**SHA-256**

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed-size 256-bit (32-byte) hash value from input data of any size. It's widely used in various applications, including data integrity verification, digital signatures, and password hashing.

**Key Features:**

1. **Deterministic**: The same input will always produce the same output.
2. **Fast Computation**: It can compute the hash value quickly for any input.
3. **Pre-image Resistance**: Given a hash value, it should be computationally infeasible to find an input that hashes to that value.
4. **Small Changes in Input Change the Output**: Even a tiny change in the input will produce a significantly different hash value (avalanche effect).
5. **Collision Resistance**: It's difficult to find two different inputs that produce the same hash output.

**Use Cases:**

* **Data Integrity**: Ensuring that data has not been altered during transmission or storage.
* **Digital Signatures**: Verifying the authenticity of a message or document.
* **Password Hashing**: Storing hashed versions of passwords to enhance security.