CS 370 Notes
week 2

What Is Cryptography
- Secret writing
- Historically to protect confidentiality
- Today Secures Info at rest, in transit and during Computation

Cryptography Tools
- Encryption (Confid., Privacy)
  - ↳ AES, and older [3DES, RSA...]
  - ↳ Symmetric
- Hashes (Integrity)
  - ↳ SHA [1, 256, 512...]
- Message Authentication Codes (Integ.)
  - ↳ HMAC-SHA256, AES-CBC-MAC
- Digital Signatures (Many)
  - ↳ RSA, DSS

Kerckhoff's Principle / Shannon's Maxim
→ Assume adversary has access to the algorithm, and not key

Attack Types
- Ciphertext only. find key or P.t.
- Plaintext only: adv has p.t and c.t and are looking for key
- Chosen Plaintext: adversery can generate ciphertext from arbitrary P.t. find key is goal
- Chosen Ciphertext: inverse of c. plaintext finding key is goal.

Encryption
- plaintext → ciphertext
- knowledge of key is needed
- 2 types. Symmetric:
  - → enciphering, deciphering key is the same } $c = E(m, K)$
  - → Historical Method
  - → $m = D(E(m, K)K)$
- Asymmetric:
  - → encrypting and decrypting Party have different, related keys.
  - → Pub, Private keys "PK" "SK" → Key pair (PK, SK)
  - → $M = D(E(m, PK), SK)$

Ciphers (Classical)
- transpositional:
  - → Scramble symbols in message
  - → rail Cipher
- Substitution Cipher
  - → substitute symbols in message
  - → One time Pad, Caesars
- Computationally Secure:
  - → secure given computing resources available

Ciphers (Modern)
- Are all product ciphers (trans + subs)
- stream cipher
  - $E_k(m) = E_K(b_1) E_K(b_2)$
  - $m = b_1 b_2$
- block cipher
  - $m = b_1 b_2 \cdots \quad k = K_1 K_2 \cdots$ } key will or may repeat
  - $E_k(m) = E_{k_1}(b_1) E_{k_2}(b_2) \cdots$