Cybersecurity

Cryptography Limitations

Cryptography Limitations

- Speed, Size, and Time
  - Too big = too much time to encrypt/decrypt
  - Too small = could be cracked easily
- Weak Keys
  - Easily decrypted
  - Example: WEP
- Longevity
  - How long can a key stay secure?
  - How do we properly dispose of a key?

Cryptography Limitations

- Predictability
  - Is there a pattern?
  - If so, easy for a malicious actor to guess
- Reuse
  - Never reuse keys!
- Entropy
  - Randomness collected by a system for use in algorithms that require random data
  - Without proper randomness, malicious users could crack the key easily

Cryptography Limitations

- Computational Overhead
  - Is the key too strong that a system cannot decrypt
- Resource Constraint
  - What level can your resources maintain?
    - Size and speed
- Security Constraint
  - What level does your company need?
    - What is too small and does not protect the data?