Block Ciphers & DES

Cryptography - CS 411 / CS 507

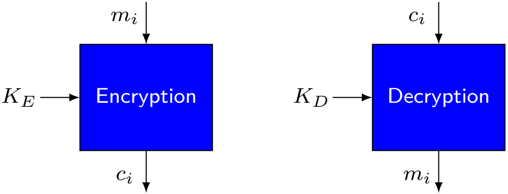
Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

October 10, 2019

Block Cipher: Definition

- A family of functions which maps n-bit plaintext blocks to n-bit ciphertext blocks;
  - n is called the <u>block-length</u>.
- The function is parameterized by a k-bit key K.
- It may be viewed as a simple substitution cipher with a large character size.

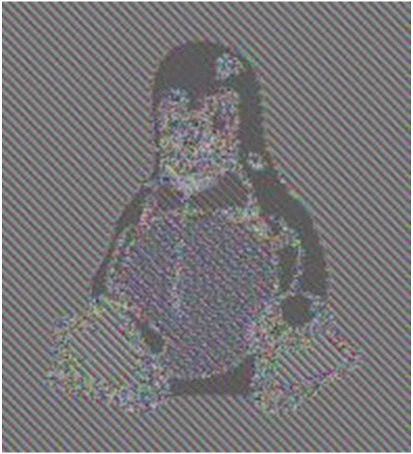


$$K_D = F(K_E)$$
$$K_E = F^{-1}(K_D)$$

- Electronic Codebook:
  - The plaintext P is broken into n-bit blocks, i.e. $P = P_1 P_2 \ldots P_L$
  - The ciphertext consists of the blocks $C = C_1 C_2 \ldots C_L$ where $C_i = E_K(P_i)$ for $i = 1, 2, \ldots, L$.
  - Identical plaintext blocks (under the same key) result in identical ciphertext blocks. (substitution cipher)
  - Each block is encrypted independently of other blocks.
  - Errors in a single block do not propagate to other blocks.
  - Malicious block substitutions does not affect decryption of other blocks.

Image Encryption with ECB

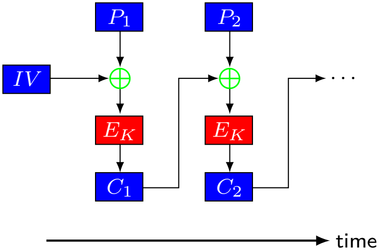
Plaintext Image



Ciphertext with ECB

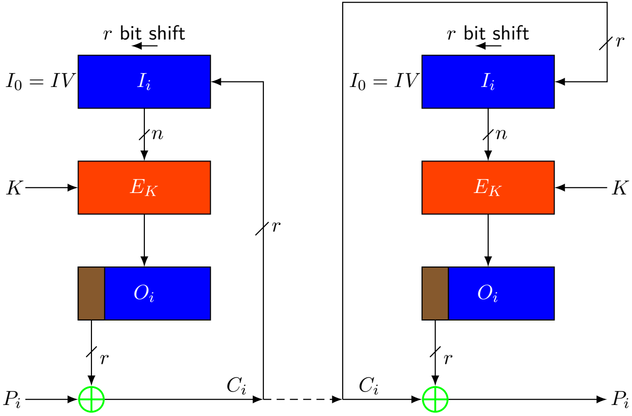
Modes of Operations

- Cipher Block Chaining (CBC):
  - $C_i = E_K(P_i \oplus C_{i-1})$
  - $P_i =$



- Encryption of a block depends on the encryption of previous blocks.
- Self-synchronizing

- Cipher Feedback (CFB) mode:
  - Stream cipher mode
  - A single 8-bit character can be encrypted without having to wait for entire block of data to be available.



Output Feedback Mode

- Similar to CFB

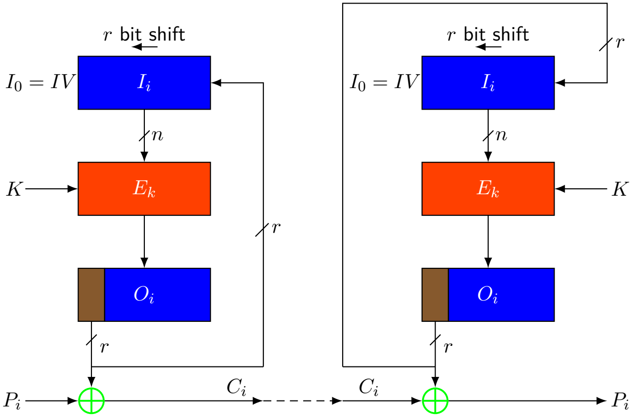
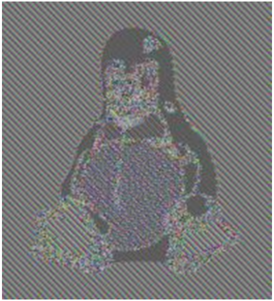
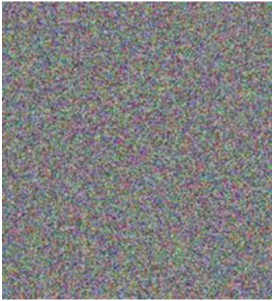


Image Encryption with Different Modes

Plaintext Image



Ciphertext with ECB



Ciphertext with other modes

Evaluating Block Ciphers

- Historical strength:
  - The longer it is exposed to public scrutiny, the higher the confidence level
- Key Size:
  - Effective key size defines an upper bound on the level of security of the cipher
  - While longer keys provides more security, they also impose additional implementation costs.
- Complexity:
  - Complexity of the mapping is good for the security
  - May be restrictive in terms of the efficiency.

Evaluating Block Ciphers

- Block Size:
  - The larger the block size the higher the security
  - Performance implications.
- Throughput:
  - Fast and easy to implement in hardware and software.
- Data Expansion:
  - Encryption should not increase the size of plaintext data.
- Error propagation:
  - Decrypting the ciphertext containing bit errors may result in various effects on the recovered plaintext.

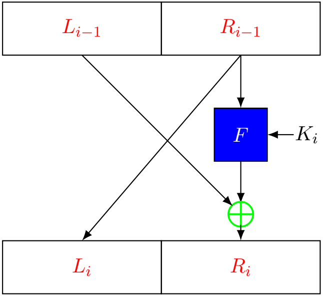
DES Algorithm

- In 1976, the NBS (later NIST) released DES and a free license for its use.
- NSA reviewed and modified the original "Lucifer" which was an IBM design to make the DES.
- Became a standard in 1977 (replaced in 2001).
- Widely used especially in banking industry since.
- Biham & Shamir in 1990, showed an efficient cryptanalysis method (differential) to attack DES.
  - The attack is more efficient for DES variants with fewer number of rounds.

DES & Feistel Ciphers

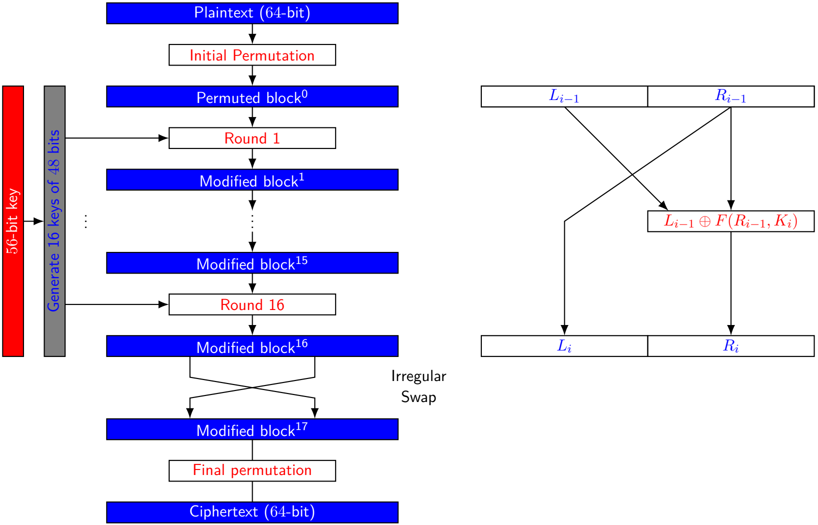
- System parameters
  - 64 bit input/output bits (block length)
  - 56 bits of key
- Principle: 16 round of Feistel system

One round of a Feistel system



$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$
$$L_i = R_{i-1}$$

16 Rounds of DES



Decryption of DES

- DES decryption function is the same as the DES encryption function
  - except the round keys are applied in the reverse order.

$$\begin{array}{ccc} L_0 & R_0 & \\ L_1 = R_0 & R_1 = L_0 \oplus F(R_0, K_1) & \text{1}^{\text{st}} \text{ round} \\ L_2 = R_1 & R_2 = L_1 \oplus F(R_1, K_2) & \text{2}^{\text{nd}} \text{ round} \\ R_2 & L_2 & \text{Irregular swap} \end{array}$$

$$\begin{array}{ccc} R_2 & L_2 & \\ L_2 = R_1 & R_2 \oplus F(L_2, K_2) = ? & \text{1}^{\text{st}} \text{ round} \\ L_1 = R_0 & R_1 \oplus F(L_1, K_1) = ? & \text{2}^{\text{nd}} \text{ round} \\ L_0 & R_0 & \text{Irregular swap} \end{array}$$

The Avalanche Effect in DES 1/2

- Avalanche Effect:
  - A small change either in the plaintext or the key should produce a significant change in the ciphertext.
- DES exhibits a strong avalanche effect.
- Example: Two plaintext which differs by one bit:
  - $P_1 : 00000000\ 00000000 \ldots$
  - $P_2 : 10000000\ 00000000 \ldots$
  - $Key : 0000001\ 1001011\ 0100100\ 1100010$
    $0011100\ 0011000\ 0011100\ 0110010$

The Avalanche Effect in DES 2/2

Round	# of bits that differ	Round	# of bits that differ
0	1	6	32
1	6	7	31
2	21	8	29
3	35	9	42
4	39	10	44
5	34	11	32

DES Properties

- A DES weak key is a key K such that
  - $E_K(E_K(x)) = x$ for all x.
  - There are four DES weak keys.
  - For each of the four DES weak keys K, there exists 2^{32} fixed points of E_K (i.e. plaintexts x such that $E_K(x) = x$)
- A pair of DES semi-weak keys is a pair (K_1, K_2) with $E_{K_2}(E_{K_1}(x)) = x$.
  - six pairs of semi-weak keys
- Is DES a group?
  - Given any two keys K_1, K_2, does there exist a third key K_3 such that $E_{K_3}(x) = E_{K_2}(E_{K_1}(x))$?
  - Is multiple encryption equivalent to a single encryption?

Attacks to DES

- Exhaustive Search:
  - Known: X and Y (known plaintext attack)
  - Unknown: K such that $Y = DES_K(X)$
  - Idea: test all possible keys.
  - Key size (56 bits) is too small
- Differential Cryptanalysis:
  - Proposed by Biham & Shamir in 1990.
  - Principle:
    - Analyze the differences in ciphertexts for suitably chosen plaintext pairs and deduce the likelihood of certain keys.

Differential Cryptanalysis

- Requirements for 16-round DES
  - With chosen plaintext $2^{47}(X, Y)$ pairs are needed.
  - With known plaintext $2^{55}(X, Y)$ pairs are needed.
  - 2^{37} arithmetic operations are needed.
  - High storage requirement for the pairs makes the attack highly impractical.
- Remark: DES s-boxes are optimized for differential cryptanalysis (i.e. the designers were aware of this attack)

Linear Cryptanalysis

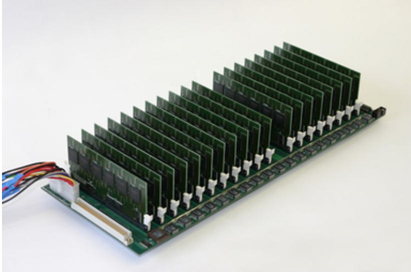
- Proposed by Matsui in 1993 & presented at CRYPTO'94
  - 2^{43} known plaintexts with complexity 2^{43} with success rate 85%.
- The actual attack is implemented
  - Using 12 HP RISC workstations running at 99 MHz
  - With 2^{47} known plaintexts, the key was discovered in 50 days.
- <u>Remark</u>: DES s-boxes are not optimized against this attack.

History of Attacks Against DES

Date	Proposed/implemented attack
1977	Diffie&Hellman, estimates the cost of key search engine ($20m)
1990	Biham&Shamir proposes differential cryptanalysis (2^{47} chosen ciphertext)
1993	Michael Wiener proposes a detailed hw design for key search engine; average search time: 3.5 hours @ less than $1m
1993	Matsui proposes linear cryptanalysis (243 known ciphertext)
Jun. 1997	DES Challenge I broken, distributed effort took 96 days
Feb. 1998	DES Challenge II-1 broken, distributed effort (distributed.net) took 41 days
July 1998	DES Challenge II-2 broken, key search machine deepcrack built by Electronic Frontier Foundation (EFF), 1800 ASICs, each with 24 search units (deepcrack) , $250K, 15 days average, (actual time 56 hours)
Jan. 1999	DES Challenge III broken, distributed.net + EFF's deepcrack, it took 22 hours and 15 minute

Final Results

- COPACOBANA
  - Cost-Optimized PArallel COde Breaker
  - 120 FPGA @ 100 MHz
  - Each FPGA can check four keys every 10 ns.
  - 120 FPGA can check 48 billion keys per second.
  - 8.7 days to break DES, on average
  - Material Cost : ~ US$ 10K



"In 2008 their COPACOBANA RIVYERA reduced the time to break DES to less than one day, using 128 Spartan-3 5000's"
http://www.sciengines.com/copacobana/

DES Alternatives

- Double DES:
  - $C = E_{K_2}(E_{K_1}(P))$ and $P = D_{K_1}(D_{K_2}(C))$, where $K_1 \neq K_2$.
- Double DES is vulnerable to meet-in-the-middle attack by Merkle and Hellman.
- Meet-in-the-middle attack
  - Assume we have P and C where $C = E_{K_2}(E_{K_1}(P))$
  - $d = E_{K_1}(P)$
  - $D_{K_2}(C) = D_{K_2}(E_{K_2}(E_{K_1}(P))) = E_{K_1}(P) = d$

Double DES

- Meet-in-the middle attack
  - Eve intercepts P and $C = E_{K_2}(E_{K_1}(P))$.
  - She computes $E_K(P)$ for all possible K and stores them.
  - She computes $D_K(C)$ for all possible K and stores them.
  - Finally, she compares the two lists.
  - If there are N keys the storage requirement is $2N$.
  - N encryption and N decryption operations and comparisons.
  - Effective key length of Double DES is 57 bits.
  - Storage requirement:
    - $N = 2^{56}, 2N = 2^{57} \rightarrow 2N \times 8 = 2^{57} * 2^3 = 2^{60}$ B

Other Alternatives

- Triple DES:
  - $C = E_{K_3}(E_{K_2}(E_{K_1}(P)))$ provides ?-bit security.
  - $C = E_{K_1}(D_{K_2}(E_{K_1}(P)))$ provides ?-bit security.
- DESX:
  - $C = K_3 \oplus E_{K_2}(K_1 \oplus P)$
  - Fairly secure
- Rijndael was elected as the Advanced Encryption Standard (AES) out of 15 candidate algorithms in 2000.