**How secure is SHA-256?**

SHA-256 is considered a highly secure cryptographic hash function, but its security can be evaluated from several perspectives:

**1. Resistance to Attacks**

* **Pre-image Resistance**: It is computationally infeasible to find an input that hashes to a given output. This makes it difficult for attackers to reverse-engineer the original data from its hash.
* **Second Pre-image Resistance**: Given an input and its hash, it should be hard to find a different input that produces the same hash. This property is crucial for ensuring data integrity.
* **Collision Resistance**: It is exceedingly difficult to find two distinct inputs that produce the same hash output. Theoretical attacks exist (like the birthday paradox), but the computational effort required to find such collisions for SHA-256 remains impractically high.

**2. Computational Strength**

* **Bit Strength**: SHA-256 produces a 256-bit hash, meaning there are 22562^{256}2256 possible hashes. As of current technology, brute-force attacks against SHA-256 are not feasible due to the enormous number of possible combinations.

**3. Cryptanalysis**

* **No Known Vulnerabilities**: As of now, there are no known practical attacks that can break SHA-256. It is not susceptible to the types of attacks that have been found against weaker hash functions (like MD5 and SHA-1).

**4. Adoption and Standards**

* **Widespread Use**: SHA-256 is widely used in various security protocols, including SSL/TLS, digital signatures, blockchain technology (like Bitcoin), and file integrity checks. Its adoption by major organizations and standards (like NIST) adds to its credibility.

**5. Future Considerations**

* **Quantum Computing Threat**: The rise of quantum computing presents a theoretical risk to SHA-256. Quantum algorithms, such as Grover's algorithm, could reduce the effective security level of hash functions. However, quantum computers capable of executing such attacks at scale do not currently exist.