

PHP

TIPOS DE ENCRYPTACION

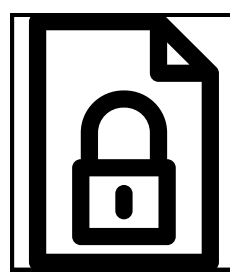
Cada tipo tiene aplicaciones y niveles de seguridad específicos, adecuados para distintas necesidades de protección de datos.

Basada en Hash

- **MD5:**
Produce un hash de 128 bits. Es rápido, pero no se recomienda para aplicaciones críticas debido a vulnerabilidades conocidas.

- **SHA-1:**
Genera un hash de 160 bits. Más seguro que MD5, pero ha sido superado por métodos más fuertes.

- **SHA-256:**
Parte de la familia SHA-2, proporciona un mayor nivel de seguridad con un hash de 256 bits. Muy recomendable para aplicaciones modernas.



ENCRYPTACIÓN ASIMÉTRICA

- **RSA:**
Un método de encriptación de clave pública, donde se utiliza un par de claves (pública y privada). Ideal para transferencias de datos seguras y autenticación.

- **OpenSSL:**
Una herramienta y biblioteca que permite implementar cifrado RSA, AES y otros algoritmos de manera robusta en PHP.

Encriptación Simétrica

- **AES (Advanced Encryption Standard):**
Un estándar de cifrado muy seguro y ampliamente utilizado. Utiliza la misma clave para cifrar y descifrar la información.

- **Mcrypt:**
Una biblioteca antigua para encriptación que soporta varios algoritmos, incluido AES. Aunque útil, ya no se mantiene activamente y se recomienda usar alternativas más actuales como OpenSSL.

