SEGURIDAD INFORMÁTICA

2º DE SISTEMAS MICROINFORMÁTICOS Y REDES

Noelia Huguet Chacón

TOBALCAIDE

TEMA 2: CRIPTOGRAFÍA

1. Introducción a la Criptografía
2. Sistemas criptográficos
3. Operaciones criptográficas básicas
4. Infraestructura de clave pública, PKI
5. Otras aplicaciones criptográficas

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

- La **criptografía** (del griego 'escritura oculta') es la ciencia de cifrar y descifrar información con técnicas especiales, usado frecuentemente en mensajes que solo puedan ser leídos por las personas a las que van dirigidos.
- Al hablar de este área se debería hablar de criptología que a su vez engloba las técnicas de cifrado (criptografía) y sus técnicas complementarias donde se incluye el criptoanálisis (técnica que estudia los métodos para romper textos cifrados con objeto de recuperar la información original en ausencia de claves).
- Se puede definir la **criptografía** como la técnica de alterar las representaciones lingüísticas de un mensaje de modo que se puedan enviar mensajes confidenciales que únicamente puedan ser comprendidos por personas autorizadas.

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

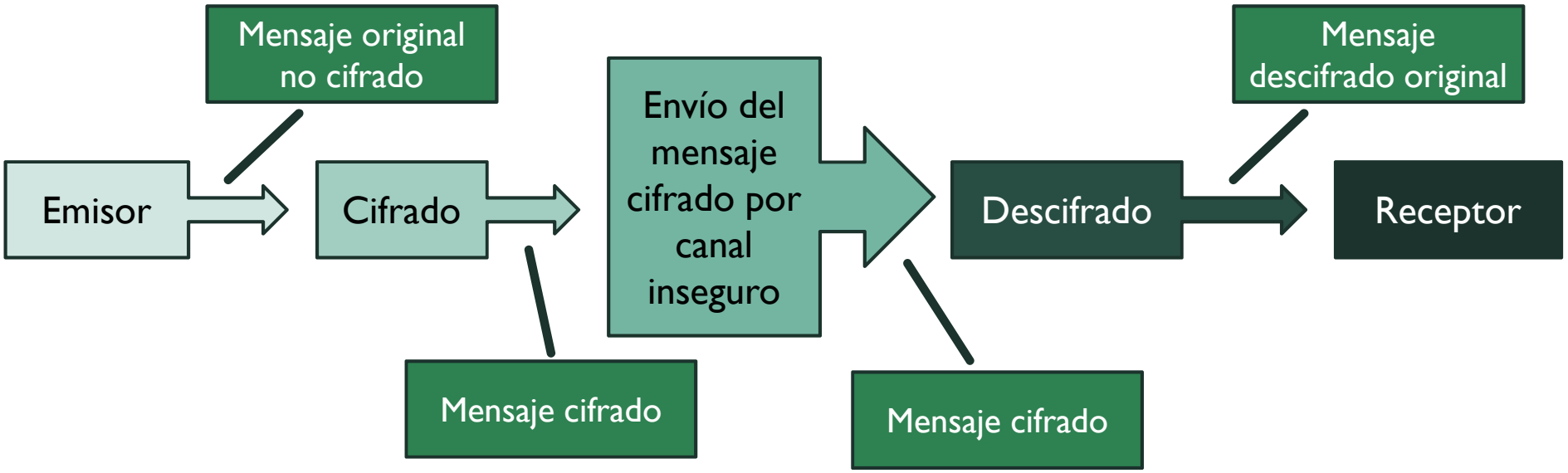
- Aspectos de la terminología de criptografía:
  - La **información original** a proteger se denomina texto en claro o texto plano.
  - El **cifrado** es el proceso de convertir texto plano en texto ilegible, se le llama texto cifrado o criptograma.
  - Los algoritmos de cifrado se clasifican en dos grupos:
    - **Cifrado en bloque**. Se divide el texto original en bloques de bits de tamaño fijo y estos se cifran de manera independiente.
    - **Cifrado de flujo.** El cifrado es bit a bit, byte a byte o carácter a carácter.

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

- Aspectos de la terminología de criptografía:
  - **Las dos técnicas más sencillas de cifrado son**:
    - La **sustitución**: consiste en cambiar el significado de los elementos básicos del mensaje, los dígitos, símbolos o caracteres.
    - La **transposición**: consiste en re-ordenar los elementos del mensaje pero sin modificarlos. HOLA => OHAL
  - El **descifrado** es el proceso inverso que recupera el texto plano a partir del criptograma y la clave.

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

ELEMENTOS QUE INTERVIENEN EN UNA COMUNICACIÓN CIFRADA



2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

- Los procesos criptográficos pretenden dar solución técnica en el ámbito de los procesos informáticos o telemáticos a las siguientes necesidades, relacionadas con los objetivos criptográficos:
  - **La privacidad.** La información solo puede ser leída (interpretada o descifrada) por destinatarios autorizados.
  - **La integridad.** La información no puede ser alterada en su transmisión sin que el destinatario lo advierta.
  - **La autenticidad**. Se puede garantizar que el mensaje procede de quien se afirma que procede.
  - **El no repudio** (o no rechazo). Si un emisor envió un mensaje, no puede negar la autoría del mismo.

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

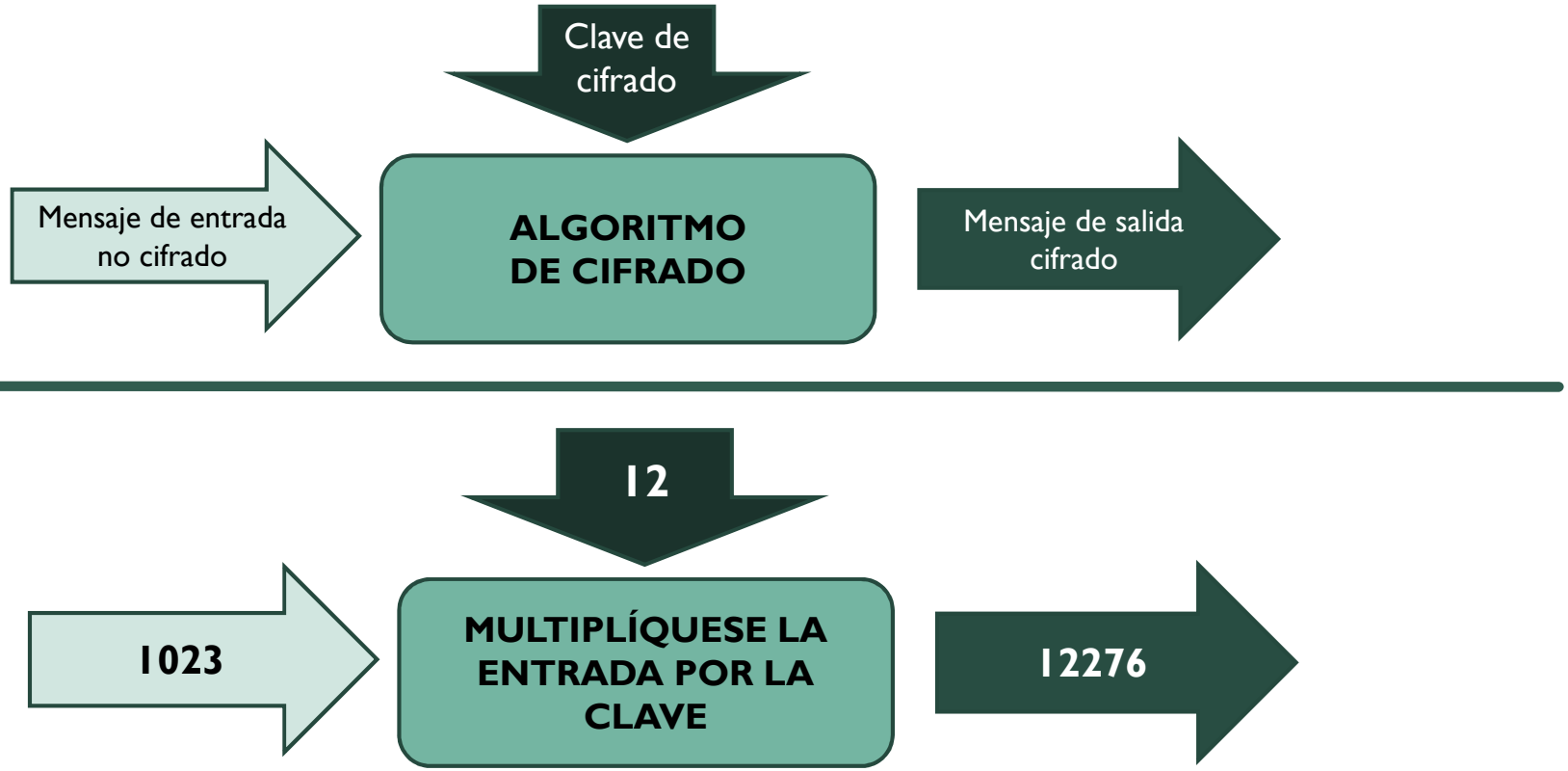
- Las claves son combinaciones de símbolos (letras, números, …) Por tanto, nuestra seguridad está expuesta a los **ataques de fuerza bruta**: probar todas las combinaciones posibles de símbolos.
- Para evitarlo tomaremos estas medidas:
  - Utilizar **claves de gran longitud** (512-1024-2048-4096 bytes), de manera que el atacante necesite muchos recursos computacionales para cubrir todo el rango rápidamente.
  - **Cambiar regularmente la clave**. De esta forma, si alguien quiere intentar cubrir todo el rango de claves, le limitamos el tiempo para hacerlo.
  - **Utilizar todos los tipos de caracteres posibles**: una clave compuesta solo de números (diez valores posibles) es más fácil de adivinar que una con números y letras (36 valores posibles).
  - **No utilizar palabras fácilmente identificables**: palabras de diccionario, nombres propios, etc.
  - **Detectar repetidos intentos fallidos** en un corto intervalo de tiempo. Por ejemplo, la tarjeta del móvil se bloquea si fallamos tres veces al introducir el PIN.
- Las claves no son el único punto débil de la criptografía; pueden existir vulnerabilidades en el propio algoritmo o en la implementación del algoritmo en alguna versión de un SO o un driver concreto. Estas vulnerabilidades las estudia el **criptoanálisis**..

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

- La operación de cifrado se puede conseguir mediante dos métodos:
  a) **Utilizando un algoritmo de cifrado que solo conozcan emisor y receptor.** Este es el método empleado por los primeros sistemas criptográficos, utilizados ya por los romanos en la antigüedad clásica. Por ejemplo, el mensaje "ACDBA" puede cifrarse para convertirse en "BDECB" sin más que desplazar cada letra una posición a la derecha en el alfabeto.
  b) **Haciendo que el algoritmo sea conocido por todos** (se hace público) pero se utiliza una clave o llave que regula el comportamiento del algoritmo. Únicamente quien conozca la clave será capaz de descifrar el mensaje encriptado. Este es el método utilizado en la actualidad.

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

- **EJEMPLO DE CIFRADO MEDIANTE EL USO DE UNA CLAVE**



2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

EJEMPLO DE CIFRADO CÉSAR (SUSTITUCIÓN)

- Supongamos que la clave es 9 y el mensaje a cifrar es:

  "EL PRÓXIMO LUNES HAY EXAMEN DE SEGURIDAD"

- Representamos en una tabla el nuevo alfabeto desplazado posiciones:

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

- Sustituimos cada letra por su correspondiente en el nuevo alfabeto. Nuestro mensaje quedará de la siguiente manera:

  "NT YAXGQUX TDVNB PJH NGJUVNV MN BNODAQMJM"

- Por tanto el emisor recibirá el siguiente mensaje:
  NTYAXGQUXTDNBPJHNGJUVNVMNBNODAQMJM

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

EJEMPLO DE CIFRADO DE LAS CAJAS (TRANSPOSICIÓN)

- Supongamos que la clave es SANDOKAN y el mensaje a cifrar es:

  "EL PRÓXIMO LUNES HAY EXAMEN DE SEGURIDAD"

1. Lo primero que debemos hacer es abrir una tabla y escribir en la primera fila la palabra clave.
2. A continuación debemos numerar las letras según el orden en que aparecen en el alfabeto. Si la letra aparece repetida le ponemos números consecutivos. Por ejemplo, la A es la primera letra, pero como hay dos, le ponemos a la primera un 1 y a la segunda un 2.
3. La siguiente letra del alfabeto que aparece es la G, luego la K y así sucesivamente.
4. A continuación, en la siguiente fila, escribimos el mensaje que queremos enviar, todo seguido, sin espacios.
5. Ahora ya tenemos construida la caja que nos va a servir para codificar el mensaje. Lo que debemos hacer ahora es escribir todos los grupos de letras que aparecen bajo cada número. Y hacerlo ordenadamente. Empezamos por el grupo que está debajo del 1, luego del 2…

2.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

EJEMPLO DE CIFRADO DE LAS CAJAS (TRANSPOSICIÓN)

S	A	N	D	O	K	A	N
8	I	5	3	7	4	2	6
E	L	P	R	O	X	I	M
O	L	U	N	E	S	H	A
Y	E	X	A	M	E	N	D
E	S	E	G	U	R	I	D
A	D						

1. LLESD
2. IHNI
3. RNAG
4. XSER
5. PUXE
6. MADD
7. OEMU
8. EOYEA

- El mensaje que recibirá será el siguiente: LLESDIHNIRNAGXSERPUXEMADDOEMUEOYEA

2.2 SISTEMAS CRIPTOGRÁFICOS

- De los sistemas criptográficos que usan claves son ampliamente utilizados dos de ellos:
  - **Simétricos** o de clave simétrica o privada: son los algoritmos que usan una clave única tanto para cifrar como para descifrar.
  - **Asimétricos** o de clave asimétrica o pública: son los algoritmos que utilizan una clave para cifrar y otra clave distinta para descifrar.
- En muchos de los procesos de criptografía se utilizan los dos simultáneamente para conseguir las propiedades criptográficas necesarias para garantizar las comunicaciones o la autoría de documentos.
- El principio de **Kerchohoff** dice que la fortaleza de un sistema o algoritmo de cifrado debe recaer en la clave y no en el algoritmo que si es conocido, si no hay clave no se podrá descifrar el mensaje

2.2 SISTEMAS CRIPTOGRÁFICOS

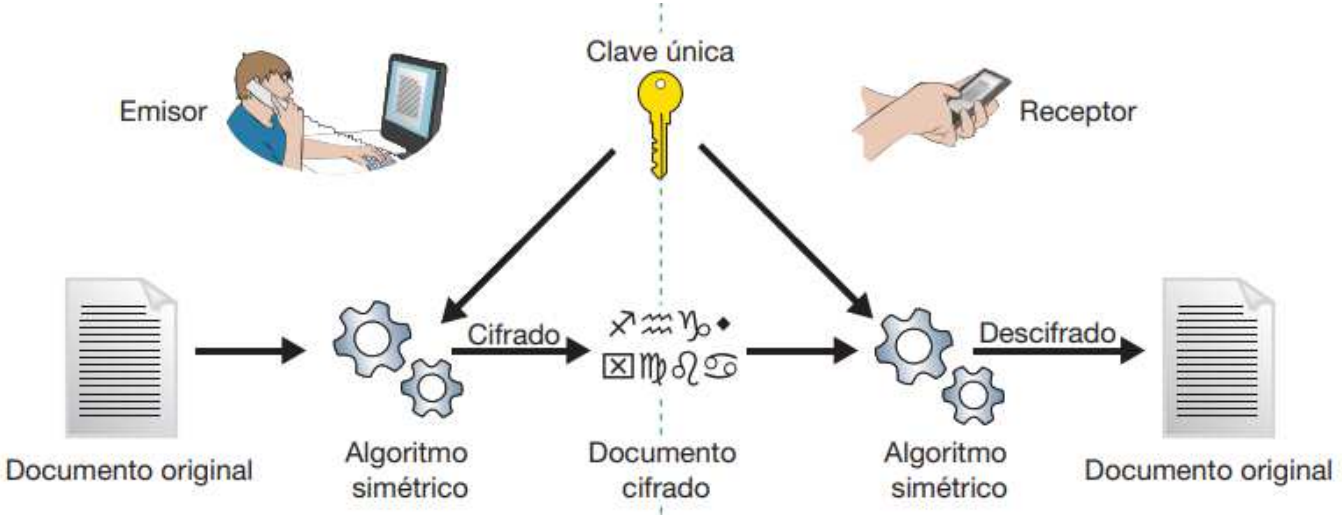
CRIPTOGRAFÍA SIMÉTRICA

- Una criptografía simétrica, de clave única o de clave privada es el conjunto de métodos que permiten tener una comunicación segura entre emisor y receptor siempre que previamente se hayan intercambiado una única clave, denominada clave simétrica ya que es utilizada por ambos.
- La simetría del proceso consiste en que la misma clave que utiliza el emisor para cifrar el mensaje es utilizada por el receptor para descifrarlo.
- El ejemplo de la multiplicación es un caso concreto de uso de clave simétrica, puesto que el "12" se utiliza multiplicando para cifrar y dividiendo para descifrar.
- Solo quien conoce la clave es capaz de descifrar por lo que la confidencialidad queda garantizada siempre y cuando la clave sea secreta únicamente sea conocida por emisor y receptor.
- Los algoritmos más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA

- El sistema de cifrado queda comprometido si un tercer agente conoce la clave y recibe el mensaje cifrado, ya que podría descifrarlo.
- La robustez de este sistema de criptografía simétrica reside en la seguridad con el que el emisor envía la clave de cifrado al receptor, así como en la longitud de la clave (que no es más que una secuencia de caracteres o bits).



2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA

- Los **principales problemas de los algoritmos** de cifrado no están relacionados con su seguridad, sino con:
  - **El intercambio de claves**. Una vez que remitente y destinatario han intercambiado las claves ya se pueden comunicar con seguridad, pero ¿que **canal de comunicación seguro** se ha usado?, esto hace que sea mas fácil para el atacante interceptar una clave que probar las posibles combinaciones para descubrirla.
  - **El numero de claves que se necesitan:** si hay un numero 'n' de personas que se tienen que comunicar entre si, se necesitan n/2 claves diferentes para cada par de personas que se quieran comunicar en privado, con un grupo reducido de personas es posible, pero con un grupo grande es imposible llevarlo a cabo, son muchas claves a custodiar (sin embargo con la asimétrica solo hay que custodiar la clave privada propia).
  - La solución a esto es la **criptografía asimétrica** y la **criptografía híbrida.**

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA: CIFRADO DE VERNAM

- El **cifrado de Vernam** es un cifrado de flujo en el que el texto en claro, de tipo binario, se combina mediante la operación XOR con un flujo de datos aleatorio o pseudoaleatorio del mismo tamaño, para generar un texto cifrado.
- Cuando la secuencia con la que se mezcla el mensaje es realmente aleatoria y se usa sólo una vez, se tiene la libreta de uso único.
- Claude Shannon demostró que la libreta de un solo uso es irrompible, es el primer y único método de cifrado para el que existe tal demostración.
- El problema de este cifrado es que en la práctica es tan difícil compartir de forma segura una clave que es tan larga como el mismo mensaje.
- El RC4 es un ejemplo de cifrado de Vernam que se utiliza con frecuencia en Internet.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA: CIFRADO DE VERNAM

1. El primer paso es cifrar con el código ASCII en binario, A1Z27.

Letra	ASCII	Letra	ASCII	Letra	ASCII	Letra	ASCII
A	0100 0001	H	0100 1000	O	0100 1111	V	0101 0110
B	0100 0010	I	0100 1001	P	0101 0000	W	0101 0111
C	0100 0011	J	0100 1010	Q	0101 0001	X	0101 1000
D	0100 0100	K	0100 1011	R	0101 0010	Y	0101 1001
E	0100 0101	L	0100 1100	S	0101 0011	Z	0101 1010
F	0100 0110	M	0100 1101	T	0101 0100		
G	0100 0111	N	0100 1110	U	0101 0101		

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA: CIFRADO DE VERNAM

2. Una vez pasado todo al binario. Elegimos lo que queramos Encriptar en esta cosa vamos a usar la Palabra "TARINGA", y elegimos una clave cualquiera pero que tenga la misma cantidad de letras que nuestra palabra, por ejemplo "MXUZOPT".

3. Juntamos las 2 Primeras Letras en este caso la Letra "T" y la letra de la clave que es "M". Una vez Juntas usando solo los **ÚLTIMOS 5 NÚMEROS** del código Binario las reemplazamos. Hacemos la Operación Matemática XOR.

OPERACIÓN XOR	
0 XOR 0 =	**0**
0 XOR 1 =	**1**
1 XOR 0 =	**1**
1 XOR 1 =	**0**

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA: CIFRADO DE VERNAM

4. Una Vez echa la Operación Matemática nos daría un valor en números 0 (ceros) y 1 (unos) y nos fijamos según el Código Binario de los **ÚLTIMOS 5 NÚMEROS** que Letra es y que valor Numérico tiene en el Código A1Z27. En este caso dio la Letra "Y" y su valor numérico es 24.

Texto Original	T	A	R	I	N	G	A
Binario	10100	00001	10010	01001	01110	00111	00001
Clave	M	X	U	Z	O	P	T
Binario	01101	1100	10101	11010	01111	10000	10100
XOR	11001	11001	00111	10011	00001	10101	10111
Texto Cifrado	Y	Y	C	S	A	U	W

5. El mensaje cifrado será "YYCSAUW"

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA: CIFRADO DE VERNAM

- Para descifrar deberías hacer los mismo, sabemos la clave "MXUZOPT" y el mensaje cifrado "YYCSAUW".

Texto Cifrado	Y	Y	C	S	A	U	W
Binario	11001	11001	00111	10011	00001	10101	10111
Clave	M	X	U	Z	O	P	T
Binario	01101	1100	10101	11010	01111	10000	10100
XOR	10100	00001	10010	01001	01110	00111	00001
Texto Original	T	A	R	I	N	G	A

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA SIMÉTRICA

Algunos ejemplos de algoritmos de cifrado simétrico son:

- Algoritmo de cifrado **DES** (Data Encryption Standard) que usa una clave de 56 bits (son 2^{56} claves posibles), pero que es fácilmente descifrable por un ordenador modernos en cuestión de días.
- Algoritmo de cifrado **3DES, Blowfish, Twoofishc o IDEA** que usan claves de 128 bits o lo que es lo mismo 2^{128} claves posibles, aunque admite entre 32 a 448 bits dependiendo del algoritmo.
- Otros algoritmos usados son **RC5 y AES** (Advanced Encryption Standard) también conocido como **Rijndael**.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA

- La criptografía asimétrica o de doble clave utiliza dos claves diferentes, pero relacionadas entre sí.
- Cada usuario del sistema criptográfico ha de poseer una pareja de claves:
  - **Clave privada:** será custodiada por su propietario y no se dará a conocer a ningún otro.
  - **Clave pública:** será conocida por todos los usuarios.
- Una clave es absolutamente privada y no debe comunicarse a nadie, mientras que la otra es pública y puede ser comunicada a cualquier posible destino.
- Fundamentalmente la criptografía asimétrica se utiliza en el proceso de firma digital para asegurar el intercambio de claves simétricas entre emisor y receptor, que ya se vio que era el punto débil de los sistemas de cifrado simétricos.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA

- La ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes **desventajas**:
  - Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
  - Las claves deben ser de mayor tamaño que las simétricas.
  - El mensaje cifrado ocupa mas espacio que el original.
- En cada sentido del envió y recepción de información, se cifra el mensaje con la clave pública de la persona a la que se envía y esta lo descifra con su clave privada que solo el conoce, cada interlocutor tiene que tener la clave publica del otro.
- En cifrado simétrico es suficiente con 128bits, pero para criptografía asimétrica se recomiendan claves publicas de 1024 bits.
- Hay dos algoritmos claves en criptografía asimétrica: RSA y Diffie-Hellman.

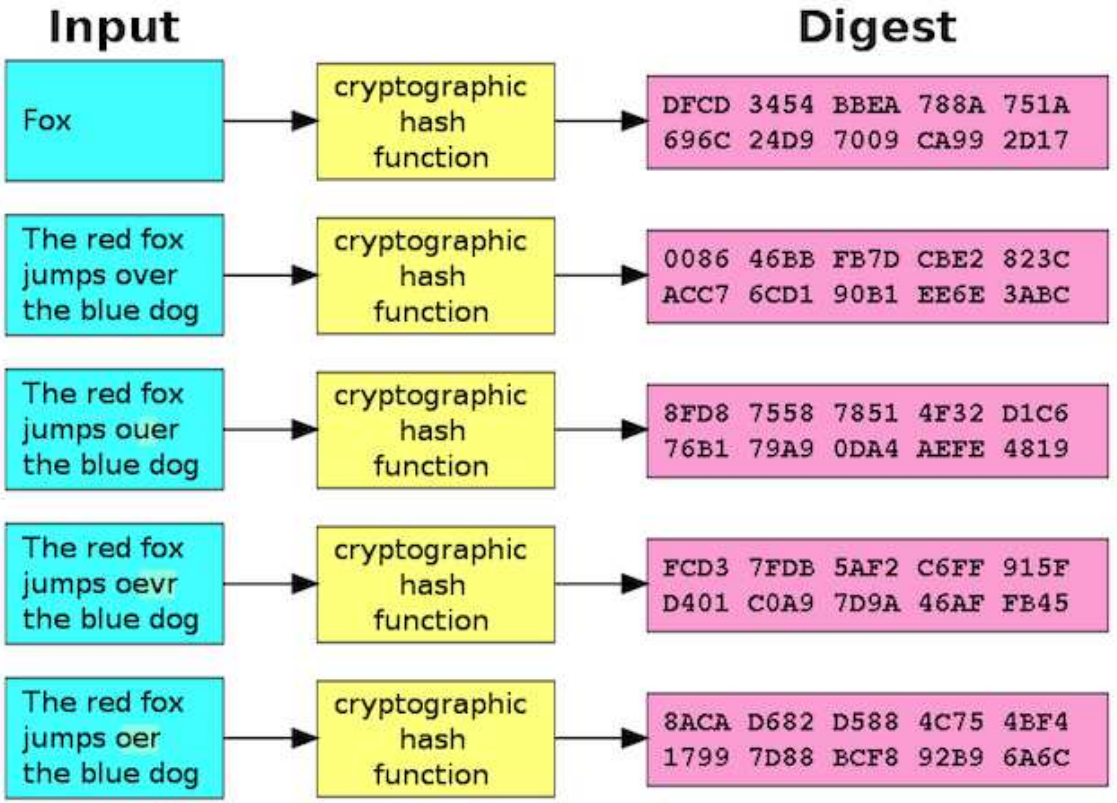
2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: FUNCIONES HASH

- Las **funciones Hash** (también conocidas como funciones resumen) son funciones que, utilizando un algoritmo matemático, transforman un conjunto de datos en un código alfanumérico con una longitud fija.
- Da igual la cantidad de datos que se utilice (muchos o pocos), el código resultante tendrá siempre el mismo número de caracteres.
- El termino Hash proviene del inglés y significa "picadillo". En consonancia con este significado, el algoritmo matemático "pica", "trocea" y "mezcla" el conjunto de datos y crea un nuevo código con una longitud indicada.
- Cuando hablamos de funciones Hash, hacemos referencia a diferentes algoritmos matemáticos de resumen, por tanto, no existe una sola función de Hash, sino que encontramos una pluralidad de ellas.
- Entre las funciones más conocidas encontramos la denominada SHA-2 (Secure Hash Algorithm), que se compone de 4 funciones: SHA-224; SHA-256, SHA-384 y SHA_512. Cada una de ellas da un Hash diferente para un mismo conjunto de datos, y la longitud del Hash es de 224, 256, 384 y 512 bits dependiendo de la función elegida.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: FUNCIONES HASH



2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: DIFFIE-HELLMAN

- No es un algoritmo asimétrico propiamente dicho, se usa para generar una clave privada simétrica a ambos extremos de un canal de comunicación inseguro.
- Se emplea para obtener la clave secreta con la que posteriormente cifrar la información, junto con un algoritmo de cifrado simétrico.
- Su seguridad radica en la dificultad de calcular el logaritmos discreto de números grandes (DH también permite el uso de curvas elípticas).
- El problema de este algoritmo es que no proporciona autenticación, no puede validar la identidad de los usuarios, por tanto si un tercer usuario se pone en medio de la «conversación», también se le facilitaría las claves y por tanto, podría establecer comunicaciones con el emisor y el receptor suplantando las identidades.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: RSA

- Aunque fue creado en 1977, RSA sigue siendo el sistema de clave pública más conocido y usado.
- Su seguridad radica en la dificultad de factorizar números enteros grandes.
- Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto conocido de dos números primos grandes elegidos al azar.
- El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada.
- Este algoritmo se basa en la pareja de claves, pública y privada.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: RSA

- **Ventajas:**
  - Resuelve el problema de la distribución de las llaves simétricas (cifrado simétrico).
  - Se puede emplear para ser utilizado en firmas digitales.
- **Desventajas:**
  - La seguridad depende de la eficiencia de los ordenadores.
  - Es más lento que los algoritmos de clave simétrica.
  - La clave privada debe ser cifrada por algún algoritmo simétrico.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Creación de claves en el sistema RSA:
  - Se buscan dos primos lo suficientemente grandes: p y q, con $p \neq q$
  - En la realidad estos números tienen centenares de dígitos.
  - En nuestro ejemplo serán: p = 3 y q = 11
  - A partir de estos números se obtiene:
    - n = p * q
    - z = (p - 1) * (q - 1)
  - En nuestro ejemplo:
    - n = 3 * 11 = 33
    - z = (p -1) * (q - 1) = (3-1)*(11-1) = 20

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Creación de claves en el sistema RSA:
  - Elige un número primo k, tal que k sea co-primo a z, por ejemplo, z no es divisible por k.
  - Tenemos varias opciones aquí, valores de k como pueden ser 7, 11, 13, 17 o 19 son válidos. 5 es primo, pero no es co-primo de k puesto que 20 (z) es divisible por 5. Elegimos k=7 para simplificarnos los cálculos con un número pequeño
  - MCD (z, k) = 1. En nuestra ejemplo: k = 7;
  - MCD (20, 7) = 1
  - La **clave pública** va a ser el conjunto de los números (k,n), es decir, (7,33).

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Creación de claves en el sistema RSA:
  - Ahora se calcula la clave privada.
  - Para ello, se elige un número j que verifique la siguiente ecuación:
    - k*j=1 (mod z)
  - En este caso:
    - 7*j=1 (mod 20), es decir, un valor que verifique que (7*j)/20 sea una división con resto «1».
  - Para trabajar con números pequeños en este ejemplo, podríamos decir que 21/20 nos devuelve «algo» con resto 1, por lo que, para este caso particular, (7*j) = 21, de modo que j=3.
  - Esta es la **clave privada** es el conjunto de (j, n), es decir, (3, 33)

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Creación de claves en el sistema RSA:
  - **Cifrado**: $C = M^k \bmod n$
  - **Descifrado**: $C^j \bmod n = M$
- Asignemos a cada letra un número:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Con las claves del ejemplo vamos a cifrar el mensaje M:

S	E	G	U	R	I	D	A	D
19	4	6	21	18	8	3	0	3

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Cifrado con Clave Pública: (7,33) → M = 19 4 6 21 18 8 3 0 3
  - 19^7 mod 33 = 893871739 mod 33 = 13
  - 4^7 mod 33 = 16384 mod 33 = 16
  - 6^7 mod 33 = 279936 mod 33 = 30
  - 21^7 mod 33 = 1801088541 mod 33 = 21
  - 18^7 mod 33 = 612220032 mod 33 = 6
  - 8^7 mod 33 = 2097152 mod 33 = 2
  - 3^7 mod 33 = 2187 mod 33 = 9
  - 0^7 mod 33 = 0 mod 33 = 0
  - 3^7 mod 33 = 2187 mod 33 = 9
  - **Por lo que C = 13 16 30 21 6 2 9 0 9**

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: Ejemplo RSA

- Descifrado con Clave Privada: (3,33) → **C = 13 16 30 21 6 2 9 0 9**
  - 13^3 mod 33 = 2197 mod 33 = 19
  - 16^3 mod 33 = 4096 mod 33 = 4
  - 30^3 mod 33 = 27000 mod 33 = 6
  - 21^3 mod 33 = 9261 mod 33 = 21
  - 6^3 mod 33 = 216 mod 33 = 18
  - 2^3 mod 33 = 8 mod 33 = 8
  - 9^3 mod 33 = 729 mod 33 = 3
  - 0^3 mod 33 = 0 mod 33 = 0
  - 9^3 mod 33 = 729 mod 33 = 3
- **Por lo que M = 19 4 6 2118 8 3 0 3**

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA ASIMÉTRICA: RSA

- Los números primos tomados son muy grandes, puesto que este es un algoritmo que basa su seguridad en la complejidad computacional.
- Los pasos siempre son:
  - Generar dos números primos muy grandes, p y q
  - Hacer n=p*q
  - Calcular z=(p-1)*(q-1)
  - Elegir un pequeño número k, co-primo de z, de modo que el Máximo Común Divisor entre z y k sea 1, con 1<k<z
  - Encontrar un número j tal que el (k*j mod z) sea 1
  - Publicar k y n como la clave pública.
  - Guardar j y n como la clave privada.

2.2 SISTEMAS CRIPTOGRÁFICOS

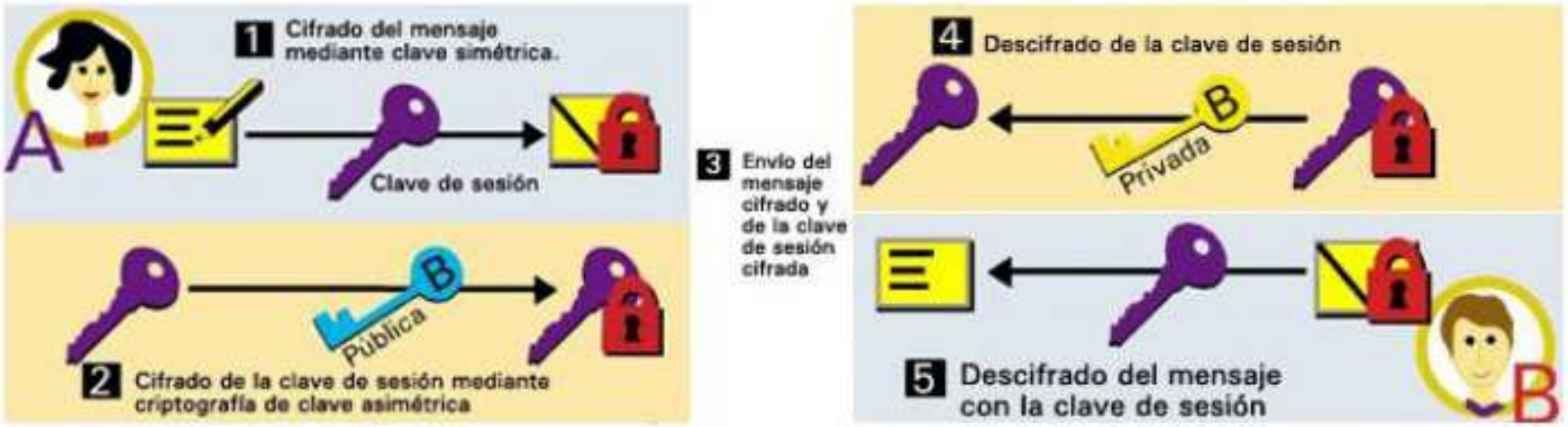
CRIPTOGRAFÍA HÍBRIDA

- Usar claves asimétricas ralentiza el proceso de cifrado, para solucionar este inconveniente se utiliza un algoritmo de clave pública para cifrar el envió de una pequeña cantidad de información como puede ser una clave simétrica y posteriormente se usa un algoritmo de clave simétrica para el cifrado del mensaje, de esta forma se reduce el coste computacional.
- El proceso seria el siguiente:
  - Ana escribe un mensaje con destino José, primeramente lo cifra con clave simétrica, esta clave se genera aleatoriamente y se llama clave de sesión, para enviar esta clave de sesión de forma segura se cifra de forma asimétrica con la clave publica de José.
  - José recibe el mensaje cifrado con la clave de sesión y la clave de sesión cifrada con su clave pública, entonces utiliza su clave privada para descifrar la clave de sesión y una vez descifrada la utiliza para descifrar el propio mensaje.

2.2 SISTEMAS CRIPTOGRÁFICOS

CRIPTOGRAFÍA HÍBRIDA

- Con el sistema de criptografía híbrida se consigue:
  - Confidencialidad: Solo podrá leer el mensaje el destinatario del mismo.
  - Integridad: El mensaje no podrá ser modificado (si se modifica no se podrá descifrar)
- Pero quedan unos problemas sin resolver:
  - Autenticación y No repudio.



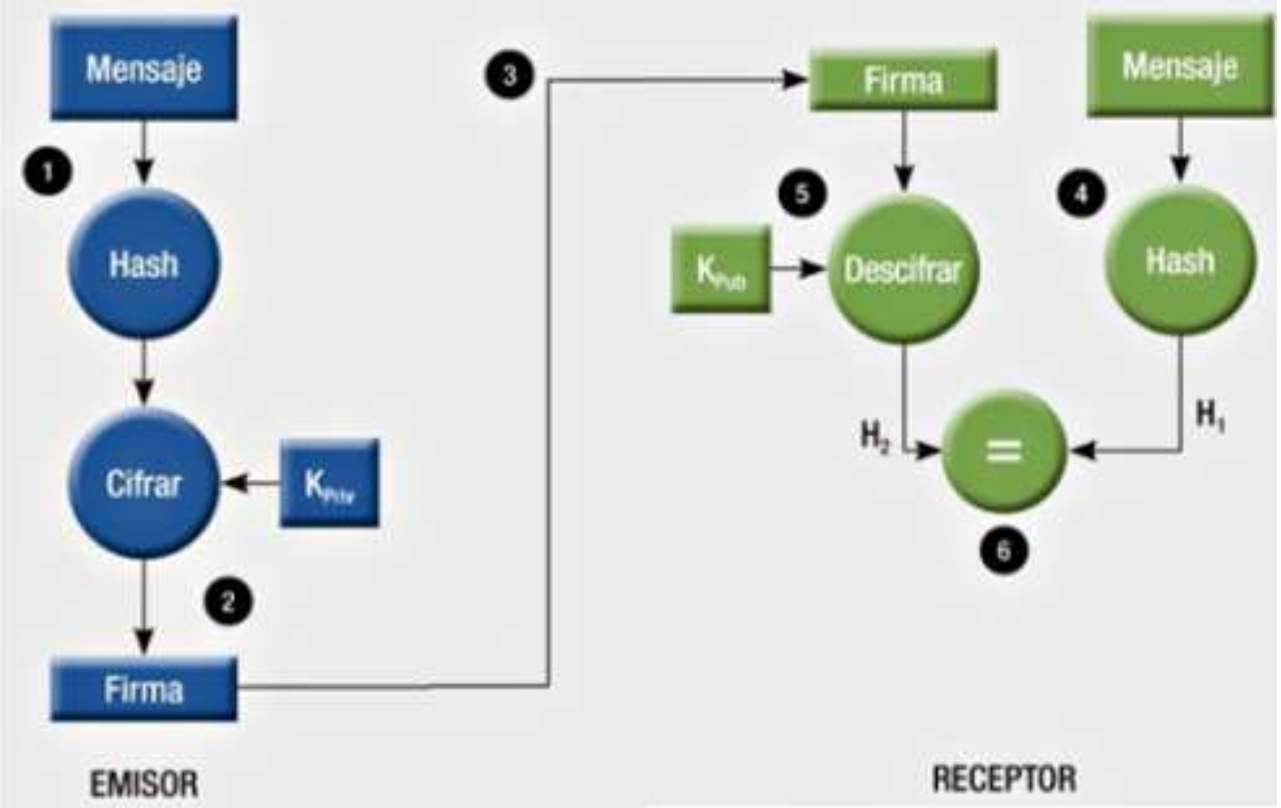
2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

FIRMA DIGITAL

- Una de las ventajas de la criptografía de clave pública es que ofrece un método de firmas digitales, esto permite al receptor de un mensaje verificar la autenticidad del origen del mismo y que además no ha sido modificado. Por lo tanto con este sistema conseguimos:
  - AUTENTICACIÓN: La firma digital es equivalente a la firma física de un documento.
  - INTEGRIDAD: El mensaje no podrá ser modificado.
  - NO REPUDIO EN ORIGEN: El emisor no puede negar haber enviado el mensaje.
- La firma digital cifra con clave privada el resumen de los datos a firmar haciendo uso de funciones de resumen o hash.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

FIRMA DIGITAL



1. Generas un resumen del documento.
2. Cifras el resumen con tu clave privada, firmando por tanto el documento, ya que nadie excepto tu conoce dicha clave privada.
3. Envías el documento junto con el resumen firmado al destinatario.
4. Este genera un resumen del documento recibido de ti, usando la misma función hash.
5. Después descifra el resumen firmado con tu clave pública, que es conocida por todos.
6. Y si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Los certificados digitales asocian una clave pública con la identidad de su propietario.
- El formato estándar de certificados digitales es **X.509** y su distribución es posible realizarla:
  - Con clave privada (suele tener extensión *.pfx o *.p12) más seguro y destinado a un uso privado de exportación e importación posterior como método de copia de seguridad.
  - Solo con clave pública (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura, para que otras entidades o usuarios solo puedan verificar la identidad, en los archivos o mensajes firmados.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Terceras partes de Confianza
  - Dos usuarios pueden confiar directamente entre si, si ambos tienen relación con una tercera parte y esta da fe de la fiabilidad de los dos.
  - La forma en que esa tercera parte avalara que el certificado es de fiar es mediante su firma digital sobre el certificado.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Las infraestructuras de Clave Pública (ICP o PKI, Public Key Infraestructures) esta formado por:
  - **Autoridad de certificación** (CA): emite y elimina los certificados digitales.
  - **Autoridad de registro** (RA): controla la generación de los certificados, procesa las peticiones y comprueba la identidad de los usuarios, mediante el requerimiento de documentación de identificación personal.
  - **Autoridades de repositorio**: almacenan los certificados emitidos y eliminados.
  - **Software** para el empleo de certificados.
  - **Política de seguridad** en las comunicaciones relacionadas con gestiones de certificados.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Documento nacional de identidad electrónico (DNIe) Emitido por la Dirección General de la Policía acredita la identidad, los datos personales que en el aparecen y la nacionalidad y con respecto al mundo digital:
  - Acreditar electrónicamente y sin posibilidad de duda, la identidad de la persona.
  - Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a las que le proporciona la firma manuscrita.
- Para la utilización del DNI electrónico se necesita:
  - Hardware especifico: como un lector de tarjetas inteligente que cumpla el estándar ISO-7816.
  - Software especifico: Controladores o módulos criptográficos para el acceso al chip y su contenido

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Incorpora un pequeño chip (circuito integrado) capaz de guardar de forma segura información en formato digital como:
  - Un certificado electrónico para autenticar la personalidad del ciudadano.
  - Un certificado electrónico para firmar electrónicamente, con la misma validez que la firma manuscrita.
  - Certificado de la autoridad de Certificación emisora.
  - Claves para su utilización.
  - La plantilla biométrica de la impresión dactilar.

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- En función de cómo utilicemos las claves, si lo hacemos en emisor o receptor y sobre qué tipo de documento o mensaje obtendremos unas propiedades criptográficas u otras.
- LAS OPERACIONES MÁS COMUNES UTILIZADAS EN CRIPTOGRAFÍA

	El remitente debe tener	El destinatario debe tener
Proceso de firmado	La clave privada del remitente (su propia clave privada)	La clave pública del remitente
Proceso de cifrado	La clave pública del destinatario	La clave privada del destinatario (su propia clave privada)

2.3 OPERACIONES CRIPTOGRÁFICAS BÁSICAS

CERTIFICACIÓN DIGITAL

- Aunque no es estrictamente necesario, un certificado digital (que siempre debe llevar una clave pública) puede incorporar también la clave privada relacionada.
- Por ejemplo, si la pareja de claves pública-privada se crea en la autoridad de certificación, esta nos expedirá un certificado con las dos claves para que tomemos posesión de la clave privada.
- Es estos casos, el certificado debe estar exquisitamente protegido, puesto que en caso contrario se corre el riesgo de comprometer la clave privada, por o que cuando un certificado lleva la clave privada esta se suele proteger con una contraseña o un PIN.
- Los certificados que llevan extensión pfx suelen incorporar esta clave privada.
- El modo de operación recomendado es que se instale el certificado pfx en el sistema del usuario, se guarde el fichero pfx en sitio protegido e inmediatamente generar a partir de él un nuevo certificado que no lleve la clave privada para distribuir entre los destinatarios que necesitaran la clave pública.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

- ¿Cómo se las arregla una autoridad certificadora para garantizar que la clave pública de un certificado se corresponda con su propietario?
- Lo hace comprobando que esto efectivamente es así, por ejemplo, haciendo personarse físicamente a la persona que se certifica para que acredite su identidad con la debida documentación oficial.
- De esta operación se encargan las oficinas o autoridades registradoras, que pueden o no coincidir con las certificadoras.
- Normalmente, una autoridad certificadora (la que expide los certificados, la que los firma con su clave privada) delega en otras entidades (autoridades registradoras) la comprobación de que los solicitantes de certificados son quienes dicen ser.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

Para conseguir un certificado tendrían que darse los pasos que se describen a continuación, aunque para algunos certificados, muchos de los pasos se pueden omitir.

a) Generar una petición de certificado (request), es decir, generar un para de claves pública-privada y su asociación con un objeto certificable (nombre de usuario, DNI, correo…)
b) La clave pública se envía (si no se generó allí) a la autoridad certificadora.
c) Antes de expedir el certificado, la autoridad certificadora nos pedirá que nos registremos en una autoridad registradora de su confianza.
d) Nos presentaremos en la autoridad registradora para demostrar documentalmente o presencialmente que somos los poseedores de la información que queremos certificar y que deseamos asociar a la clave pública.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

e) Si la autoridad registradora valida nuestra documentación informará a la autoridad certificadora que efectivamente cumplimos los requisitos necesarios para que se nos expida el certificado solicitado.

f) La autoridad certificadora, que se fía de la autoridad registradora, firma con su clave privada el certificado solicitado y nos proporciona el certificado expedido. Probablemente, habremos tenido que realizar algún pago previo a su obtención.

g) Una vez recibido el certificado, deberemos instalarlo en el SO o en la aplicación que lo necesite, junto con los certificados de todas las autoridades de certificación que aparezcan en la cadena de confianza de la oficina certificadora (normalmente las claves públicas de todas estas oficinas suelen incorporarse al certificado expedido para que en una única operación de instalación se instale todo lo necesario para establecer la relación de confianza completa.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

h) A partir de ese momento y durante el período de validez del certificado, este es totalmente operativo para las funciones para las que se expidió (firmado, cifrado…)

i) Si la clave privada es comprometida (por ejemplo, es robada) entonces el sistema criptográfico se rompe y deberemos solicitar a la oficina certificadora que revoque el certificado para que no se pueda utilizar. En este caso, solicitaremos un nuevo certificado con una nueva pareja de claves privada-pública. La oficina de certificación publicará en una lista el certificado revocado para consulta de los usuarios y que así puedan conocer que ese certificado, aún dentro del período de validez, ha quedado revocado y no debe usarse.

j) Antes de que un certificado expire, debe solicitarse una renovación del mismo. Esta renovación puede realizarse utilizando la misma pareja de claves pública-privada (si la clave privada no ha sido comprometida) o generando una nueva pareja de claves.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

- Un **PKI** (Public Key Infrastructure) es el conjunto de elementos (hardware y software incluidos) que se necesitan para crear un sistema de certificación.
- Por tanto, un PKI se compone de una o más autoridades de certificación jerarquizadas, autoridades de registro, servidores web que publiquen los certificados revocados…
- Las autoridades de certificación pueden ser de muchos tipos, pero aquí nos centraremos en dos tipos básicos:
  - **Autoridades raíz**. No dependen de ninguna otra autoridad y, por tanto, sus certificados son firmados por ellas mismas (son autofirmados).
  - **Autoridades subordinadas**. Dependen en la cadena de confianza de otra autoridad de orden superior. Sus certificados propios (no lo que ellas expiden a otros) están firmados con la clave privada de la autoridad de la que dependen.

2.4 INFRAESTRUCTURA DE CLAVE PÚBLICA, PKI

- En el mundo Windows el software de un PKI se puede instalar como un rol sobre servidores Windows Server y define dos tipos de oficinas de certificación:
  - **Oficina independiente:** se establece sobre servidores que no se relacionan con un Directorio Activo.
  - **Oficina empresarial.** Requieren la presencia de un Directorio Activo en el que se integran y automatizan gran parte de las tareas de gestión de la oficina, las peticiones de los certificados de los usuarios y los equipos, así como su distribución por toda la red de equipos integrados en los dominios del Directorio Activo.
- Una vez instalado el software, la autoridad de certificación se puede gestionar desde la consola MMC específica. Los certificados también se pueden solicitar a través de un servicio web.
- Para sistemas GNU/Linux, el software más utilizado es OpenSSL, que instala todo el software y características necesarias para montar oficinas de certificación.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

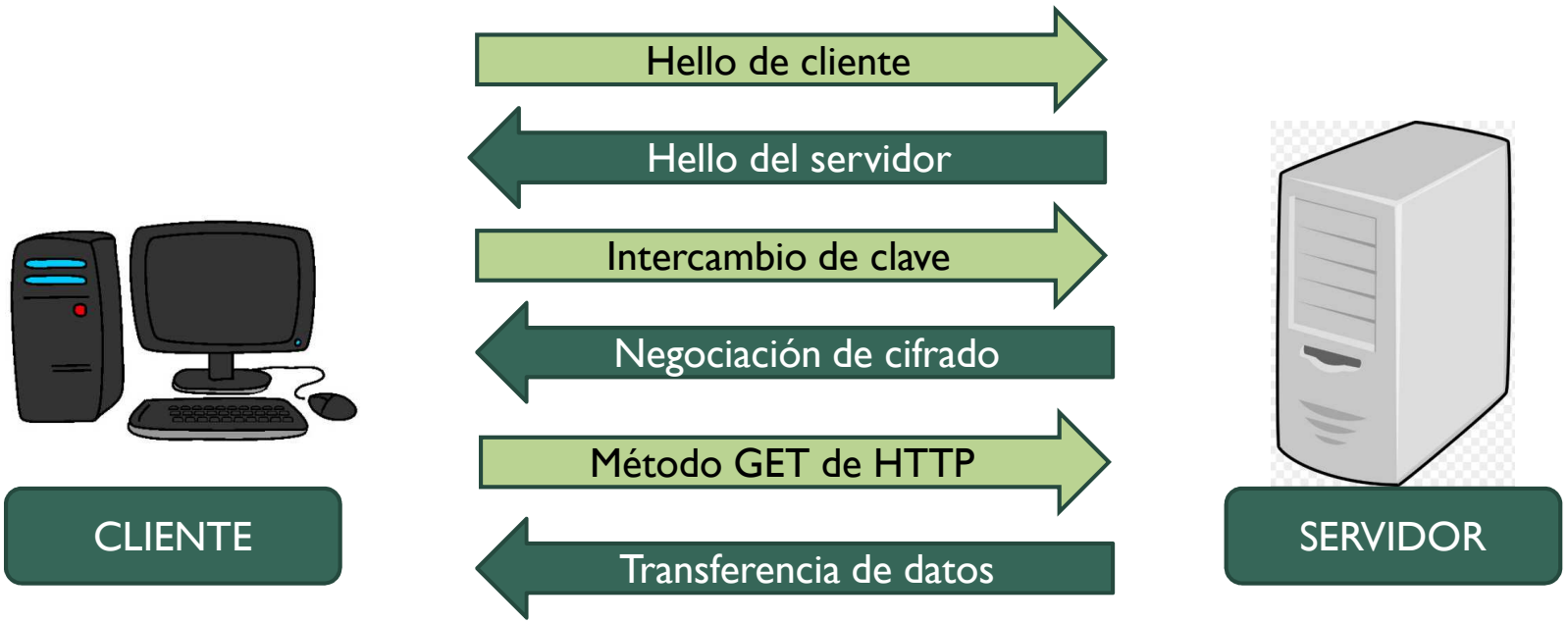
PROTOCOLO SSL/TLS

- En el protocolo SSL se utiliza tanto criptografía asimétrica como simétrica.
- La primera se utiliza para realizar el intercambio de las claves, que a su vez serán usadas para cifrar la comunicación mediante un algoritmo simétrico.
- En el caso de los sitios web, para el funcionamiento de este protocolo, lo que se necesita utilizar es un certificado SSL.
- El servidor web tendrá instalado uno y cuando un cliente intente acceder a él, le remitirá el mismo con la clave pública del servidor, para enviar de esta forma la clave que se usará para realizar la conexión de manera segura mediante un cifrado simétrico.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

PROTOCOLO SSL/TLS

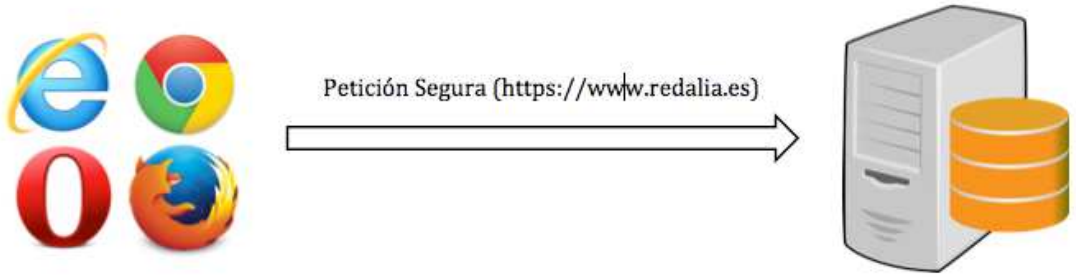
- Flujo de operación en SSL/TLS



2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

EJEMPLO SSL/TLS

- Un usuario realiza una petición HTTP segura a través de un navegador a un sitio web (HTTPS://www.redalia.es/)

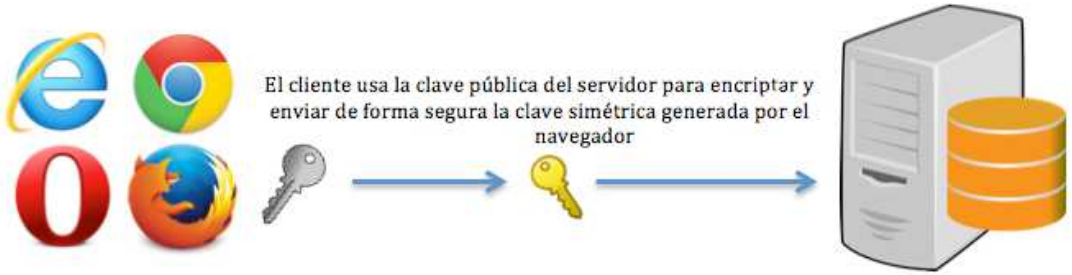


- El servidor donde está alojado el sitio web, envía (si lo tiene) el certificado que incluye la clave pública del servidor. En caso de no tener certificado SSL, se producirá un error.

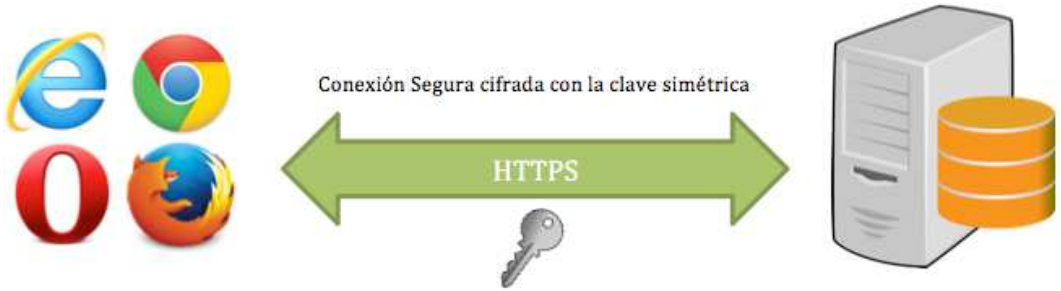
2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

EJEMPLO SSL/TLS

- El navegador comprueba que la entidad emisora del certificado o CA sea de confianza. En caso contrario, pedirá al usuario que acepte el certificado bajo su responsabilidad.
- Llegados a este punto, el navegador generará una clave simétrica, que será cifrada mediante la clave pública del servidor para ser enviada de manera segura al mismo.



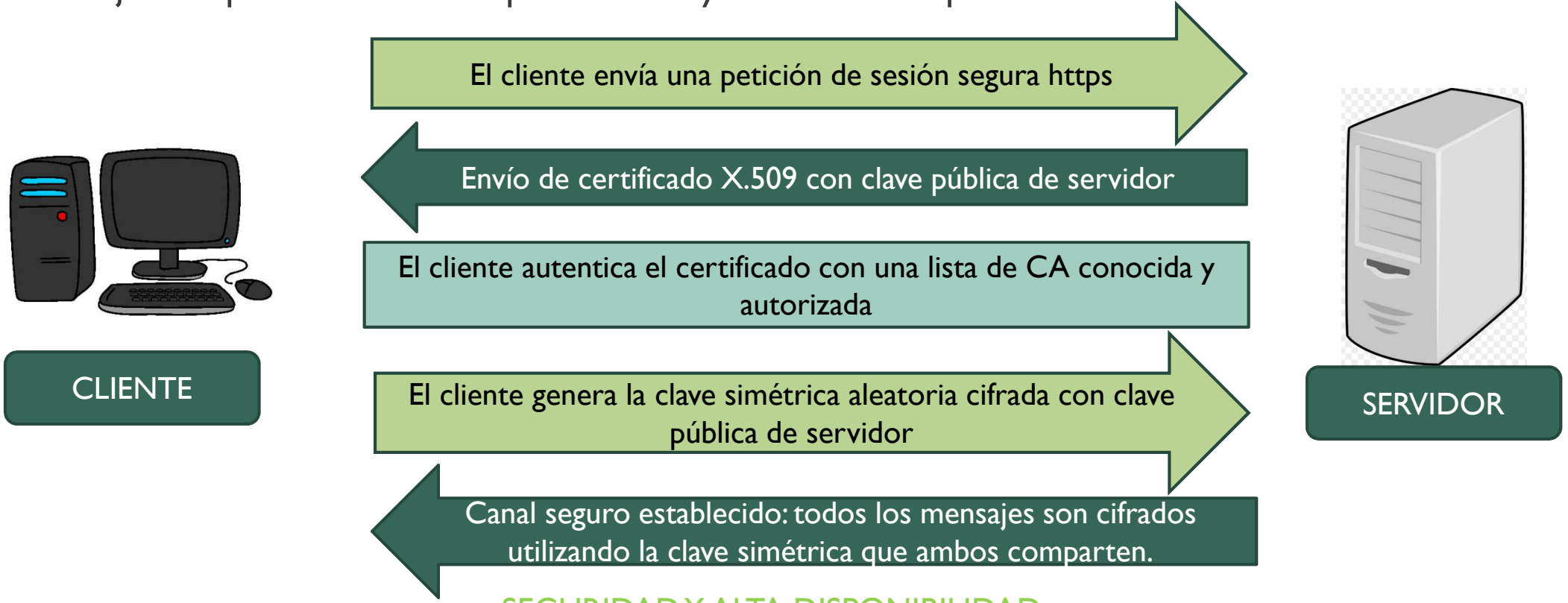
- De esta forma, la comunicación ya se ha establecido de manera segura, y será cifrada en ambos sentidos mediante la clave generada en el punto anterior.



2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

CIFRADO SSL/TLS

- Flujo de operación SSL/TLS para cifrado y autenticación para autenticación del servidor.



2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

ACTUALIZACIÓN SSL/TLS

- ¿Cómo se consigue la autenticación, es decir, cómo se sabe que tanto el servidor como el cliente son quienes dicen ser? Para garantizar esto, SSL/TLS proporciona capacidad de autenticación.
- Se ha visto cómo el servidor presenta su certificado público al cliente haciéndole poseedor de su clave publica con la que podrá cifrar mensajes que solo el servidor podrá descifrar con su clave privada relacionada.
- Si cliente y servidor se fían de la autoridad certificadora que expidió el certificado del servidor, el cliente tendrá seguridad (confianza) en que el servidor es quien dice ser en su certificado.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

ACTUALIZACIÓN SSL/TLS

- Del mismo modo, si invertimos la dirección del proceso, puede hacerse que el cliente también quede autenticado en el servidor.
- Para ello, basta que el cliente posea también un certificado reconocido por el servidor y en la fase de intercambio de claves cliente y servidor se intercambian los certificados y se autentiquen recíprocamente.
- Esta es la técnica utilizada para autenticar transacciones electrónicas mediante criptografía asimétrica con doble autenticación: en cliente y en servidor.
- Esos certificados y las claves privadas son los datos que suelen registrase en el DNI electrónico, las bandas magnéticas de las tarjetas de crédito, los tokens de seguridad para el acceso a sistemas…

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

INTEGRIDAD SSL/TLS

- Como se ha descrito al principio, el protocolo SSL/TLS no sólo proporciona confidencialidad en la información, también garantiza su integridad.
- Para ello se vale de un código de autenticación de mensaje (MAC, Message Authentication Code).
- Este código se calcula mediante una función hash con una clave secreta que sólo conocen el emisor y el receptor de la comunicación (el cliente y el servidor).
- De esta forma, si un sólo bit de toda la información es modificado, el MAC será totalmente diferente, y ambas partes podrían saber en ese punto que la información ha sido modificada.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

PROTOCOLO SSH

- SSH (Secure Shell) es una colección de protocolos y utilidades que proveen autenticación y cifrado en el establecimiento de conexiones entre dispositivos de red de modo semejante a como lo hace SSL/TLS, pero orientado a aplicaciones más que a protocolos de la capa de aplicación.
- Por ejemplo, con SSH podríamos presentarnos en un equipo remoto con una conexión segura.
- De hecho, SSH es un sustituto que añade capacidad de cifrado al protocolo telnet, que no cifra las conexiones.
- SSH también puede ejecutar comandos remotos en un host e incluso copiar ficheros desde una localización remota a otra mediante transporte cifrado.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

PROTOCOLO SSH

- SSH se encarga de cifrar los datos transportados en toda una sesión mediante la **creación de un túnel de cifrado** de modo que todo lo que se envíe por uno de los extremos del túnel es cifrado y aparecerá por el otro extremo del mismo túnel que descifra la información a su salida.
- Con esto evitamos muchos problemas de seguridad como los de suplantación IP (IP shoofing), suplantación de DNS (DNS spoofing) o interceptación de datos.
- Para cifrar las comunicaciones, SSH puede utilizar los protocolos DES, 3DES, RSA y Kerbero entre otros.
- Además es altamente configurable, lo que le proporciona una flexibilidad tan grande que es una de las herramientas más útiles en mano de los administradores de redes y sistemas.
- Por desgracia, también es muy útil para hackers, por lo que si aparecen túneles SSH inesperados en la red, habrá que sospechar de actividades no autorizadas.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

PROTOCOLO SSH

- Como el túnel crea conexiones cifradas, el contenido de lo que viaja por el túnel está vetado para los escuchadores de red que solo captarán tráfico cifrado con una clave que ellos desconocen puesto que so lo está en posesión de emisor y receptor.
- Para que dos aplicaciones, una en el emisor y otra en el receptor, puedan utilizar un túnel SSH deben redireccionar su salida/entrada hacia los extremos del túnel.
- SSH es capaz de crear túneles y de cifrar la información que viaja a su través.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

DIFERENCIA ENTRE SSL/TLS Y SSH

- **SSL:**
  - Es una manera de proteger la información que está viendo con un navegador Web.
  - Es la mejor manera de acceder a cuentas bancarias y enviar las contraseñas a los servidores Web en Internet.
  - Sabes que utilizan SSL si la dirección Web que está accediendo está prologada con HTTPS en lugar de HTTP, que no está protegido.
- **SSH**:
  - Se utiliza para forma segura enviar comandos de texto o archivos a un servidor Web en Internet.
  - Una conexión SSH encripta todo lo que usted envía a través de él para que su información no puede ser interceptada sin su conocimiento.
  - Para aprovechar las ventajas de SSH se debe usar a un cliente SSH.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

CIFRADO DE SISTEMAS DE FICHEROS EN LOS SO

- Una de las aplicaciones más útiles de la criptografía aplicada a los medios de almacenamiento es el cifrado de ficheros y carpetas.
- Esto viene a resolver el problema de la privacidad de documentos.
- Se trata de que los ficheros estén disponibles para todos los usuarios del sistemas pero que solo sus propietarios puedan interpretar correctamente su contenido.
- Por ejemplo, el operador de backup de un sistema tiene que poder acceder al contenido, aunque tenga derechos de lectura de la información, no tiene que comprender su contenido, aunque tenga derechos de lectura sobre los ficheros que tiene obligación de salvar.
- Esta funcionalidad se consigue con técnicas de cifrado.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

CIFRADO DE SISTEMAS DE FICHEROS EN LOS SO

- En Windows, el sistema emplea las características EFS (Encriypted File System), que solo está disponible para sistemas de ficheros NTFS, nunca para FAT o FAT32.
- El modo de operación es el siguiente:
  1. Se selecciona con el botón derecho del ratón el fichero o carpeta a cifrar.
  2. Se accede a la ficha de propiedades del menú contextual y opciones avanzadas.
  3. Se activa la casilla "Cifrar contenido" para cifrar los datos con una clave ligada al usuario que abrió sesión en el sistema y que Windows crea automáticamente cuando el administrador crea la cuenta del usuario. La información cifrada aparecerá en color verde.
  4. Si se desea descifrar, basta con desmarcar la casilla de "Cifrar contenido"

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

CIFRADO DE SISTEMAS DE FICHEROS EN LOS SO

- Para que un fichero pueda ser descifrado hay que presentarse con la sesión del usuario que lo cifró.
- ¿Qué pasaría si la cuenta de ese usuario ya no existe? A priori, se perdería el fichero, pues aunque físicamente resida en el disco y sea accesible, no se podrá descifrar.
- Para evitar este problema y por seguridad, Windows ha previsto un mecanismo de exportación de claves a un certificado de modo que, aunque se borre la cuenta de usuario, se pueda recuperar la información cifrada por el usuario de esa cuenta a partir del certificado exportado.
- EFS es sistema nativo de Windows, pero hay muchos distribuidores de software que comercializan productos de cifrado de sistemas de ficheros tanto para Windows como para GNU/Linux u otros sistemas, por ejemplo, Cryptoforge.

2.5 OTRAS APLICACIONES CRIPTOGRÁFICAS

CIFRADO DE SISTEMAS DE FICHEROS EN LOS SO

- En el mundo GNU/Linux también hay multitud de aplicaciones, mayoritariamente open source, para realizar operaciones de cifrado con ficheros, carpetas o particiones de disco, por ejemplo, la utilidad fuse.
- Con esta utilidad enlazamos dos carpetas una de cifrado y otra de descifrado lo que se hace bajo la supervisión de una contraseña de enlace que solo conoce el usuario.
- Cualquier fichero que añadamos a la carpeta de descifrado aparecerá reflejado en la de cifrado como un fichero equivalente pero ilegible por el cifrado.
- Una vez desmontando el enlace entre las dos carpetas, toda la información de la carpeta de descifrado desaparece y quedará únicamente la información cifrada en la carpeta de cifrado.
- Para volver a descifrar el contenido se necesitará volver a enlazar las carpetas, lo que exigirá conocer la contraseña del enlace.