Week 4: Symmetric Encryption

Dr. Qublai K. Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

Overview

Symmetric encryption

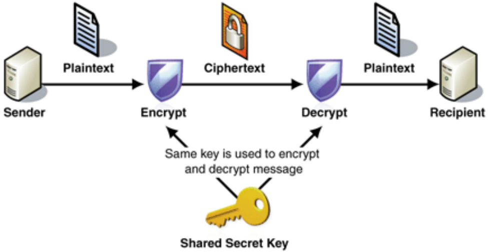

Figure: Symmetric encryption overview, from [2]

Block vs Stream ciphers

- Stream ciphers
  - Encrypt a stream of plaintext one byte at a time
  - Performs `XOR` operation between each plaintext and key bits
  - E.g., Vernam cipher, Vigenère cipher
- Block ciphers
  - Encrypt a *block* of plaintext at a time
  - Block size typically start at 64 bits
  - E.g., DES, AES

Overview

- Based on *invertible product* cipher
- Input broken down into two halves
- Based on round function of right half and subkey
- Consists of multiple operations consisting of:
  - Performing *substitution* on the left half of data
  - Permutation operation through swapping halves

UNIVERSITY OF GLOUCESTERSHIRE

Claude Shannon's *Diffusion & Confusion*

- Based on the principle that a cryptography system must be resilient against statistical attacks
- Diffusion
  - Making the relationship between the *plaintext* and the *ciphertext* as complex as possible
  - Achieved through *permutation*
- Confusion
  - Making the relationship between the *ciphertext* and the *encryption key* as complex as possible
  - Achieved through *substitution*

Operation

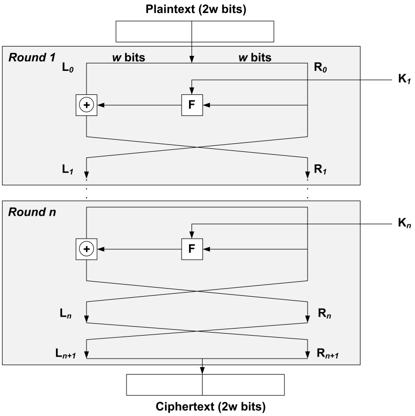

Figure: Fiestel Network, adapted from Fig. 3.5 of [5]

Properties

- Block size
  - Number of input blocks used
- Key size
  - *Length* of the encryption key used
- Number of rounds
  - Number of left/right rounding operations used
- Subkey generation
- Round function

UNIVERSITY OF GLOUCESTERSHIRE

Data Encryption Standard

- One of the most widely used encryption algorithms around
- Developed by IBM researchers led by Horst Fiestel
- Adopted in 1977 by the then National Bureau of Standards (now NIST) as *FIPS 46*
- Designed to be implemented in both *hardware* and *software*

DES Features

- Block cipher
- Features the use of the *Fiestel* cipher algorithm
- Block size: 64 bits (for *both* input and output)
- Same size for key, but only *56-bits* used
  - Remaining 8-bits used for error-checking
- Number of possible key combination then becomes: 2^{56}

Operation

- Involves the transformation of plaintext using 16 rounds
- Each transformation round features the use of Fiestel cipher
- 64 bit input first broken into *two* 32-bit chunks
- Consists of substitution and permutation operations

Operation overview

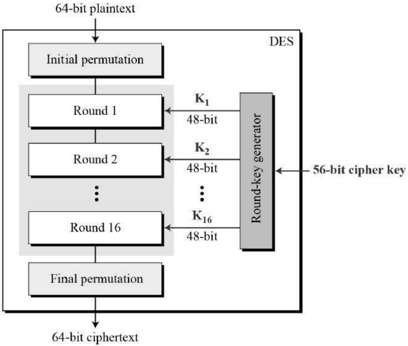

Figure: DES Operation, from [3]

Initial and Final Permutations

- Features the use of permutation boxes (*P-Boxes*)
- Designed to achieve Shannon's Confusion rule
- Keyless
- Each of the permutations takes a 64-bit input and permutes (changing the order) them according to a predefined rule.

Initial and Final Permutations

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Figure: Initial and Final Permutations in DES

UNIVERSITY OF GLOUCESTERSHIRE

Initial and Final Permutations

- Initial Permutation
  - Used right at the beginning of a DES round
  - Reorders the input data bits
  - Even bits to the left half, Odd bits to the right
- Final Permutation
  - Used right at the end of a DES round
  - Switches the left and right halves
  - Also referred to as "switchers"

DES Round Structure

- 64-bit input is first divided into two *left* and *right* halves of 32-bit
- Feistel cipher is applied on both halves using:

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

DES Round Structure

- Each round of DES consists of 3 stages, namely
  1. Expansion of right half using D-box
  2. Bit substitution using S-boxes
  3. Final permutation using 32-bit permutation matrix P

Detailed DES operation

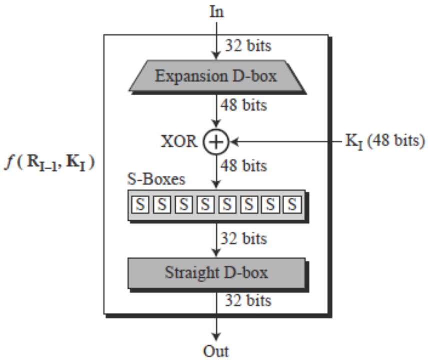

Figure: DES round detailed, from [4]

Bit expansion using D-box

- The right half of the 64 bit input R_{i-1} is 32-bit
- However the input key K_i is 48 bit
- The expansion of R_{i-1} is done using *D-Box*
- `XOR` operation is then done on the expanded R_{i-1} and K_i, before being passed into S-boxes

D-box

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Figure: D-box expansion table

UNIVERSITY OF GLOUCESTERSHIRE

Bit substitution using S-boxes

- Designed to achieve confusion
- Involves the use of 8 S-boxes
  - Each S-box uses a unique table to perform bit substitution
- Each S-box accepts 6 input bits and produces 4 outputs
  - The first and last bits refer to the table *row*
  - The middle 4 bits refer to the table *column*

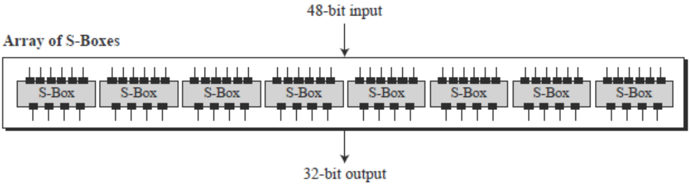

Figure: S-boxes overview, from [4]

Stage-level permutation

- Before passing onto the next round, permutation is performed on the S-box output
- It is done using a unique permutation table, similar in principle to the permutation stage at the beginning

UNIVERSITY OF GLOUCESTERSHIRE

Strengths

- Avalanche Effect
  - A small change in plaintext P needs to result in *significant* change in the resulting ciphertext
- Use of a 56-bit key
  - Allows for approximately 7.2×10^{16} keys
- Use of the same algorithm for both encryption and decryption

UNIVERSITY OF GLOUCESTERSHIRE

Limitations

- Susceptible against *brute-force* and *linear cryptanalysis* attacks
- S-boxes can produce the same output for two different inputs
- Possible to predict through *complementary* encryption

Bringing it together

- Today we looked at symmetric encryption
- We also looked at stream and block ciphers
- We looked at DES and how it works
- Next week: *Symmetric encryption: AES*

UNIVERSITY OF GLOUCESTERSHIRE

Post-sessional work

- Using Subsection 1.3 of [1] (available on *Moodle*) as a starting point, write a critical review of the different block cipher modes of operation.
- Upload your completed work to *Moodle* before next *Monday*.

UNIVERSITY OF GLOUCESTERSHIRE

References

- Debrup Chakraborty and Francisco Rodríguez Henríquez. "Block cipher modes of operation from a hardware implementation perspective". In: *Cryptographic Engineering*. Springer, 2009, pp. 321–363.
- *Data Confidentiality*. https://msdn.microsoft.com/en-us/library/ff650720.aspx. Accessed: 2018-01-17.
- *Data Encryption Standard*. https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm. Accessed: 2018-01-20.
- *Data Encryption Standard (DES)*. http://highered.mheducation.com/sites/dl/free/007070208x/877405/Chapter_06_Data_Encription_Standard.pdf. Accessed: 2018-01-17.

Q & A