CRYPTOGRAPHIC HASHING

ZACHARY LEWIS

WHAT IS CRYPTOGRAPHIC HASHING?

- A cryptographic hash function(CHF) is a hash function designed for better security
- Takes in a message and outputs a numerical string of a fixed-size that appears random

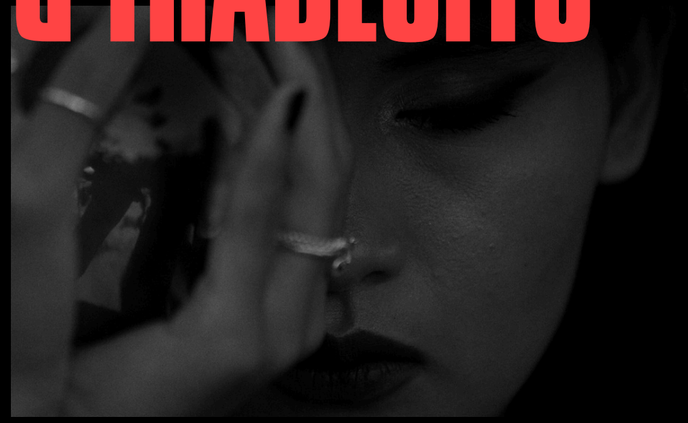
- One way
- The slightest change in the message completely changes output
- Used to verifying file downloads, securing passwords, blockchain mining, digital certificates

HOW IT WORKS

- Input → Compression functions that use modular math and bitwise ops → Fixed-length output

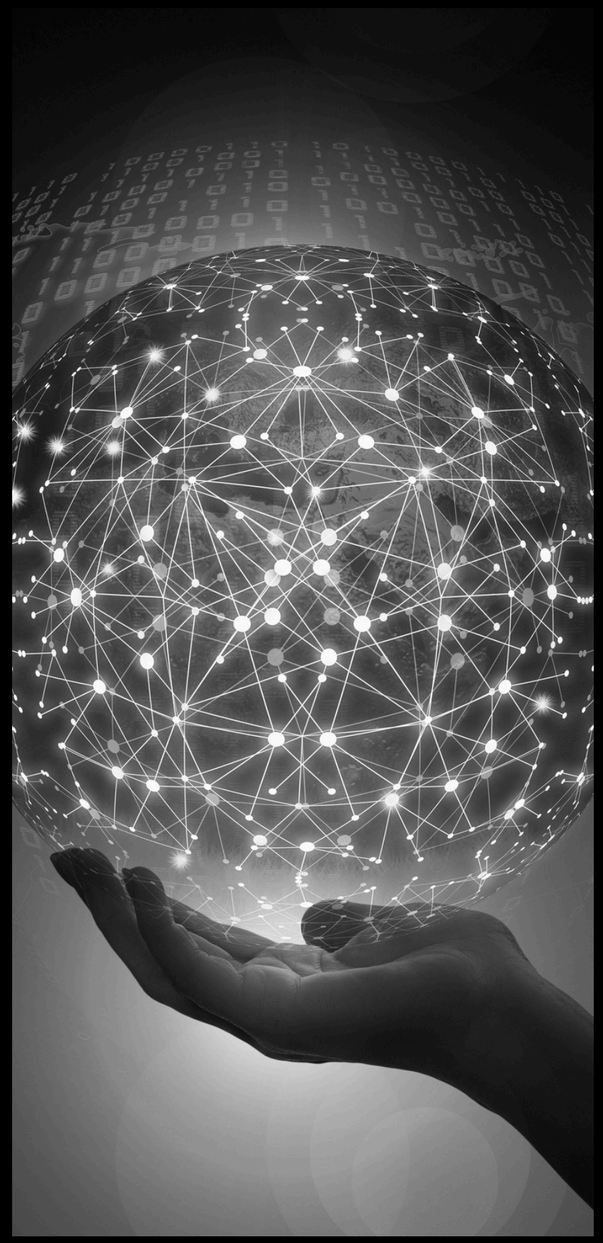
- Popular Algorithms:
  - MD5: Fast, but broken
  - SHA-1: Slightly better, still insecure
  - SHA-256: Currently secure and widely used
  - BLAKE2 / SHA-3: Modern, fast, and secure options

KEY PROPERTIES & TRADEOFFS



- What makes it cryptographic?:
  - Deterministic
  - Fast to compute
  - Pre-image resistance
  - Second pre-image resistance
  - Collision resistance
  - Avalanche effect

- Tradeoffs / Challenges:
  - Performance vs. security
  - Vulnerabilities in older algorithms



USES

- Password storage
- Blockchain
- Data Integrity
- Digital Signatures

THANK YOU!

SOURCES

https://www.fool.com/terms/c/cryptographic-hash-functions/

https://freemanlaw.com/preimage-resistance-second-preimage-resistance-and-collision-resistance/

https://www.amazon.com/Hashtag-Keyboard-Character-Sticker-Decal/dp/B0180BJV10?th=1

https://www.geeksforgeeks.org/cryptography-hash-functions/

https://www.investopedia.com/news/cryptographic-hash-functions/#:~:text=A%20cryptographic%20hash%20function%20is,hash%20functions%20with%20security%20properties.

Chatgpt.com