📘 Glosario: Criptografía Básica para Aplicaciones Web

---

1. Criptografía

Disciplina matemática que utiliza algoritmos para cifrar o encriptar información, protegiéndola contra accesos no autorizados y asegurando la confidencialidad, integridad y autenticidad de los datos.

---

2. Cifrado (Encryption)

Proceso de transformar datos legibles en un formato ilegible para evitar que sean leídos por personas no autorizadas. Puede ser **simétrico** (misma clave para cifrar y descifrar) o **asimétrico** (dos claves diferentes).

---

3. Cifrado Simétrico (Symmetric Encryption)

Método de cifrado donde la misma clave es utilizada tanto para cifrar como para descifrar los datos. Ejemplo: **AES** (Advanced Encryption Standard). Es rápido y eficiente, pero requiere un intercambio seguro de claves.

---

4. Cifrado Asimétrico (Asymmetric Encryption)

Método de cifrado que utiliza un **par de claves**: una **clave pública** para cifrar los datos y una **clave privada** para descifrarlos. Ejemplo: **RSA**. Ideal para **autenticación** y establecer **conexiones seguras** (como HTTPS).

---

5. Hashing

Proceso irreversible mediante el cual se genera un valor único (hash) a partir de datos de entrada. No puede deshacerse para recuperar los datos originales, y se utiliza principalmente para almacenar contraseñas de manera segura. Ejemplos: **SHA-256**, **bcrypt**.

---

6. Salting

Técnica que consiste en añadir datos aleatorios (sal) a las contraseñas antes de aplicarles el algoritmo de **hashing**. Esto ayuda a proteger las contraseñas de ataques como el de **rainbow tables**.

---

7. SHA-256 (Secure Hash Algorithm)

Algoritmo de hashing criptográfico que genera un valor hash de 256 bits. Es ampliamente utilizado en aplicaciones de seguridad, como la verificación de la integridad de los datos y el almacenamiento de contraseñas.

---

8. bcrypt

Algoritmo de hashing diseñado específicamente para almacenar contraseñas de manera segura. Introduce un retraso intencional para dificultar los ataques de **fuerza bruta** y permite el uso de **salting** de manera fácil.

---

9. AES (Advanced Encryption Standard)

Estándar de cifrado simétrico utilizado globalmente para asegurar datos en reposo o en tránsito. AES es un algoritmo de **bloques** que cifra y descifra datos de manera rápida y segura utilizando claves de 128, 192 o 256 bits.

---

10. RSA

Algoritmo de cifrado **asimétrico** ampliamente utilizado en **protocolos de seguridad** como **SSL/TLS** para establecer comunicaciones seguras. Utiliza un par de claves: una **pública** (para cifrar) y una **privada** (para descifrar).

---

11. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Protocolos criptográficos que proporcionan seguridad en las comunicaciones por Internet, como en **HTTPS**. Usan cifrado asimétrico para la autenticación y cifrado simétrico para la protección de datos en tránsito.

---

12. HTTPS (HyperText Transfer Protocol Secure)

Versión segura del protocolo HTTP, que utiliza **SSL/TLS** para cifrar la comunicación entre el cliente (navegador) y el servidor, asegurando la privacidad y la integridad de los datos.

---

13. Firma Digital

Técnica de autenticación que permite verificar la **autenticidad** y **la integridad** de un mensaje o documento, utilizando un par de claves **públicas** y **privadas**. Asegura que los datos no han sido alterados y que provienen de una fuente confiable.

---

14. Integridad

Garantía de que los datos no han sido alterados de forma no autorizada durante su almacenamiento o transmisión. La criptografía asegura la integridad mediante la verificación de los datos usando técnicas como **hashing** o **firmas digitales**.

---

15. Confidencialidad

Asegura que la información solo pueda ser leída por las partes autorizadas. El **cifrado** se utiliza para mantener la confidencialidad de los datos sensibles, como contraseñas, tarjetas de crédito y comunicaciones privadas.

---

16. No Repudio

Garantiza que una parte no pueda negar la autenticidad de una transacción. Esto se logra mediante el uso de **firmas digitales**, que permiten demostrar que una acción fue realizada por una persona específica.

---

17. Clave Pública y Clave Privada

En el cifrado **asimétrico**, se utiliza un **par de claves**:

- **Clave pública**: Se utiliza para cifrar datos y se puede compartir con cualquier persona.
- **Clave privada**: Se utiliza para descifrar los datos cifrados con la clave pública. Debe mantenerse secreta.

---

18. Certificado Digital

Un documento electrónico utilizado para verificar la identidad de una entidad y habilitar la comunicación segura en redes. Utiliza **cifrado asimétrico** para garantizar la autenticidad y la integridad de los datos.

---

19. Vulnerabilidad de Fuerza Bruta (Brute Force Attack)

Método de ataque en el que un atacante prueba todas las combinaciones posibles para descifrar una contraseña o clave. **bcrypt** y otros algoritmos de **hashing** con **salting** son efectivos para ralentizar estos ataques.

---

20. Ataque de Man-in-the-Middle (MITM)

Ataque en el que un atacante intercepta la comunicación entre dos partes, con la posibilidad de leer, alterar o falsificar la información. **TLS/SSL** y **HTTPS** protegen las comunicaciones contra este tipo de ataque.
