Computer Security

Reagan Shirk

October 13, 2020

Hash Function Applications

- **Just a recap from last class, not a lot of detail**
- File Authentication
- User Authentication
- Commitment Protocols
- Digital Signatures

Modern Hash Functions

- MD5
  - Not used anymore but still need to learn
  - Broken in 2004, collisions were published
  - Previous versions are too weak to be used for serious applications
  - *One quarter* of widely used content management systems were reported to still use MD5 for password hashing as of 2019 (yikes)
- SHA (Secure Hash Algorithm)
  - Weaknesses were found
- SHA-1
  - Cracked in 2017
  - Collisions in 2^{69} hash operations, much less than the birthday attack of 2^{80} operations *SHA-256, SHA-364...

MD5

- Take a message of arbitrary length, run it through MD5, output a 128-bit digest
- Called a compression function