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

- cyphertext 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 cyphertext from arbitrary p.t. find key is goal
- Chosen cyphertext: 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
  - → Historical Method

  $\Big\}\ c=E(m,k)$

  - → $m=D(E(m,K)K)$
- 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

  $E_k(m) = E_k(b_1)E_k(b2)$

  $m=b_1b_2$
- block cipher

  $m=b_1b_2\cdots \quad k=K_1K_2\cdots$

  $E_k(m) = E_{k1}(b_1)E_{k2}(b_2)\cdots$ } key will or may repeat

Encryption Standards

- DES ('till 2001)
  → block cypher
  → 64 bits data + 56bit key
  ↓
  64 bits c.t

- AES
  → block cypher
  → 128 bits data + [128|196|256] bits Key
  ↓
  128 bits c.t.

Avalanche Effect

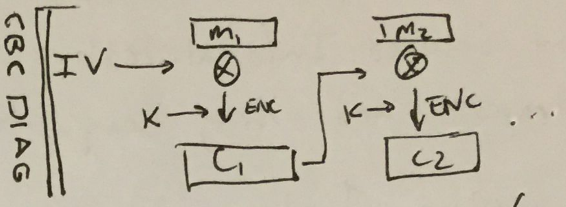
- desireable
- changing one key bit or input causes >50% of cyphertext to change.

Encryption Modes

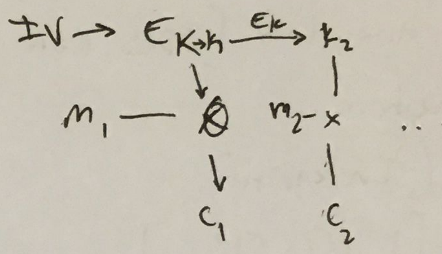
- Electronic Code Book Mode
  → simply break up message into blocks.
  → information patterns are leaked
  → ECB encrypted images will not be "hidden" for sure after encryption
- CBC (cypher Block chaning)
  → $C_i = E_K(M_i \otimes C_{i-1})$
  → $C_0 = E_K(m_0 \otimes$ ~~key~~ IV$)$ → Init Vector

Self Healing Property

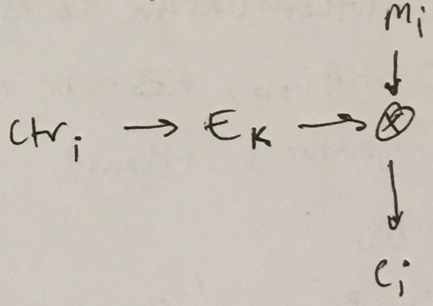
- If cyphertext is altered, the error propagates for at most 2 messages/blocks



Output Feedback Mode (OFB)



Counter Mode


mi
ctri
EK
ci