CRIPTOGRAFIA Y AUTENTICACION

Criptografía

Es la ciencia que protege la información mediante técnicas matemáticas que permiten cifrar (ocultar) y descifrar (revelar) datos.

Objetivos

- **Confidencialidad**: Solo las partes autorizadas pueden leer los datos.
- **Integridad**: Garantiza que el mensaje no ha sido alterado.
- **Autenticación**: Verifica la identidad del remitente o receptor.
- **No repudio**: Impide que el emisor niegue haber enviado el mensaje.

Ejemplos

- Funciones hash: generan un resumen único del mensaje (SHA-256, SHA-3).
- Números primos y factorización: base de RSA.
- Logaritmo discreto: base de DSA y ElGamal.
- Curvas elípticas: base de ECC.

Tipos de Criptografía

Asimetrica

- Usa la misma clave para cifrar y descifrar.
- Es rápida, pero requiere que ambas partes compartan la clave de forma segura.
- Ejemplos: AES, DES, 3DES, Blowfish.
- Problema: la distribución de claves es difícil en sistemas grandes.

Simetrica

- Usa dos claves relacionadas matemáticamente:
- Clave pública: se comparte abiertamente.
- Clave privada: se mantiene en secreto.
- Si se cifra con una, solo se puede descifrar con la otra.
- Ejemplos: RSA, ECC, ElGamal.
- Ventajas: facilita autenticación y distribución segura de claves.

Tipos de Claves

- Clave pública: accesible a cualquiera; usada para cifrar o verificar firmas.
- Clave privada: mantenida en secreto; usada para descifrar o firmar.
- Clave de sesión: clave temporal generada para una comunicación concreta (usada en TLS).
- Clave maestra: usada para generar otras claves derivadas o de sesión.

Firmas Digitales

Mecanismo criptográfico que permite verificar la autenticidad y autoría de un mensaje o documento digital.

Funcionamiento

- El emisor genera un hash (resumen) del mensaje.
- Ese hash se cifra con su clave privada.
- El receptor descifra la firma con la clave pública del emisor.
- Si el hash coincide con el suyo propio, la firma es válida.

Garantiza

- Autenticidad → el remitente es quien dice ser.
- Integridad → el mensaje no fue modificado.
- No repudio → el autor no puede negar su participación.

Ejemplos de algoritmos de firma:

- RSA
- DSA
- ECDSA
- EdDSA

Protocolos de Autenticación

Conjunto de reglas que permiten verificar la identidad de usuarios o dispositivos en una red.

Tipos

- Basados en contraseñas: Ej. HTTP Basic, PAP (inseguros).
- Basados en desafío-respuesta: Ej. CHAP (usa hash para verificar identidad sin enviar contraseñas).
- Basados en certificados digitales: Ej. SSL/TLS (usa criptografía asimétrica y firmas).
- Basados en tokens: Ej. OAuth 2.0, OpenID Connect (para aplicaciones web y móviles).
- Kerberos: utiliza tickets cifrados con claves simétricas para autenticar usuarios en redes locales.

Relacion con la criptografia

- Usa claves simétricas/asimétricas para autenticar.
- Usa firmas digitales o certificados para verificar identidades.
- Protege las credenciales durante la transmisión.