

## ALGORITMOS SIMETRICOS:

Ventajas:

* Sencillez de implementación
* Robustez
* Velocidad de Cifrado
* Longitud del mensaje

Desventajas:

* La clave debe ser compartida previamente con seguridad
* La comunicación entre multiples actores requiere numerosas claves

## ALGORITMO SIMETRICOS DE BLOQUE:

1. XOR: Conmutativa, Asociativa, Autoinversa:

* 0 y 0 = 0;
* 1 y 1 = 0;
* 0 y 1 = 1;
* 1 y 0 = 1;

1. ECB (Electronic codebook): El mensaje se fracciona en partes y cada parte es cifrada de manera independiente.
2. PADDING O ESQUEMA DE RELLENO: Como los algoritmos simétricos de bloque requieren que los bloques sean iguales, cuando el último bloque es menor se recurre a los métodos Padding para resolver este problema.

* Bit Padding: Opera a nivel Bit, adiciona 1 y todos 0 hasta completar.
* ISO/IEC 7816-4: Opera a nivel Bit, adiciona 80 y todos 0 hasta completar.
* PKCS7 (RFC5652); Opera a nivel Byte, adiciona bytes idénticos cuyo valor es la cantidad de bytes agregados.
* ISO 10126: Opera a nivel Byte, adiciona bytes aleatorios excepto el último que es la cantidad de bytes agregados.
* ANSI X.923: Opera a nivel Byte, adiciona todos 0 excepto el último que es la cantidad de bytes agregados.

1. CBC (Cipher block chaining): El mensaje se fracciona en partes, y se realiza un XOR con el bloque previo antes de cifrar cada parte.
2. CFB (Cipher Feedback): El mensaje se fracciona en partes , se cifra el vector de inicialización y al resultado se le realiza un XOR con el bloque del mensaje. Los bloques posteriores utilizan como entrada el texto cifrado para reemplazar el vector de inicialización.
3. OFB (Output Feedback): Similar a CFB con la diferencia que el bloque a ser utilizado como entrada del siguiente proceso es tomado de la salida del algoritmo justo antes de realizar el XOR.

## FUNCIONES DE HASH

Función o método no reversible para generar un valor que represente de manera casi univoca un dato.

Principales usos

* Soporte para criptografía asimétrica
* Tablas de Hash
* Verificación de integridad

## FUNCIONES DE HASH-MAC (Message Authentication Code):

Adiciona criptografía al proceso de hash para aumentar la seguridad del mismo.

Tipos de implementaciones:

* Basado en cifrados por bloques
* -HMAC
* -Basados en generadores de secuencias

Funciones: MD4, MD5, SHA-1, SHA-2, SHA-3, RIPEMD-160.

## FUNCIONES DE DERIVACION DE CLAVES (KDF)

Son funciones no reversibles que tienen como objetivo generar una o mas claves en base al valor maestro o clave inicial secretos.

## REFERENCIA ARITMETICA MODULAR

Es un sistema aritmético para clases de equivalencia de números enteros llamadas clases de congruencia.

## ALGORITMOS ASIMETRICOS

Este algoritmo nos permite compartir un mensaje cifrado entre dos actores que

no han tenido contacto previo. El sistema de cifrado de clave publica usa un par de claves para el envio de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave publica del destinatario para cifrar el mensaje, y una vez cifrado, solo la clave privada del destinatario podra descifrar este mensaje.

Ventajas:

* No requiere confidencialidad en la distribución de clave
* La misma clave puede ser utilizada por multiples actores en la comunicación.
* Permite autentificar mensajes

Desventajas

* Velocidad de cifrado/descifrado
* Longitud de mensaje limitado
* Tamaño de mensaje cifrado es mayor
* Se requieren claves de gran extensión

Ejemplos: Diffie-Hellman, RSA, DSA, ElGamal, Criptografia de curva elíptica.

## ALGORITMOS ASIMETRICOS-AUTENTIFICACION

Autentificacion de mensajes (firma): Algunos algoritmos asimetricos permiten que se pueda

autenticar un mensaje para garantizar su integridad. En este caso la clave que se emplea para cifrar es la clave privada, justo al reves que para la simple codificacion de mensajes.

## ALGORITMOS ASIMETRICOS – RSA

Se basa en la dificultad para factorizar grandes números.

## ALGORITMOS ASIMETRICOS – ElGamal

Se basa en el problema de logaritmos discretos.

**clave pública (p,y,n) a = p^n (mod n)**

**la clave privada (p,x,n) b = y^k m (mod n)**

## ALGORITMOS ASIMETRICOS – DSA (Digital Signature Algorithm)

Es una parte estándar de la firma digital DSS (digital signature standard). Este algoritmo es una variante del método asimétrico ElGamal.

## ALGORITMOS PUBLICOS Y PRIVADOS

Publicos: son aquellos cuya definicion y funcionamiento se ponen a disposicion publica, permitiendo que cualquier persona o entidad acceda al mismo para su evaluacion o investigacion.

Privados: son aquellos cuyo funcionamiento interno es desconocido; en el ambito de la criptografia estos ultimos son considerados menos confiables.

Nota: Las patentes pueden condicionar el uso de ambos tipos de algoritmos.

## SEGURIDAD POR CAPAS

1. APLICACIÓN
2. TRANSPORTE
3. RED
4. ENLACE
5. FISICA

## HTTP / HTTPS

HTTP: Protocolo para transmisión de información en plano, sin cifrado. Puerto 80 por defecto.

HTTPS (secure): Protocolo para transmisión de información cifrada mediante SSL o TLS. Puerto 443 por defecto.

## SSL (Secure Sockets Layers)

Protocolo que proporciona privacidad e integridad entre 2 aplicaciones. Es independiente del protocolo utilizado. Se sitúa en la capa de aplicación sobre el protocolo TCP, pude proporcionar seguridad a cualquier aplicación que corra sobre TCP, principalmente se usa en HTTP, SMTP, NNTP. En HTTP da lugar a HTTPS.

Fases:

* Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación, a partir del conjunto de algoritmos soportados por cada uno de los interlocutores
* Intercambio de claves, empleando algún mecanismo de clave, y autentificación de los interlocutores a partir de sus certificados digitales.
* Cifrado simétrico del tráfico.

## TLS (Transport Layer Secutiry)

Es una evolución del protocolo SSL. Es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y el servidor.

Una de las ventajas sobre SSL es que puede ser iniciado a partir de conexión TCP ya existente.

Características:

* Uso de funciones MAC en lugar de MDC únicamente.
* Numeración secuencial de todos los campos que componen la comunicación, e incorporación de esta información al calculo de los MAC.
* Protección frente a ataques que intentan forzar el empleo de versiones antiguas –menos seguras- del protocolo o cifrados más débiles.
* El mensaje que finaliza la fase de establecimiento de la conexión icorpora un HASH de todos los datos intercambiados por ambos interlocutores.

## FIRMA ELECTRONICA

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o sociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

## FIRMA DIGITAL

Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Propiedades:

* Va ligada indisolublemente al mensaje
* Solo puede ser generada por su legítimo titular
* Es públicamente verificable

## CERTIFICADO DIGITAL

Documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Campos estándar X.509: CLAVE PRIVADA NO

* Versión.
* Número de serie.
* Identificador del algoritmo empleado para la firma digital.
* Nombre del certificador.
* Periodo de validez.
* Nombre del sujeto.
* Clave pública del sujeto.
* Identificador único del certificador.
* Identificador único del sujeto.
* Extensiones.
* Firma digital de todo lo anterior generada por el certificador.

## PKI – Infraestructura de clave Publica

* Autoridad de certificación
* Autoridad de registro
* Autoridad de validación
* Autoridad de sellado de tiempo
* Los repositorios
* Los usuarios y entidades finales

## LEY DE FIRMA DIGITAL ARGENTINA

**LEY 25.506**