Alejandro Uribe A00227656

Efrain Vazquez Hernandez A01612936

Reflection on the importance and efficiency of the use of hash tables

SHA-256 is a cryptographic hashing algorithm widely used for ensuring data integrity and security. In the context of a domain access monitoring system backed by a hash table, SHA-256 could play a pivotal role in generating hash values for domain names, ensuring that key collisions are minimized. This document examines whether SHA-256 is adequate and sufficient for such purposes, alongside its advantages, disadvantages, alternative uses, and computational complexity.

It is adequate for domain access monitoring when high security and resistance to collisions are priorities. It generates a 256-bit hash value that uniquely represents input data. This property minimizes the chances of collisions , which is essential for a system managing potentially millions of domain entries.

Advantages

1. **Collision Resistance**: Offers strong guarantees against collisions, ensuring that even slight differences in input result in entirely different hash values.
2. **Uniform Distribution**: The algorithm produces well-distributed hash values, reducing clustering in the hash table and improving access efficiency.
3. **Security**: While not necessary for basic domain monitoring, the cryptographic strength of SHA-256 could be beneficial in systems where domain data integrity or security against tampering is critical.

Disadvantages

1. **Computational Cost**: Is computationally intensive compared to non-cryptographic hash functions, which could introduce unnecessary overhead in real-time systems.
2. **Memory Overhead**: Its 256-bit output requires more storage, which could be inefficient for applications handling vast amounts of data where space is a concern.
3. **Overkill for Non-Secure Applications**: For scenarios where collision resistance or cryptographic security is not a primary concern, simpler hash functions are more efficient and practical.

Other Uses of

Beyond hash table key generation, SHA-256 is extensively used in various fields:

- **Data Integrity**: Ensuring that files, messages, or databases remain unaltered by hashing their content and comparing it to a known hash.
- **Cryptocurrency**: Is integral to blockchain technology, where it secures transactions and enables mining.
- **Digital Signatures**: It provides a secure hash for digital certificates, ensuring document authenticity.

Computational Complexity

SHA-256 operates with a computational complexity of O(n), where n is the length of the input message. This is because the algorithm processes data in fixed-size blocks (512 bits) and performs a series of rounds to produce the final hash. While O(n) ensures scalability with input size, the high constant factors associated with its cryptographic operations make it slower than simpler, non-cryptographic alternatives.