Crypto: Symmetric-Key Cryptography

Slides credit: Dan Boneh, David Wagner, Doug Tygar

Overview

- Cryptography: secure communication over insecure communication channels
- Three goals
  - Confidentiality
  - Integrity
  - Authenticity

Brief History of Crypto

- 2,000 years ago
  - Caesar Cypher: shifting each letter forward by a fixed amount
  - Encode and decode by hand
- During World War I/II
  - Mechanical era: a mechanical device for encrypting messages
- After World War II
  - Modern cryptography: rely on mathematics and electronic computers

Modern Cryptography

- Symmetric-key cryptography
  - The same secret key is used by both endpoints of a communication
- Public-key cryptography
  - Two endpoints use different keys

Attacks to Cryptography

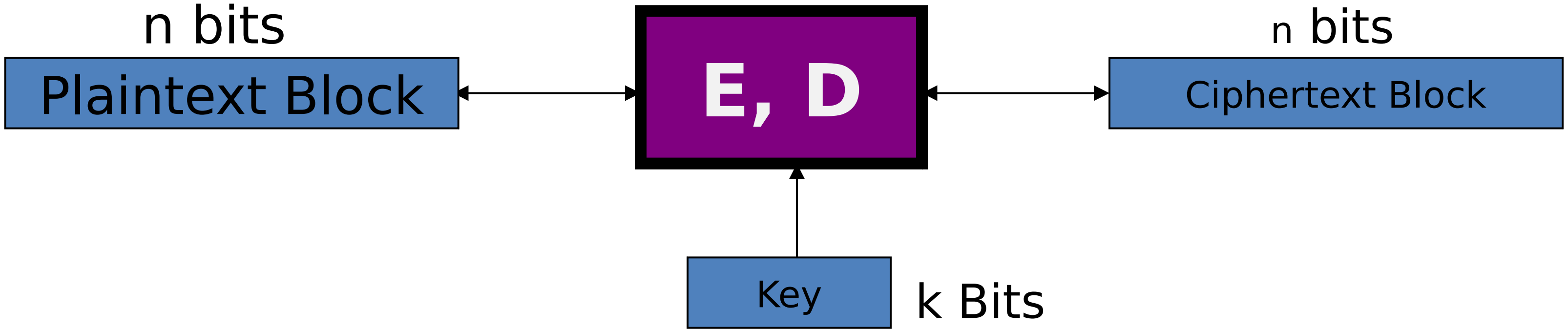
- Ciphertext only
  - Adversary has $E(m_1)$, $E(m_2)$, …
- Known plaintext
  - Adversary has $E(m_1)\&m_1$, $E(m_2)\&m_2$, …
- Chosen plaintext
  - Adversary picks m_1, m_2, … (potentially adaptively)
  - Adversary sees $E(m_1)$, $E(m_2)$, …
- Chosen ciphertext
  - Adversary picks $E(m_1)$, $E(m_2)$, … (potentially adaptively)
  - Adversary sees m_1, m_2, …

One-time Pad

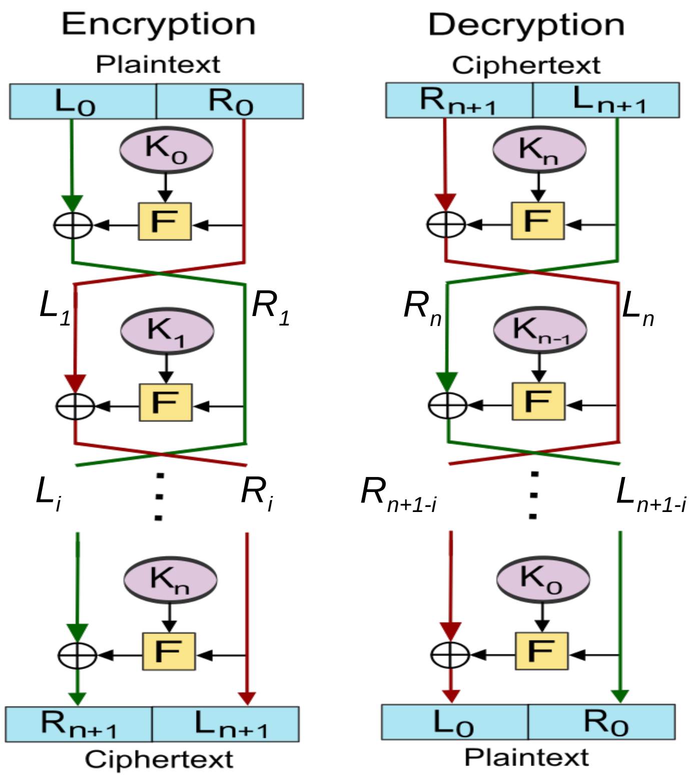
- K: random n-bit key
- P: n-bit message (plaintext)
- C: n-bit ciphertext
- Encryption: C = P xor K
- Decryption: P = C xor K
- A key can only be used once
- Impractical!

Block Cipher

- Encrypt/Decrypt messages in fixed size blocks using the same secret key
  - k-bit secret key
  - n-bit plaintext/ciphertext



Feistel cipher



Encryption

Start with (L_0, R_0)

$L_{i+1}=R_i$

$R_{i+1}=L_i \text{ xor } F(R_i,K_i)$

Decryption

Start with (R_{n+1}, L_{n+1})

$R_i=L_{i+1}$

$L_i=R_{i+1} \text{ xor } F(L_{i+1},K_i)$

DES - Data Encryption Standard (1977)

- Feistel cipher
- Works on 64 bit block with 56 bit keys
- Developed by IBM (Lucifer) improved by NSA
- Brute force attack feasible in 1997

AES – Advanced Encryption Standard (1997)

- Rijndael cipher
  - Joan Daemen & Vincent Rijmen
- Block size 128 bits
- Key can be 128, 192, or 256 bits

Abstract Block Ciphers: PRPs and PRFs

PRF: $F: K \times X \rightarrow Y$ such that:

exists "efficient" algorithm to eval. F(k,x)

PRP: $E: K \times X \rightarrow X$ such that:

1. Exists "efficient" algorithm to eval. E(k,x)
2. The func $E(k, \cdot)$ is one-to-one
3. Exists "efficient" algorithm for inverse D(k,x)

A block cipher is a PRP

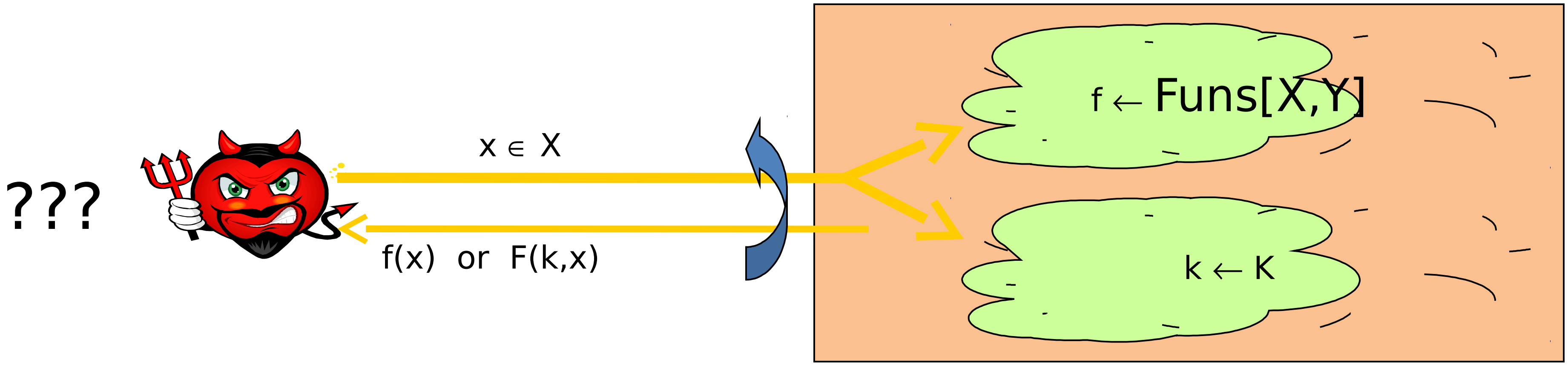
Secure PRF and Secure PRP

- A **PRF** $F: K \times X \rightarrow Y$ is secure if

  $F(k, \cdot)$ is indistinguishable from a random func. $f: X \rightarrow Y$

- A **PRP** $E: K \times X \rightarrow X$ is secure if

  $E(k, \cdot)$ is indisting. from a random perm. $\pi: X \rightarrow X$



Modes of Operation

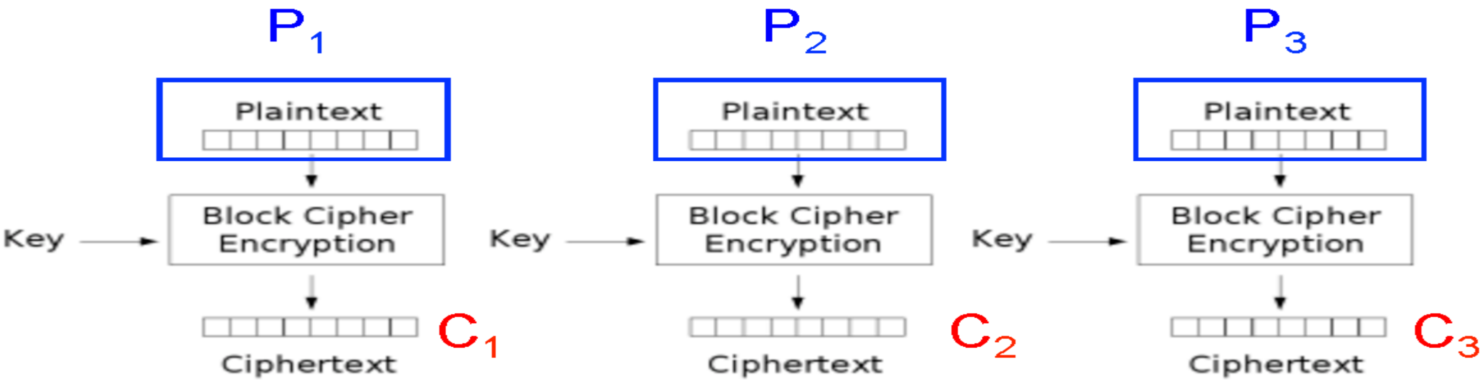
- Block ciphers encrypt fixed size blocks
  - eg. DES encrypts 64-bit blocks with 56-bit key
- Need to en/decrypt arbitrary amounts of data
- NIST SP 800-38A defines 5 modes
- **Block** and **stream** modes
- Cover a wide variety of applications
- Can be used with any block cipher

Electronic Code Book (ECB)

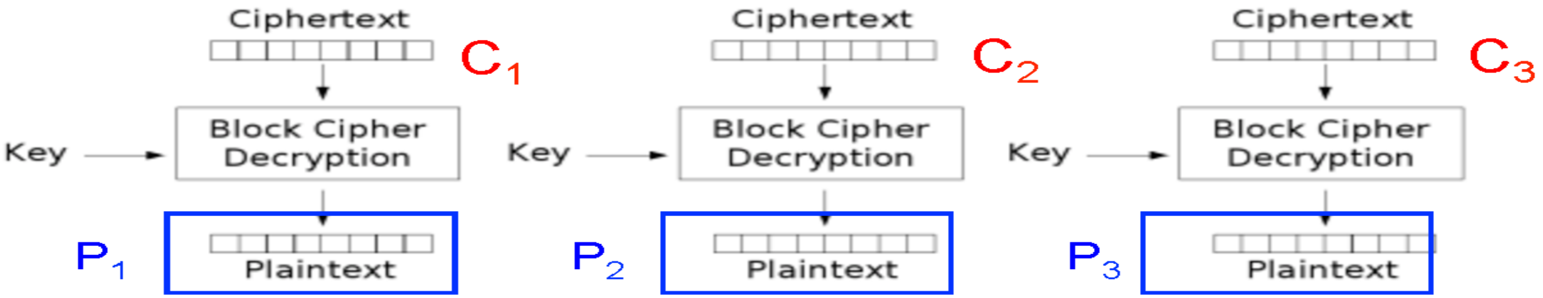
- Message is broken into independent blocks which are encrypted
- Each block is a value which is substituted, like a codebook
- Each block is encoded independently of the other blocks

$$C_i = E_K(P_i)$$

- Uses: secure transmission of single values



Electronic Codebook (ECB) mode encryption

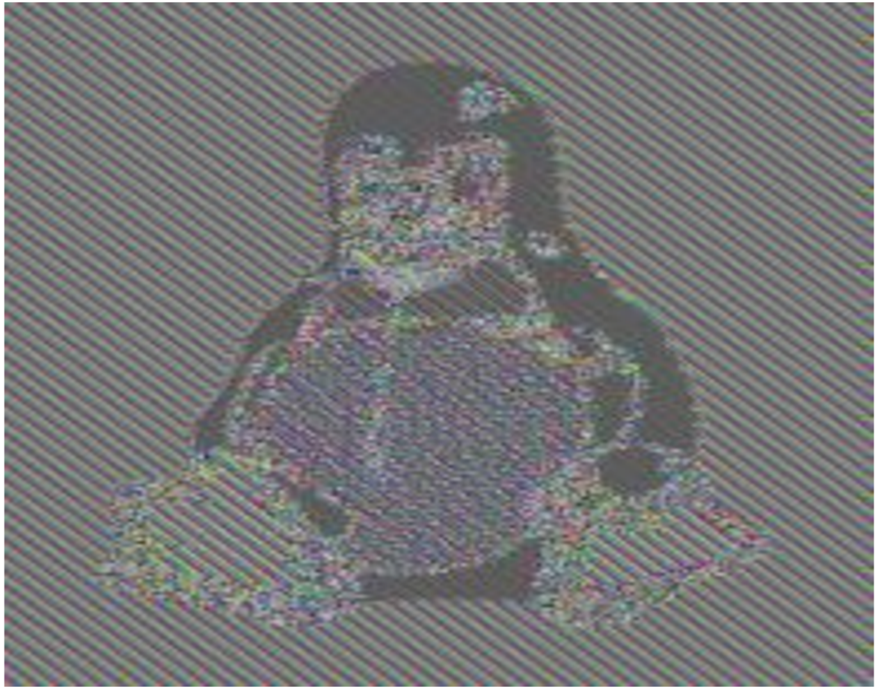


Electronic Codebook (ECB) mode decryption

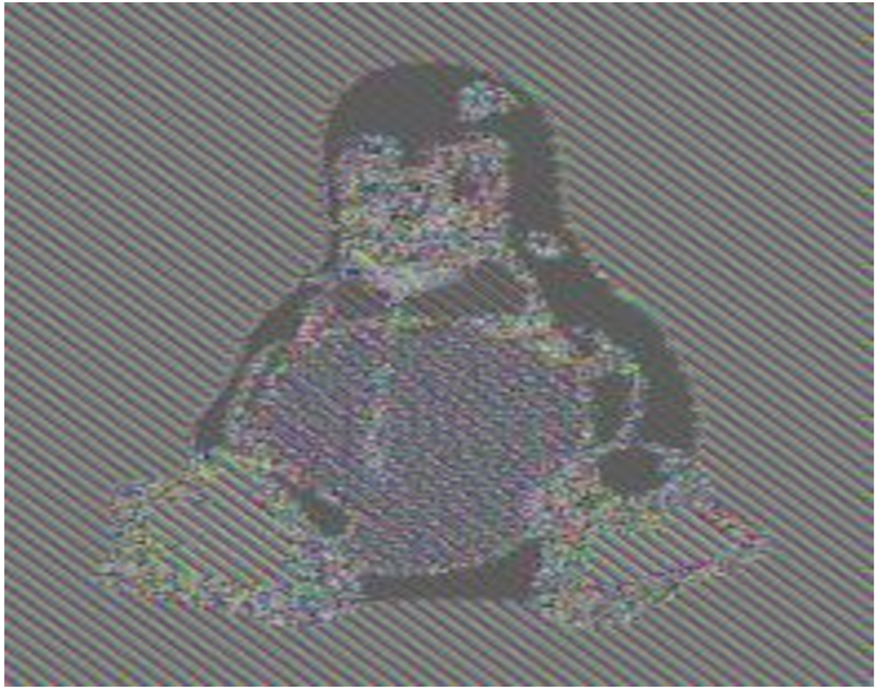
Advantages and Limitations of ECB

- Message repetitions may show in ciphertext
  - If aligned with message block
  - Particularly with data such graphics
  - Or with messages that change very little
- Encrypted message blocks independent
- Not recommended

Original image

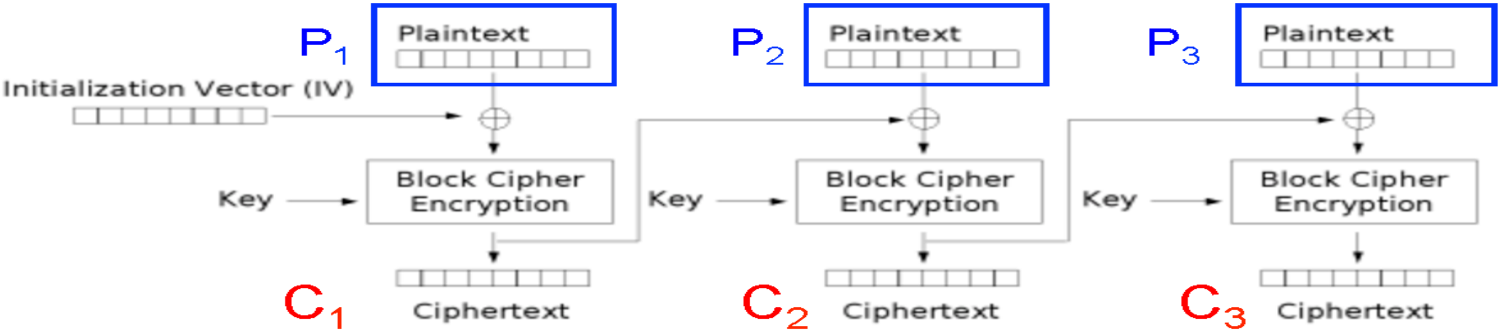


Encrypted with ECB



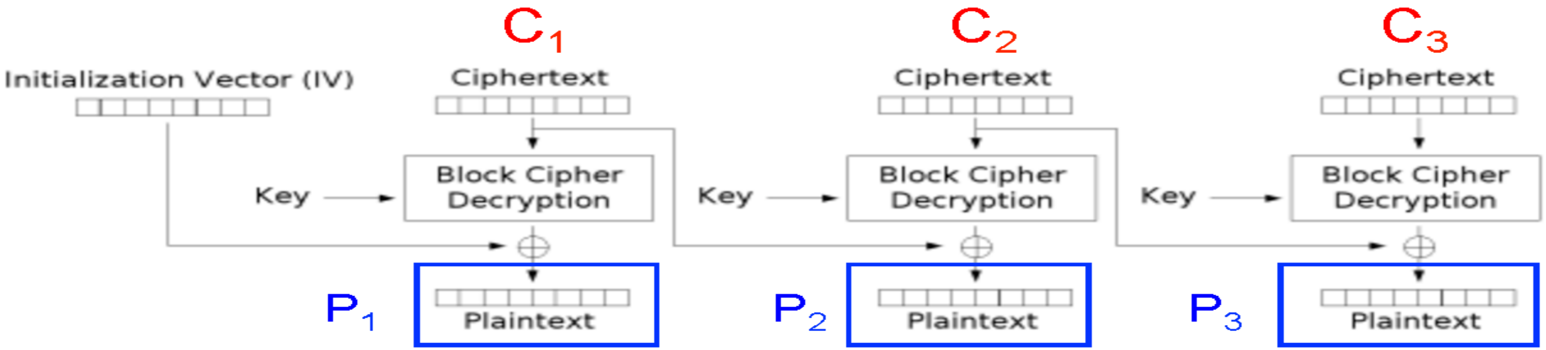
Later (identical) message again encrypted with ECB

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

Dawn



Cipher Block Chaining (CBC) mode decryption

Dawn

Advantages and Limitations of CBC

- Ciphertext block depends on **all** blocks before it
- Change to a block affects all following blocks
- Need **Initialization Vector** (IV)
  - Random numbers
  - Must be known to sender & receiver

Original image

Encrypted with CBC

Stream Modes of Operation

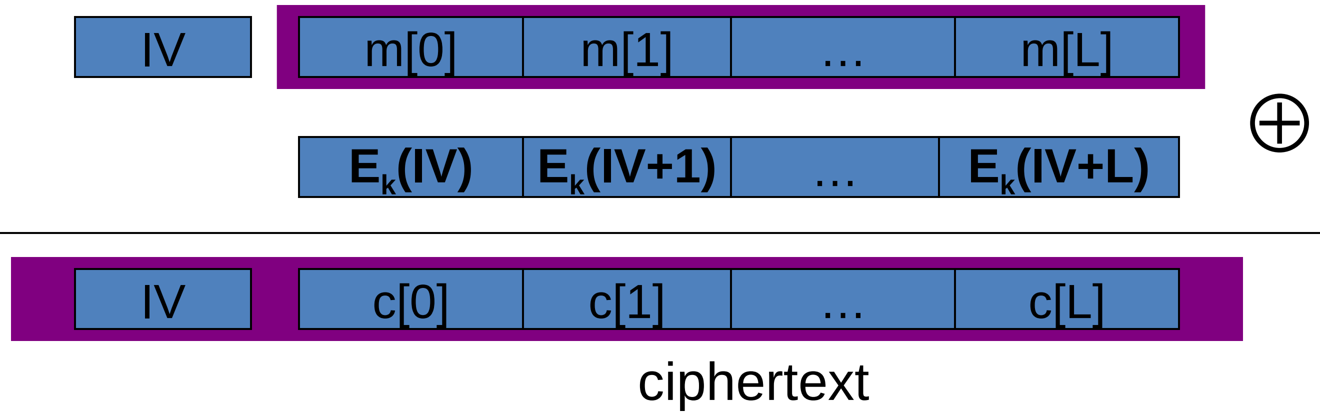
- Block modes encrypt entire block
- May need to operate on smaller units
  - Real time data
- Convert block cipher into stream cipher
  - Counter (CTR) mode
- Use block cipher as PRNG (Pseudo Random Number Generator)

Counter (CTR)

- Encrypts counter value
- Need a different key & counter value for every plaintext block
  - $O_i = E_K(IV+i)$
  - $C_i = P_i \text{ xor } O_i$
- Uses: high-speed network encryption

Counter (CTR)

Counter mode with a random IV: (parallel encryption)



Advantages and Limitations of CTR

- Efficiency
  - Can do parallel encryptions in h/w or s/w
  - Can preprocess in advance of need
  - Good for bursty high speed links
- Random access to encrypted data blocks
- Must ensure never reuse key/counter values, otherwise could break