Intro to IT Security

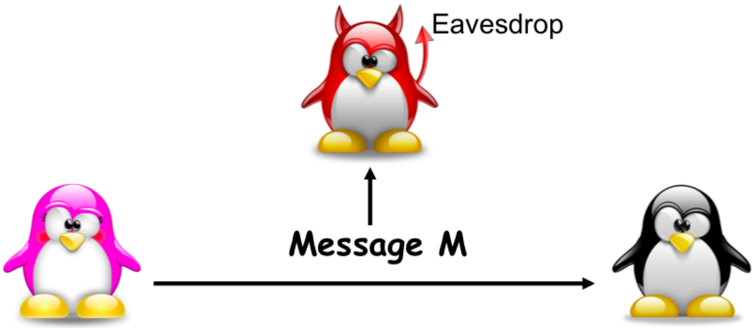
CS306C—Fall 2022

Prof. Antonio R. Nicolosi

Antonio.Nicolosi@stevens.edu

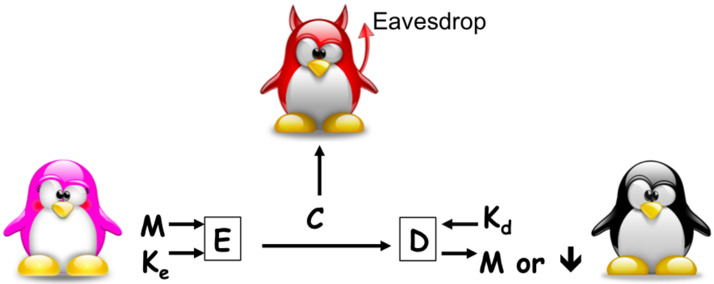
Symmetric Setting

Crypto Requirements: Data Secrecy



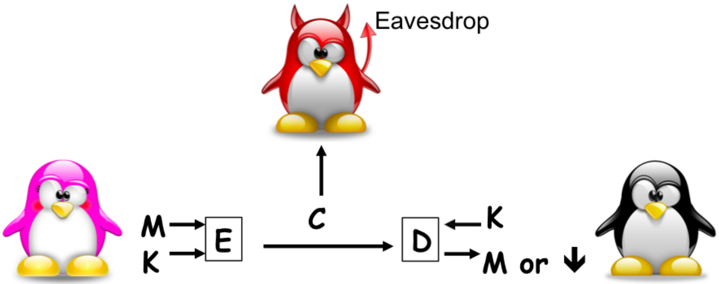
- Protect against unauthorized disclosure of the msg
  - If **A** sends a msg to **B**, no one else should understand its content

Achieving Data Secrecy: Encryption



- Notation
  - **M**: msg or plaintext
  - **C**: encrypted msg or ciphertext
  - **E**: encryption algorithm
  - **D**: decryption algorithm
  - K_e: encryption key
  - K_d: decryption key

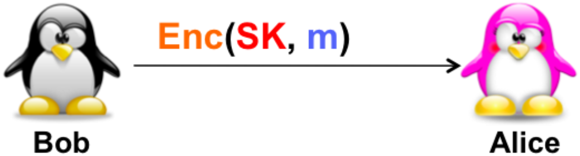
Symmetric Encryption



- **A** and **B** share the same secret information
  - $K = K_e = K_d$: secret

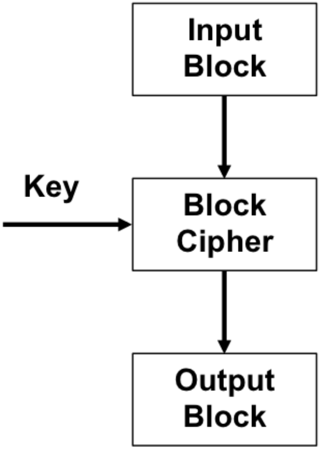
Symmetric Encryption

- Defined by three algorithm:
  - Gen(λ) → (SK) outputs secret key SK
  - Enc(SK, m) → c encrypt m using secret key SK
  - Dec(SK, c) → m decrypt c using SK



Towards Encryption: Block Ciphers

- Most practical symmetric encryption schemes based on a building block called *block cipher*



Block Ciphers

- Ideal Cipher: for each key, get *independent, random* permutation
  - This is impossible!
- A good block cipher yields a (pseudo)-random permutation starting with a *random* key

Permutations

- A function $f : \{0,1\}^\ell \to \{0,1\}^\ell$ is a permutation if there is an inverse function $f^{-1} : \{0,1\}^\ell \to \{0,1\}^\ell$ satisfying

$$\forall x \in \{0,1\}^\ell : f^{-1}(f(x)) = x$$

- This means f must be *one-to-one* and *onto*
  - For every $y \in \{0,1\}^\ell$ there is a unique $x \in \{0,1\}^\ell$ such that $f(x) = y$.

Permutations: Example

- $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $QR_{11} \subset Z_{11} := \{1, 3, 4, 5, 9\}$
- $f : QR_{11} \rightarrow QR_{11}$
- $f(x) = x^2 \mod 11, \quad x \in QR_{11}$
  - $1^2 \mod 11 = 1$
  - $3^2 \mod 11 = 9$
  - $4^2 \mod 11 = 5$
  - $5^2 \mod 11 = 3$
  - $9^2 \mod 11 = 4$
- $f^{-1}(x) = x^3 \mod 11, \quad x \in QR_{11}$
  - $1^3 \mod 11 = 1$
  - $3^3 \mod 11 = 5$
  - $4^3 \mod 11 = 9$
  - $5^3 \mod 11 = 4$
  - $9^3 \mod 11 = 3$

Permutations: Example

- $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $QR_{11} \subset Z_{11} := \{1, 3, 4, 5, 9\}$
- $f : QR_{11} \to QR_{11}$
- $f(x) = x^2 \mod 11, \quad x \in QR_{11}$
  - $1^2 \mod 11 = 1$
  - $3^2 \mod 11 = 9$
  - $4^2 \mod 11 = 5$
  - $5^2 \mod 11 = 3$
  - $9^2 \mod 11 = 4$
- $f^{-1}(x) = x^3 \mod 11, \quad x \in QR_{11}$
  - $1^3 \mod 11 = 1$
  - $3^3 \mod 11 = 5$
  - $4^3 \mod 11 = 9$
  - $5^3 \mod 11 = 4$
  - $9^3 \mod 11 = 3$

Block Ciphers

- Operate on blocks of plaintext of a certain size
- Produces outputs of the same length
- Output block should look like the result of a random permutation
- Not impossible to break—just very expensive
  - Can be broken using brute-force attacks

Block Ciphers

- $B : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$
- For a key K and input block x, output block is $B(K,x)$
- For each key K, denote $B_K : \{0,1\}^\ell \to \{0,1\}^\ell$ the function $B_K(x) = B(K,x)$.
- Syntactic Properties
  1. $B_K : \{0,1\}^\ell \to \{0,1\}^\ell$ is a permutation for every K , meaning B_k has an inverse B_K^{-1}
  2. B, B^{-1} are efficiently computable, where
  $$B^{-1}(K,x) = B_K^{-1}(x)$$
- Security Property
  1. If key is random, then $B_K(x_0)$ and $B_K(x_1)$ look independent, for any $x_0 \neq x_1$

Block Ciphers: A Broken Example

- Let $\ell = k$ and define $B : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ by

$$B_K(x) = B(K, x) = K \oplus x$$

- Then B_k has inverse B_k^{-1} where

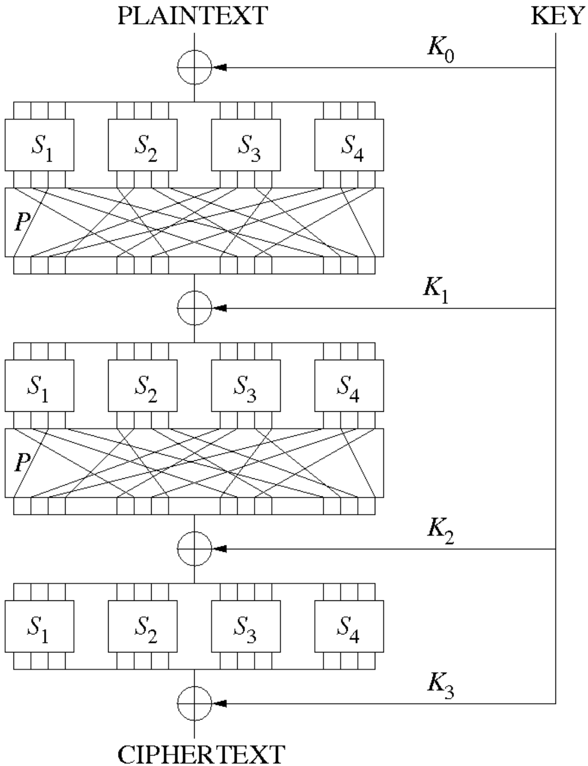
$$B_K^{-1}(y) = K \oplus y$$

- Does not satisfy the security property
  - $y_0 = B_k(x_0) = K \oplus x_0$
  - $y_1 = B_k(x_1) = K \oplus x_1$
  - $y_0 \oplus y_1 = x_0 \oplus x_1$
  - $y_0 = y_1 \oplus (x_0 \oplus x_1)$

Structure of a Typical Block Ciphers

- Block ciphers are usually comprised of a network of substitutions and permutations
- The network is then iterated through many rounds

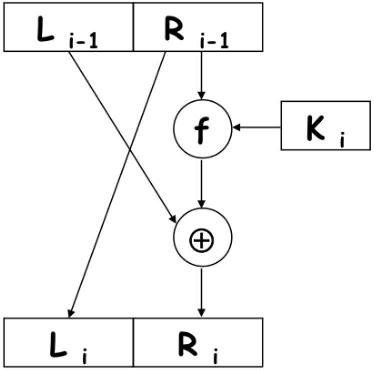
A Substitution-Permutation Network



Data Encryption Standard (DES)

- 1972 - NBS (now NIST) asked for a block cipher for standardization
- 1974 - IBM designs Lucifer
  - Lucifer eventually evolved into DES
- Widely adopted as a standard including by ANSI and American Bankers association
  - Used in ATM machines
- Based on Feistel Structure
  - 56-bit key; 64-bit input/output block + 8 bits for parity checks
  - After 3 rounds, output block indistinguishable from a random permutation (Luby-Rackoff)

Feistel Round

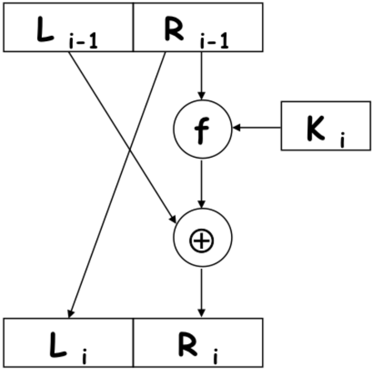


$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f_{k_i}(R_{i-1})$$

Therefore:

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus f_{k_i}(L_i)$$

Feistel Round

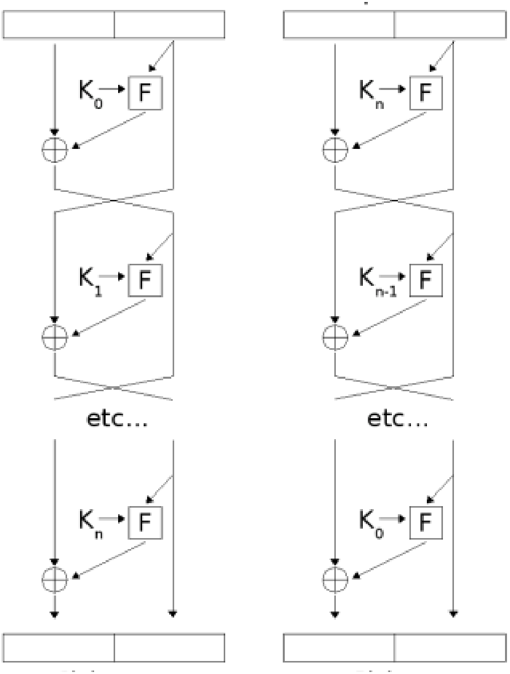


$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f_{k_i}(R_{i-1})$$

Therefore:

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus f_{k_i}(L_i)$$

Feistel Structure



Concerns about DES

- Short key length
  - Can be broken in days
  - Computation can be distributed to make it faster
- Short block length
  - Repeated blocks happen too frequently
- Some theoretical attacks have been found
- Non-public design process

Triple DES (3DES)

- Expand the key length
  - $K = (K_1, K_2), |K| = 112$ bits
- $E_{K_1,K_2}(x) = DES_{K_1}(DES^{-1}_{K_2}(DES_{K_1}(x)))$
- Fairly slow, but widely used in practice

Advanced Encryption Standard (AES)

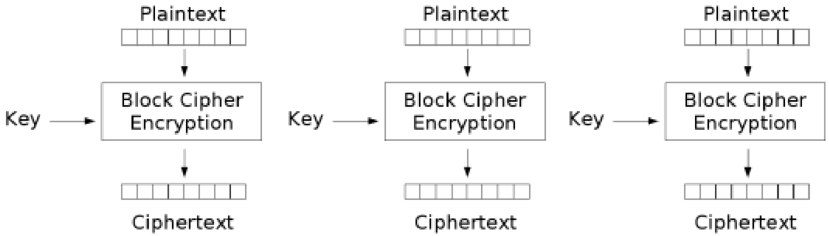
- 1998: NIST announces competition for a new block cipher
- 2001: NIST selects the Rijndael
  - 128-bit key
  - 128-bit input/output block
  - Faster than DES in software

Block Ciphers and Modes of Operations

- To encrypt m, split m in blocks $m_1, \ldots, m_n$, where each block m_i has length ℓ, and process each block with a block cipher.
- How should the processing proceed?
  - Different Modes of Operations!

Electronic Code Book (ECB) Mode—(Broken!)

- $Enc_K(m_i)$:
  - $c_i = B_K(m_i), \forall i = 1, \ldots, n$
  - output $c_1, \ldots, c_n$

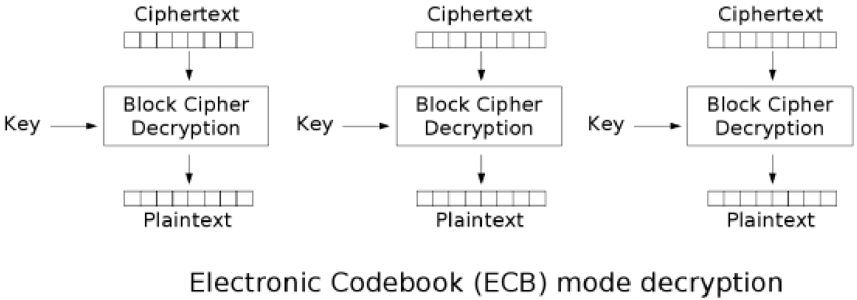


Electronic Codebook (ECB) mode encryption

Pictures from Wikipedia entry on "Modes of Operation"

Electronic Code Book (ECB) Mode—(Broken!) (cont'd)

- $Dec_K(c)$:
  - $m_i = B_K^{-1}(c_i), \forall i = 1, \ldots, n$



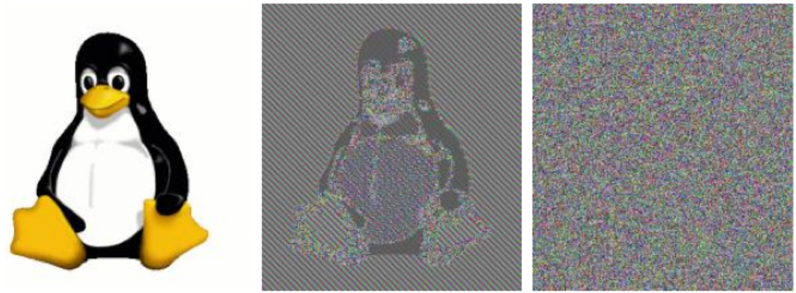
Pictures from Wikipedia entry on "Modes of Operation"

Electronic Code Book (ECB) Mode—(Broken!) (cont'd)

- Deterministic: therefore not CPA-secure
- Not even indistinguishable against eavesdroppers
  - A given input block maps always to same output block
- No Integrity
  - Can mix blocks
- Completely broken: Should never be used!

Electronic Code Book (ECB) Mode—(Broken!) (cont’d)

- Completely broken: Should never be used!

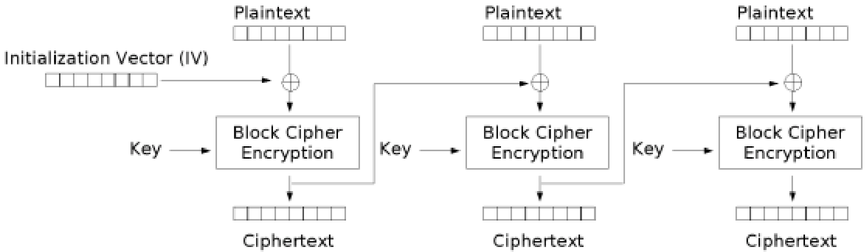


Original *Encrypted using ECB mode* *Encrypted using other modes*

Pictures from Wikipedia entry on "Modes of Operation"

Cipher Block Chaining (CBC) Mode

- Select random IV; Set $c_0 = IV$
- $Enc_K(m_i)$:
  - $c_i = B_K(c_{i-1} \oplus m_i), \forall i = 1, \ldots, n$
  - Output $(c_0, c_1, \ldots, c_n)$

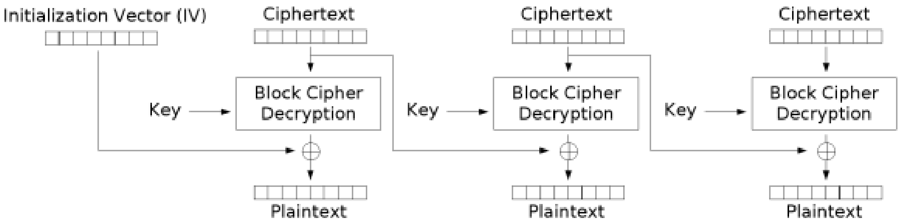


Cipher Block Chaining (CBC) mode encryption

Pictures from Wikipedia entry on "Modes of Operation"

Cipher Block Chaining (CBC) Mode (cont'd)

- $Dec_K(c)$:
  - $m_i = B_K^{-1}(c_i) \oplus c_{i-1}, \forall i = 1, \ldots, n$



Cipher Block Chaining (CBC) mode decryption

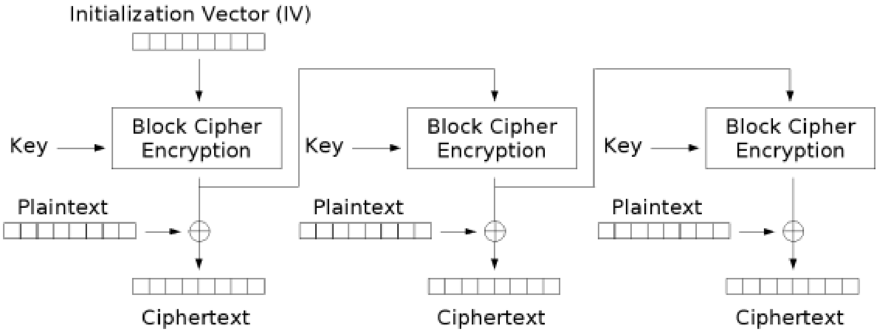
Pictures from Wikipedia entry on "Modes of Operation"

Cipher Block Chaining (CBC) Mode (cont'd)

- Randomized (IV)
- If B_K is a good block cipher, then CPA-secure
- Encryption cannot be parallelized
- No Integrity
  - Can append extra block at the end

Output Feedback (OFB) Mode

- Select random IV; Set $c_0 = r_0 = IV$
- $Enc_K(m_i)$:
  - $r_i = B_K(r_{i-1})$
  - $c_i = r_i \oplus m_i, \forall i = 1, \ldots, n$
  - Output $(c_0, c_1, \ldots, c_n)$

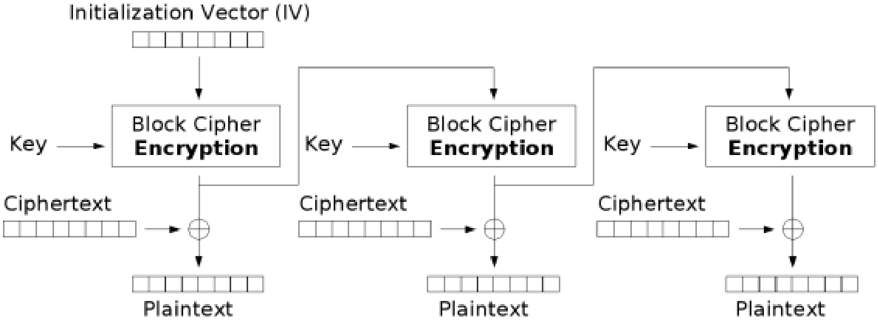


Output Feedback (OFB) mode encryption

Pictures from Wikipedia entry on "Modes of Operation"

Output Feedback (OFB) Mode (cont'd)

- $Dec_K(c)$:
  - $r_0 = IV$
  - $r_i = B_K(r_{i-1})$
  - $m_i = r_i \oplus c_i, \forall i = 1, \ldots, n$



Output Feedback (OFB) mode decryption

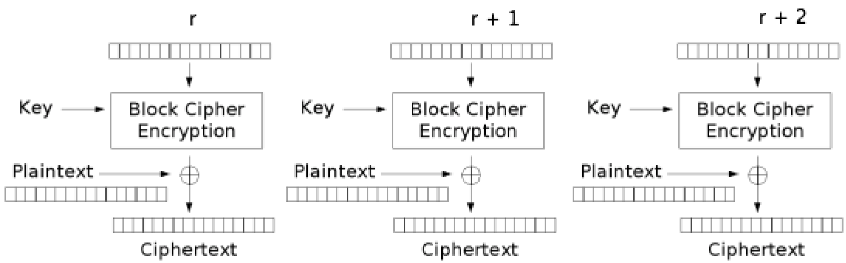
Pictures from Wikipedia entry on "Modes of Operation"

Output Feedback (OFB) Mode (cont'd)

- Randomized
- If B_K is a good block cipher, then CPA-secure
- Neither encryption nor decryption can be parallelized

Random Counter (R-CTR) Mode

- Select random r. Set $c_0 = r$
- $Enc_K(m_i)$:
  - $c_i = B_K(r + i) \oplus m_i, \forall i = 1, ..., n$
  - output $(c_0, c_1, ..., c_n)$

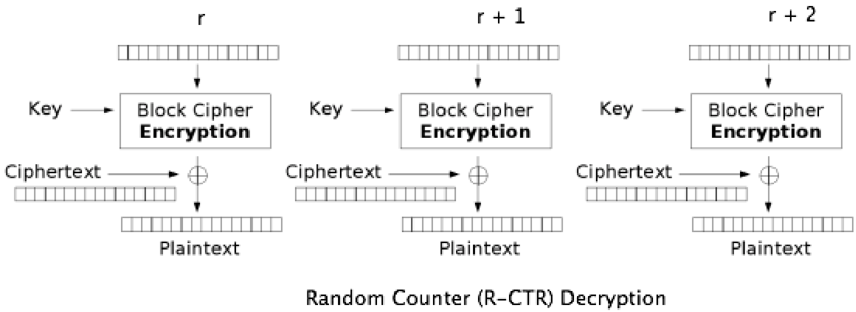


Random Counter (R-CTR) Encryption

Pictures from Wikipedia entry on "Modes of Operation"

Random Counter (R-CTR) Mode (cont'd)

- $Dec_K(c)$:
  - $m_i = B_K(r+i) \oplus c_i, \forall i = 1, \ldots, n$



Pictures from Wikipedia entry on "Modes of Operation"

Random Counter (R-CTR) Mode (cont'd)

- Randomized
- If B_K is a good block cipher, then CPA-secure
- Both encryption and decryption can be parallelized

Random IV (R-IV) Cipher

Random Counter (R-CTR) Mode for 1 block

The sender selects a random value IV for each encryption

- $(IV, c) = (IV, B_k(IV \oplus m))$
- $m = B_k^{-1}(c) \oplus IV$