sustantiva
CON•SENTIDO

Criptografía Básica para Aplicaciones Web: Fundamentos, Algoritmos y Buenas Prácticas

Introducción

Introducción

- La **criptografía** es esencial para la seguridad de las aplicaciones web.
- **Objetivo:** Garantizar la **confidencialidad, integridad, autenticidad y no repudio** de la información intercambiada entre usuarios y sistemas.
- Aplicada a contraseñas, transacciones y comunicaciones seguras.

¿Qué es la Criptografía?

¿Qué es la Criptografía?

- **Definición:** Ciencia que emplea técnicas matemáticas para proteger la información.

- **Objetivos clave:**
  - **Confidencialidad:** Asegura que solo los usuarios autorizados accedan a los datos.
  - **Integridad:** Garantiza que los datos no sean alterados sin permiso.
  - **Autenticidad:** Verifica la identidad de los interlocutores.
  - **No repudio:** Impide que una parte niegue haber enviado información.

¿Cómo se Usa la Criptografía en la Web?

¿Cómo se Usa la Criptografía en la Web?

- **HTTPS/TLS:** Cifra la comunicación entre cliente y servidor.
- **Almacenamiento de contraseñas:** Utiliza técnicas de **hashing** como **bcrypt.**
- **Cifrado de datos sensibles:** Protege información como tarjetas de crédito o historiales médicos.

Diferencias entre Cifrado y Hashing

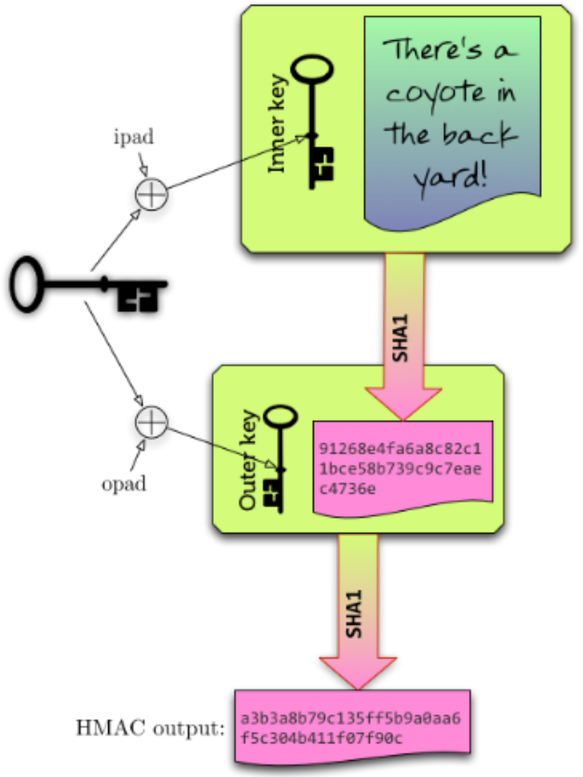
Diferencias entre Cifrado y Hashing

Cifrado	Hashing
Reversible	Irreversible
Protege la confidencialidad	Verifica integridad y autenticidad
Usa una clave	No necesita clave
Ejemplos: AES, RSA	Ejemplos: SHA-256, bcrypt

Buenas Prácticas de Criptografía

Buenas Prácticas de Criptografía

- **Usar algoritmos confiables:**
  - **AES** para cifrado simétrico, **RSA** para cifrado asimétrico.
  - **SHA-256 y bcrypt** para hashing de contraseñas.
- **Proteger las claves:** No almacenar claves en texto claro. Usar gestores de claves.
- **Usar protocolos actualizados:** TLS 1.2 o superior.
- **Realizar auditorías regulares** y mantener actualizados los mecanismos criptográficos.



Tipos de Cifrado

Tipos de Cifrado

- **Cifrado Simétrico (AES)**
  - Usa la misma clave para cifrar y descifrar.
  - Ejemplo: **AES-256** en modos **CBC** o **CTR**.
  - **Ventajas:** Rápido y eficiente.
  - **Desventajas:** Requiere intercambio seguro de claves.

- **Cifrado Asimétrico (RSA)**
  - Usa un par de claves: pública para cifrar, privada para descifrar.
  - Ideal para la autenticación y el intercambio de claves seguras.
  - Más lento que el cifrado simétrico, pero más seguro para compartir claves.

Hashing Seguro para Contraseñas

Hashing Seguro para Contraseñas

- **SHA-256:**
  - Usado para comprobar la integridad de los datos.
  - Rápido, pero vulnerable a ataques de fuerza bruta si se usa solo para contraseñas.

- **bcrypt:**
  - Recomendado para el almacenamiento de contraseñas.
  - Introduce un retraso intencional para dificultar ataques de fuerza bruta.
  - Soporta **salting** (añadir datos aleatorios a las contraseñas).

Conclusión

Conclusión

- La **criptografía** es esencial para la **seguridad de las aplicaciones web.**
- Implementar **cifrado, hashing y protocolos seguros** garantiza la **confidencialidad, integridad, y autenticidad** de los datos.
- Aplicar **buenas prácticas criptográficas** ayuda a proteger contra vulnerabilidades comunes y a fortalecer la seguridad web.


Energiza!