TEMA-2.-Seguridad-en-las-comunic...

_GxIIsi7

Redes y Seguridad I

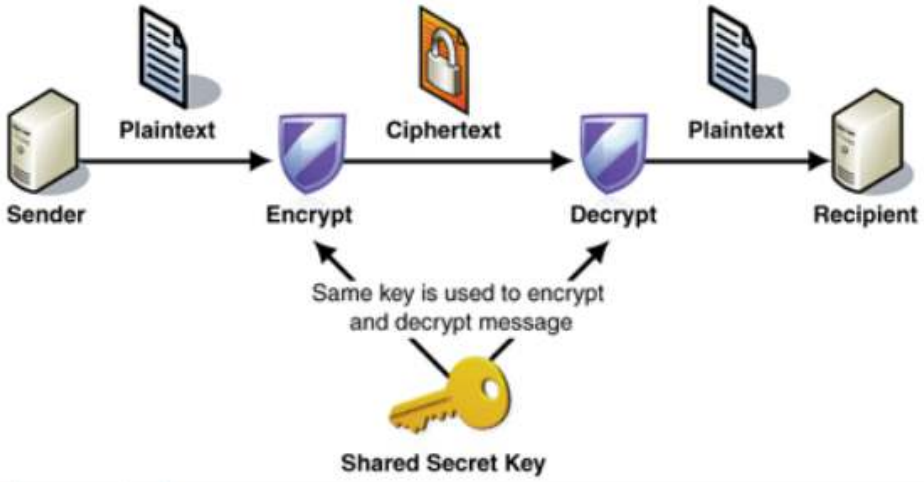
3º Grado en Ingeniería Informática

Facultad de Informática
Universidad Complutense de Madrid

TEMA 2. Seguridad en las comunicaciones

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

Clave: INFORMATICAINFO
Texto en claro: REDESYSEGURIDA
Texto cifrado: ZRISJKSXOWRQQFR



ÍNDICE

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos Holandés con una garantía de hasta 100.000 euros por depositante. Consulta más información en ing.es

Que te den **10 € para gastar** es una fantasía. ING lo hace realidad.

Abre la **Cuenta NoCuenta** con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Quiero el cash

Consulta condiciones **aquí**

do your thing

Redes y Seguridad I

Banco de apuntes de la

WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

Introducción a la criptografía

Sistema de comunicación seguro

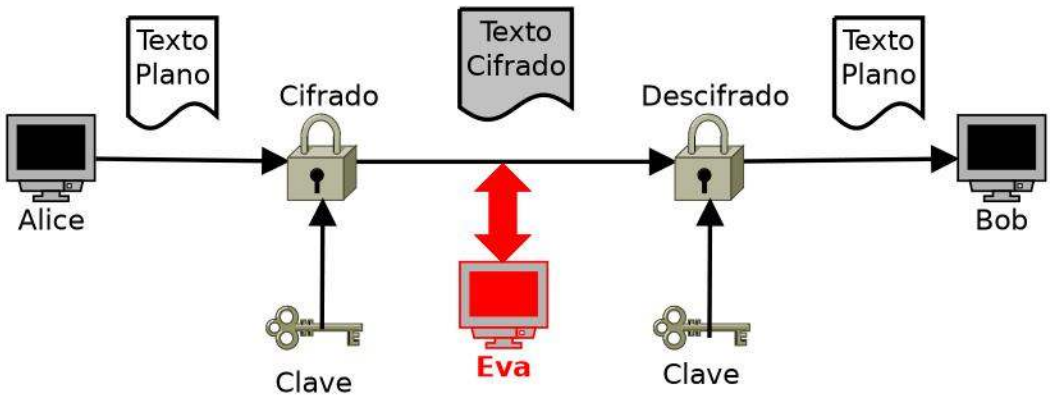
Debe proporcionar: Autenticación en cada parte, Confidencialidad de datos, Integridad de datos y no repudio.
Como se consigue: Mediante técnicas criptográficas.

Criptografía-Criptoanálisis-Criptología

- **Criptografía:** Conjunto de técnicas o algoritmos que sirven para proteger la información (almacenada o transmitida) y evitar que pueda ser leída y/o detectar que haya sido modificada por usuarios no autorizados. También proporciona autenticación entres las partes que se comunican.
- **Criptoanálisis:** Estudio de técnicas que tratan de revertir el proceso de cifrado, descubriendo el contenido del mensaje o la clave a partir de la información disponible.
- **Criptología:** Ciencia que estudia la criptografía y el criptoanálisis.

Definiciones

- **Texto en claro:** Información original, inteligible por una persona (documento) o computador (código ejecutable).
- **Texto cifrado:** Información modificada, no comprensible para ninguna persona o computador antes de ser descifrada.
- **Algoritmo:** Conjunto de reglas que determinan cómo se realizan los procesos de cifrado y descifrado.
- **Clave:** Cadena de caracteres o secuencia de bits aleatorios que se usan, junto con el algoritmo de cifrado, para cifrar el texto en claro.
- **Sistema criptográfico:** Sistema capaz de cifrar y descifrar. Consta de algoritmos de cifrado, claves y protocolos.



Algoritmos de cifrado

Según las operaciones que se realizan en el proceso de cifrado pueden ser de:

- **Sustitución:** A cada elemento del texto en claro se le asigna otro elemento en el texto cifrado.
- **Transposición/permutación:** Reordenar los elementos del texto en claro.
- **Sistemas producto:** Varias etapas de sustituciones y transposiciones.
- **Numérica:** Los elementos del texto en claro se tratan como números a los que se aplican algunas propiedades y relaciones matemáticas

Por el número de claves usadas:

- **Simétrico o de clave secreta**: Misma clave para cifrar y descifrar.
- **Asimétrico o de clave pública:** Una clave para cifrar, otra para descifrar.

Por la forma en la que se procesan los mensajes:

- **De bloque:** Procesa un bloque del mensaje cada vez, produciendo un bloque de salida por cada bloque de entrada.
- **De flujo:** Procesa los elementos de entrada de forma continua, produciendo un elemento de salida cada vez.

Ataques de fuerza bruta

Implican intentar todas las posibles claves hasta que se obtenga una traducción inteligible del texto cifrado. En promedio, se debe intentar la mitad de todas las posibles claves para tener éxito. Si el tamaño de la clave es grande se trata de un trabajo computacionalmente costoso.

Técnicas de criptoanálisis

Para reducir el coste computacional del ataque se aplican técnicas de criptoanálisis.

- **Análisis de frecuencias:** Estudiar la frecuencia de aparición de letras o patrones en el texto cifrado.
- **Diccionario:** Usar muchas contraseñas (≠claves) comunes .
- **Colisiones de claves:** Aprovechar la paradoja del cumpleaños para producir colisiones de claves que revelen información acerca del texto claro.
- **Criptoanálisis diferencial:** Analizar cómo las diferencias en el texto en claro se corresponden con diferencias en el texto cifrado.
- **Criptoanálisis lineal:** Usar aproximaciones lineales del comportamiento para derivar bits de la clave o del texto en claro.
- **Claves relacionadas:** Usar textos cifrados con dos claves diferentes con alguna relación (ej. compartiendo algunos bits).
- **Claves débiles:** Aprovechar claves que hacen que el cifrado funcione de forma no deseable.

Sistema de cifrado seguro

La robustez de un sistema criptográfico de cifrado simétrico dependerá de: El algoritmo de cifrado, la longitud de la clave, la clave sea secreta y los vectores de inicialización.
El **algoritmo** utilizado debe conseguir que el texto cifrado sea estadísticamente independiente de la clave y del texto en claro.

- **Difusión:** Consiste en dispersar la estructura estadística del texto en claro a lo largo del texto cifrado. Cada dígito del texto en claro afecta a varios dígitos del texto cifrado y al revés: **Permutaciones.**
- **Confusión:** La relación estadística entre el texto cifrado y la clave debe ser lo más compleja posible: **Sustituciones.**

Un esquema de cifrado será **computacionalmente seguro** si el texto cifrado generado por el esquema cumple uno o ambos de los siguientes criterios:

- El **coste** de romper el cifrado excede el **valor** de la información.
- El **tiempo** requerido para romper el cifrado excede la **vida útil** de la información.

Algoritmos de cifrado

Proceso de cifrado

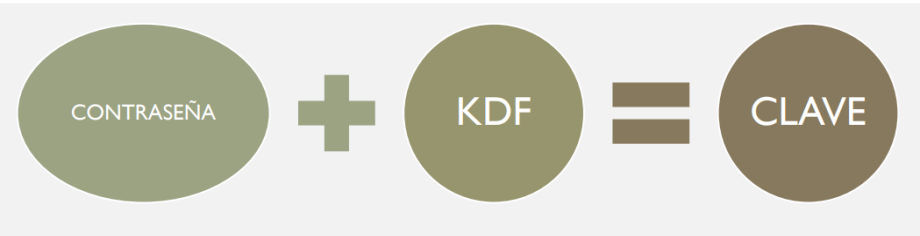
El proceso de cifrado consta de dos componentes principales:

- **El algoritmo de cifrado:** Conjunto de complejas fórmulas matemáticas aplicadas en un orden determinado para convertir el texto en claro en texto cifrado.
- **La clave:** Cadena de bits aleatoria que se usa junto al algoritmo para añadir aleatoriedad al texto cifrado.

En los procesos de cifrado y descifrado se usará el mismo algoritmo y a veces la misma clave.

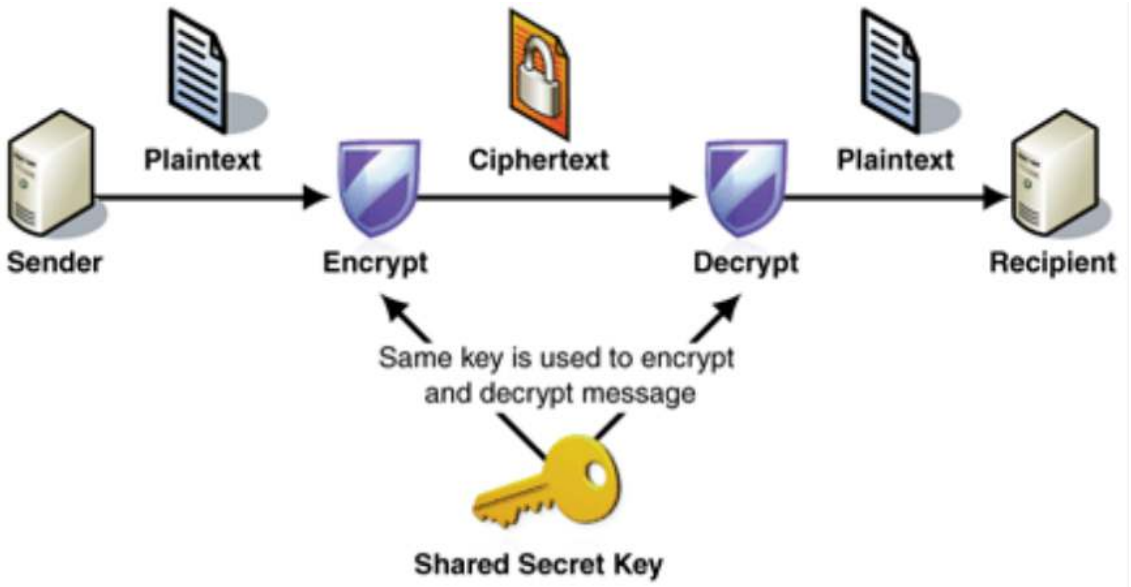
Generación claves

Las claves se generan a partir de KDFs (Key Derivation Functions): Un algoritmo que aplica varias rondas (cuantas más, mayor seguridad) de funciones matemáticas a una determinada entrada.
La entrada puede ser una función resumen (hash), una contraseña y/o una sal (nº aleatorio).



Cifrado simétrico

Misma clave y algoritmo para cifrar y descifrar. La seguridad del cifrado simétrico depende en gran medida de la clave que tiene que ser secreta y guardarse de forma segura. Proporciona **confidencialidad.**



Para que este cifrado sea seguro se deben cumplir los siguientes requisitos:

- Que el algoritmo de cifrado sea seguro.
- Que emisor y receptor hayan obtenido una copia de la clave secreta de forma segura y que esta permanezca segura.
- Que la clave sea robusta (longitud adecuada).

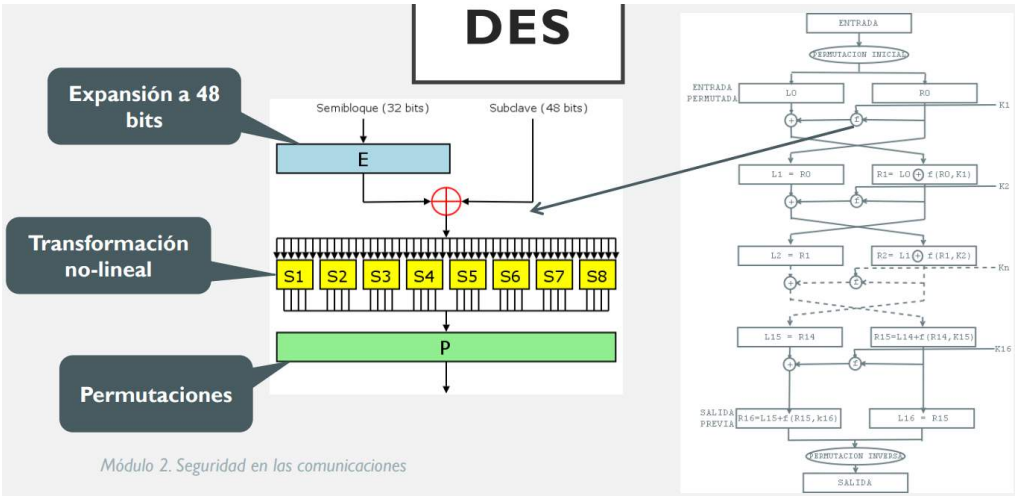
Cifrado simétrico: Algoritmos de bloque

Procesan la entrada de texto en claro en bloques de tamaño fijo y producen un bloque de texto cifrado de igual tamaño para cada bloque de entrada (DES, 3DES, AES). Estos algoritmos para ser seguros deben cumplir que:

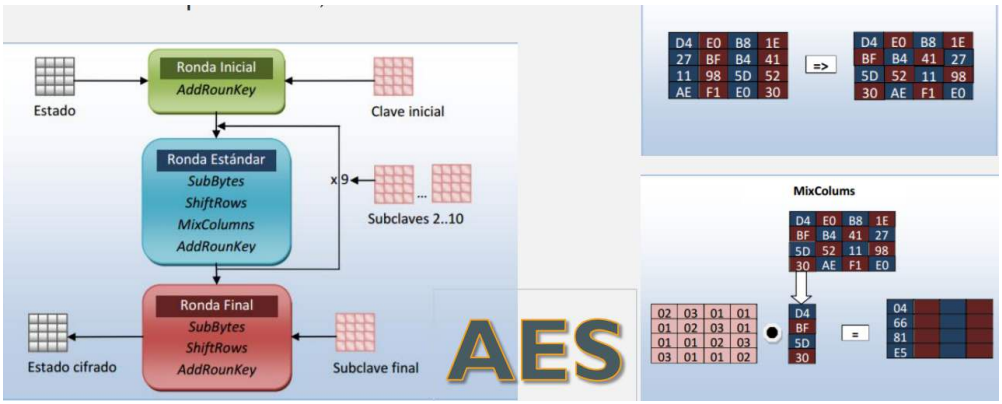
- Cada bit del texto cifrado dependa de todos los bits de la clave y del texto en claro.
- No haya relación estadística evidente entre el texto en claro y el texto cifrado.
- Alterar un simple bit del texto en claro altere cada bit del texto cifrado con una probabilidad del 50%.
- Alterar un bit del texto cifrado suponga un cambio impredecible en la recuperación del texto en claro.

Algoritmos de bloque:

- **Data Encryption Standard (DES):** Tamaño de bloque de 64 bits, clave de 56 bits, red de Feistel con pequeñas variaciones y 16 rondas de procesamiento. Es vulnerable, ya no se usa.

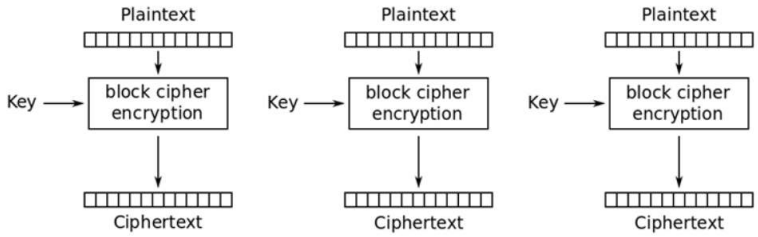


- **Triple DES (3DES O TDEA):** Para solucionar los problemas del algoritmo DES.
- **Advanced Encryption Standard (AES):** Tamaño de bloque de 128 bits, claves de 128, 192 y 256 bits y red de sustitución-permutación.



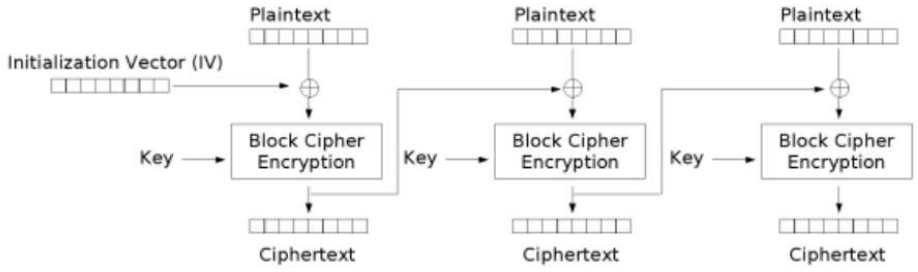
Los modos de operación especifican cómo opera cada cifrador de bloque y cómo se interconectan los cifradores entre sí:

- **ECB:** Fallan cifrando datos de gran tamaño, el mismo texto en claro con la misma clave genera el mismo texto cifrado y no oculta patrones. Se usan para cifrar PINs, respuestas de retos en procesos de autenticación y claves de cifrado.



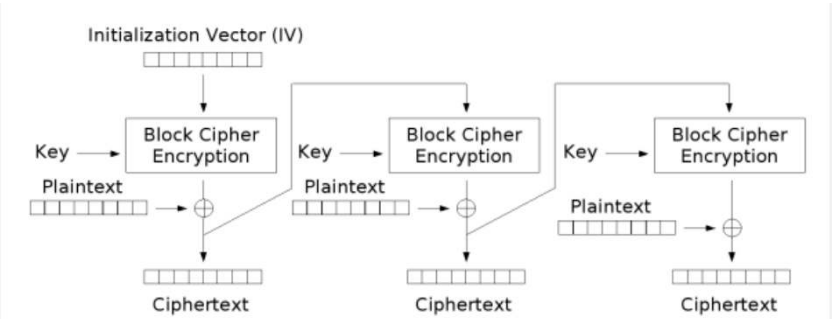
Electronic Codebook (ECB) mode encryption

- **CBC:** Mayor aleatoriedad en el texto cifrado, el efecto cadena oculta patrones, ideal para cifrar datos de gran tamaño, la salida de un bloque depende de todos los bloques anteriores y se necesita usar un vector de inicialización (IV) para el primer bloque (aleatorio y distinto para cada cifrado).



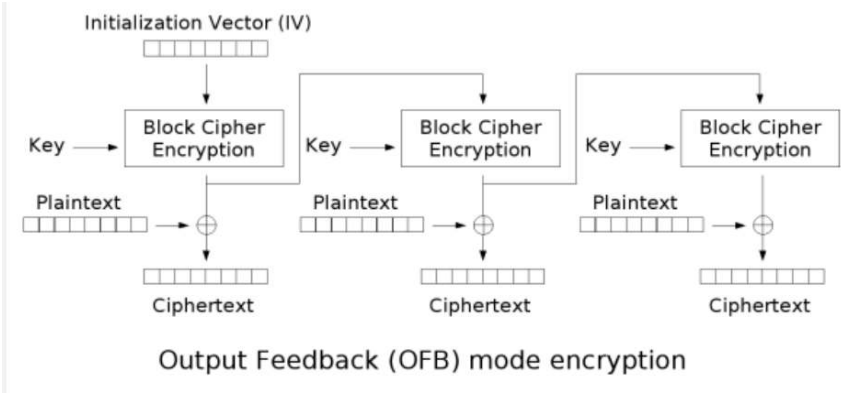
Cipher Block Chaining (CBC) mode encryption

- **CFB:** Emula un algoritmo de cifrado de flujo, la clave y el IV se usan para crear el flujo de claves y se usan para cifrar mensajes pequeños.

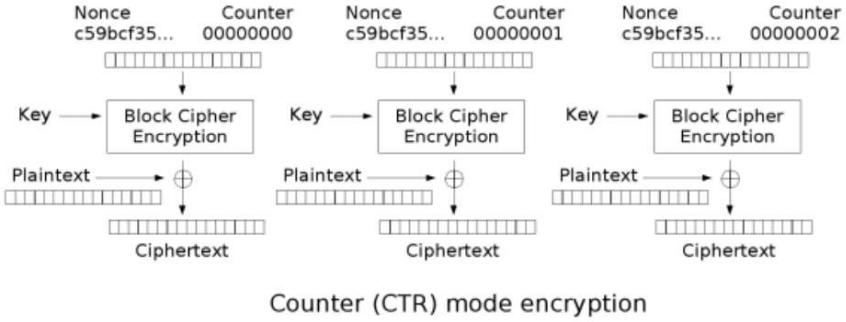


Cipher Feedback (CFB) mode encryption

- **OFB:** Garantiza que errores generados en la salida de un bloque no van a afectar el proceso de cifrado de los demás bloques. Se usa cuando se necesita cifrado de flujo y los datos cifrados son sensibles a errores. Ejemplo: Vídeo y voz digital.



- **CTR:** El IV se genera a partir de un contador. Alto rendimiento (el cifrado de bloques se realiza en paralelo). Usado en celdas ATM, IPsec y en seguridad WIFI.



Cifrado simétrico: Algoritmos de flujo

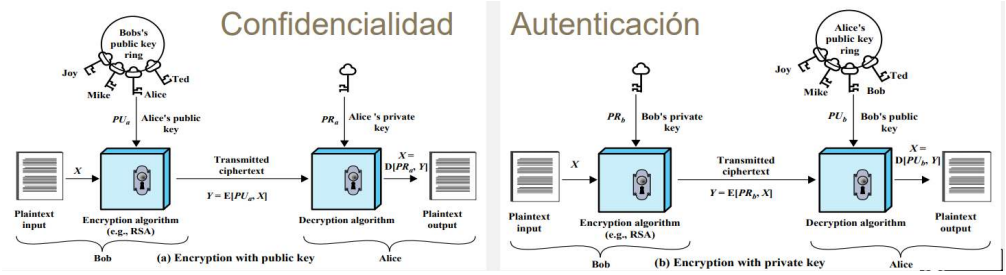
Los dígitos del texto claro se combinan (XOR) con un flujo pseudoaleatorio de dígitos denominado flujo de claves. En el cifrado de flujo síncrono, el flujo de claves (aleatorio e impredecible) se genera en función de la clave. Se usan en aplicaciones de tiempo real como VoIP o multimedia.
Estos algoritmos para ser seguros deben cumplir que:

- El flujo de claves debe tener un periodo largo. Cuanto más tarde en repetirse, más difícil será el criptoanálisis.
- El flujo de claves debe parecerse lo máximo posible a un flujo de números aleatorios reales.
- Flujo de claves estadísticamente no sesgado.

Más débiles que los algoritmos de cifrado de bloque: Muy difícil conseguir un flujo de clave totalmente aleatorio y no sesgado.

Cifrado asimétrico

Usan dos claves, una clave pública, conocida por todos, y una clave privada que solo conoce el propietario. Se basan en **funciones matemáticas en lugar de realizar operaciones sobre patrones de bits.**
Se cifra con una clave y se descifra con la otra. Dependiendo del servicio buscado se cifra con la clave pública o la privada.



Los algoritmos de clave pública tratan los datos de entrada como un número.

- El tamaño máximo de los datos depende del tamaño de la clave.
- El cifrado de ciertos datos puede ayudar al criptoanálisis.
- Mucho más lentos que los algoritmos de clave secreta.

Solamente deben usarse para cifrar datos **aleatorios** (ej. claves de sesión) o **pseudoaleatorios** (ej. códigos hash).
Aplicaciones del cifrado asimétrico:

- **Firma digital:** El emisor garantiza la autenticidad (integridad y autenticidad de origen) de un documento o un mensaje.
- **Intercambio de clave:** Dos partes cooperan para establecer una clave secreta compartida con la que cifrar un documento, un mensaje o una comunicación, confidencialidad de la clave.

Cifrado asimétrico: Algoritmos

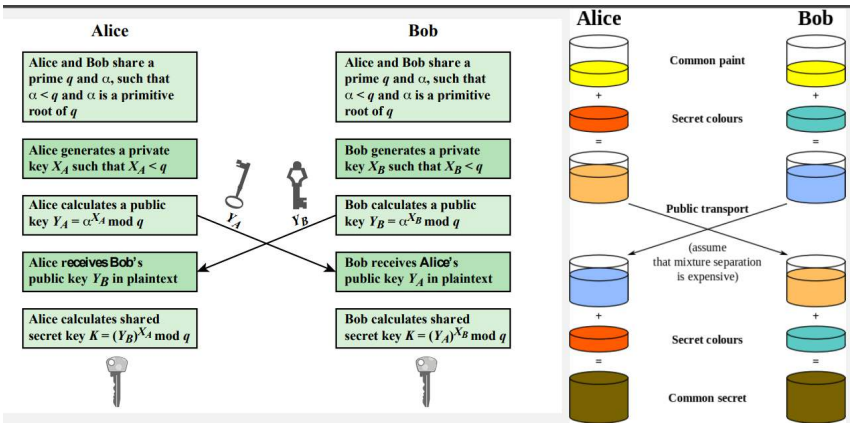
Algoritmo	Cifrado	Firma digital	Intercambio de clave
RSA	Sí	Sí	Sí
Diffie-Hellman	No	No	Sí
DSA	No	Sí	No
ECDH	No	No	Sí
ECDSA	No	Sí	No

- **RSA:** Se usa como protocolo de intercambio y transporte de clave.
  - El sistema de cifrado genera una clave simétrica.
  - Esta clave se cifra con la clave pública del receptor.
  - El receptor la descifra con su clave privada, que solo él conoce.

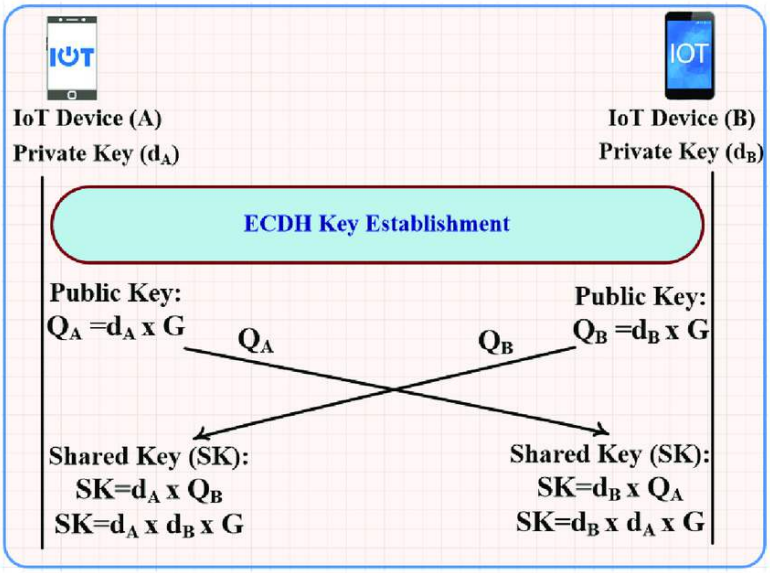
1. Seleccionar dos números primos distintos p y q
2. Calcular $n = p \cdot q$ y $\phi(n) = (p - 1) \cdot (q - 1)$
3. Seleccionar un entero e tal que $1 < e < \phi(n)$ y $\text{mcd}(\phi(n), e) = 1$
   - Se suele tomar $e = 65.537$ (0x10001)
4. Calcular d tal que $d \cdot e \bmod \phi(n) = 1$
5. La clave pública es $\{e, n\}$
6. La clave privada es $\{d, n\}$

Cifrado	Descifrado
Dado un texto claro $M < n$, el texto cifrado es $C = Me \bmod n$	Dado un texto cifrado C, el texto claro es $M = Cd \bmod n$

- **DH:** Su propósito es permitir a dos partes acordar una clave secreta de forma segura. El intercambio de clave con DH se denomina **acuerdo de clave**.
  - La clave secreta no viaja, sino que la genera cada parte.
  - Proporciona secreto perfecto hacia delante (Perfect Forward Secrecy). Si la clave privada se descubre la información intercambiada con anterioridad sigue estando protegida.



- **ECDH:** Se basa en una curva elíptica sobre un cuerpo finito y la operación de multiplicación escalar. Ofrece la misma seguridad con un tamaño de clave menor, lo que reduce el tiempo de procesamiento.
  - Las partes acuerdan los parámetros de dominio.
  - Cada parte genera un par de claves (d, Q) usando curvas elípticas. d: Número entero aleatorio (clave privada). Q: punto de la curva (clave pública) tal que Q=d•G (producto escalar).
  - El intercambio se hace de modo similar a DH.



Cifrado híbrido

Combina el uso de algoritmos de cifrado simétrico con algoritmos de clave pública:

- Los algoritmos de cifrado simétrico se usan para cifrar con una clave secreta toda la información compartida durante una sesión.
- Los algoritmos asimétricos se usan para intercambiar la clave secreta (clave de sesión) .

Solución más usada

- ECDHE para acordar la clave secreta
- AES-256 para cifrar y descifrar con la clave secreta acordada

Funciones Resumen y Firma digital

Funciones resumen (Hash)

Tienen un mensaje M de tamaño variable como entrada y producen un resumen (digest) del mensaje H(M) de tamaño fijo como salida. Son funciones que solo se ejecutan en un sentido. Siempre dan el mismo resultado. Tamaño variable como entrada, tamaño fijo de salida:

Hash	Cadena de texto	Resultado
md5	Redes	2A9C31CDB6A758C90485380AAEAD1130
md5	Redes y	0C9728B6E5AA0DC8FDDB3D8A09D2A969
md5	Redes y Seguridad	AA80388469EEB0BF98CD2CEFD6BF6075
md5	Redes y Seguridad I	3A0ABA1538F3595ED87A066E1A6CC0CE

El tamaño del resultado de la función resumen depende del algoritmo utilizado:

Hash	Texto	Resultado
md5	Redes y Seguridad I	3A0ABA1538F3595ED87A066E1A6CC0CE
SHA1	Redes y Seguridad I	06D79560A1F1A8B294B21853486B57B34A05ECA8
SHA256	Redes y Seguridad I	32C53BA0000532936965722 6B313B344AE560F8DF706C4C7355E274394CE93E8
Haval-128	Redes y Seguridad I	FB684EE936DE2F1AFEE17531B13C49E8

Pequeños cambios en la cadena de entrada producen grandes cambios el resultado:

Hash	Frase	Resultado
md5	Redes y Seguridad I	3A0ABA1538F3595ED87A066E1A6CC0CE
md5	Redes y Seguridad II	862295E7366BE40DE34F17AFFF4FD928

Se usan para la autenticación de mensajes y software, el almacenamiento de contraseñas y la firma digital. Producen una huella (fingerprint) de un fichero, mensaje o cualquier otro bloque de datos. También se usan para la generación de números pseudo-aleatorios.

Funciones resumen seguras

Un algoritmo de hashing es seguro si está libre de colisiones. Si un algoritmo genera el mismo valor para dos mensajes diferentes se dice que se ha producido una colisión.

Una función resumen H será segura si cumple que:

- La función H se computa sobre el mensaje completo.
- Dado h, sea computacionalmente inviable encontrar x con H(x) = h.
- Resistente a colisiones:
    - Dado x, sea inviable encontrar y con H(y) = H(x)
    - Sea inviable encontrar x e y tal que H(x) = H(y)

Ataques contra funciones resumen

Los algoritmos que generan funciones resumen se pueden atacar con:

- **Criptoanálisis:** explotar debilidades lógicas del algoritmo.
- **Fuerza bruta:** la fortaleza de la función resumen depende únicamente del tamaño del código hash producido por el algoritmo (2^n mensajes aleatorios en el peor caso 2^n/2 siendo n el tamaño en bits).
- **Paradoja de cumpleaños**

Algoritmos de funciones resumen

- **MD5:** Función resumen de 128 bits. Vulnerable a ataques por colisión.
- **Secure Hashing Algorithm (SHA):**
  - **SHA-1:** Más resistente a colisiones, pero insegura. Sistemas afectados: Firma digital, Certificados https, Control de versiones (git) y Sistemas de backup. Solución: Migrar a SHA-256 o SHA-3.
  - **SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512):** Seguro.

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
	← SHA-2 →				
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Todos los tamaños están expresados en bits

  - **SHA-3:** Alternativa a SHA-2. Seguro.

Servicios de seguridad

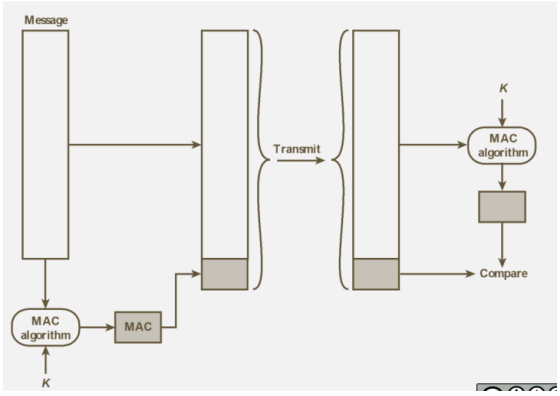
Proporciona integridad:

- Si la información es transmitida solo puede detectar modificaciones del mensaje no intencionadas.
- Si una tercera persona modificara la comunicación entre dos partes cambiando el hash, el receptor no se enteraría. Solución: Usar un código MAC o firma digital.

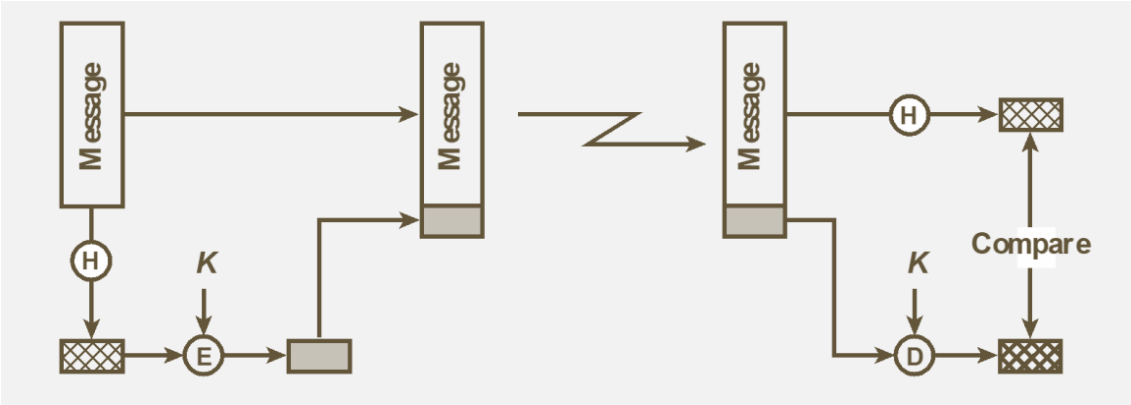
No proporciona confidencialidad ni autenticación.

Autenticación de mensajes

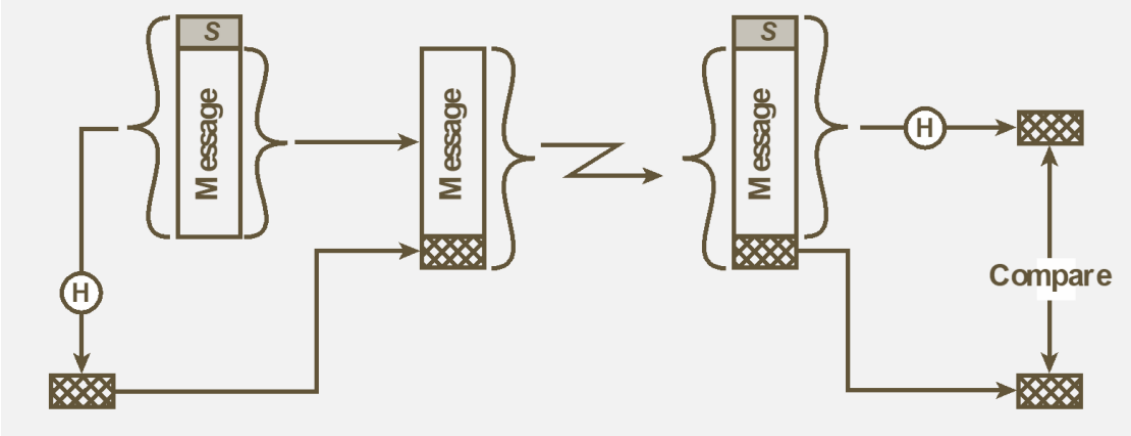
Se debe adjuntar un código de autenticación (Message Authentication Code, MAC) a cada mensaje. Para obtener el MAC se aplica una clave al mensaje.



Autenticación de mensajes: **con una función resumen y cifrado simétrico.**

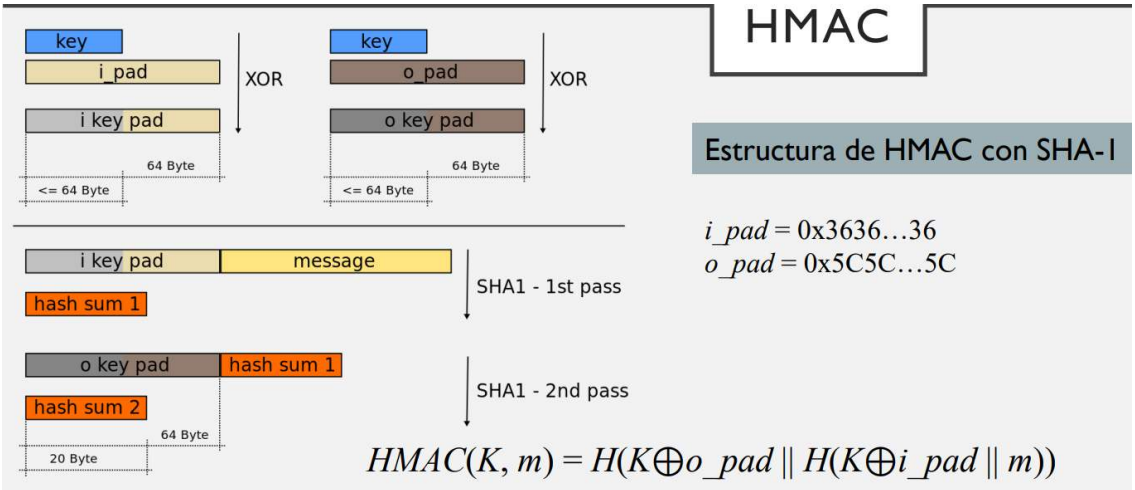


Autenticación de mensajes: **con una función resumen sin cifrado, usando una sal.**

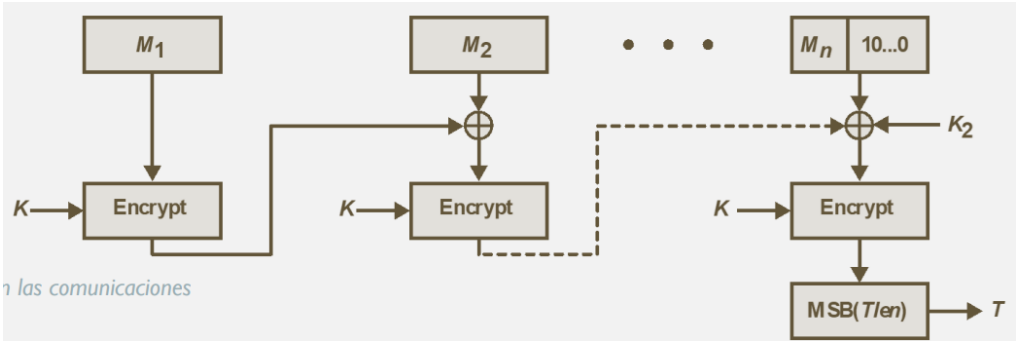


Algoritmos MAC

- **Keyed-Hash MAC (HMAC):** Se buscaba un MAC basado en una función resumen.

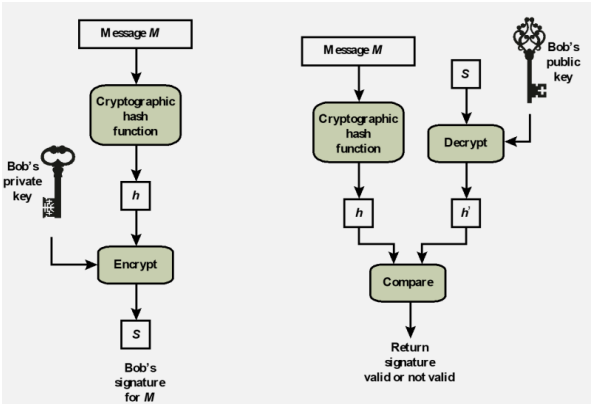


- **Cipher-Based MAC (CMAC):** Usa cifrado de bloque en modo CBC y se queda solo con el último bloque. Genera dos subclaves K1 y K2 a partir de la clave K. Si el tamaño del mensaje es múltiplo del tamaño de bloque, en el último bloque la XOR se hace con K1 sino con K2.

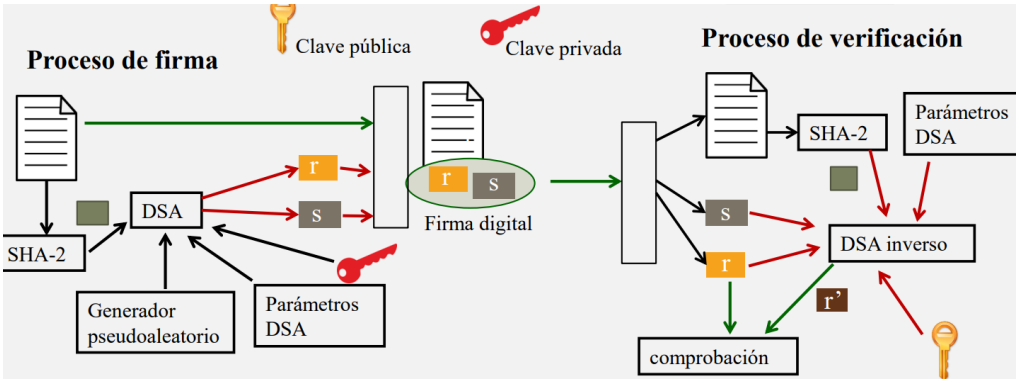


Firma Digital

La firma digital es una función resumen que ha sido cifrada con la clave privada del emisor. Proporciona integridad, autenticación y no repudio.



- **Digital Signature Algorithm (DSA):** Su seguridad se basa, como DH, en la dificultad de calcular logaritmos discretos. Solo proporciona la función de firma digital.



- **ECDSA (Curvas elípticas + DSA):** El par de claves (d,Q) se generan usando curvas elípticas (ver en ECDH).

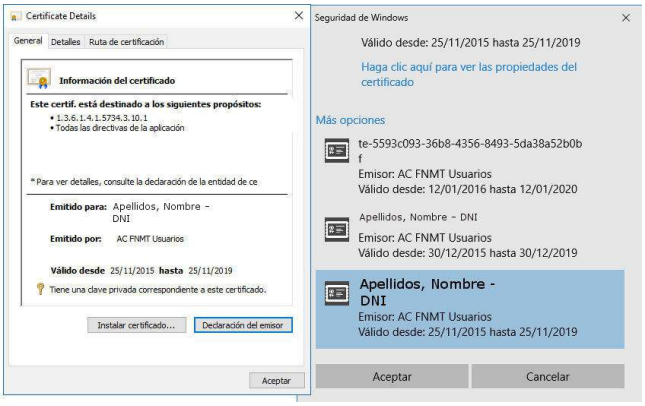
Proceso de firma mensaje *m*
1. Seleccionar nº k aleatorio
2. Calcular $k \cdot G = (x_1, y_1)$
3. Calcular $r = x_1 \bmod n$
4. Calcular $(k^{-1}) \bmod n$
5. Calcular $s = k^{-1} \cdot (H(m) + d \cdot r) \bmod n$
6. La firma del mensaje *m* son los números *r* y *s*

Proceso de verificación
1. Verificar que *r* y *s* están en el rango $[1, n-1]$.
2. Calcular $w = s^{-1} \bmod n$.
3. Calcular $u_1 = H(m) \cdot w \bmod n$.
4. Calcular $u_2 = r \cdot w \bmod n$.
5. Calcular $u_1 P + u_2 Q = (x_0, y_0)$
6. Calcular $v = x_0 \bmod n$
7. La firma se verifica si y solo si $v = r$

Certificados Digitales y Autoridades de certificación

Certificado digital

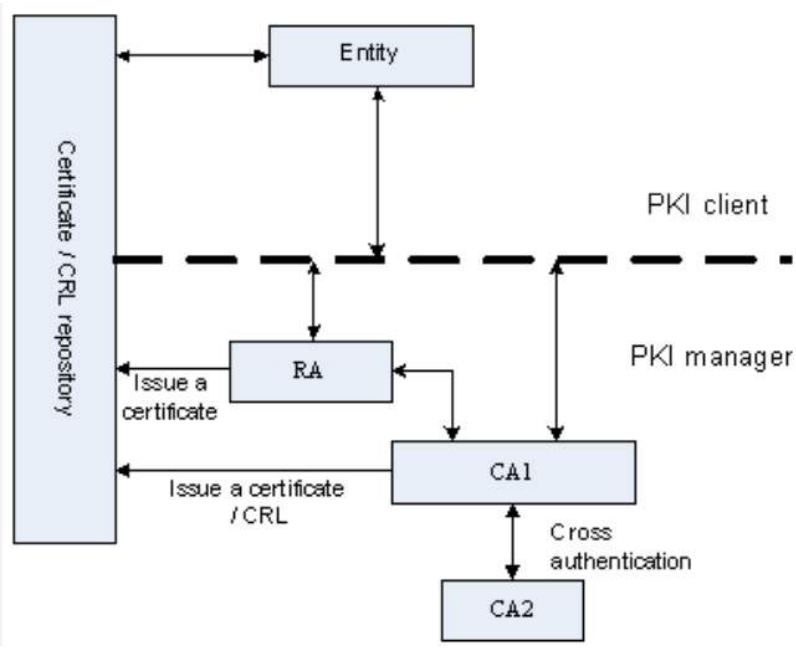
Documento electrónico que usa la **firma digital** de una tercera parte de confianza para **vincular una clave pública con una identidad.** Se usa para verificar que una clave pública pertenece a un individuo, organización o servicio.



Confianza jerárquica: Infraestructura de clave pública PKI

Hay varios certificados raíz (trust anchors) que firman certificados finales o certificados intermedios que pueden a su vez firmar otros. Los certificados se verifican siguiendo la cadena de firmas hacia atrás, hasta que se encuentra un certificado raíz de confianza.
Infraestructura de clave pública o PKI es una infraestructura de gestión de certificados que especifica cómo crear, distribuir, mantener y revocar certificados.

Confianza jerárquica: Arquitectura PKI



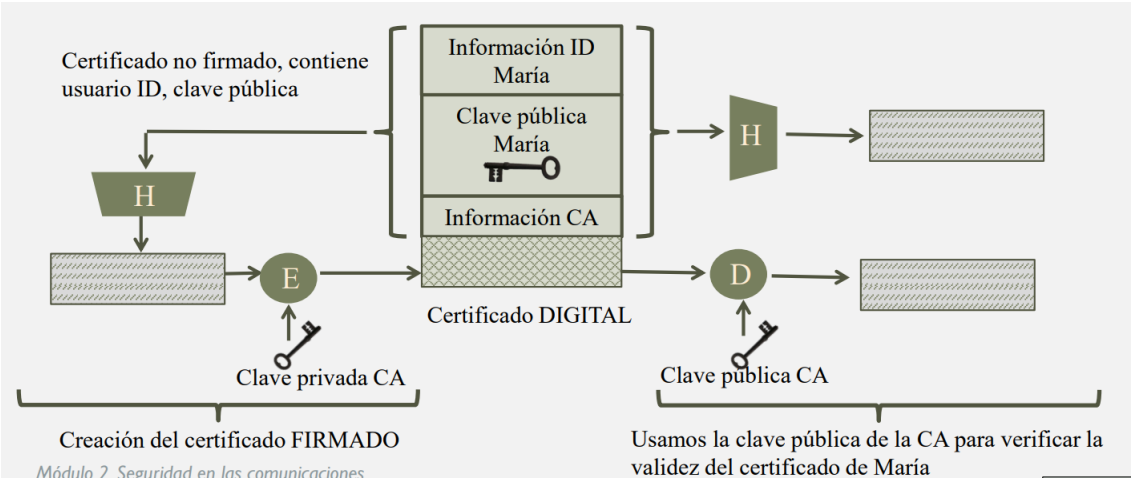
- **La autoridad de certificación (CA, Certificate Authority):** es una organización de confianza que crea, firma, mantiene y revoca certificados digitales. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- **La autoridad de registro (RA, Registration Authority):** es una entidad que identifica de forma inequívoca al solicitante de un certificado. Suministra a la CA los datos verificados del solicitante a fin de que la CA emita el correspondiente certificado.
- **Los repositorios:** son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados.
- **La autoridad de validación (VA, Validation Authority):** es la encargada de comprobar la validez de los certificados digitales.
- **La autoridad de sellado de tiempo (TSA, TimeStamp Authority):** es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- **Los usuarios y entidades finales:** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.

Solicitud de un certificado:

- Usuario solicita certificado a la RA.
- RA verifica la identidad del usuario y solicita la emisión del certificado a la CA.
- La CA crea y firma el certificado y lo envía al usuario.

Creación de certificados:

- Se genera un CSR (Certificate Signing Request): Se genera un par de claves pública y privada.
- Se verifican los datos del solicitante. Directamente la CA o a través de una RA.
- La CA genera el certificado.



Confianza jerárquica: Estructura de un certificado

Formato de un certificado X.509:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After : Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                 OU=Certification Services Division,
                 CN=Thawte Server CA/Email=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                    68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                    85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                    6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                    6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                    29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                    6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                    3a:c2:b5:66:22:12:d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
        a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

Revocación de certificados:
Cada certificado incluye un periodo de validez. Sin embargo, puede ser necesario revocar un certificado antes de que expire debido a las siguientes razones:

- Se cree que la clave privada del usuario ha sido comprometida.
- El usuario ya no está certificado por esta CA.
- Se cree que el certificado de la CA ha sido comprometido.

En una **lista de revocación de certificados (CRL, Certificate Revocation List)** se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

Validación de certificados:

- Localizar la CA que firmó el certificado y validar firmas.
- Verificar fechas y políticas.
- Comprobar si el certificado ha sido revocado. Existen dos posibilidades:
    - Consultar listas de revocación (CRL).
    - Usar el protocolo OCSP (Online Certificate Status Protocol). Más moderno y eficiente.

Estas tareas las puede realizar una autoridad de validación (VA).

Red de confianza (Web of trust) PGP

Se puede confiar en un certificado de forma directa o porque está firmado por otro de confianza (trusted introducer).

Modelo de confianza descentralizado: Hay muchas redes de confianza independientes, y un usuario puede ser parte de varias de ellas y servir de enlace entre ellas.

Características:

- Los certificados son parecidos a los de X.509: Incluyen una auto-firma y pueden tener varias firmas de otros individuos.
- Cualquier usuario puede actuar como autoridad de certificación.
- A puede validar las claves de B, pero cualquier otro usuario no considerará válidas estas claves salvo que un tercer usuario C reconozca a A como fiable.
- **Validez:** Propiedad que certifica que una clave pública pertenece al aparente propietario. Se **recalcula de forma automática** mediante un algoritmo.
- **Confianza:** Es la creencia en la responsabilidad del dueño de una clave a la hora de firmar otras claves. Se basa en la **percepción del dueño del anillo**, que la **asigna manualmente**.

El valor de validez y confianza puede ser: desconocida, ninguna, dudosa, total o absoluta (unknown, none, marginal, full o ultimate).

Anillos:

- **Anillo público:** Almacena las claves públicas de todos los usuarios conocidos.
    - Cuando un usuario incorpora una nueva clave a su anillo le asigna un nivel de confianza.
    - Si la clave es del **propio usuario** tendrá **confianza absoluta.**
    - Cuando un usuario firma una clave del anillo, PGP busca en el anillo al firmante. Si está le asigna una confianza a la firma (sigtrust) igual al valor de confianza del firmante en el anillo sino le asigna el valor de "desconocida".
    - La validez de las claves es recalculada cada cierto tiempo, en base a la confianza de las claves que las firman.
- **Anillo privado:** Contiene la clave pública y privada del usuario.

La **validez** de la clave se calcula a partir de la **confianza en el propietario** de las claves que la firman. Una clave tiene **validez total** si está firmada por suficientes claves válidas, lo que significa que:

- El dueño del anillo la ha firmado con su clave, con **confianza absoluta.**
- O ha sido firmada por **una clave con confianza total.**
- O ha sido firmada por **tres claves con confianza dudosa.**