algoritmo de encriptación estándar en 1976. Lo sustituye por AES 26 años después. A lo largo de todos esos años, se ha demostrado bastante inseguro. No obstante, hay algunas variantes (como el Triple DES) que se siguen utilizando en algunas aplicaciones de no muy alta seguridad.
- AES (Advanced Encryption Standard) 2002. El gobierno de EEUU realizó una convocatoria pública para sustituir su antiguo algoritmo DES por otro más moderno y seguro. Se presentaron varios algoritmos, y el escogido fue el que se presentó con el nombre de Rijndael (sus creadores se llamaban Joan Daemen y Vincent Rijmen, de la Universidad Católica de Lovaina, Bélgica). Tras ser escogido, se adoptó el nombre de AES. Por las cláusulas de la convocatoria, el algoritmo
  - Es de dominio público

- Simétrico
  - Admite claves de 128, 192 y 256 bits
  - Se puede implementar por software (programas) y hardware (chips)
- Con iguales características que AES, también se utilizan frecuentemente los otros finalistas de la convocatoria (Todos ellos publicados entre el año 2000 y el 2002, y de excelente funcionalidad)
- Serpent,
  - Twofish, evolución de otro algoritmo anterior conocido como Blowfish. Normalmente algo más lento que AES
  - RC6. Un desarrollo privado de la empresa RSA Security, evolución del anterior RC4 y RC5

## 5. Criptografía asimétrica

### 5.1. Características principales:

- Se utiliza un algoritmo que debe ser público y conocido por todos los que participen en el cifrado o descifrado. Así pues, toda la seguridad reside en la fortaleza de la clave, y no en la utilización de un algoritmo secreto.
- Se utilizan dos claves para cada persona o entidad que participe en la comunicación cifrada. Cada persona o entidad X que quiera recibir información cifrada debe tener éstas dos claves:
  - Una clave pública asociada a su identidad, y que cualquiera puede conocer. La clave pública se utiliza para que los demás cifren información dirigida a X.
  - Una clave privada que debe mantener en secreto, y que servirá para descifrar los mensajes que los demás dirigen a X.
- Es el tipo de cifrado más moderno. Se desarrolla durante la segunda mitad del siglo XX (antes de la aparición de los ordenadores es impensable, debido a la gran cantidad de cálculos necesarios)
- Se basan en funciones u operaciones matemáticas de un solo sentido: aquellas que es sencillo realizar en un sentido, pero computacionalmente poco viable en sentido contrario. Una de las más significativas de éstas operaciones es la descomposición en factores primos.

Supongamos un número  $n$  que está compuesto por sólo dos factores primos, es decir,  $n = p \cdot q$ , siendo  $p$  y  $q$  primos.  
Si sabemos  $p$  y  $q$  es fácil saber el valor de  $n$ : basta multiplicar.  
Sin embargo, si sólo sabemos el valor de  $n$ , para hallar  $p$  o  $q$  es necesario aplicar fuerza bruta, probando a dividir por todos los factores primos.

Por ejemplo:  $396307523 = 563 \times 839$ .  
Si sólo te doy el primer número y te digo que está compuesto por dos primos... sólo puedes hallarlos probando a dividir.

Eso es computacionalmente muy costoso y lento.

Si  $p$  y  $q$  tuvieran unos pocos cientos de cifras, obtenerlos podría llevar años, utilizando ordenadores muy rápidos.

En el algoritmo RSA, el más utilizado de los asimétricos, la clave pública contiene el número  $n$  mientras que la privada contiene a  $p$  y  $q$  por separado.

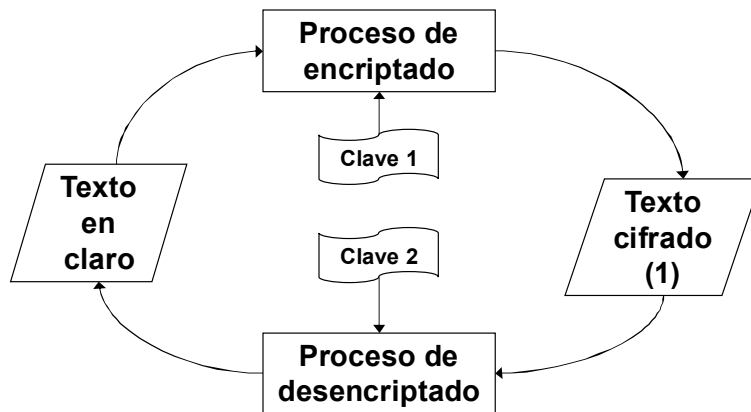


Figura 5: Cifrado asimétrico

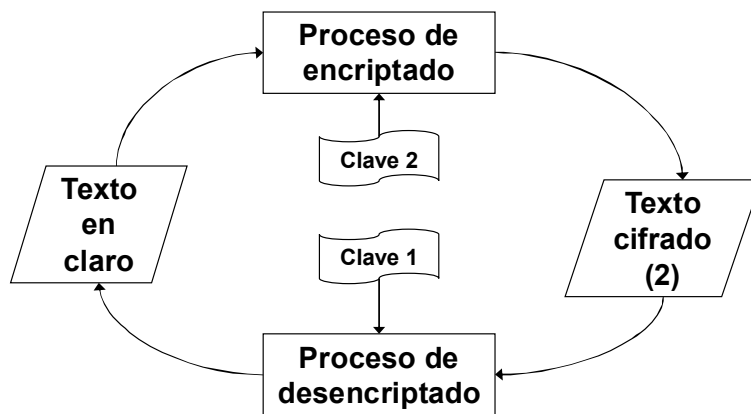


Figura 6: Cifrado asimétrico

- 
- Se utiliza también para la firma digital. En la firma digital, un trozo de información se firma con la clave privada, y cualquiera puede comprobar su integridad, autenticar al emisor o incluso evitar un repudio utilizando la clave pública del firmante.
  - A día de hoy son algoritmos muy seguros
  - Son bastante costosos computacionalmente: consumen recursos de tiempo de CPU y de espacio en memoria.
  - A diferencia de los simétricos, no necesitan compartir nada por un canal seguro.

Algoritmos simétricos comunmente usados:

- RSA (Rivest-Shamir-Adleman) 1977. El más utilizado. Respaldado por una empresa: RSA Security, que mantiene su patente
- Diffie-Hellman 1976. Se utiliza en las mismas aplicaciones que RSA
- Elgamal 1984. Basado en principios similares al de Diffie-Hellman, pero con técnicas más modernas. No está bajo ninguna patente, y su licencia permite libre uso y modificación. (Utilizado por el programa GnuPG, y versiones recientes de PGP)
- ECC 1985. Sujeto a patentes. Se puede utilizar en el cifrado de ficheros de Windows 7 y Server 2008.

## 5.2. El desafío/respuesta criptográfico.

Es un mecanismo para evitar que las contraseñas viajen, basado en la criptografía. Por ejemplo, es el que se utiliza entre un ordenador Windows y el servidor de dominio. La contraseña introducida no viaja por la red, en lugar de ello se desencadena un desafío/respuesta.

El escenario es que una parte hay una entidad A (por ejemplo, Windows Server) que quiere verificar a otra entidad B (por ejemplo, el puesto de trabajo Windows). Se supone que ambas partes tienen constancia de la clave, pero se quiere evitar que viaje para evitar que pueda ser interceptado.

- **A** genera un mensaje aleatorio, que **B** debe cifrar con la clave y un algoritmo simétrico.
- El mensaje cifrado se envía a **A**.
- **A** intenta descifrar el mensaje cifrado recibido de **B** con la clave que se supone que ambos conocen.
- Si se descifra es que **B** conocía la clave correcta.
- Si no, es que **B** no conocía la clave correcta.

Este proceso puede hacerse también posteriormente en sentido contrario, para que **B** verifique a **A**. Por supuesto, hay muchas variantes más o menos complejas, pero la idea básica es la expuesta.

## 6. Criptografía híbrida

Combina un algoritmo asimétrico inicial para intercambiar una clave simétrica, con la que se continúa la comunicación.

- Crea un canal seguro inicial para el intercambio de claves simétricas, lo que elimina el problema de intercambio de claves de la criptografía simétrica.

- Utiliza algoritmos simétricos para el grueso de la comunicación, lo que elimina el problema de la gran necesidad de cálculo de la criptografía asimétrica.

Este sistema se utiliza, por ejemplo, en el protocolo https

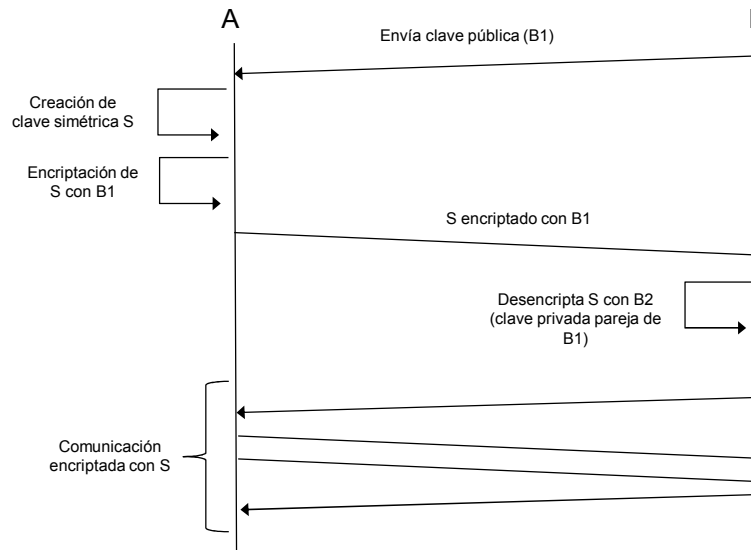


Figura 7: Proceso simplificado de criptografía híbrida

## 7. Firma digital

Permite garantizar cualquiera de estas tres cualidades de una pieza de información:

- Que no ha sido alterada durante su almacenamiento o transporte (integridad)
- Que el emisor de la información es quien realmente dice ser (autenticación)
- Que el emisor de una información no puede negar que él es el emisor original (no repudio, una de las propiedades seguras adicionales)

### 7.1. Algoritmos de resumen criptográficos.

La firma digital se basa en ellos, además de en la criptografía asimétrica, así que debemos empezar por describirlos.

Son algoritmos que se aplican a un conjunto de datos (una tira de bytes) y tienen como propósito principal detectar cambios accidentales o deliberados en una secuencia de datos para proteger su integridad, verificando que no haya discrepancias.

La idea es que se transmita el conjunto de dato junto con su valor de resumen criptográfico., de esta forma el receptor puede calcular el valor de resumen de la secuencia recibida y la puede comparar con el valor de resumen recibido. Si hay una discrepancia se pueden rechazar los datos o pedir una retransmisión.

En cierto modo, son una evolución de otros algoritmos de comprobación, como el CRC, sólo que el CRC se ideó para detectar errores producidos por fallos físicos de dispositivos y los algoritmos de resumen criptográfico también contemplan manipulaciones deliberadas.

Los más conocidos son:

- 
- El MD5, de 128 bits. (Message Digest version 5). Obtiene un resumen de 128 bits (32 bytes) de cualquier cantidad de bytes. Los bytes del resumen suelen expresarse con dígitos hexadecimales.
  - Los algoritmos SHA, que son una familia de varios algoritmos relacionados con el gobierno de los EEUU. (Secure Hash Algorithm) Existen varias versiones, que se suelen identificar con números: SHA-0, SHA-1 y SHA-2. Este último tiene distintas variantes [conocidas como SHA-224, SHA-256, SHA-384, y SHA-512] La cantidad de bytes del resumen varía de uno a otro.

## 7.2. El mecanismo de la firma digital.

- La información a firmar se resume con un algoritmo de resumen
- El resumen se cifra utilizando la clave privada
- Utilizando la clave pública se puede comprobar la firma.

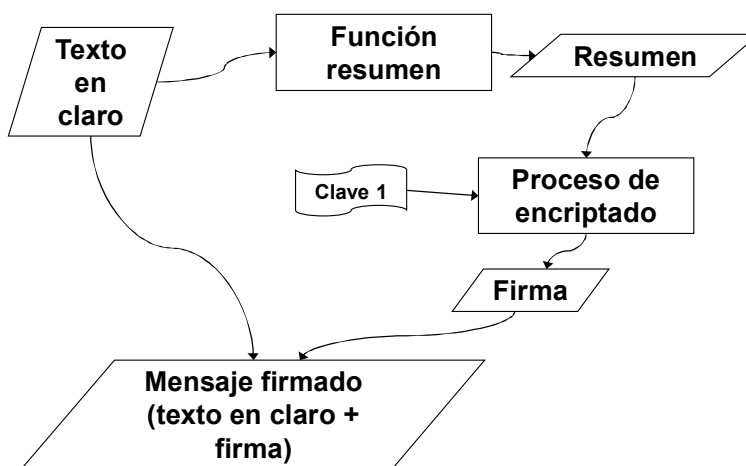


Figura 8: Generación de la firma digital

## 8. Sistemas de confianza e intercambio de claves: la PKI y PGP

La criptografía asimétrica tiene una utilidad apasionante, pero también tiene un punto débil. Si bien proporciona un cifrado prácticamente imposible de romper, se basa en la difusión de una clave pública, por mecanismos públicos, y que siempre va asociada a una identidad. Es decir, yo puedo generar una clave pública para mí y publicarla donde sea asociada a mi nombre o a mi dirección de correo... o a cualquier otro dato que me identifique... pero cualquiera puede hacer lo mismo suplantando mi identidad. En ese supuesto caso... si un intruso pone en algún lugar público una dirección de correo y una clave pública diciendo que soy yo... un posible emisor de un mensaje podría confundirse y enviarle a él un mensaje cifrado pensando que soy yo. Él lo podría descifrar, dado que ha sido él quien ha creado la clave pública.

La criptografía asimétrica necesita un mecanismo para autenticar la identidad de los receptores de los mensajes.

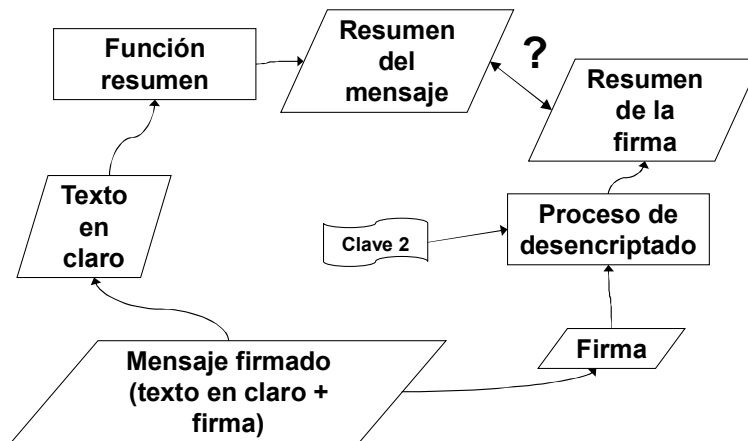


Figura 9: Comprobación de la firma digital

### 8.1. PGP (Pretty Good Privacy)

PGP es un programa creado en 1991, para el intercambio de mensajes cifrados utilizando criptografía asimétrica. El programa sigue hoy en día actualizado.

El grupo GNU tiene un programa parecido GnuPG y en cierto modo, compatible con PGP. Con este programa uno puede generar sus propias claves, y difundir la pública.

Hay servidores web con aplicaciones web para intercambiar claves públicas. Estos funcionan bien para pequeñas organizaciones, donde la identidad de cada uno se pueda autenticar por otros medios.

Cuanto más grande el conjunto de usuarios de usuarios, también es más fácil la intrusión mediante suplantación de la clave pública en uno de éstos servidores de claves públicas PGP.

PGP es un buen medio para enviar mensajes cifrados, pero no para autenticar.

## 9. x509 y la Public Key Infrastructure (PKI)

En otro ámbito, existe un estándar llamado x509, y propuesto por la ITU (Unión Internacional de Telecomunicaciones).

Es un formato de intercambio de claves públicas, en lo que ellos llaman “certificados”. Un certificado es un fichero que contiene en su interior al menos uno de éstos elementos:

- Datos de identificación de una persona u organización
- Una clave privada
- Una clave pública
- Una firma digital.

En cierto modo, x509 puede hacer lo mismo que PGP, sólo que con un propósito más general (PGP está orientado a los mensajes -nivel aplicación- y x509 es más multifuncional).

Alrededor del sistema x509 se ha montado un sistema llamado la PKI (Public Key Infrastructure).

En él, algunas entidades son EMISORAS DE CERTIFICADOS. Emiten certificados para otras entidades o personas. Generar un certificado es sencillo... pero además de eso, estas entidades FIRMAN el certificado que generan. A estas entidades se les denomina Autoridades de Certificación (CA).

---

El sistema PKI está basado en que en el mundo existen una serie de CA, que garantizan la identidad de otras organizaciones... A partir de ahí, las otras organizaciones a su vez pueden generar y firmar nuevos certificados para otras entidades o personas.

En resumen... cualquier persona u organización puede tener un certificado y hacerlo público, que contenga: su identidad, su clave pública y una firma digital de quien lo ha emitido. Para verificar su identidad, podemos comprobar la firma del certificado. Si quien lo ha emitido no es una CA, su certificado irá a su vez firmado por otra entidad... repetimos el proceso de verificación hasta llegar a la CA.

La PKI consiste en la infraestructura que permite la verificación de la identidad a partir de los certificados x.509 hechos públicos por distintos medios.

Si por cualquier motivo, no se puede autenticar un certificado x.509 (es decir, no se puede demostrar que la persona u organización que exhibe el certificado es quien dice ser), entonces el certificado vale igualmente para cifrar... pero ¿nuestro interlocutor es quien dice ser o podría ser un intruso suplantador?

Cada certificado cuenta con una firma que es posible verificar, hasta llegar a una CA. En el sistema PKI, a eso se le llama la ruta de certificación.

Ej: En la dirección web <https://www.lacaixa.es> me muestran un certificado x509 para su uso en TLS. Si miro los detalles, veo que el certificado de La Caixa va firmado por la empresa USERTrust... que a su vez va firmado por Entrust.net.

## 10. Aplicaciones

Vamos a dar un repaso a algunas aplicaciones de lo que hemos visto hasta ahora, pero en el mundo real.

### 10.1. Cifrado/descifrado en información almacenada

#### 10.1.1. El Encrypted File System de Windows 7 y Server 2008.

Ambos sistemas operativos disponen de la capacidad de encriptar ficheros individuales o carpetas enteras, mediante el sistema EFS (**Encrypted File System**). Desde el entorno gráfico, basta con activar una casilla en la hoja de propiedades del archivo o carpeta (Botón derecho/Propiedades/Avanzados/Cifrar contenido...)

Al activarla, Windows cifrará el contenido del objeto seleccionado con una clave que genera a partir de la contraseña del usuario, de tal modo que ante una sustracción física del almacenamiento, no sea posible acceder a los datos. También es posible hacerlo, con mucha más flexibilidad utilizando el comando cipher.

EFS soporta los algoritmos

- AES (simétrico) con claves de 256 bits
- RSA (el más popular de los asimétricos) con claves de hasta 16384 bits (una locura)
- ECC (otro algoritmo asimétrico) con claves de hasta 512 bits

Si no se indica lo contrario, windows 7 utiliza un algoritmo simétrico, con una clave auto-generada.

Para utilizar los otros algoritmos, es necesario disponer de un certificado (en el formato x509). El cifrado de EFS se gestiona a través de las políticas de seguridad de Windows

```
Muestra o altera el cifrado de directorios [archivos] en particiones NTFS.

CIPHER [/E | /D | /C]
        [/S:directorio] [/B] [/H] [nombreDeRuta [...]]

CIPHER /K [/ECC:256|384|521]

CIPHER /R:nombreDeArchivo [/SMARTCARD] [/ECC:256|384|521]

CIPHER /U [/N]
```



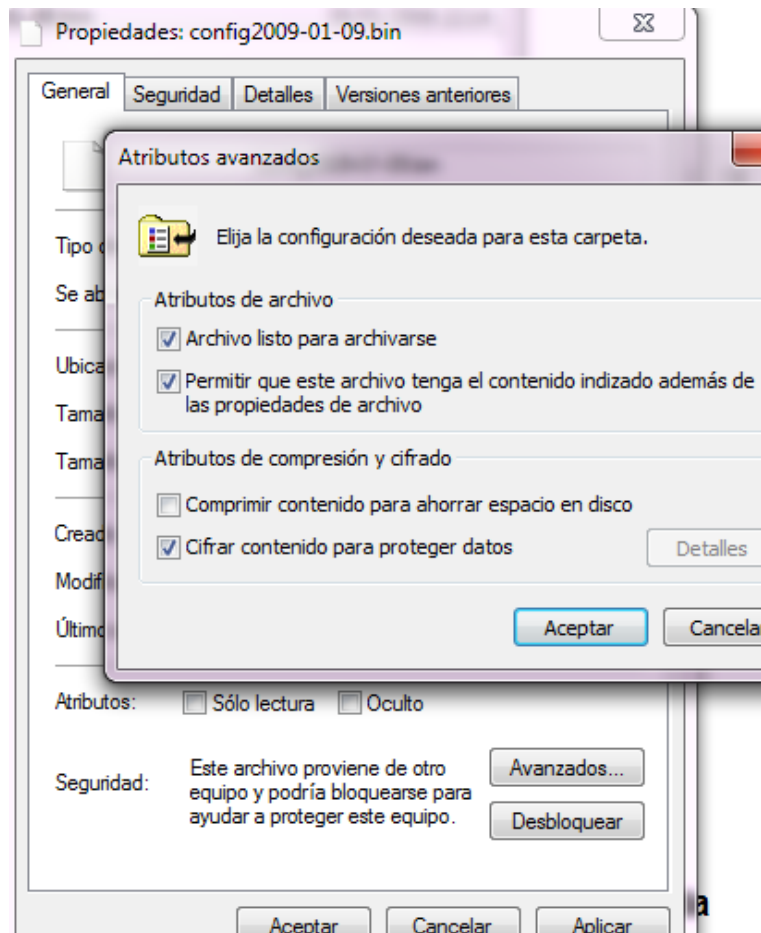


Figura 10: Activación de encriptación a nivel de fichero

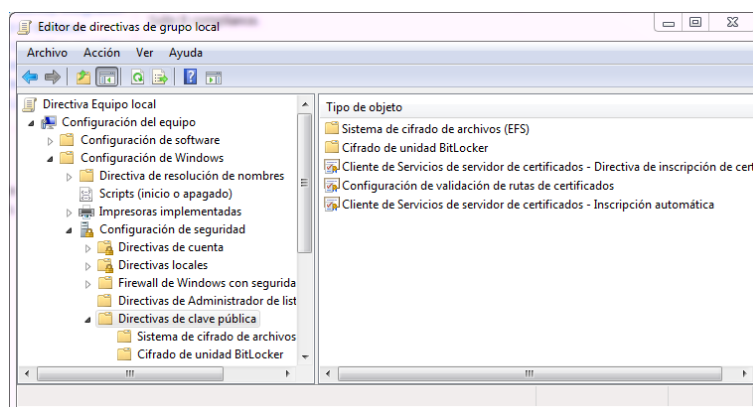


Figura 11: Directiva de seguridad del cifrado en Windows (EFS y Bitlocker)

```

CIPHER /W:directorio

CIPHER /X[:archivoEfs] [nombreDeArchivo]

CIPHER /Y

CIPHER /ADDUSER
[/CERTHASH:hash | /CERTFILE:nombreDeArchivo | /USER:nombreDeUsuario]
[/S:directorio] [/B] [/H] [nombreDeRuta [...]]

CIPHER /FLUSHCACHE [/SERVER:nombreDeServidor]

CIPHER /REMOVEUSER /CERTHASH:hash
[/S:directorio] [/B] [/H] [nombreDeRuta [...]]

CIPHER /REKEY [nombreDeRuta [...]]

/B      Anular si se detecta un error. De forma predeterminada, CIPHER
        continúa ejecutándose aunque se detecten errores.
/C      Muestra información sobre el archivo cifrado.
/D      Descifra los archivos o directorios especificados.
/E      Cifra los archivos o directorios especificados. Los directorios
        se marcarán para que los archivos agregados posteriormente se
        cifren. El archivo cifrado podría descifrarse al modificarse si
        el directorio principal no está cifrado. Se recomienda cifrar
        el archivo y el directorio principal.
/H      Muestra los archivos con los atributos de sistema u ocultos.
        Estos archivos se omiten de forma predeterminada.
/K      Crea un nuevo certificado y una nueva clave para usar con EFS.
        Si se elige esta opción, se omite el resto de opciones.

        Nota: de forma predeterminada, /K crea un certificado y una
        clave que siguen la directiva de grupo actual. Si se
        especifica EEC, se creará un certificado autofirmado
        con el tamaño de clave especificado.

/N      Esta opción sólo funciona con /U e impedirá que se actualicen
        las claves. Se usa para buscar todos los archivos cifrados en
        las unidades locales.
/R      Genera una clave y un certificado EFS, los guarda en un
        archivo .PFX (que contiene el certificado y la clave privada)
        y en un archivo .CER (que contiene sólo el certificado).
        Un administrador puede agregar el contenido del
        archivo .CER a la directiva de recuperación EFS para crear la
        clave de recuperación para los usuarios e importar el archivo
        .PFX para recuperar archivos individuales. Si se especifica
        SMARTCARD, escribe el certificado y la clave de recuperación en
        una tarjeta inteligente. Se genera un archivo .CER (que contiene
        sólo el certificado). No se genera ningún archivo .PFX.

        Nota: de forma predeterminada, /R crea un certificado y una
        clave de recuperación RSA de 2048 bits. Si se especifica
        ECC, debe ir seguido de un tamaño de clave de 256, 384
        o 521.

/S      Realiza la operación especificada en el directorio indicado y en
        todos sus archivos y subdirectorios.
/U      Intenta procesar todos los archivos cifrados en unidades
        locales. Esto actualizará la clave de cifrado de archivos del
        usuario o las claves de recuperación a las actuales en caso de
        que hayan cambiado. Esta opción no funciona con otras opciones a
        excepción de /N.
/W      Quita datos de espacio en disco disponible en todo el
        volumen. Si se elige esta opción, se omitirán todas las demás
        opciones. El directorio especificado puede estar en cualquier
        ubicación del volumen local. Si es un punto de montaje o apunta
        a un directorio en otro volumen, se quitarán los datos del
        volumen.
/X      Hace una copia de seguridad del certificado y las claves EFS en
        el archivo nombreDeArchivo. Si el archivoEfs se proporciona, se
        hará una copia de seguridad del certificado o certificados

```

```

    actuales del usuario usados para cifrar el archivo. De lo
    contrario, se hará una copia de seguridad
    del certificado y las claves EFS actuales del usuario.
/Y      Muestra la vista en miniatura del certificado EFS actual en el
        equipo local.
/ADDUSER  Agrega un usuario a los archivos cifrados especificados. Si se
        proporciona CERTHASH, el cifrado buscará un certificado con este
        hash SHA1. Si se proporciona CERTFILE, el cifrado extraerá el
        certificado del archivo. Si se proporciona USER, el cifrado
        intentará ubicar el certificado del usuario en Servicios
        de dominio de Active Directory.
/FLUSHCACHE
        Borra la memoria caché de claves EFT del usuario que realiza
        la llamada en el servidor especificado.
        Si no se proporciona el nombre del servidor, CIPHER borra
        la memoria caché de claves de usuario en el equipo local.
/REKEY    Actualiza los archivos cifrados especificados para usar la clave
        EFS configurada actual.
/REMOVEUSER
        Quita un usuario de los archivos especificados. CERTHASH
        debe ser el hash SHA1 del certificado que se va a quitar.

directorio      Ruta de acceso de un directorio.
nombreDeArchivo Nombre de archivo sin extensión.
nombreDeRuta    Especifica un patrón, archivo o directorio.
archivoEfs      Ruta de acceso de un archivo cifrado.

Si se usa sin parámetros, CIPHER muestra el estado del cifrado del
directorio actual y de todos los archivos que contiene. Puede usar varios
nombres de directorio y caracteres comodín. Debe usar espacios entre
los diferentes parámetros.

```

Listing 1: Ayuda de la utilidad `cipher` para EFS mediante línea de comandos

### 10.1.2. Bitlocker: Cifrar volúmenes completos en Windows 7 y 2008 Server

**Bitlocker** permite tener volúmenes completos cifrados en sistemas Windows 7 y 2008 server. Los volúmenes se protegen mediante una clave protegida por una contraseña.

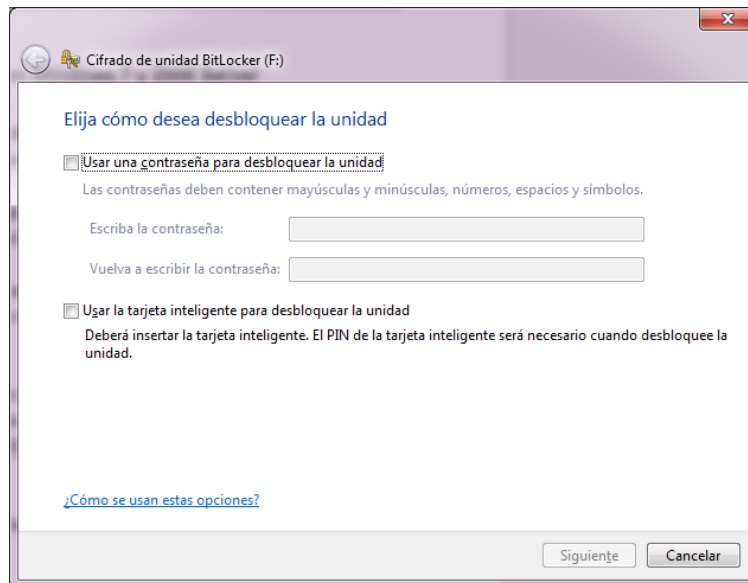
Bitlocker se puede aplicar tanto a volúmenes fijos como a dispositivos extraíbles. Para cifrar una unidad basta con hacer click con el botón derecho sobre el icono de la unidad y seleccionar “Activar Bitlocker”.

A partir de ahí, comienza un asistente que nos ayuda con el cifrado. Cada vez que se inicia el sistema y se quiere utilizar la unidad cifrada es necesario montarla, proporcionando la contraseña. Otras opciones de BitLocker se controlan desde el panel de control.

Por defecto, utiliza un algoritmo AES, aunque si se dispone de un certificado x509 con una clave asimétrica puede utilizarse el algoritmo RSA o ECC, seleccionándolo en las políticas de seguridad de Windows. Bitlocker también admite claves guardadas en tarjetas criptográficas SmartCard (como el DNIe, por ejemplo).

Para crear unidades cifradas es necesaria la versión Professional o Ultimate de Windows 7, aunque el resto de versiones podrán montar la unidad.

Para los dispositivos extraíbles (pendrives, HDDs y SSDs...) windows incluye en la propia unidad un pequeño programa sin cifrar: Bitlocker On The Go, de tal manera que si se inserta el dispositivo en un sistema XP o cualquier otro compatible, pero sin Bitlocker, se ejecuta ese pequeño programa que permite leer el contenido de la unidad, aunque no escribir en ella.



### 10.1.3. Archivos comprimidos encriptados.

La mayor parte de formatos de archivos comprimidos (Ej: zip, rar, 7z) admiten cifrado simétrico además de la compresión. Estos algoritmos obtienen una clave a partir de una contraseña suministrada por el usuario en el momento de cifrar, que debe ser también proporcionada al descifrar.

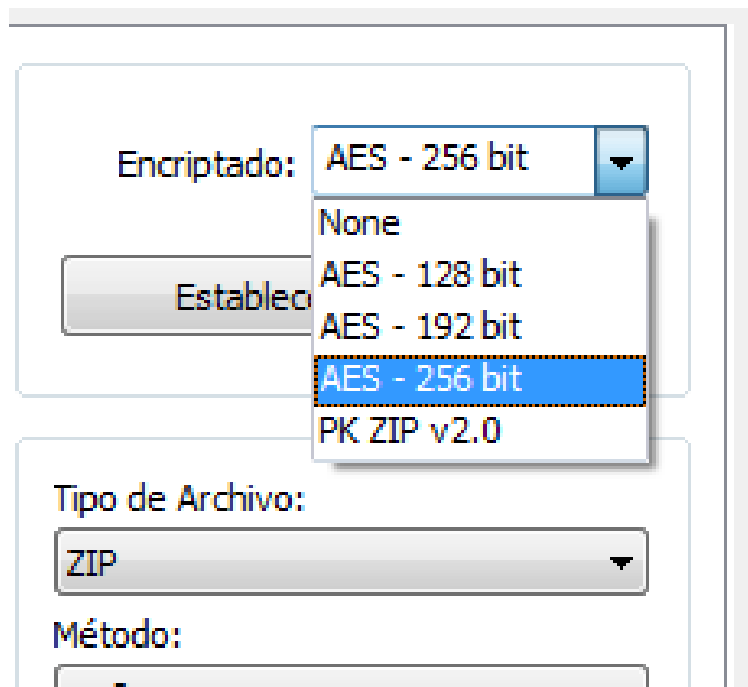


Figura 12: El programa IZarc, mostrando las opciones de cifrado de un archivo comprimido zip

---

#### 10.1.4. Copias de seguridad encriptadas.

Todos los sistemas de copia de seguridad permiten que la copia tenga algún tipo de encriptación.

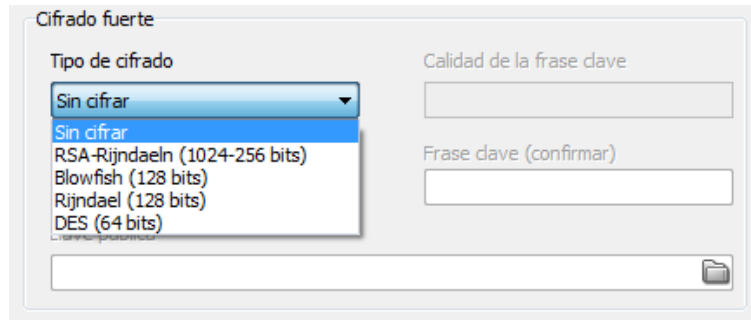


Figura 13: Opciones de encriptación de Cobian Backup (NOTA: Rijndael = AES)

## 10.2. Cifrado/descifrado en la red

### 10.2.1. Wifi (IEEE802.11)

Es una tecnología para la comunicación de tramas Ethernet a través de conexiones inalámbricas. En su nivel físico y de enlace, admite varios tipos de cifrado

- WEP
- WPA
- WPA2

### 10.2.2. WEP (Wired Equivalent Privacy - Privacidad tan buena como la del cable)

Se basa en un cifrado RC4 con claves de 64 o 128 bits. La autenticación de los clientes en el punto de acceso se realiza conociendo esa clave, que se suele representar como un conjunto de dígitos hexadecimales. El algoritmo RC4 tenía algunas vulnerabilidades conocidas. Al ser implementado en WEP y popularizarse, no tardó en ser atacado por técnicas de criptoanálisis. Hoy en día se considera absolutamente inseguro, y no hay ningún motivo para utilizarlo.

### 10.2.3. WPA. (Wifi Protected Access)

Fue un intento de los fabricantes de componentes Wifi de paliar la vulnerabilidad de WEP sin necesidad de cambiar el hardware: de hacer WEP más seguro sólo con una actualización de software.

La base de WPA es seguir utilizando RC4, pero con una serie de mejoras que lo fortalecieron, conocidas como TKIP (Temporal Key Integrity Protocol). Aunque complicadas de explicar a nivel matemático, la idea que subyace es una evolución en la clave que utiliza RC4... es decir, ir variando la clave con el tiempo de manera transparente para los clientes, junto con otros mecanismos de integridad.

No obstante, fue solo una solución temporal. A día de hoy, RC4 con TKIP también se considera inseguro.

#### 10.2.4. WPA2 (La segunda versión de WPA).

Data de 2004 (IEEE802.11i) Se introduce AES como algoritmo criptográfico. WPA2 es extensible, de tal manera que aceptará fácilmente cambios de algoritmo si algún día AES es vulnerado.

También admite que se combine AES con la técnica de TKIP, que lo fortalece aún más. Hoy en día, es la única opción sensata.

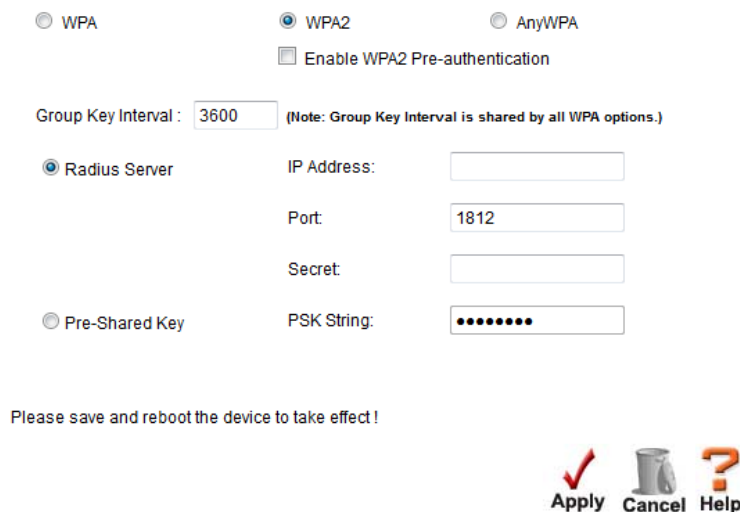
En WPA2 se introducen dos formas de autenticar a un cliente (una tarjeta inalámbrica) en la red, y darle acceso al nivel de enlace. Se debe escoger una u otra en la configuración del punto de acceso.

- PSK (Pre-Shared-Key): consiste en compartir una clave (una contraseña alfanumérica) conocida por todos los usuarios de la red. Esa contraseña es la que se utiliza para generar la clave AES y realizar el cifrado.
- IEEE 802.1x: consiste en la utilización de un servidor de autenticación que siga el protocolo RADIUS (Remote Access Dial-In User Server). Un servidor RADIUS se instala en un ordenador de la red, y almacena nombres de usuario y contraseña. Cuando está activado IEEE802.1x, el punto de acceso preguntará al usuario un nombre de usuario y una contraseña. . . consultará entonces al servidor RADIUS y si este contesta afirmativamente se le dejará pasar. La clave que se genera para cifrar es **única** para ese usuario.

PSK tiene algunos problemas. En caso de que llegue a manos de un intruso, se le permitirá entrar en la red, y también espiar los paquetes dirigidos a otros usuarios. Éste sistema PSK es, por tanto, de baja seguridad: sólo recomendable en una de éstas dos situaciones

- para grupos muy pequeños y estables de usuarios (SoHo)
- para redes sin información sensible (ej: una red sólo para dar acceso a internet).

Todos los sistemas servidores de Windows tienen el servicio de RADIUS, que además, puede asociarse a Active Directory. También existen aplicaciones independientes que pueden instalarse por separado, tanto en Windows como en sistemas Unix/Linux (Ej: FreeRADIUS)



☐ WPA      ☒ WPA2      ☐ AnyWPA

☐ Enable WPA2 Pre-authentication

Group Key Interval :  (Note: Group Key Interval is shared by all WPA options.)

☒ Radius Server      IP Address:

Port:

Secret:

☐ Pre-Shared Key      PSK String:

Please save and reboot the device to take effect !




  

Figura 14: Router Conceptronic C54APRA2+) mostrando las opciones del servidor RADIUS

---

## 11. El nivel de red/transporte: TLS y SSL

En el nivel de red y transporte existe desde hace mucho un protocolo llamado SSL (Secure Socket Layer-Capa de Sockets Seguros) y que hoy en día conocemos como **TLS** (Transport Layer Security)

Está íntimamente relacionado con el intercambio de certificados x509 y con el sistema de distribución y verificación de claves PKI, y permite que se abran transportes extremo a extremo entre un cliente y un servidor que están:

- siempre cifrados
- opcionalmente autenticados

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar. SSL implica una serie de fases y pasos:

### 1. Negociación (HandShaking)

- Negociar entre las partes un algoritmo asimétrico
- Intercambiar claves públicas y autenticación basada en certificados digitales
- Se comprueban las firmas de los certificados mediante la PKI hasta llegar al CA
- Se negocia un algoritmo simétrico, y se pacta una clave para él, que se transmite utilizando el cifrado asimétrico con las claves públicas de los certificados.

### 2. Cifrado del tráfico basado en cifrado simétrico

- En el momento en que se ha intercambiado una clave simétrica se pasa a cifrado simétrico, mucho más rápido y efectivo.

En resumen, la clave pública asimétrica se utiliza para negociar una clave secreta simétrica, de un solo uso.

## 12. El nivel de aplicación

Es muy común que haya aplicaciones que, en vez de definir un nuevo mecanismo de cifrado, sean montadas sobre transportes seguros SSL/TLS.

SSL/TLS es la base de protocolos de aplicación cifrados

- HTTPS, es el protocolo de aplicación HTTP sobre un transporte SSL/TLS
- Los clientes de correo de escritorio (Outlook, Mozilla Thunderbird, etc) admiten comunicaciones sobre transportes SSL/TLS
- Los protocolos de escritorio remoto, como Remote Desktop de Microsoft (RDP) o VNC (Virtual Network Computing) admiten transportes SSL/TLS.
- etc.

También hay otras aplicaciones con un sistema de cifrado. Aplicaciones con su propio sistema de cifrado. En este caso, la aplicación más popular es PGP, y su equivalente GnuPG, bastante orientadas a los mensajes de texto (e-mail, principalmente y similares). Aunque tiene bastante difusión en el ámbito del software libre, a nivel de implementación comercial apenas tiene penetración.

---

## 12.1. Ejemplo: HTTPS

En una conexión https se utiliza el protocolo TLS/SSL sobre HTTP. El servidor debe disponer de un certificado x.509. La conexión siempre está cifrada con un algoritmo simétrico, y a menudo (aunque no es obligatorio) se garantiza la autenticidad del servidor mediante la firma digital del certificado.

Pasos que se siguen, a grandes rasgos, al conectarse por https, (Ej: <https://facebook.com>)

1. El servidor envía al navegador un certificado x509 con información de su identidad, una clave pública, y una firma digital.
2. Si la firma digital corresponde a una CA de la cual tenemos su clave pública previamente almacenada en el navegador, entonces se puede comprobar la firma del certificado recibido de facebook, y tener seguridad de que el certificado es verdadero.
3. Ahora se continúa la comunicación cifrada con un algoritmo asimétrico.
4. El navegador escoge una clave al azar para un algoritmo simétrico, y se la envía al servidor, pero cifra la comunicación con la clave pública del servidor.
5. El servidor responde ya enviando la página con información cifrada con el algoritmo simétrico y la clave que le ha enviado el navegador.

Por supuesto, el proceso incluye muchos pasos intermedios no descritos aquí, por ejemplo, la negociación de qué protocolos van a utilizarse.

## 13. Firma digital

En el contexto de la firma digital, en España tenemos dos aplicaciones clave. Ambas sirven para identificarse ante las administraciones públicas, y firmar actos administrativos (solicitudes, informes, declaraciones, etc...)

Fuera de las administraciones públicas, también lo utilizan algunas empresas privadas, principalmente para autenticación (bancos, aseguradoras y otras entidades financieras principalmente).

### 13.1. FNMT

La Fábrica Nacional de Moneda y Timbre (FNMT) emite a cualquier ciudadano español un certificado x509 en la que ella es CA (Autoridad Certificadora) y que contiene nuestra identidad y una clave privada que permite firma electrónica. Se descarga en forma de fichero, y se puede instalar en el almacén de certificados de Windows, o de algunos navegadores, como FireFox.

### 13.2. DNIe

La Policía Nacional expide el DNI electrónico (DNIe) que es una tarjeta que además de hacer las mismas funciones físicas que un DNI tradicional permite la firma electrónica. Dispone de un Chip criptográfico tipo SmartCard, que contiene en su interior la identidad del ciudadano y una clave privada que permite la firma electrónica. También tiene en sus interior otros datos del ciudadano.

Puede utilizarse para identificarse ante la administración, y para firma electrónica, pero necesita de un lector de tarjetas SmartCard compatible, y de la instalación de algún software en los ordenadores en que se vaya a utilizar.



---

La ventaja del DNIE reside en que la clave privada no se puede extraer del chip. Realmente... es el propio chip del DNI el que realiza la firma de manera autónoma. No obstante, para que el DNI firme se requiere de un PIN, que es susceptible de ser interceptado.

Para completar el tema, te remito al apartado de la web de la asignatura en el que puedes ver una animación realizada por INCIBE con los puntos clave del DNIE, así como un vídeo con la mecánica de utilización del DNIE y el certificado de la FNMT. <https://www.incibe.es/extfrontinteco/dnie/swf/dnie.html>

## 14. Referencias

[Versión en PDF](#)