Encryption – taking plaintext and feeding it to an encryption algorithm and getting cipher text back
  • performance heavy
  • Symmetric encryption
    • Can attack the algorithm or attack the key
      • Cryptanalysis
    • Can try to brute force the key

DES – Data encryption standard
  • Most widely used
  • Most studied
  • No weaknesses found yet, but only 56 bit key size (which is a weakness)

Triple DES
  • DES with 3 keys
  • More performance heavy

NIST proposal (1997)
  • Must be as strong as triple DES but overcome the performance issues
  • Key lengths must be variable
  • AES chosen (Advanced Encryption Standard)

Collisions
  • Multiple things mapping to one

Hash Algorithms
  • Want it to be computationally unfeasible to detect collisions
  • Longer keys reduce detectable collisions

Symmetric Encryption (Single-key encryption)
  • Need
    • Strong encryption algorithm
    • A key that has been shared in some fashion
  • Attacks
    • Cryptanalytic
      • Need to know nature of the algorithm
      • Need sample plaintext → ciphertext pairs
    • Brute force
      • On average half of the keys must be tried

Strength of Algorithms measured by how long it takes to crack

Block and Stream ciphers
  • Block
    • More common
    • Can reuse keys
    • Processes the input one block at a time
    • Produces output block for each input block
  • Stream
    • Processes input elements continuously
Message Authentication
  • Want to protect against active attacks

Hash Function Requirements
  • Easy to compute
  • Produce fixed length output
  • One way resistant
  • Impossible to find another message with the same hash code
  • SHA – Most widely used hash algorithm