SEOULTECH

Block Cipher and Data Encryption Standard (DES)

2021.03.09

Presented by:
Mikail Mohammed Salim

Professor 박종혁
Cryptography and Information Security

SEOULTECH

Contents

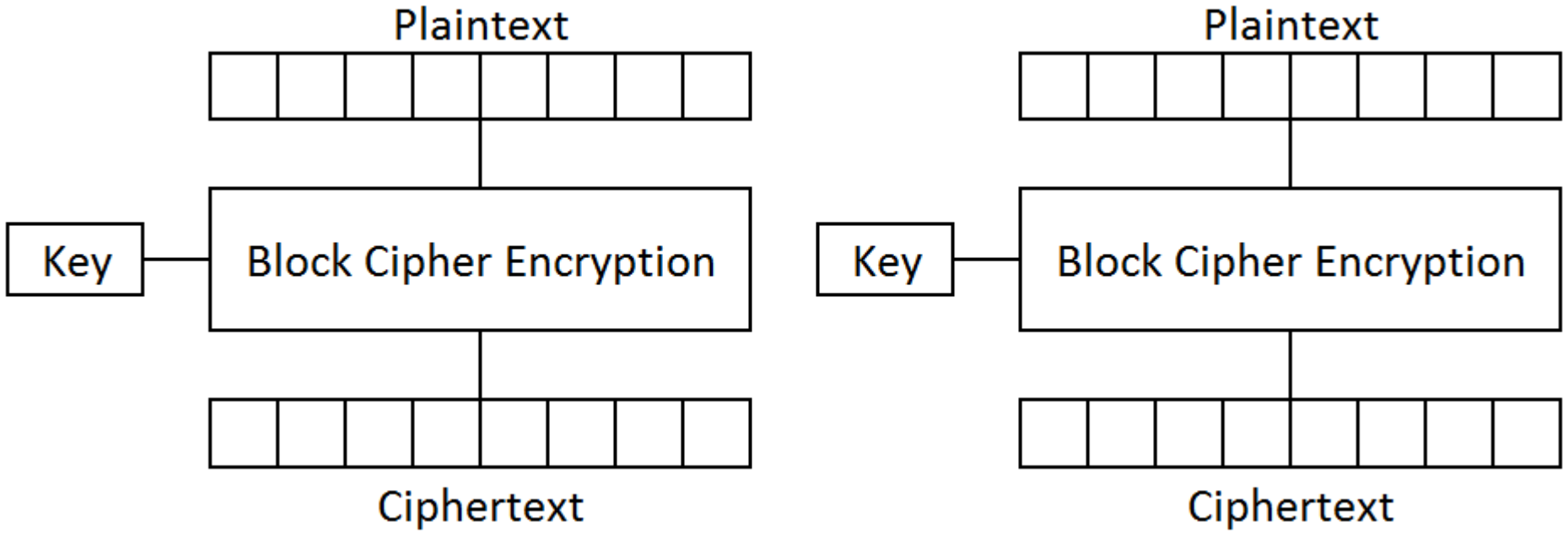
- What is Block Cipher?
- Padding in Block Cipher
- Ideal Block Cipher
- What is DES?
- DES- Key Discarding Process
- Des- 16 rounds of Encryption
- How secure is DES?

SEOULTECH

What is Block Cipher?

- An encryption technique that applies an algorithm with parameters to encrypt blocks of text.
- Each plaintext block has an equal length of ciphertext block.
- Each output block is the same size as the input block, the block being transformed by the key.
- Block size range from 64 -128 bits and process the plaintext in blocks of 64 or 128 bits.
- Several bits of information is encrypted with each block. Longer messages are encoded by invoking the cipher repeatedly.

What is Block Cipher?



- Each message (p) grouped in blocks is encrypted (enc) using a key (k) into a Ciphertext (c). Therefore, $c = enc_k(p)$
- The recipient requires the same k to decrypt (dec) the p.
  Therefore, $p = dec_k(c)$

SEOULTECH

Padding in Block Cipher

- Block ciphers process blocks of fixed sizes, such as 64 or 128 bits. The length of plaintexts is mostly not a multiple of the block size.
- A 150-bit plaintext provides two blocks of 64 bits each with third block of remaining 22 bits.
- The last block of bits needs to be padded up with redundant information so that the length of the final block equal to block size of the scheme.
- The remaining 22 bits need to have additional 42 redundant bits added to provide a complete block.
- Too much padding makes the system inefficient and may render the system insecure if the padding is done with same bits repeatedly.

SEOULTECH

Ideal Block Cipher

- In an ideal block cipher, the relationship between the input blocks and the output block is completely random. But it must be invertible for decryption to work.
- The encryption key for the ideal block cipher is the codebook itself, meaning the table that shows the relationship between the input blocks and the output blocks.

P	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12
00	00	00	00	00	00	00	01	01	10	10	11	11
01	01	01	10	10	11	11	00	00	00	00	00	00
10	10	11	01	11	01	10	10	11	01	11	01	10
11	11	10	11	01	10	01	11	10	11	01	10	01

P	K13	K14	K15	K16	K17	K18	K19	K20	K21	K22	K23	K24
00	01	01	10	10	11	11	01	01	10	10	11	11
01	10	11	01	11	01	10	10	11	01	11	01	10
10	00	00	00	00	00	00	11	10	11	01	10	01
11	11	10	11	01	10	01	00	00	00	00	00	00

SEOULTECH

Ideal Block Cipher

- In block cipher, we replace a block of N bits from the plaintext with a block of N bits from the ciphertext.
- With 2-bits, there are 4 possible plaintext inputs
- There are 24 different possible permutations of the ciphertext output.
- The Sender is required to send the exact key mapping used to the Receiver.
- For example, if Sender choose to encrypt Plaintext using mapping to Key_8, then Sender must tell Receiver that Key_8 is,

Key_8
00
01
10
11

SEOULTECH

Ideal Block Cipher

- The Receiver will know how to perform the decryption, as follows,

$P\ (Mes)$	Key_8
00	00
01	01
10	10
11	11

- If the Receiver receives ciphertext '11', then they will know to decrypt it to ‘10’.
- The encryption key for the ideal block cipher is the codebook itself, meaning the table that shows the relationship between the input blocks and the output blocks.

SEOULTECH

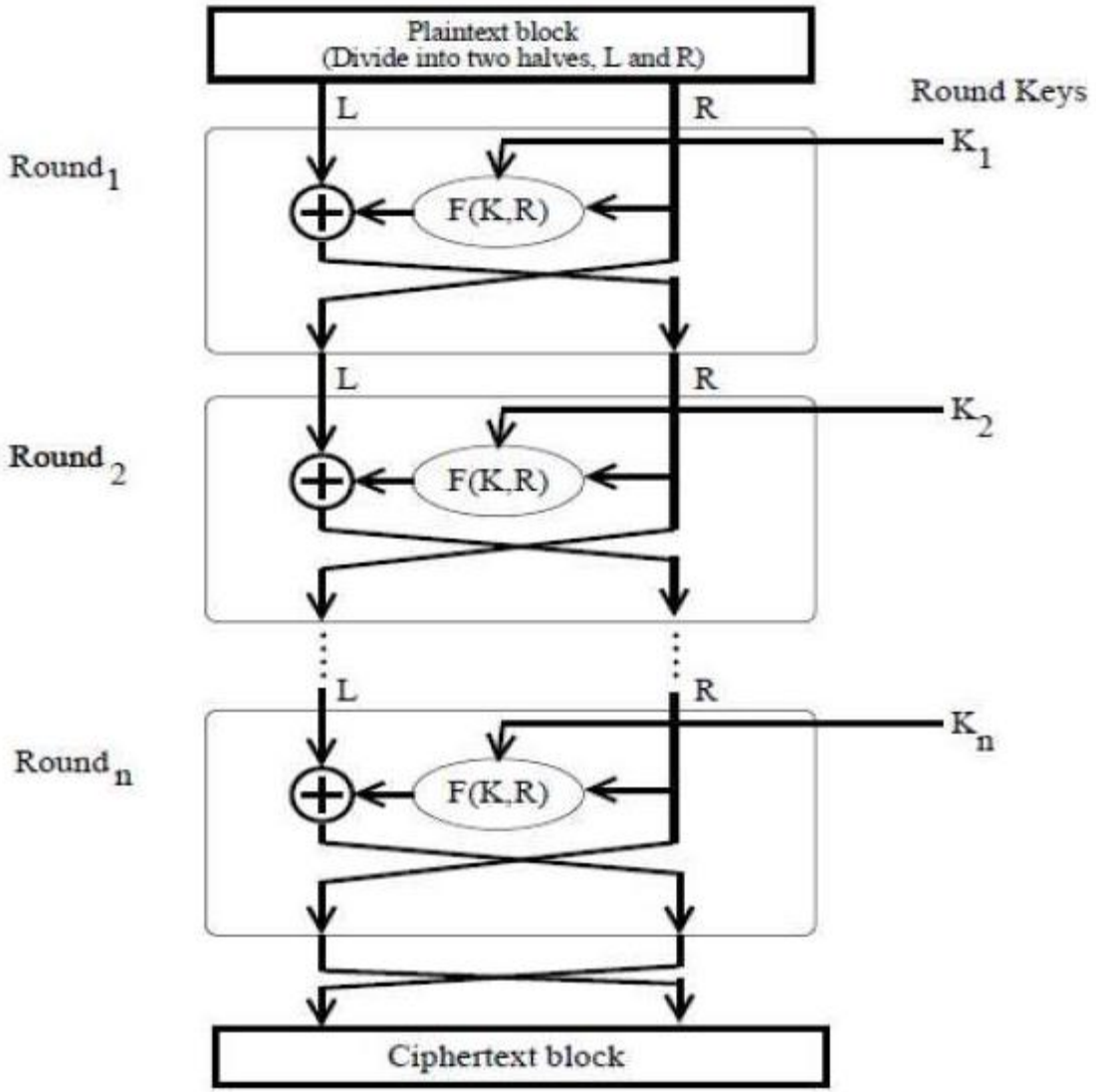
Size of the encryption key for the ideal Block Cipher

- There are 2^n possible plaintexts and in the example of a 64-bit block encryption, there are 2^{64} possible plaintext inputs.
- $2^n!$ number of possible keys can be generated. For 64-bit block, there are possible mappings of $2^{64}! \approx 10^{10^{88}}$.
- This illustrates one of the problems of an ideal block cipher is that the key size and length is not manageable. It takes too much space.
- To overcome this limitation, the Feistel structure was proposed. It allows smaller keys but maintains security by applying multiple rounds.

SEOULTECH

Construction of Block Cipher

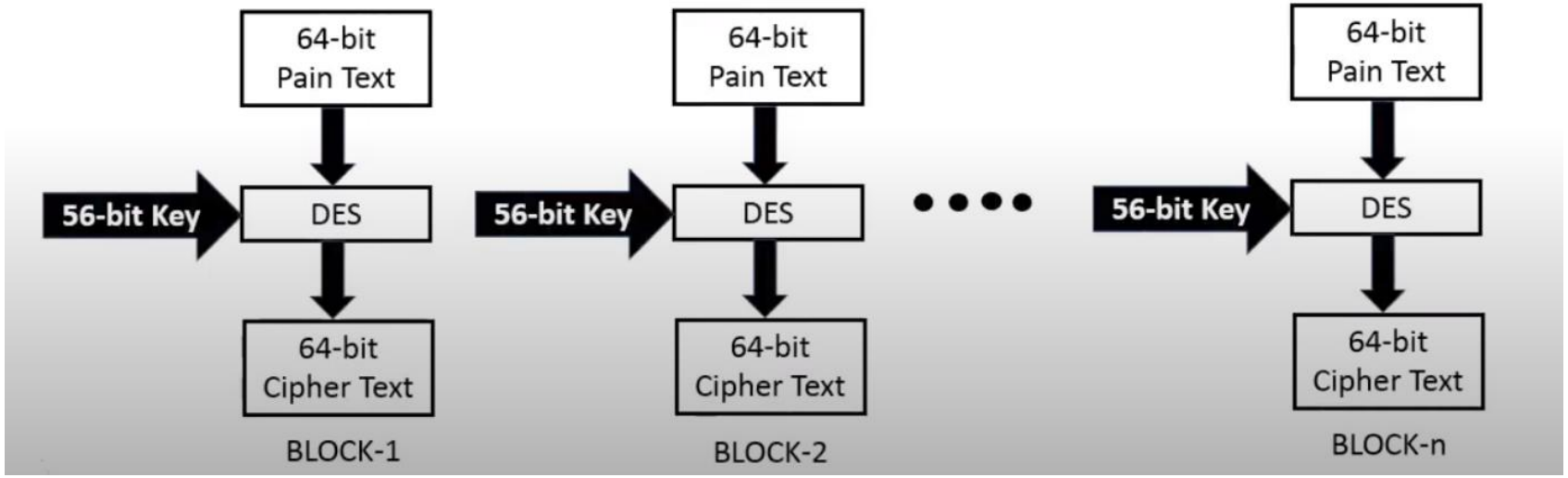
- In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers.
- A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.
- Data Encryption Standard uses the Feistel Cipher method.



SEOULTECH

What is Data Encryption Standard (DES)?

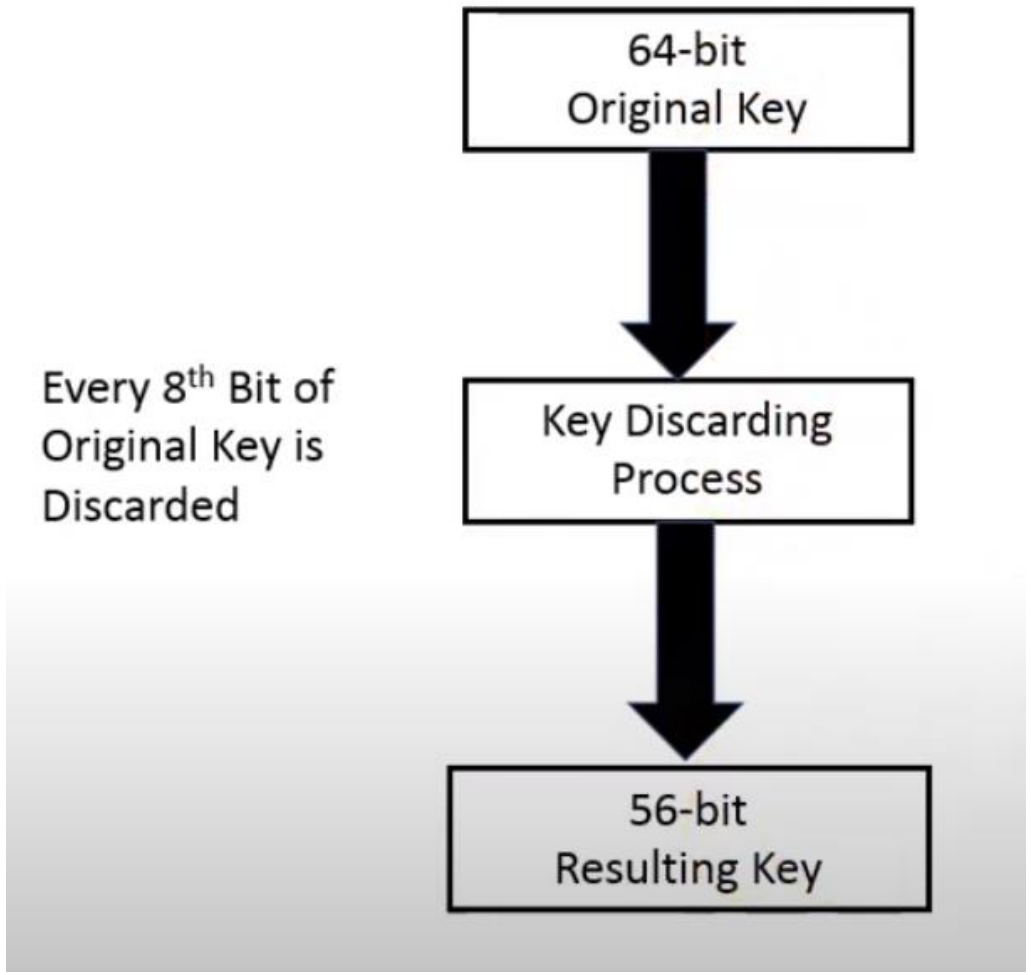
- The Data Encryption Standard (DES) is a symmetric-key block cipher.
- It is now considered as a ‘broken’ block cipher, due primarily to its small key size.
- DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.
- The General Structure of DES is depicted as follows,



SEOULTECH

DES - The Key Discarding Process

- We have mentioned that DES uses a 56-bit key. The initial key consists of 64 bits.
- Before the DES process begins, every 8th bit of the key is discarded to produce a 56-bit key.
- The Key Discarding Process – conversion of a 64-bit key to a 56-bit key.
- Before we enter the key to the DES process, the original key size is 64-bit and is converted to a 56-bit key.



SEOULTECH

DES - The Key Discarding Process

- The 64-bit original key is converted to a 56-bit resulting key.
- Every 8-bit is discarded from the original key.
- This results in generating a (7*8 = 56) 56-bit key.

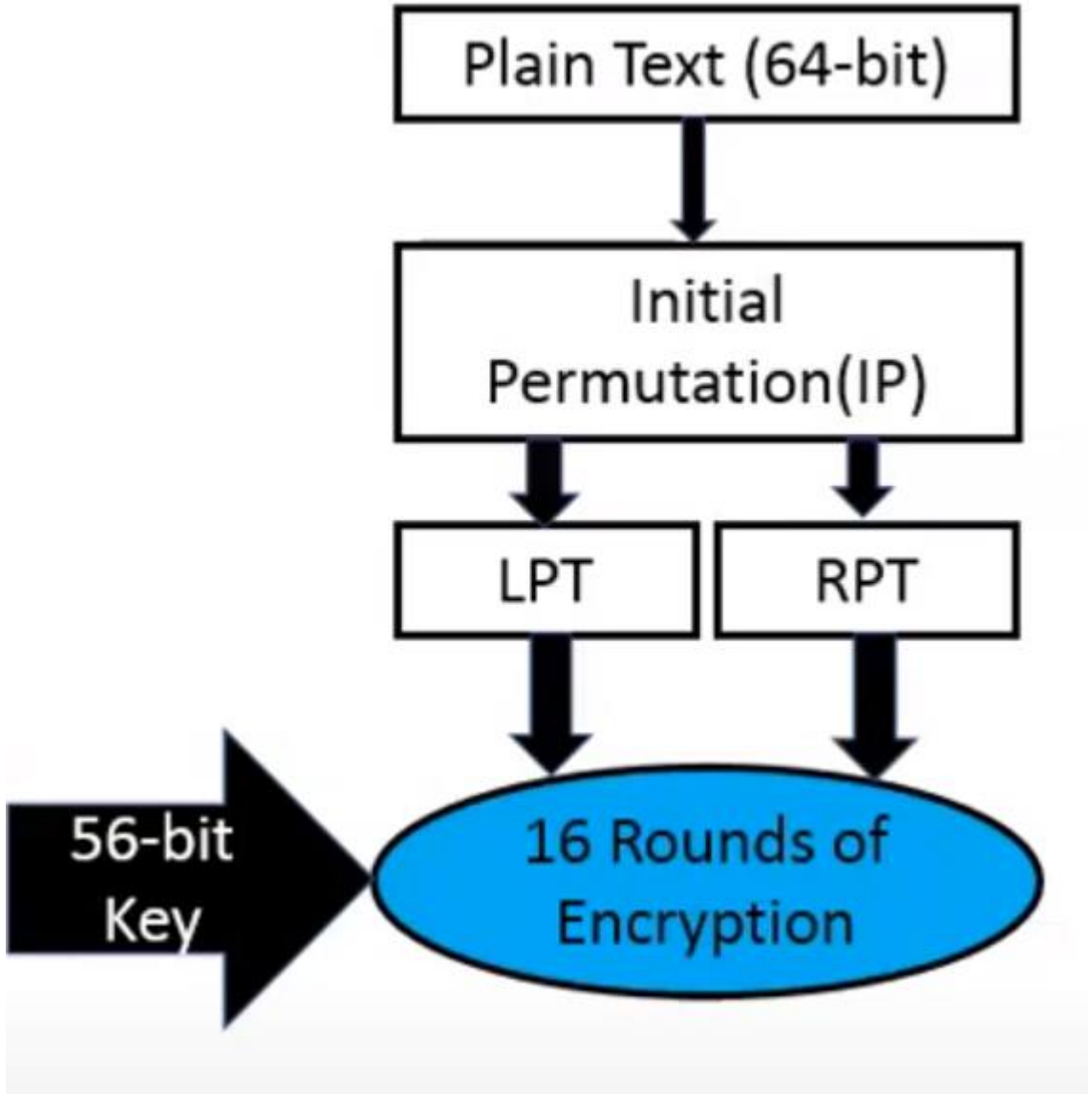
1	2	21	38	58	15	37	26
22	55	44	3	53	27	11	60
49	28	14	42	61	48	63	41
18	39	56	10	64	16	62	8
45	40	20	54	4	33	34	52
7	30	47	59	32	5	35	25
29	12	13	6	24	46	57	36
17	23	50	31	43	51	9	19

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

SEOULTECH

DES – Steps of DES

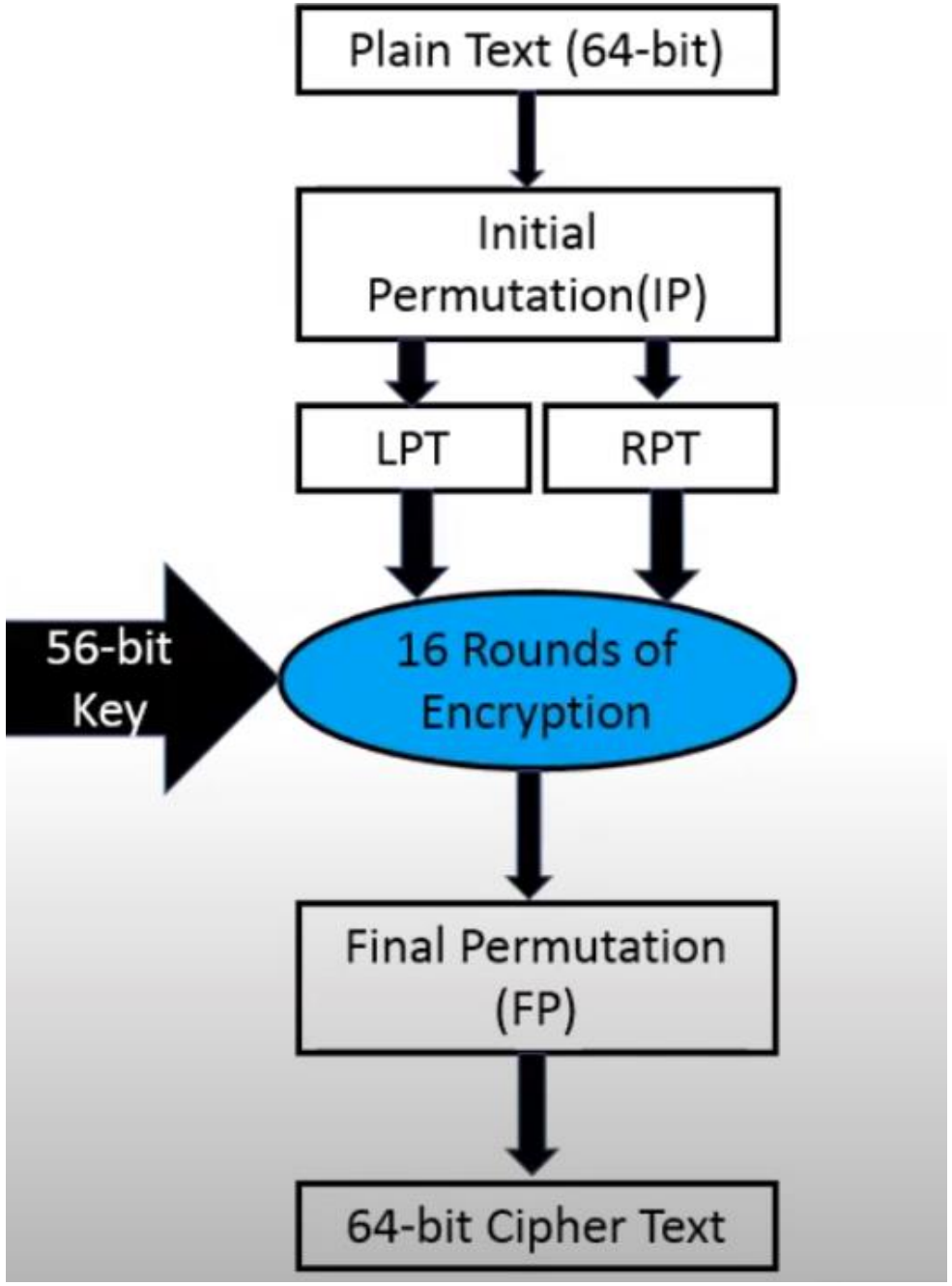
- 64-bit plain text block is given to Initial Permutation (IP) function.
- IP is performed on 64-bit plain text block.
- After IP, the plaintext is converted into two same size blocks, Left plain text (LPT) and Right plain text (RPT).
- After forming LPT and RPT, it serves as an input for 16 rounds of encryption.



SEOULTECH

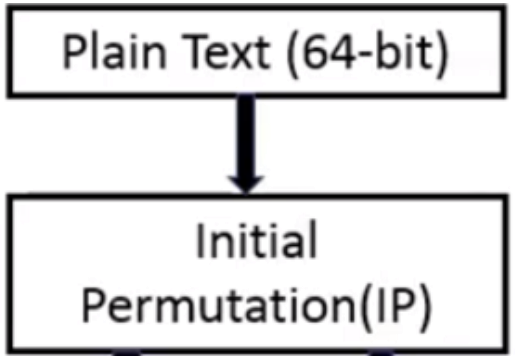
DES – Steps of DES

- The 56-bit key also serves as the input for the 16 rounds of encryption.
- LPT and RPT are rejoined, and the Final permutation is performed on the combined block.
- Finally, a 64-bit Cipher text block is generated.
- 6 tasks are performed to generate the Cipher text from the Plain text.



DES 16 rounds of encryption – Initial Permutation and Generation of LPT and RPT

- Before permutation, plain text is divided into 64-bit blocks.
- The 64-bit block is given to the IP table. Bit sequences change.
- 1st bit takes 40th position and 58th bit takes the 1st position.
- Permutation is transposition, changing location of bits.

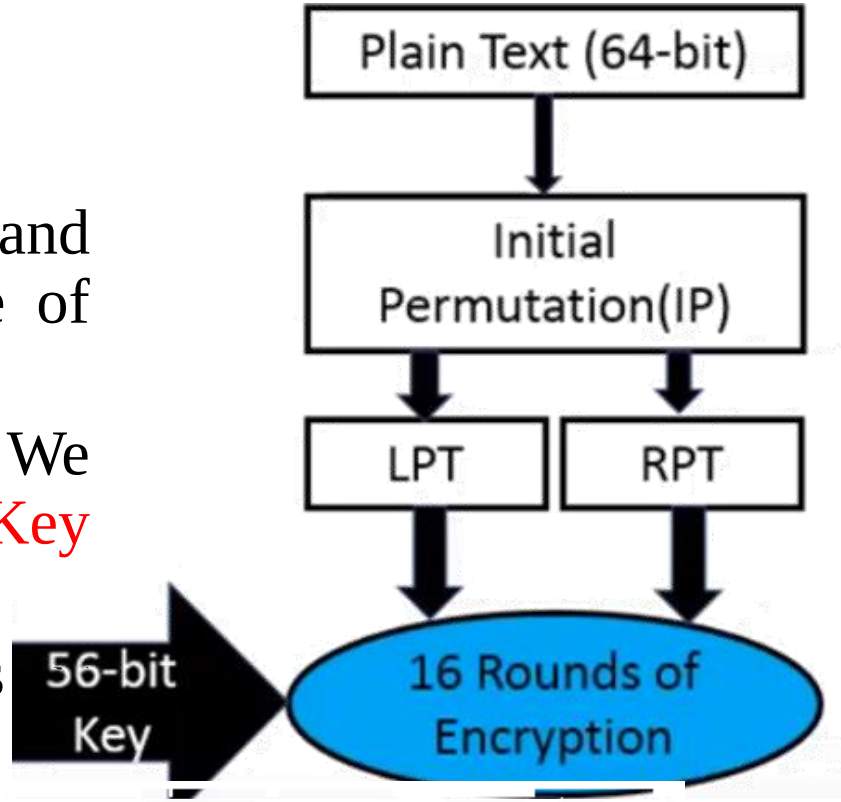


58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

SEOULTECH

DES 16 rounds of encryption – Initial Permutation and Generation of LPT and RPT

- Output of the IP is divided into two halves, LPT and RPT. These are both of 32-bits. The original size of plain-text was 64-bits.
- The next process is the 16 rounds of encryption. We have already generated the 56-bit key using Key discarding process.
- The key, LPT, and RPT are inputs for 16 rounds encryption.



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

SEOULTECH

DES - 16 rounds of encryption – First step: Key transformation

- There are 5 steps in the 16 rounds of encryption.
- In the first step, we perform Key transformation of the 56-bit key and then Compression Permutation.
- The 56 –bit key is divided into two halves each of 28-bits.
- Circular left shift (moving the final bit to the first position while shifting all other bits to the next position) on each halves of 28-bits.
- Shifting of the bit-position depends upon the round, how many shifts do we have to shift as per the round. There are 16 rounds of encryption.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key bit shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

SEOULTECH

DES - 16 rounds of encryption – First step: Key transformation

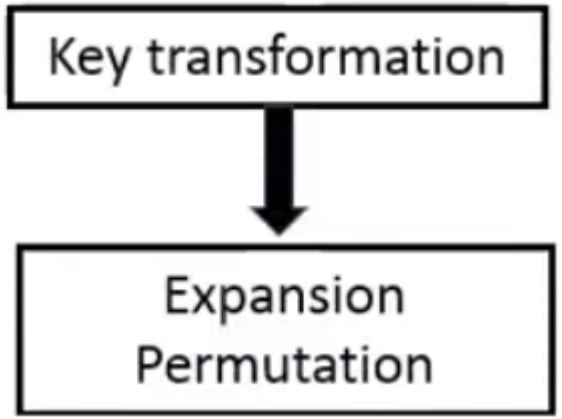
- In DES, we use left circular shift. We are going to move the bits. Shifting of bits depends on the round number.
- If round number is 1,2,9 and 16, shift is done by one left shift.
- The remaining rounds 3-8, 10-15 perform two-bit left shift.
- This is the key-bit shifted per round.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Key bit shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

SEOULTECH

DES - 16 rounds of encryption – First step: Compression Permutation

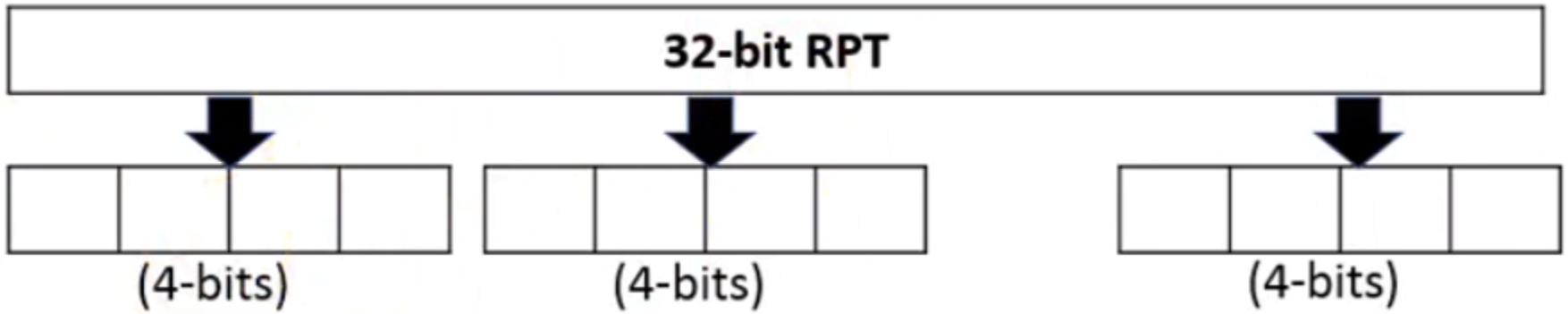
- We obtain a 48-bit key using a 56-bit input with bit shifting position.
- We compress the 56-bit key to achieve a 48-bit key.
- We drop 8 bits from the table, 9, 18, 22, 25, 35, 38, 43 and 54 bits. This bit is fixed, and we no longer find them on the table below.
- We now proceed to step 2, Expansion Permutation.



14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

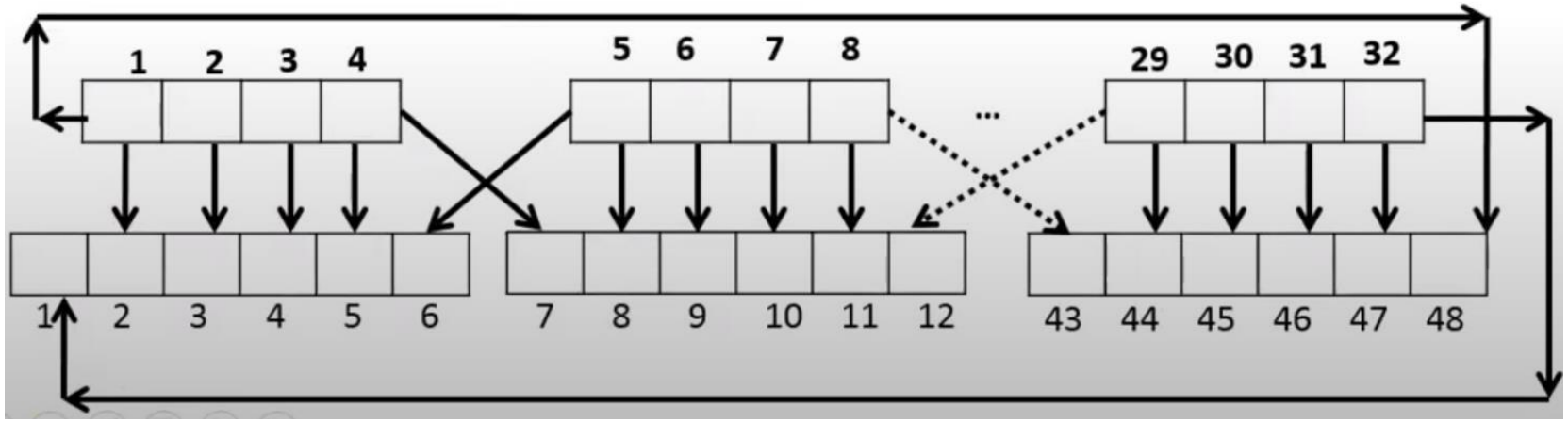
DES - 16 rounds of encryption – Second step: Expansion Permutation

- 32-bit Right Plain Text of Initial Permutation is expanded to 48-bits because our key-size in 48-bits and we must perform XOR after expansion permutation.
- Expansion Permutation steps:
  - A 32-bit RPT is divided into 8-blocks each of 4-bits (4*8).



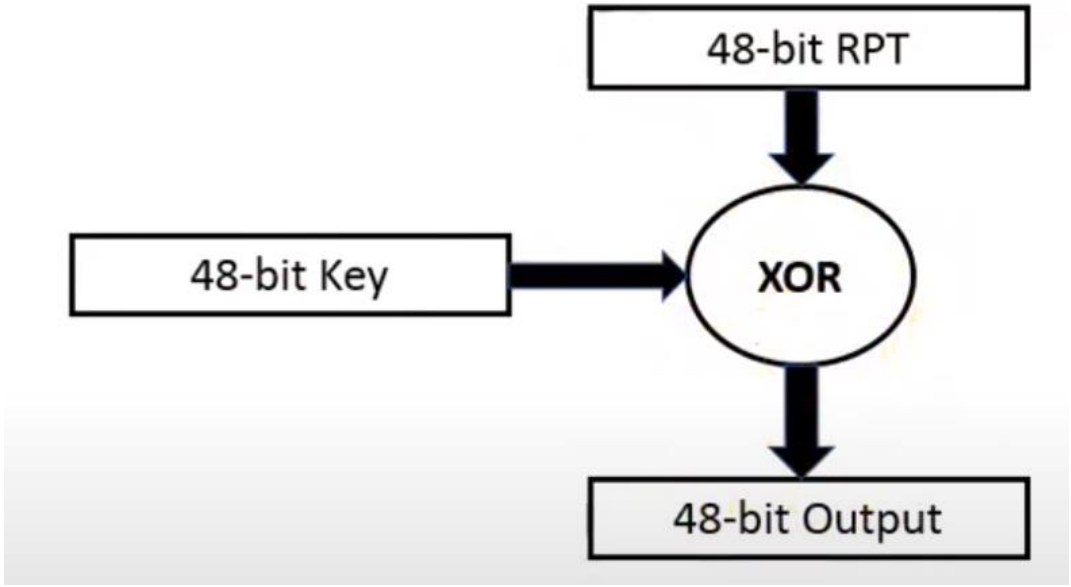
DES - 16 rounds of encryption – Second step: Expansion Permutation

- Expansion Permutation steps: (cont.)
  - The following 4 blocks are converted into 6 blocks because we must convert the 32-bit block to 48-bits. (6*8 = 48).
  - Two outer bits are added, 1 and 6.
  - The last bit in block 32 is added to block 1.
  - The first bit, block 5 is added as block 6.
  - This generates a 6-block resulting in a total of 48-bits.

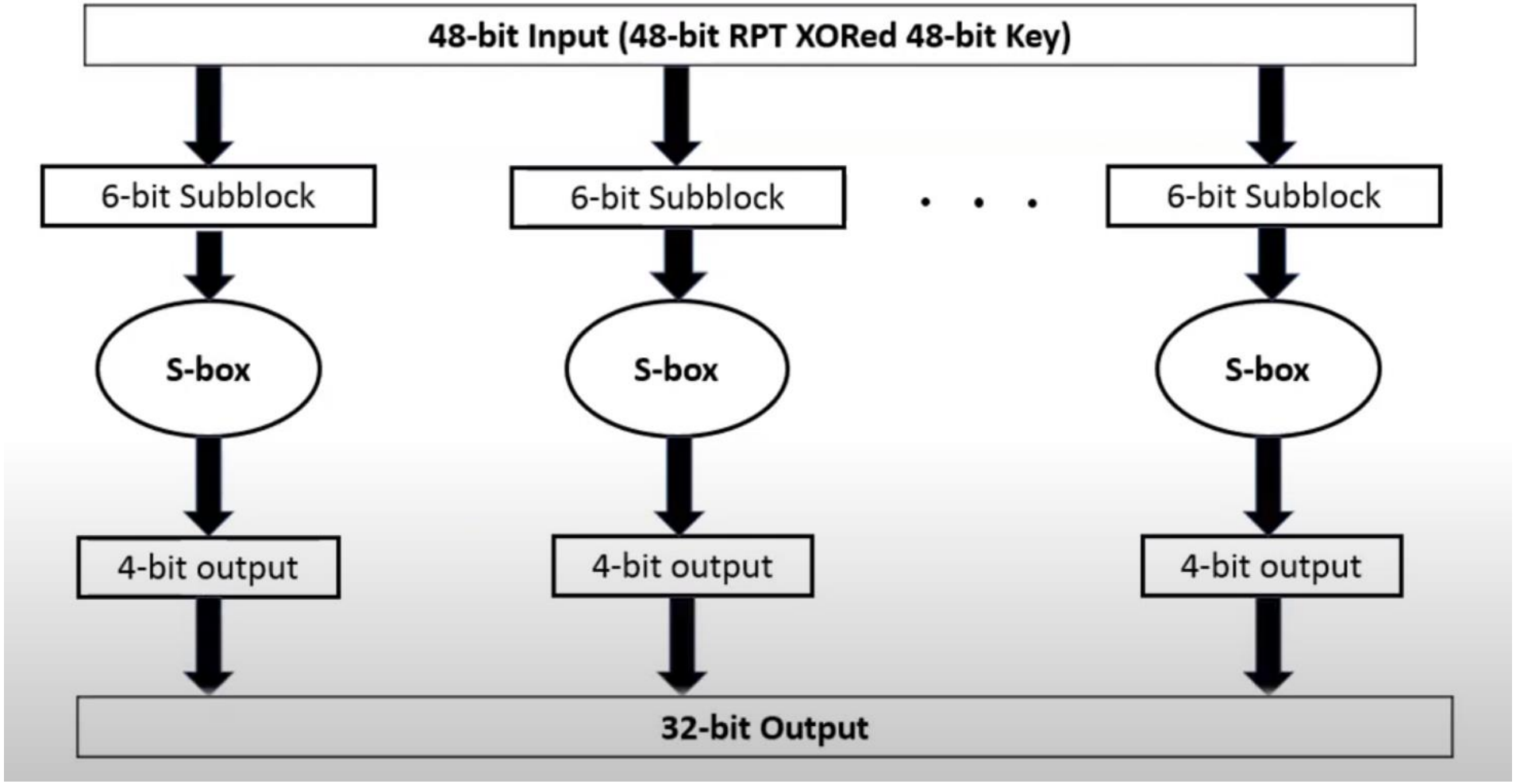


DES - 16 rounds of encryption – Second step: Expansion Permutation

- Expansion Permutation steps: (cont.)
  - Here we perform XOR operation with two 48-bit inputs, RPT and the Key.
  - A 48-bit output is generated.
  - The 48-bit XORed output is given to the S-box because 48-bit RPT is converted into 32-bit as LPT is 32-bit.

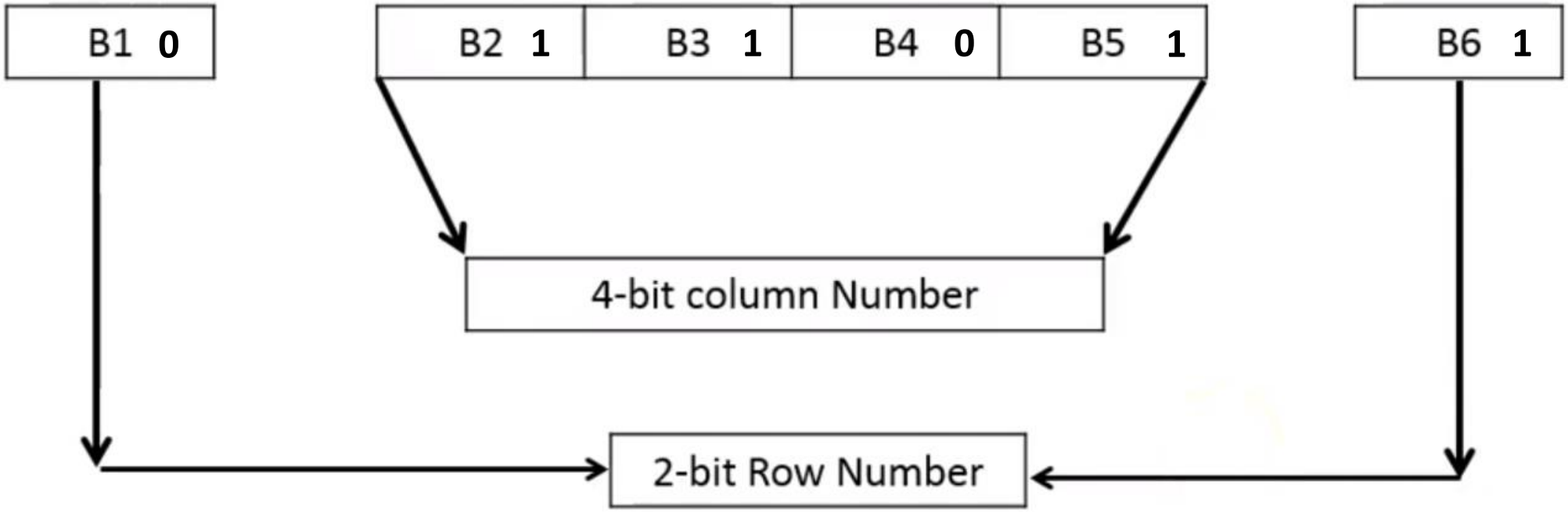


DES - 16 rounds of encryption – Third step: S-Box Substitution



DES - 16 rounds of encryption – Third step: S-Box Substitution (Converting 6-bits into 4-bits)

- S-Box process steps:
  - B1 and B6 are outer bits and B2-B5 are inner bits.
  - A 4-bit column number and a 2-bit row number is generated.



SEOULTECH

DES - 16 rounds of encryption – Third step: S-Box Substitution (Converting 6-bits into 4-bits)

- S-Box process steps to convert 6-bits into 4-bits:
  - For example, we convert 011011 (6-bits) into 4-bits.
  - We check the column number of the middle bits 1101, corresponding to the row number 01.
  - The number 1001 is generated which is 4-bits.
  - The next and fourth step is P-box or permutation.

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

SEOULTECH

DES - 16 rounds of encryption – Fourth step: P-Box Permutation

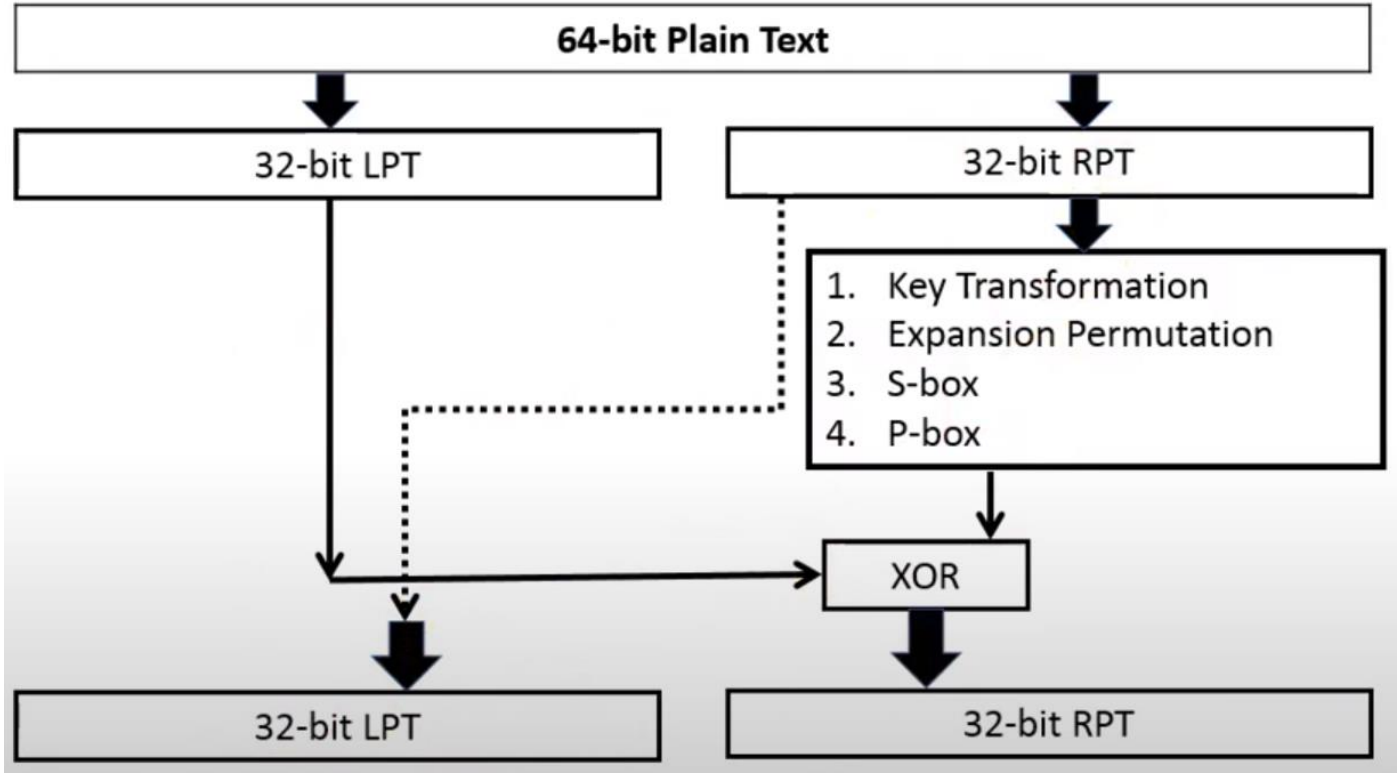
- The 32-bit output of S-Box is given to the P-box.
- So, 32-bit is permuted with 16*2 permutation table.
- 16th bit of S-box takes 1st position as per the below table.

P – Box Table															
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

SEOULTECH

DES - 16 rounds of encryption – Fifth step: XOR and SWAP

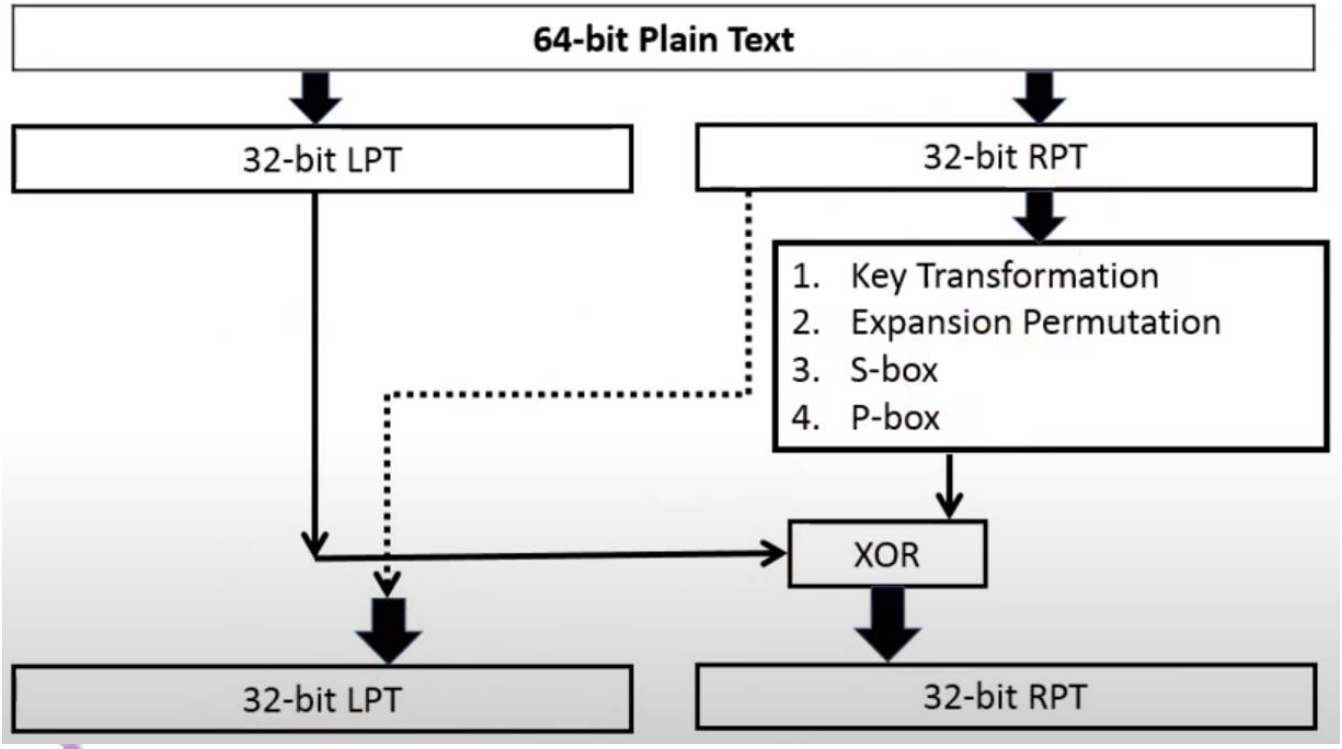
- A 32-bit LPT is XORed along with 32-bit P-box.
- The 32-bit output of the P-box is given as input to the XOR.
- The 32-bit LPT is the input of the XOR process.



SEOULTECH

DES - 16 rounds of encryption – Fifth step (cont.): XOR and SWAP

- Both units are XORed which generates a 32-bit RPT.
- The 32-bit RPT is also swapped with the 32-bit LPT.
- The first round of encryption is complete and the remaining 15 rounds will be performed, like the first round. Total rounds are 16 in DES.



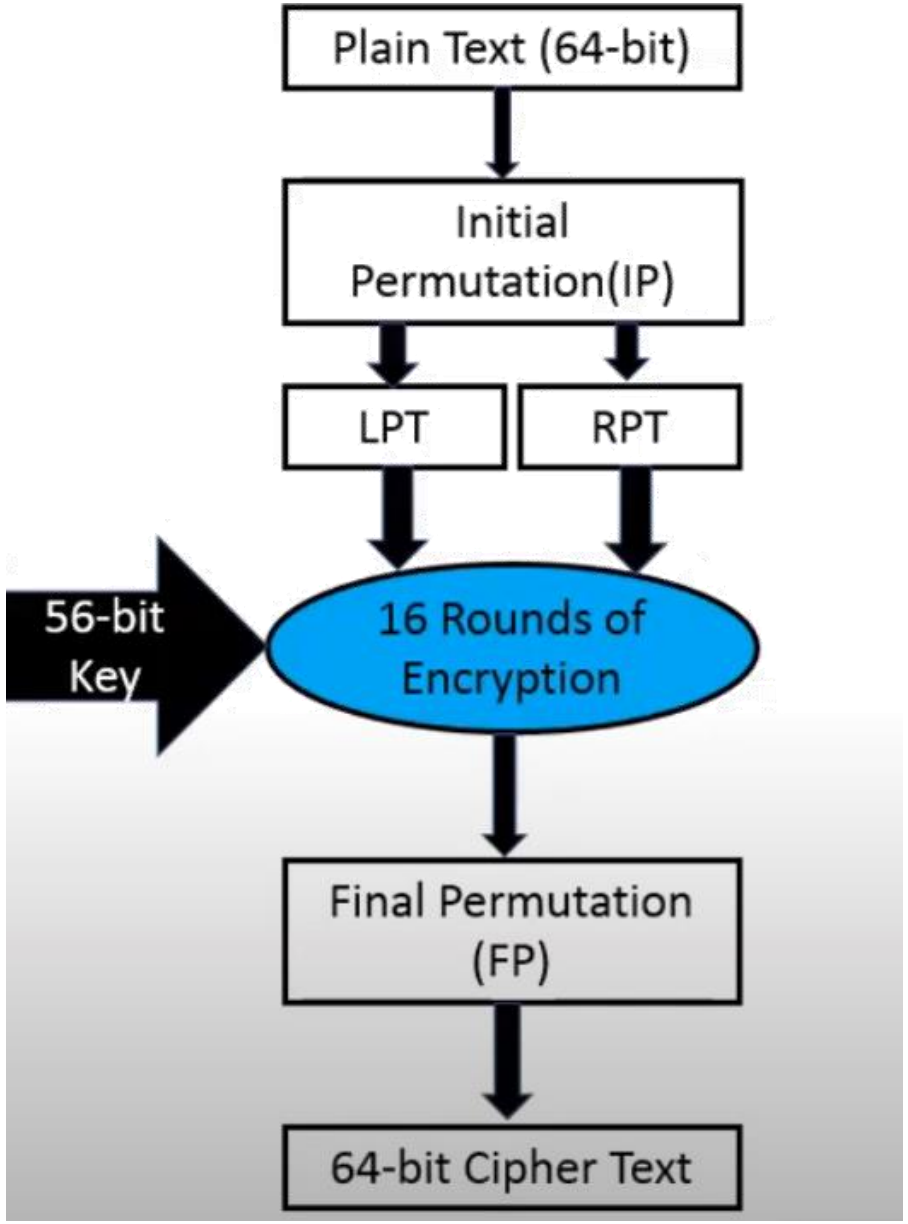
SEOULTECH

DES - 16 rounds of encryption – Final Permutation and generation of 64-bit encrypted block

- After completion of the 16 rounds of Encryption, DES performs a Final Permutation (FP).
- FP is performed only once.
- For example, the 40th bit of the input takes the 1st position.

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

- The output of the final permutation is the 64-bit encrypted Cipher text block.



SEOULTECH

How secure is DES?

- There are 2^{56} possible keys in DES leading to 72,057,594,037,927,936 possible key combinations.
- The 56-bit key is too short making it vulnerable to brute-force attacks.
- Longer keys protect against brute-force attacks.
- In 1998, the Electronic Frontier Foundation built a DES-cracking machine. It can find a DES key in an average of a few days' search.
- In 1999, in a DES contest, a Deep Crack computer (IBM's Deep Blue chess computer) found the 56-bit key and deciphered the message which read, “See you in Rome (Second AES Candidate Conference, March 22-23, 1999)”.

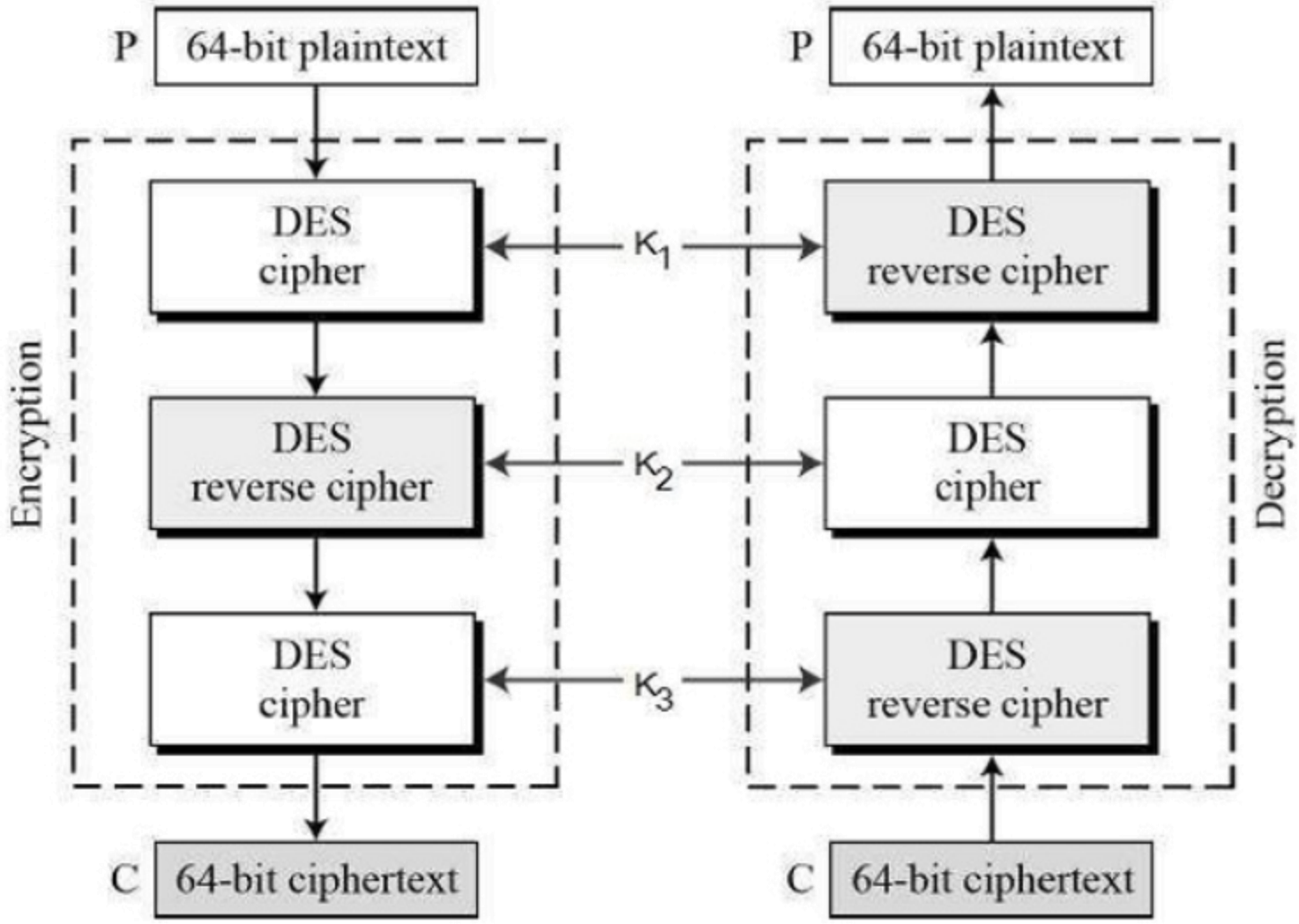
SEOULTECH

Triple Round DES

- Weakness found in DES required a new encryption standard.
- DES was widely implemented in several security programs used by large enterprises.
- Instead of abandoning DES, a new modified version of it known as Triple DES was designed.
- A modified scheme of Triple DES was proposed which was less expensive for large organizations to adopt rather than implement a new encryption standard system.

SEOULTECH

Triple Round DES



SEOULTECH

Triple Round DES – Encryption/Decryption process

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

SEOULTECH

Triple Round DES – Encryption/Decryption process

- A second variant of Triple DES (2TDES) is identical to 3TDES except that K_3 is replaced by K_1 .
- user encrypt plaintext blocks with key K_1 , then decrypt with key K_2, and finally encrypt with K_1 again.
- Therefore, 2TDES has a key length of 112 bits.
- Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value.
- This provides backwards compatibility with DES.

SEOULTECH

Conclusion

- In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks.
- Block ciphers serve as building blocks in other cryptographic protocols such as DES and Advanced Encryption Algorithm (AES).
- Though DES's short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.
- It has a relatively short key length of the symmetric-key block cipher design.
- The intense academic scrutiny of the DES algorithm received over time led to the modern understanding of block ciphers such as AES.
- Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

SEOULTECH

Thank you!

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory