Report on SHA-256 – The Cryptographic Hash Function

**1. Introduction**

In today’s digital world, the need for secure and reliable data protection methods is more important than ever. From online banking to file sharing, billions of transactions occur every day, and the security of this data is critical.  
One of the most widely used tools for ensuring data integrity and authenticity is hashing — a process of transforming readable data into an unreadable, fixed-size value.

Among various hashing algorithms, SHA-256 (Secure Hash Algorithm – 256 bit) has earned its reputation for security, efficiency, and resistance to attacks.  
This report explains the concept of hashing, details the working of SHA-256, lists its features, applications, and concludes with its importance in modern cryptography.

**Characteristics of hashing:**

* **Irreversible:** Once the data is converted into a hash, it cannot be converted back into the original form.
* **Deterministic:** The same input always produces the same output.
* **Fixed Length:** No matter how large or small the input is, the output size remains constant.
* **Unique Output:** Even a small change in the input results in a drastically different output (known as the avalanche effect). **Applications of Hashing**
* Hashing plays a vital role in many areas of technology and cybersecurity:
* **Password Storage:** User passwords are stored in a hashed format to prevent theft.
* **Data Integrity Verification:** Ensures that files have not been modified during transmission.
* **Blockchain Technology:** Maintains the security and linking of blocks.
* **Digital Signatures:** Verifies the authenticity of digital documents.
* **Network Security:** Used in SSL/TLS protocols for secure communication.
* **Message Authentication Codes:** Ensures messages have not been altered.

**4. Introduction to SHA-256**

* SHA-256 is part of the SHA-2 family of cryptographic hash functions, developed by the National Institute of Standards and Technology (NIST) in collaboration with the National Security Agency (NSA) in 2001.  
  It was designed to replace SHA-1, which had become vulnerable to collision attacks.
* Basic Facts about SHA-256:
* Output Size: 256 bits (32 bytes).
* Block Size: Processes messages in 512-bit chunks.
* Rounds: Performs 64 rounds of computation on each block.
* Security Level: Highly resistant to collision and preimage attacks.
* Common Uses: Blockchain, password hashing, SSL/TLS, and file verification
* 5. Features of SHA-256
* Fixed Digest Size: Output is always 256 bits regardless of input length.
* Collision Resistance: Extremely hard to find two different inputs with the same hash.
* Preimage Resistance: Impossible to find an input that corresponds to a given hash.
* Avalanche Effect: A single bit change in input completely changes the output.
* Uniform Distribution: Outputs are spread evenly across the possible hash values.
* Platform Independence: Works the same way across all platforms and programming languages.
* 6. Steps in the SHA-256 Algorithm
* The SHA-256 algorithm works in several well-defined stages:
* Step 1: Padding the Message
* The message is extended so that its length is 64 bits less than a multiple of 512.
* First, append a 1 bit to the message, followed by enough 0s to reach the required length.
* Step 2: Appending the Message Length
* A 64-bit binary representation of the original message length is added to the end of the padded message.
* Step 3: Initializing Buffers
* Eight 32-bit buffers (H0 to H7) are initialized with fixed hexadecimal values:
* H0 = 6a09e667
* H1 = bb67ae85
* H2 = 3c6ef372
* H3 = a54ff53a
* H4 = 510e527f
* H5 = 9b05688c
* H6 = 1f83d9ab
* H7 = 5be0cd19
* 64 constant words (K0 to K63) are also predefined.
* Step 4: Processing Message Blocks
* The message is divided into 512-bit blocks.
* Each block goes through 64 rounds of operations, including:
* Logical functions (AND, OR, XOR)
* Bitwise rotations and shifts
* Modular additions
* The result from one block is fed into the next block.
* Step 5: Producing the Final Digest
* After the last block is processed, the eight buffers (H0–H7) are concatenated to form the final 256-bit hash.

**Applications of SHA-256**

1. **Blockchain Networks:**
   * Bitcoin uses SHA-256 to link blocks securely and verify transactions.
   * Prevents data alteration by requiring proof-of-work.
2. **Digital Signatures:**
   * Used to generate a digest of a document before signing.
   * Any modification to the document changes the hash, invalidating the signature.
3. **Password Security:**
   * Stores hashed passwords instead of plain text in databases.
   * Even if the database is hacked, the original password cannot be retrieved.
4. **SSL/TLS Handshakes:**
   * Protects the exchange of encryption keys during secure web sessions.
5. **File Integrity Verification:**
   * Checks if downloaded files are exactly the same as the original.
   * Commonly used in software distribution.
6. **Certificate Authentication:**
   * Used in digital certificates for website verification and secure communication.

**9. Advantages of SHA-256**

* Highly secure against modern attacks.
* Fixed-size output simplifies storage.
* Widely adopted and supported.
* Fast and efficient for large-scale use.
* Maintains data integrity over networks.

**Conclusion**

SHA-256 stands as one of the most trusted cryptographic hash algorithms in use today.  
Its irreversibility, collision resistance, and efficiency make it suitable for a wide range of applications — from securing passwords and digital signatures to protecting blockchain networks.

In a world where cyber threats are constantly evolving, SHA-256 offers a robust defense mechanism to ensure that digital data remains authentic, unaltered, and secure.  
Its role in modern technology is indispensable, and it is likely to remain a cornerstone of digital security for years to come.