



Subject Name: Cryptography and System Security

Unit No: 01 Unit Name: Introduction & Number Theory

Faculty Name :
Dr. Dhananjay Dakhane
Dr. Sangita Chaudhari
Dr. Prajka Dere

Index

Lecture 1 – Data Encryption Standard(DES) 3

Lecture 2 – Double DES, Triple DES 26

Lecture 3 – Advanced Encryption Standard (AES) 44

**Unit No: 1
Theory**

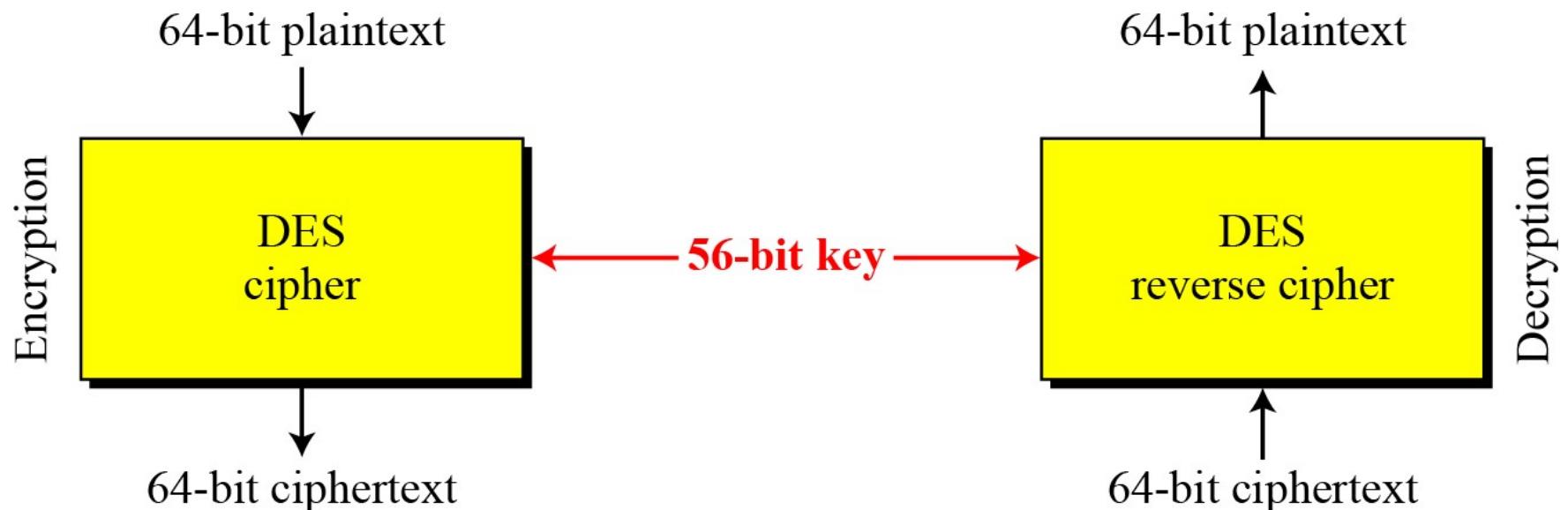
Unit Name: Introduction & Number

Lecture No: 1 Data Encryption Standard(DES)

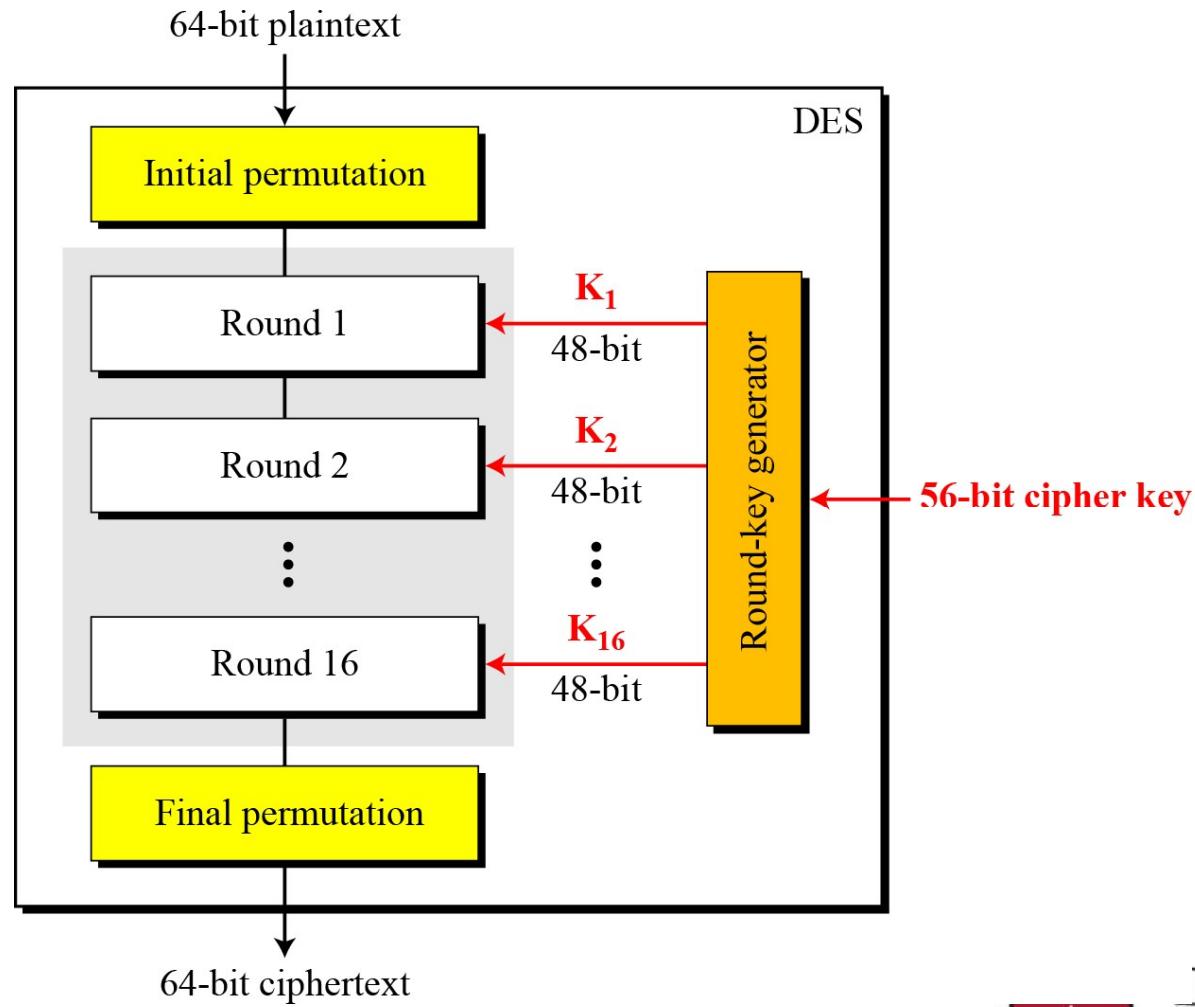


Data Encryption Standard

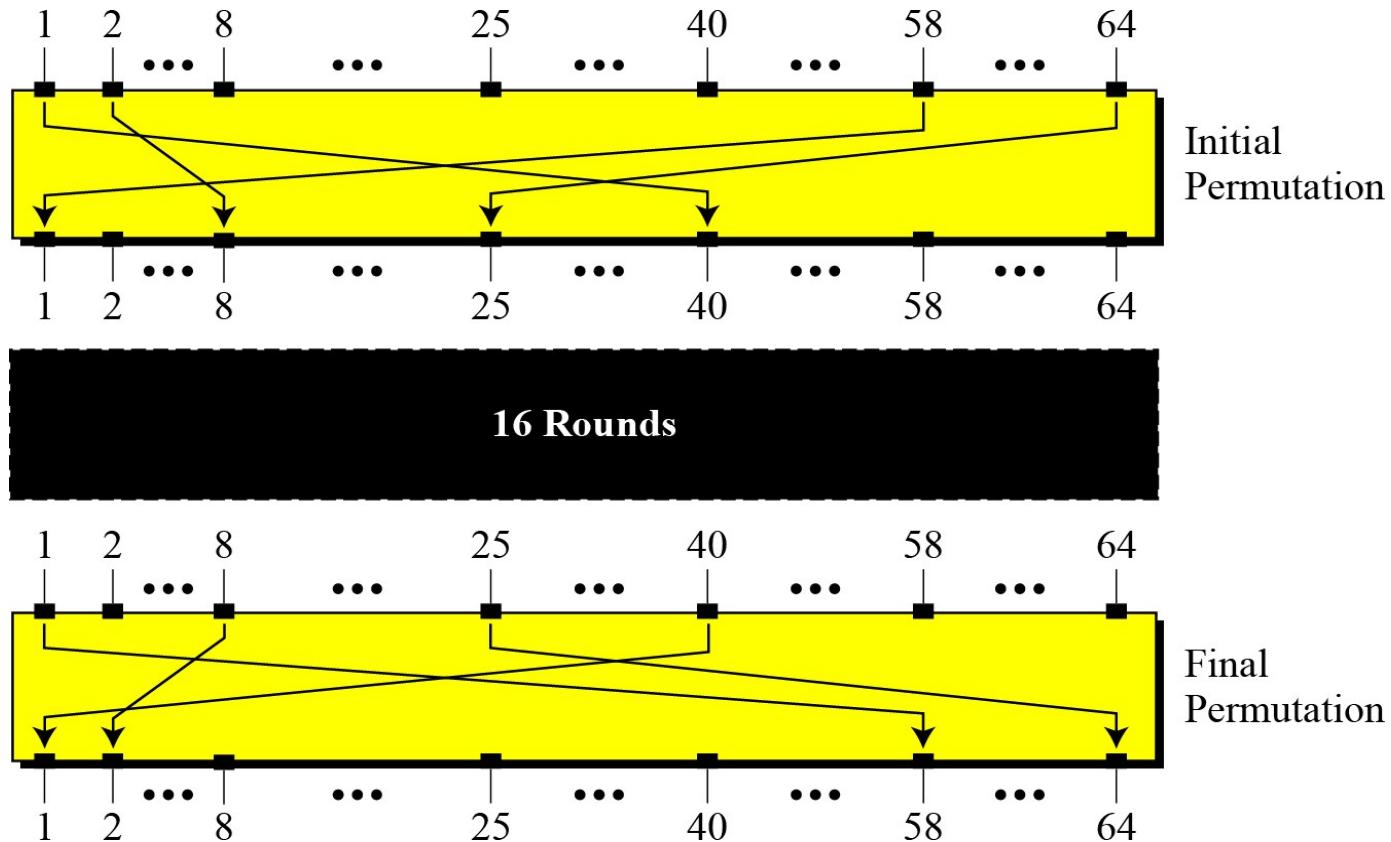
- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).



General Structure of DES



Initial and Final Permutations



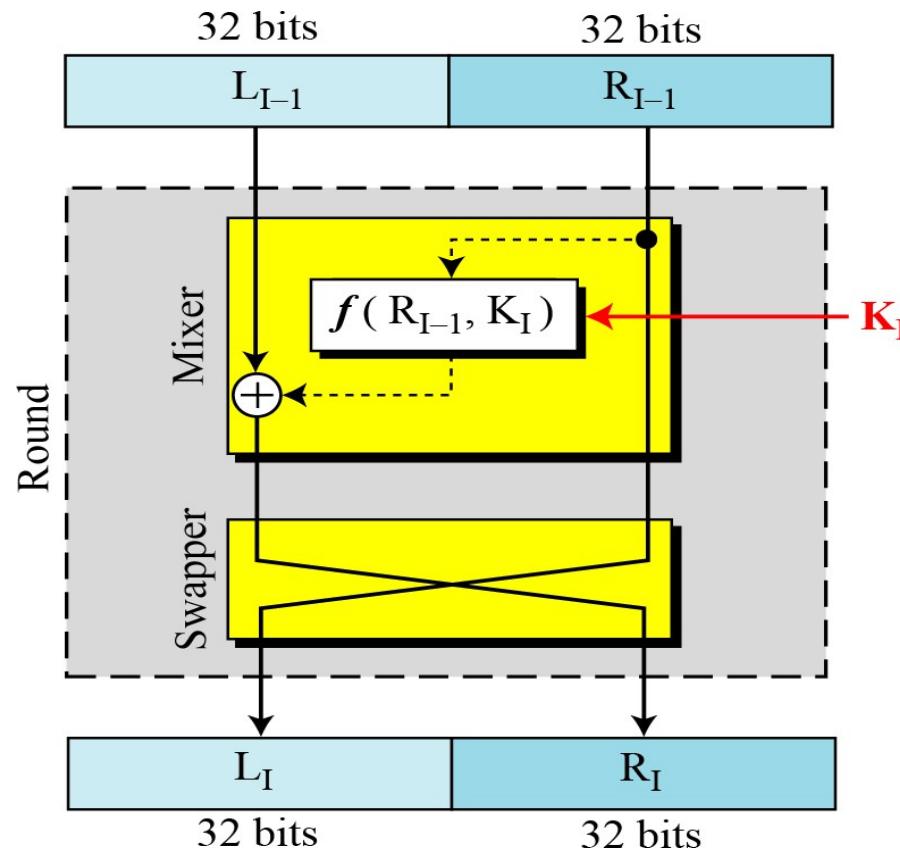
Initial and Final Permutation Tables

<i>Initial Permutation</i>	<i>Final Permutation</i>
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

The initial and final permutations are straight P-boxes that are inverses of each other. They have no cryptography significance in DES.

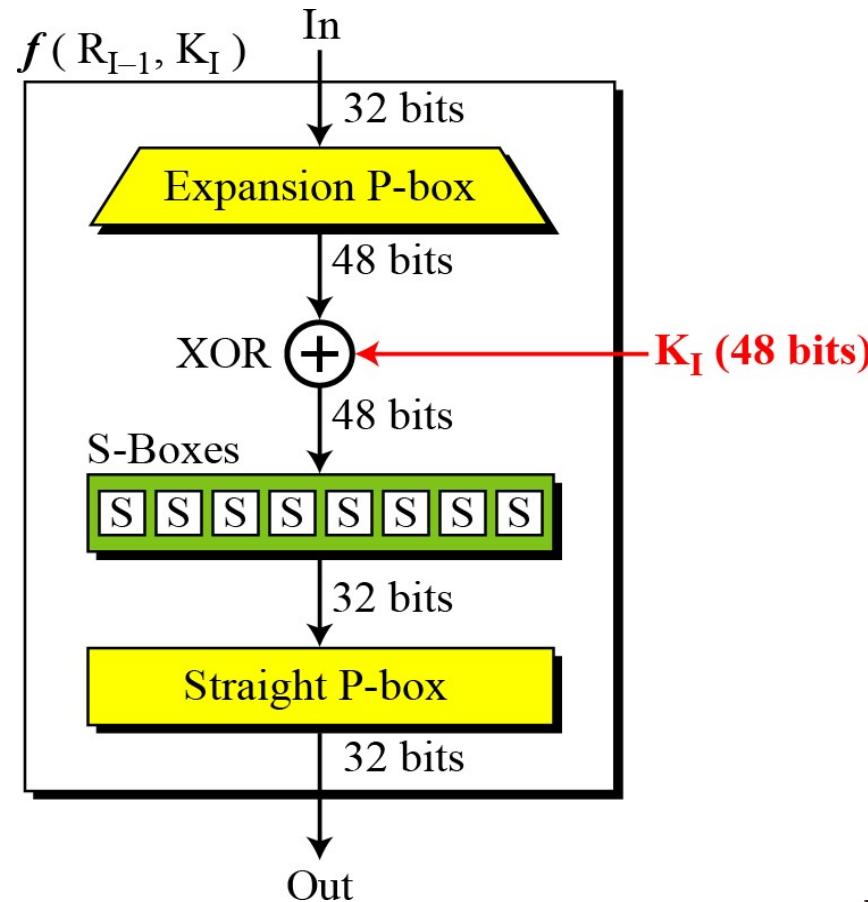
DES Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher.



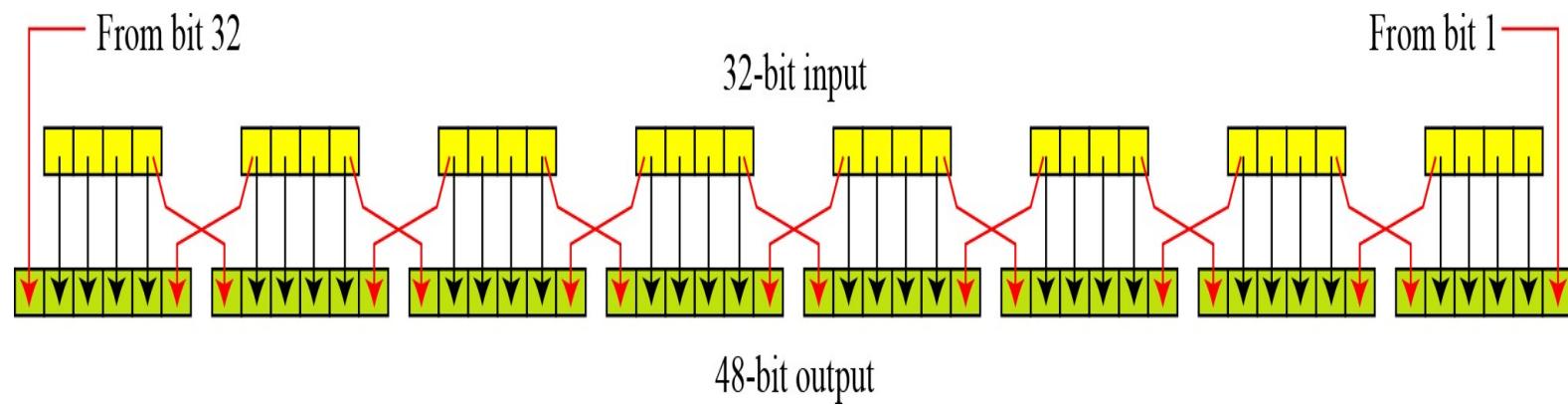
DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



Expansion P-Box

Since R_{l-1} is a 32-bit input and K_l is a 48-bit key, we first need to expand R_{l-1} to 48 bits.



Expansion permutation

Expansion P-Box Table

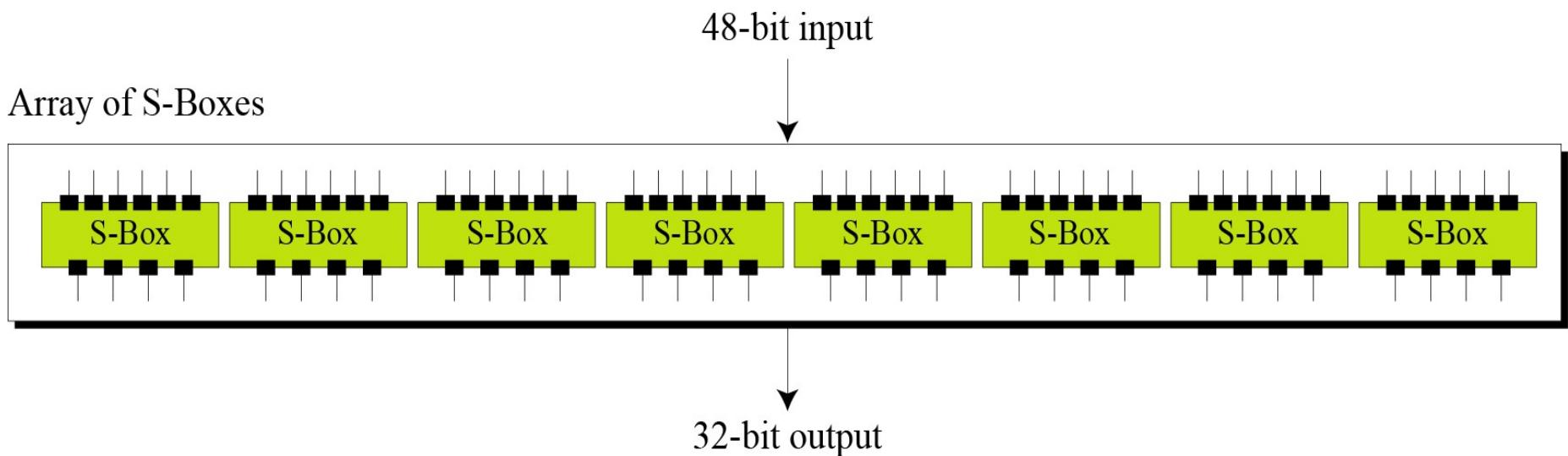
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Whitener(XOR)

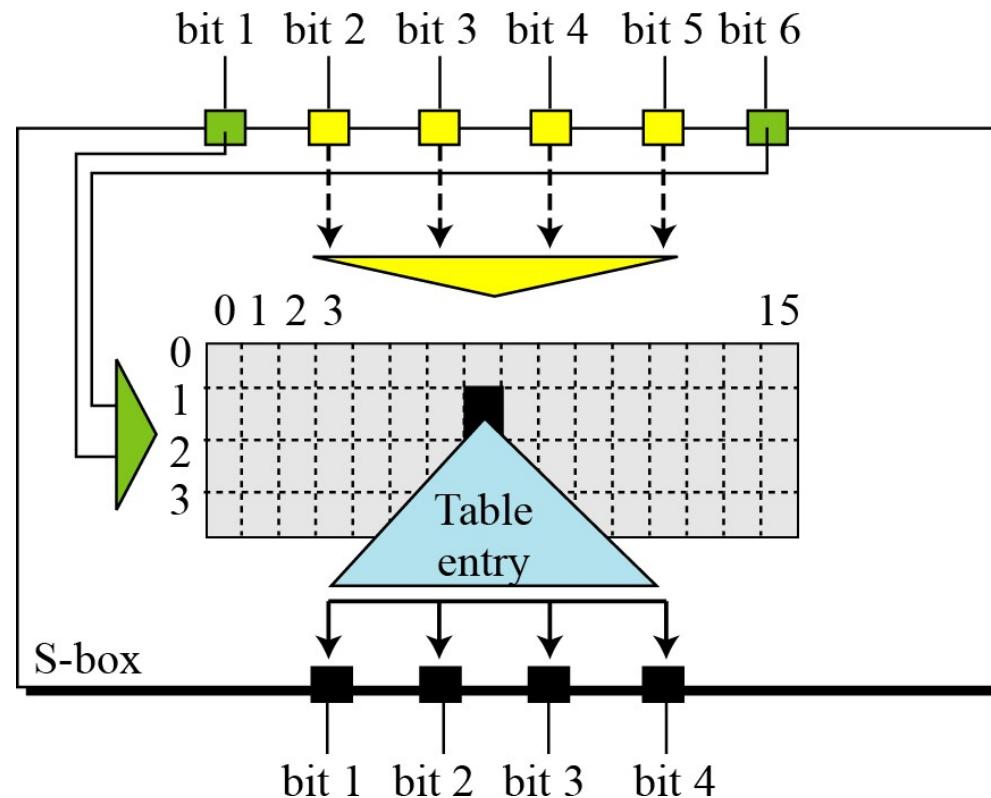
- After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.
- Both the right section and the key are 48-bits in length. Also note that the round key is used only in this operation.

S-Boxes

The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



S-box Rule

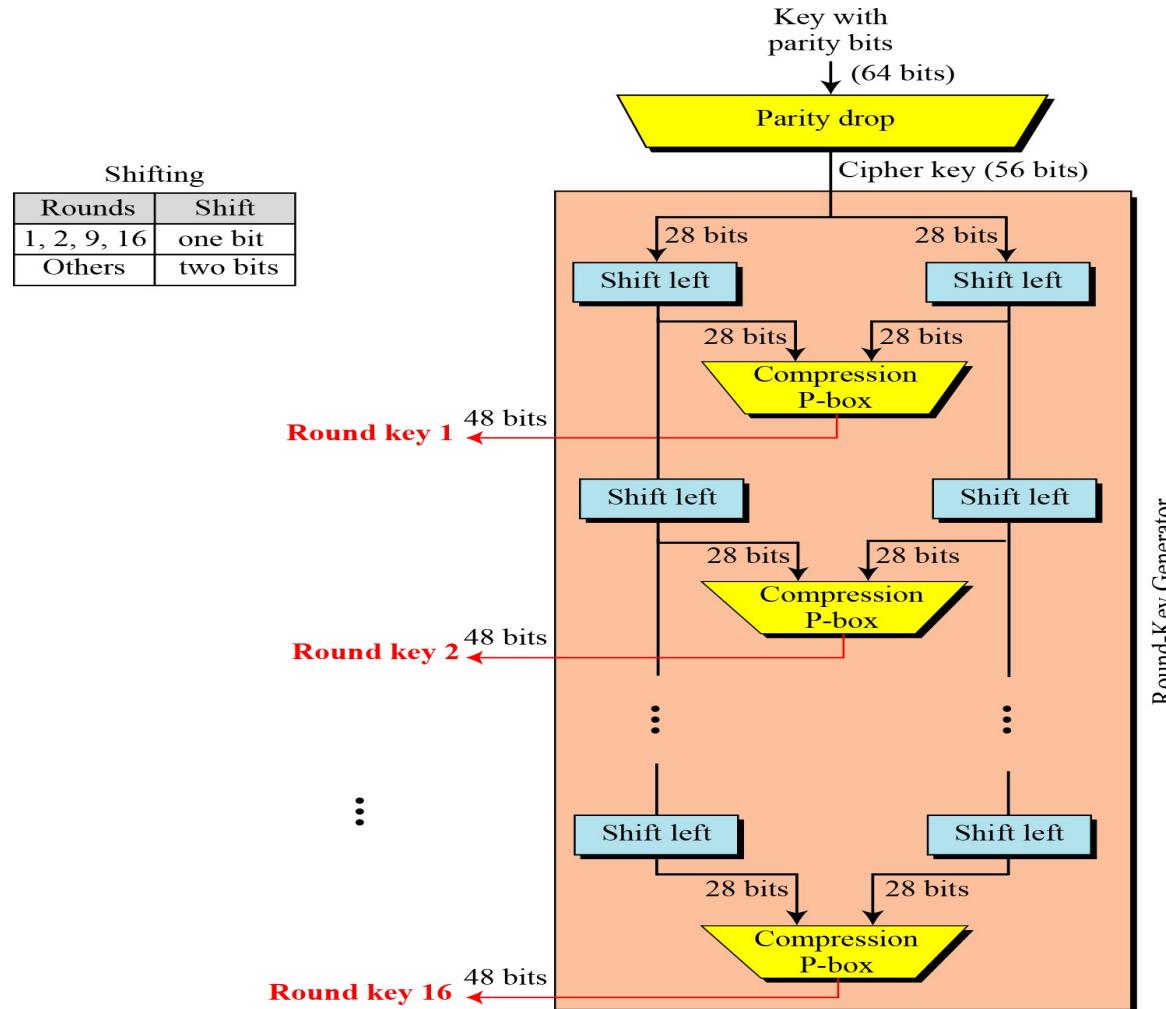


Straight Permutation

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Straight permutation table

Key Generation



Key Generation

Parity-bit drop table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Number of bits shifts

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Key Generation

Key-compression table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Cipher and Reverse Cipher

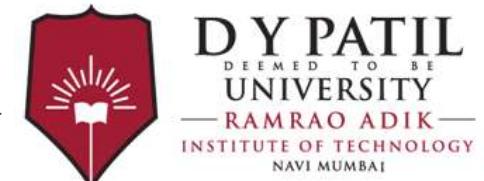
Using mixers and swappers, we can create the cipher and reverse cipher, each having 16 rounds.

First Approach :

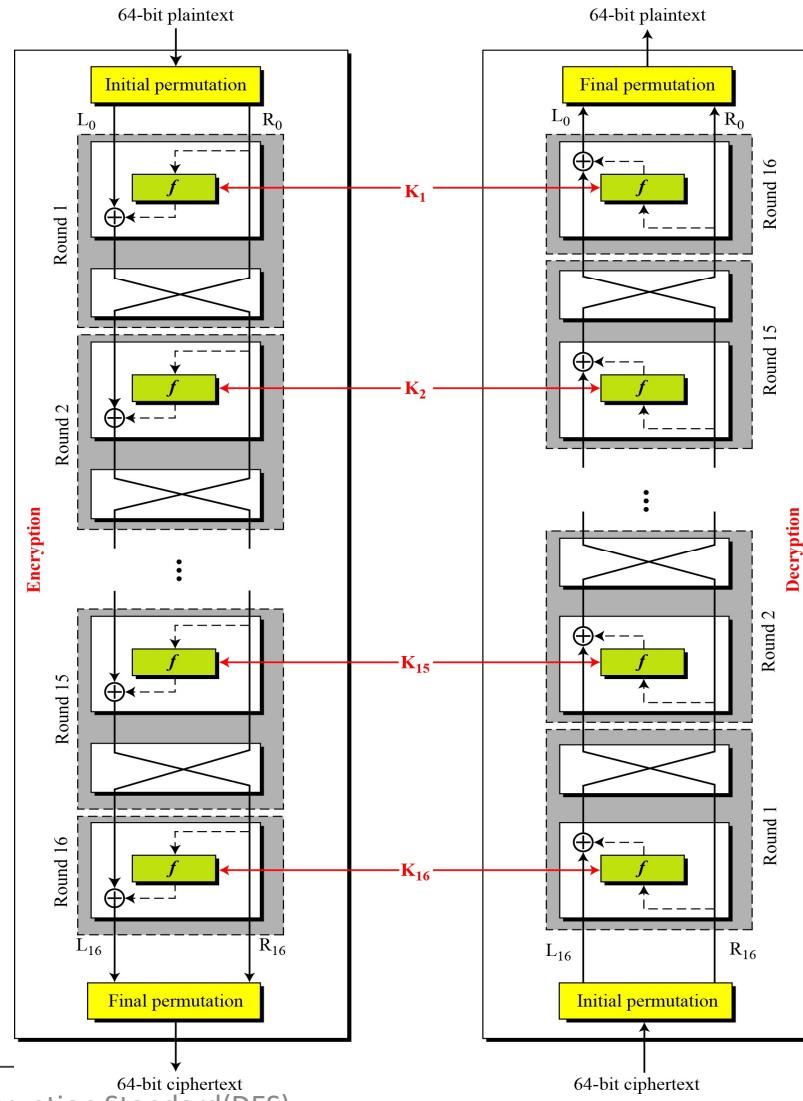
To achieve this goal, one approach is to make the last round (round 16) different from the others; it has only a mixer and no swapper.

Alternative Approach :

We can make all 16 rounds the same by including one swapper to the 16th round and add an extra swapper after that (two swappers cancel the effect of each other).



DES Cipher and Reverse Cipher for the first Approach



DES Example

Plaintext: 123456ABCD132536

CipherText: C0B7A8D05F3A829C

Key: AABB09182736CCDD

Plaintext: 123456ABCD132536

After initial permutation: 14A7D67818CA18AD

After splitting: L₀=14A7D678 R₀=18CA18AD

<i>Round</i>	<i>Left</i>	<i>Right</i>	<i>Round Key</i>
<i>Round 1</i>	18CA18AD	5A78E394	194CD072DE8C
<i>Round 2</i>	5A78E394	4A1210F6	4568581ABCCE
<i>Round 3</i>	4A1210F6	B8089591	06EDA4ACF5B5
<i>Round 4</i>	B8089591	236779C2	DA2D032B6EE3

DES Example(Cont....)

<i>Round 5</i>	236779C2	A15A4B87	69A629FEC913
<i>Round 6</i>	A15A4B87	2E8F9C65	C1948E87475E
<i>Round 7</i>	2E8F9C65	A9FC20A3	708AD2DDB3C0
<i>Round 8</i>	A9FC20A3	308BEE97	34F822F0C66D
<i>Round 9</i>	308BEE97	10AF9D37	84BB4473DCCC
<i>Round 10</i>	10AF9D37	6CA6CB20	02765708B5BF
<i>Round 11</i>	6CA6CB20	FF3C485F	6D5560AF7CA5
<i>Round 12</i>	FF3C485F	22A5963B	C2C1E96A4BF3
<i>Round 13</i>	22A5963B	387CCDAA	99C31397C91F
<i>Round 14</i>	387CCDAA	BD2DD2AB	251B8BC717D0
<i>Round 15</i>	BD2DD2AB	CF26B472	3330C5D9A36D
<i>Round 16</i>	19BA9212	CF26B472	181C5D75C66D
<i>After combination:</i> 19BA9212CF26B472			
<i>Ciphertext:</i> C0B7A8D05F3A829C		<i>(after final permutation)</i>	

DES Properties

Avalanche effect

- Avalanche effect means a small change in the plaintext (or key)
should create a significant change in the ciphertext
- DES strongly support this property

Plaintext	0000000000000000
Key	22234512987ABB23
Ciphertext	4789FD476E82A5F1
Plaintext	0000000000000001
Key	4789FD476E82A5F1
Ciphertext	0A4ED5C15A63FEA3

DES Properties

Completeness

- Completeness effect means that each bit of the ciphertext needs to depend on many bits on the plaintext.
- The confusion and diffusion produced by P-boxes and S-boxes in DES show a very strong completeness effect.

DES Design Criteria

S-Box:

- S-boxes are non-linear.
- If we change single bit in the input, two or more bits will be changed in the output.
- The design provides confusion and diffusion of bits from each round to the next.

P-Box:

- Provide diffusion of bits

Number of Rounds:

- DES uses sixteen rounds of Feistel ciphers.
- The ciphertext is thoroughly a random function of plaintext.



**Unit No: 1
Theory**

Unit Name: Introduction & Number

Lecture No: 2 Double DES, Triple DES



DES Weaknesses

1. Weaknesses in S-boxes

- In S-box 4, the last 3 output bits can be derived in the same way as the first output bit by complementing some of the input bits.
- Two specifically chosen inputs to an S-box array can create the same output
- It is possible to obtain the same output in a single round by changing bits in only three neighboring S-boxes.

DES Weaknesses

2. Weaknesses in P-boxes

- It is not clear why the designers of DES used initial and final permutations; these have no security benefits.
- In the expansion permutation (inside the function), the first and fourth bits of every 4-bit series are repeated.

DES Weaknesses

3. Weaknesses in Key

Table 6.18 *Weak keys*

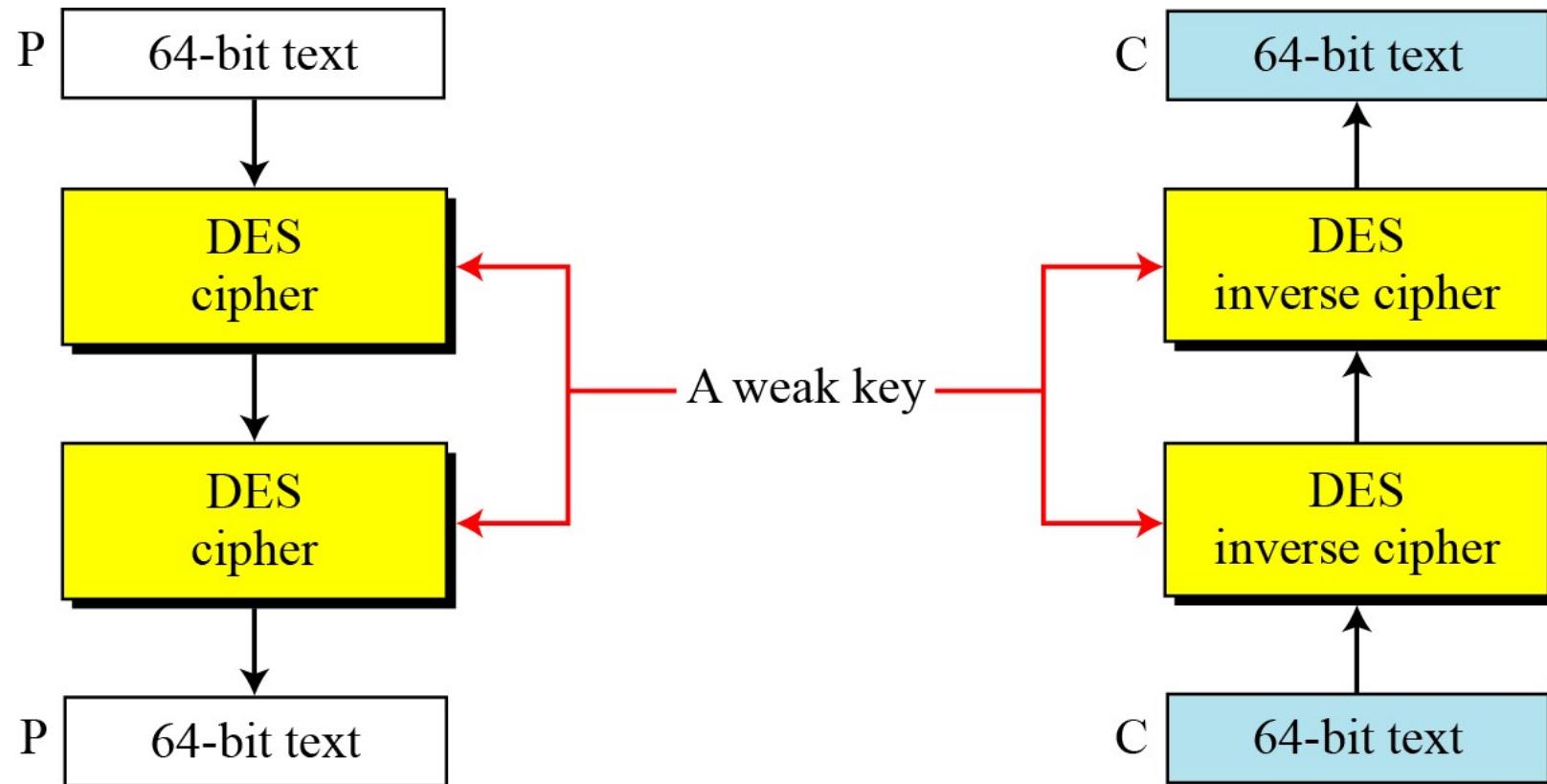
<i>Keys before parities drop (64 bits)</i>	<i>Actual key (56 bits)</i>
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF

DES Weaknesses

3. Weaknesses in Key

- Let us try the first weak key to encrypt a block two times. After two encryptions with the same key the original plaintext block is created
- The encryption algorithm is used two times, not one encryption followed by another decryption

Double Encryption and Decryption with Weak Key



DES Weaknesses

Weaknesses in Key

Table 6.19 *Semi-weak keys*

<i>First key in the pair</i>	<i>Second key in the pair</i>
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E1 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
EOF E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

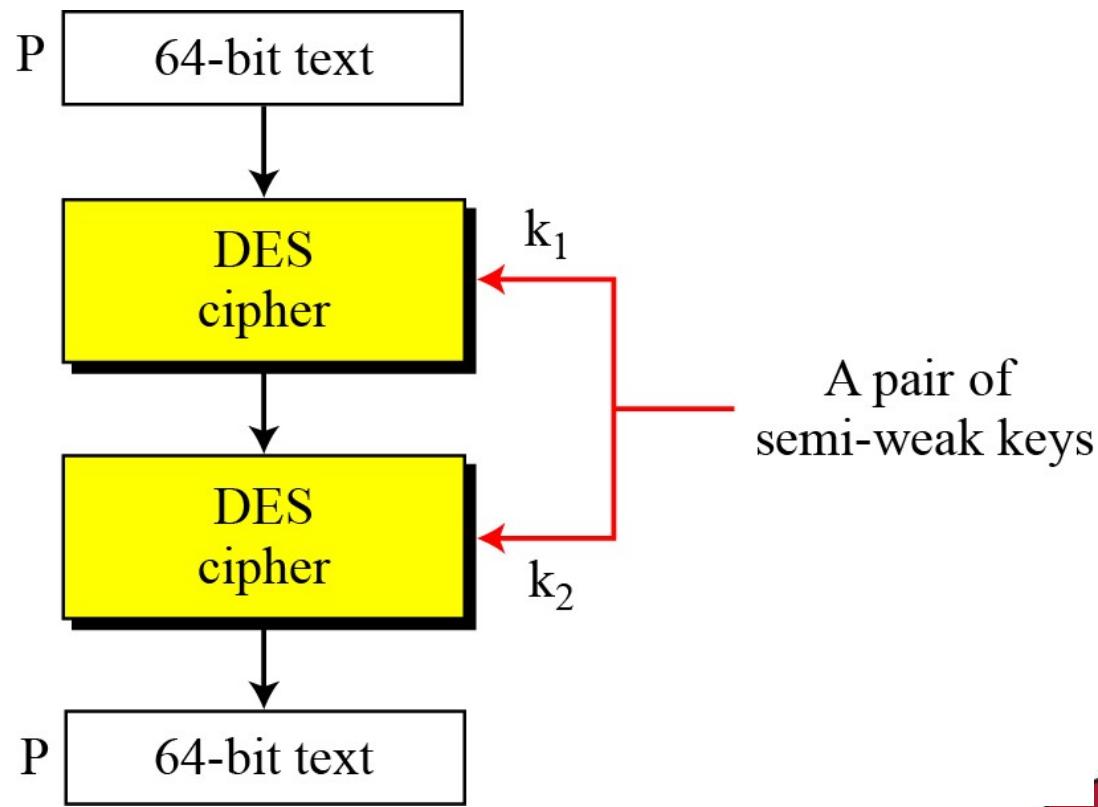
DES Weaknesses

Weaknesses in Key

<i>Round key 1</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 2</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 3</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 4</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 5</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 6</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 7</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 8</i>	6EAC1ABCE642	9153E54319BD
<i>Round key 9</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 10</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 11</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 12</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 13</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 14</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 15</i>	9153E54319BD	6EAC1ABCE642
<i>Round key 16</i>	6EAC1ABCE642	9153E54319BD

DES Weaknesses

Weaknesses in Key



Double DES

- The first approach is to use double DES (2DES).

Meet-in-the-Middle Attack

- However, using a known-plaintext attack called meet-in-the-middle attack proves that double DES improves this vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112})

Security of DES

Brute-Force Attack

- DES can be broken using 2^{55} encryptions.

Differential Cryptanalysis

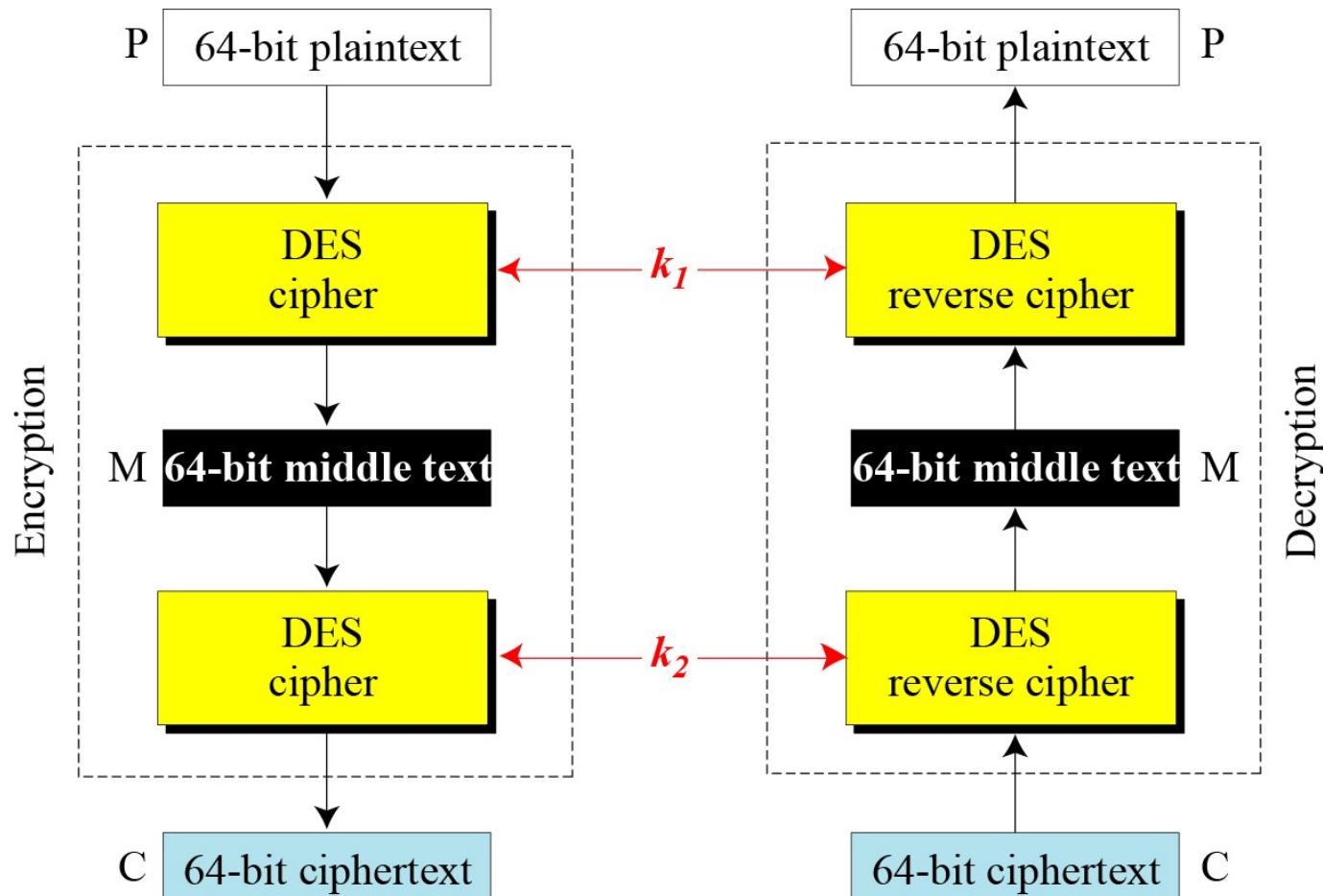
- Chosen Plaintext Attack has been revealed that the designers of DES already knew about this type of attack and designed S-boxes and chose 16 as the number of rounds to make DES specifically resistant to this type of attack

Security of DES

Linear Cryptanalysis

- known Plaintext attack
- Linear cryptanalysis is newer than differential cryptanalysis.
- DES is more vulnerable to linear cryptanalysis than to differential cryptanalysis.
- S-boxes are not very resistant to linear cryptanalysis.
- It has been shown that DES can be broken using 2^{43} pairs of known plaintexts. However, from the practical point of view, finding so many pairs is very unlikely.

Double DES



Double DES

$$M = E_{k_1}(P)$$

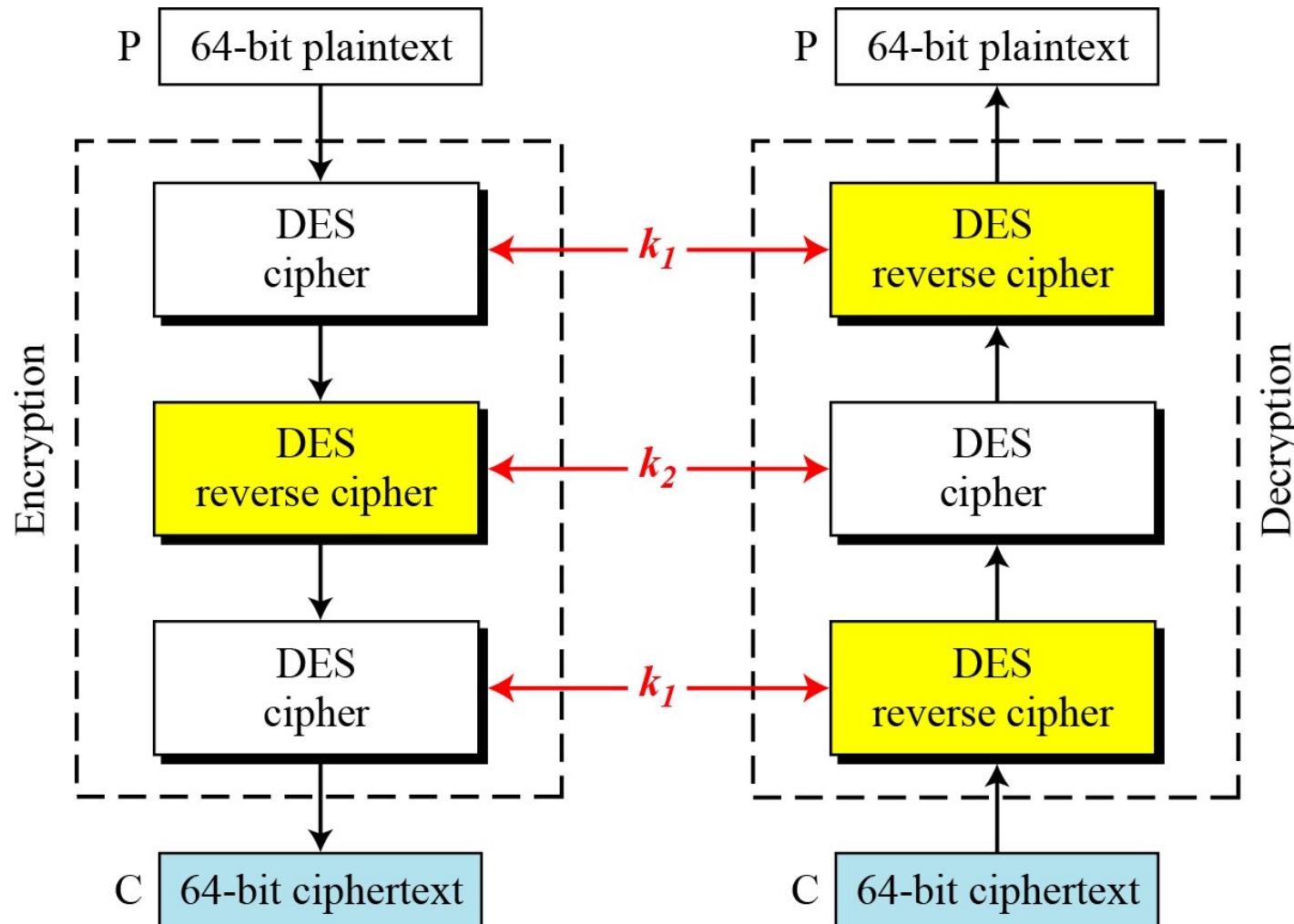
M	k_1
●	

$$M = D_{k_2}(C)$$

M	k_2
●	

Find equal M's and record
corresponding k_1 and k_2

Triple DES



Triple DES

Triple DES with Three Keys

- The possibility of known-plaintext attacks on triple DES with two keys has enticed some applications to use triple DES with three keys
- Triple DES with three keys is used by many applications such as PGP

Security of DES

- DES, as the first important block cipher, has gone through much scrutiny.
- Among the attempted attacks, three are of interest:
 - Brute-Force Attack
 - Differential Cryptanalysis
 - Linear Cryptanalysis

Advanced Encryption Standard(AES)

- Developed at NIST in 1997
- AES is a non-Feistel cipher(only invertible components) that encrypts and decrypts a data block of 128 bits
- It uses 10, 12, or 14 rounds
- The key size, which can be 128, 192, or 256 bits, depends on the number of rounds

**Unit No: 1
Theory**

Unit Name: Introduction & Number

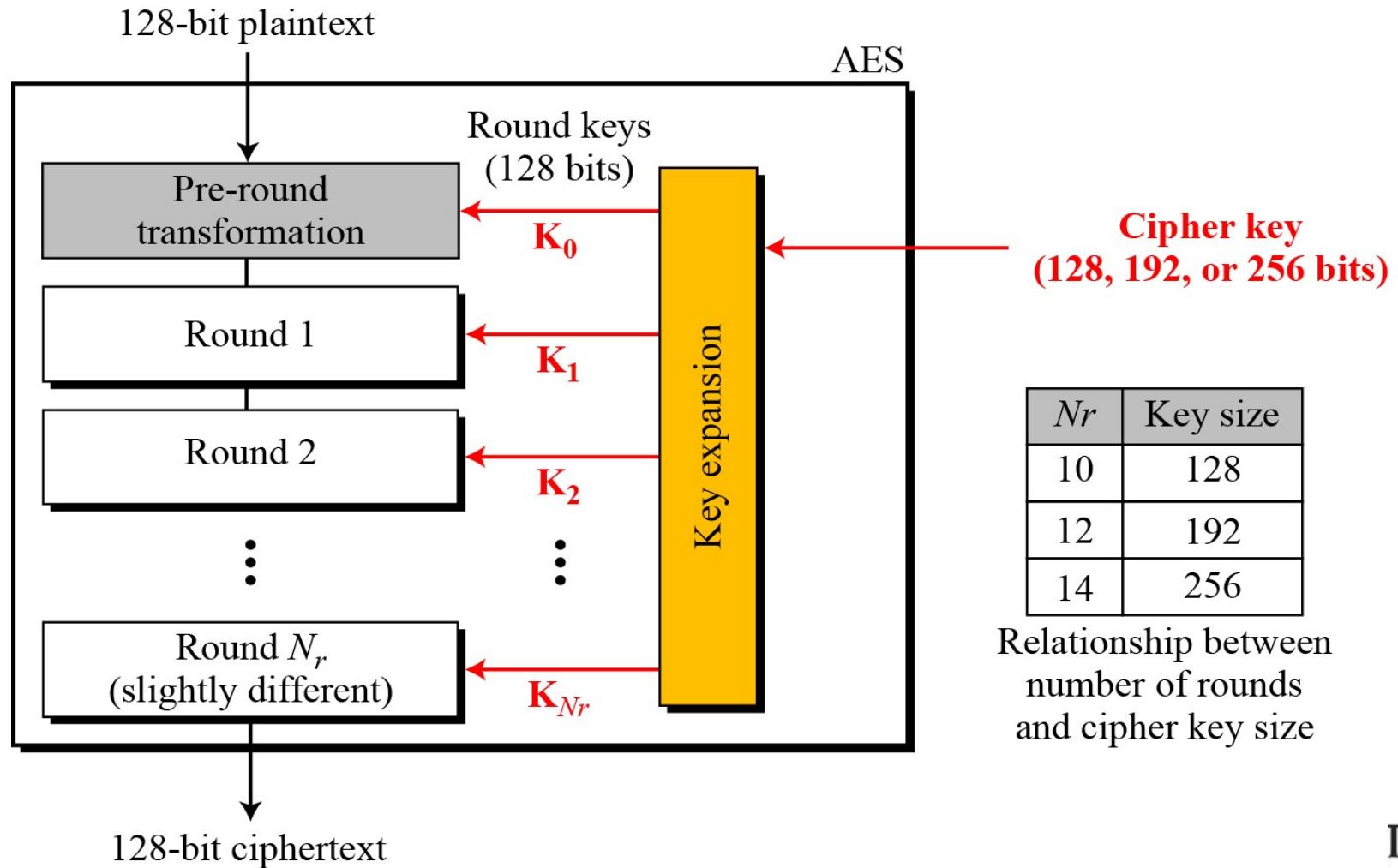
Lecture No: 1

Advanced Encryption

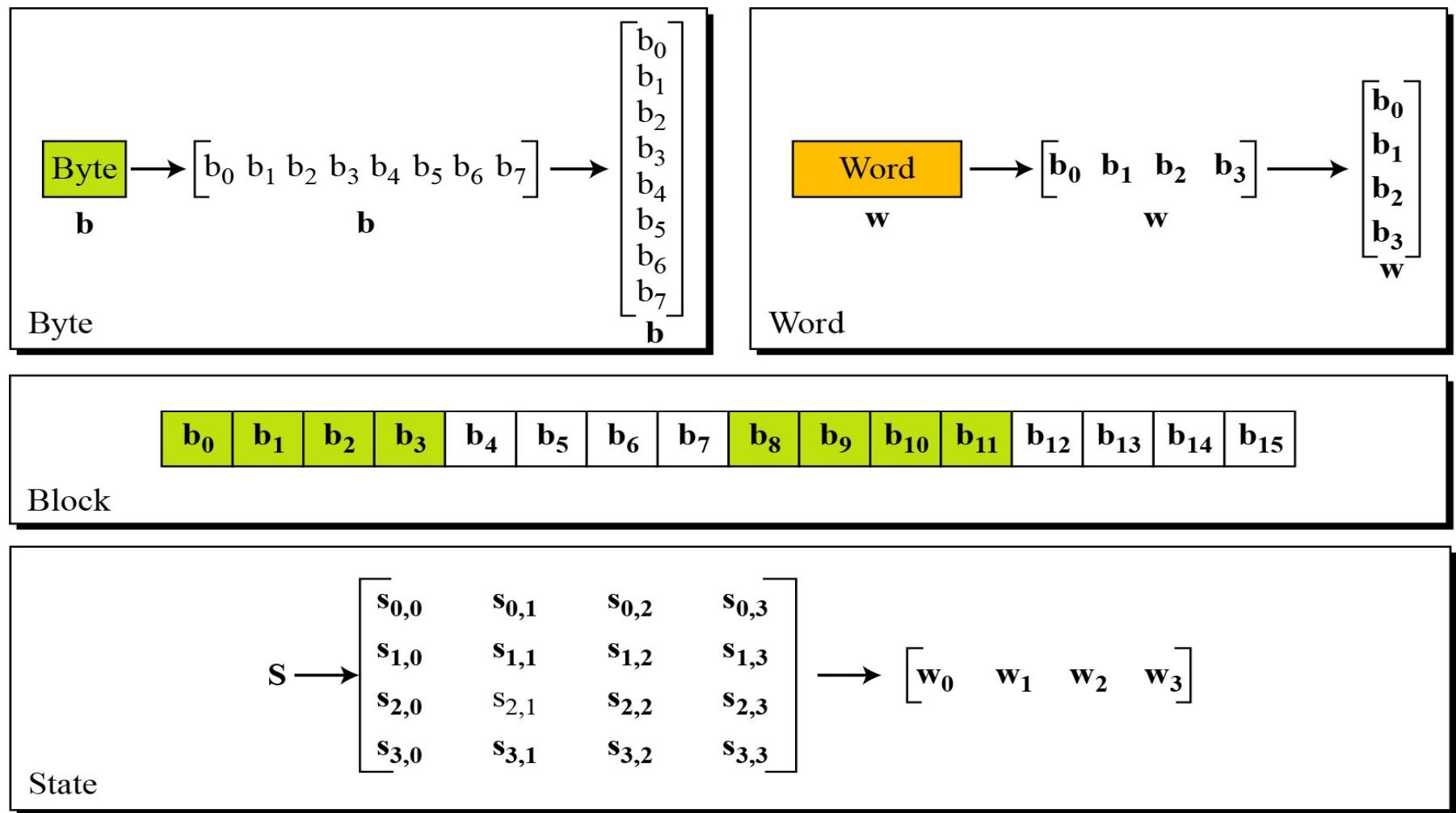
Standard(AES)



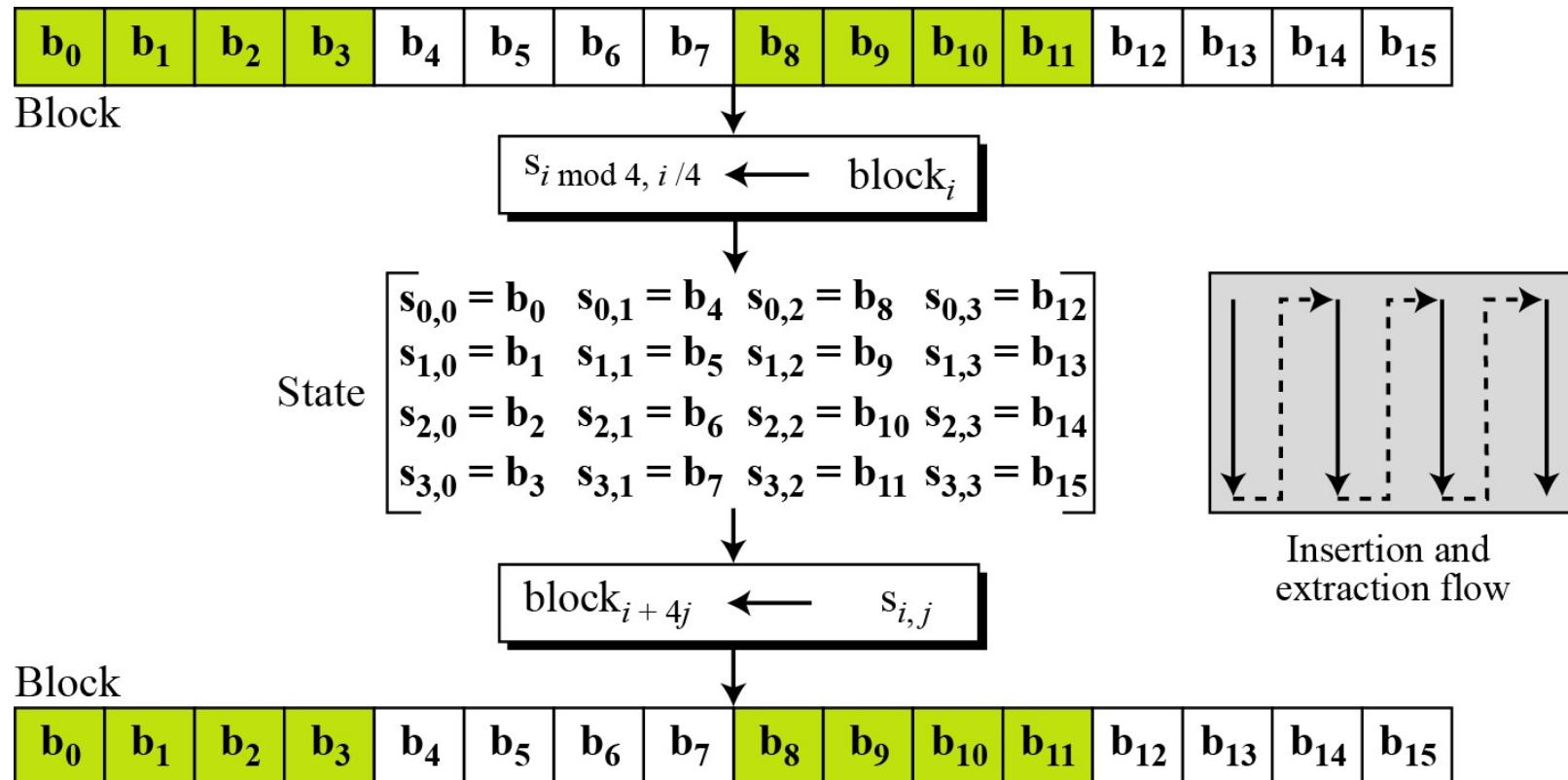
Advanced Encryption Standard(AES)



Data Units in AES



Block-to-state and state-to-block Transformation

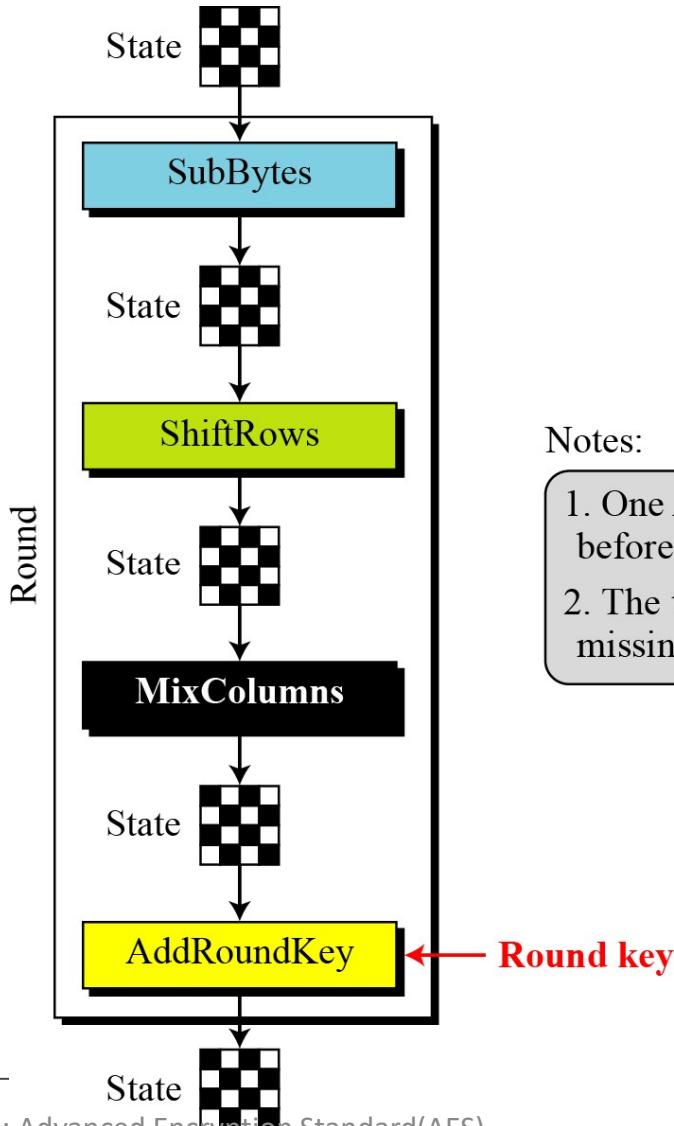


Changing Plaintext to State

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	23	19	19

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \text{ State}$$

Structure of Each Round at the Encryption Side



Notes:

1. One AddRoundKey is applied before the first round.
2. The third transformation is missing in the last round.

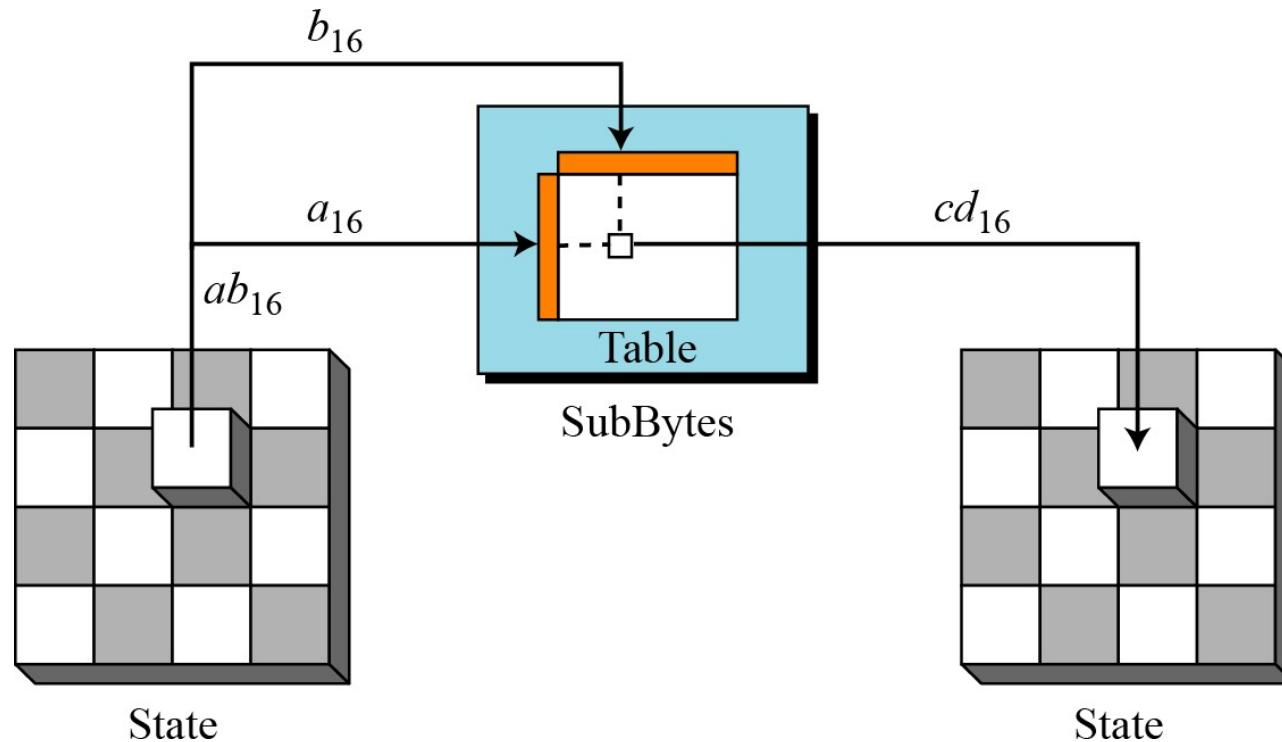
AES: Transformations

- AES uses four types of transformations:
 - ✓ Substitution
 - ✓ Permutation
 - ✓ Mixing
 - ✓ key-adding

AES: Transformations

- AES uses two invertible substitution transformations :
 - ✓ SubBytes :Byte is substituted as two hexadecimal digits.
 - ✓ InvSubBytes

SubBytes Transformations



SubBytes Transformations

Table 7.1 SubBytes transformation table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8

SubBytes Transformations

Table 7.1 SubBytes transformation table (continued)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

InvSubBytes Transformations

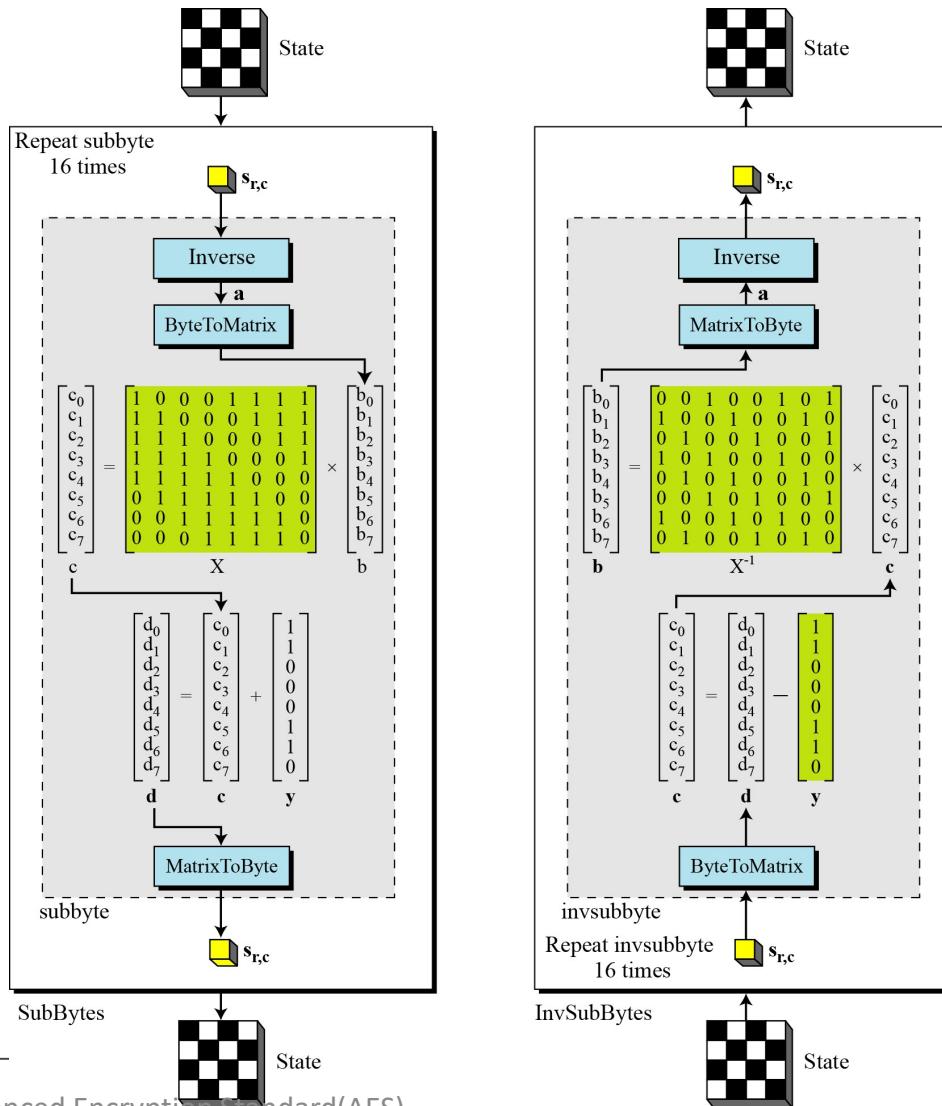
Table 7.2 *InvSubBytes transformation table*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B

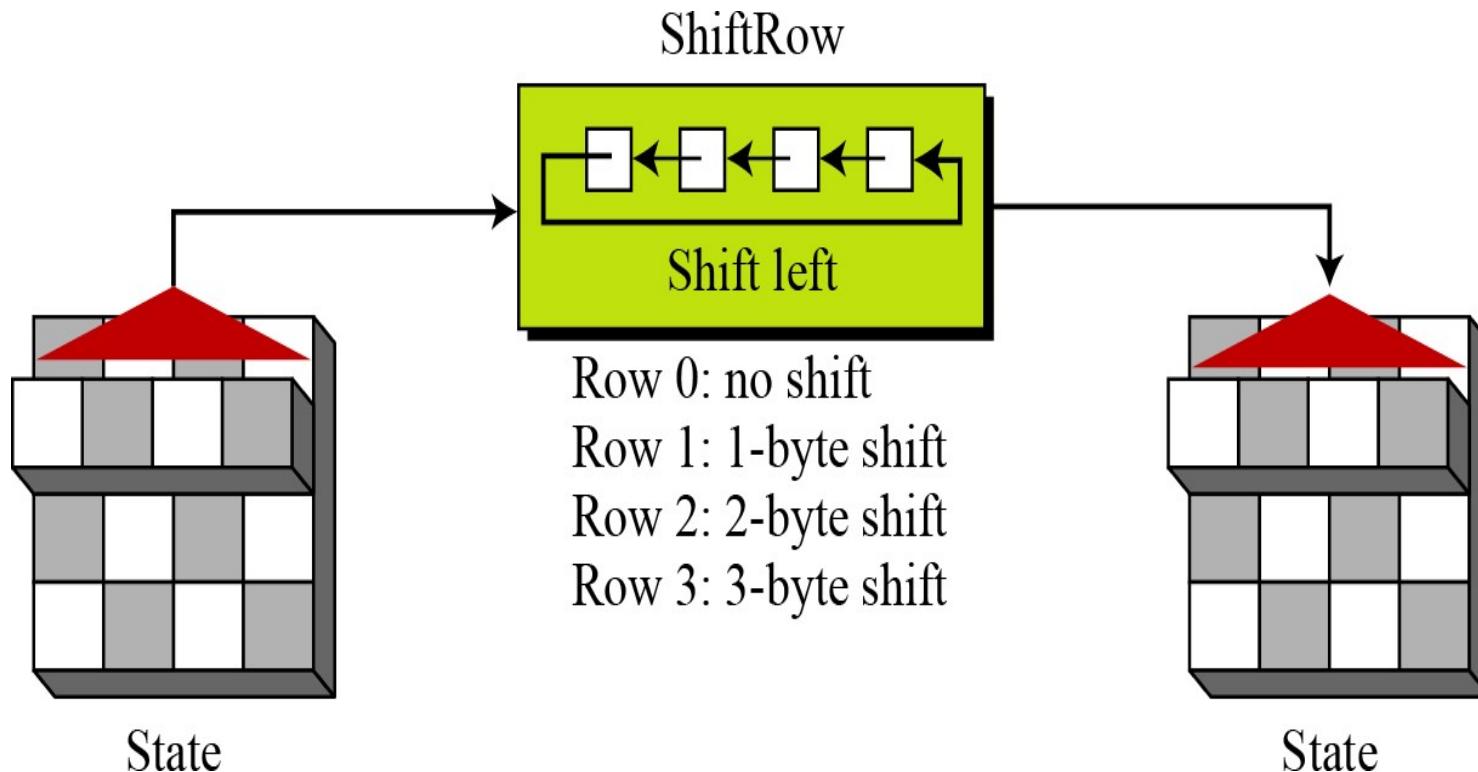
InvSubBytes Transformations

8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

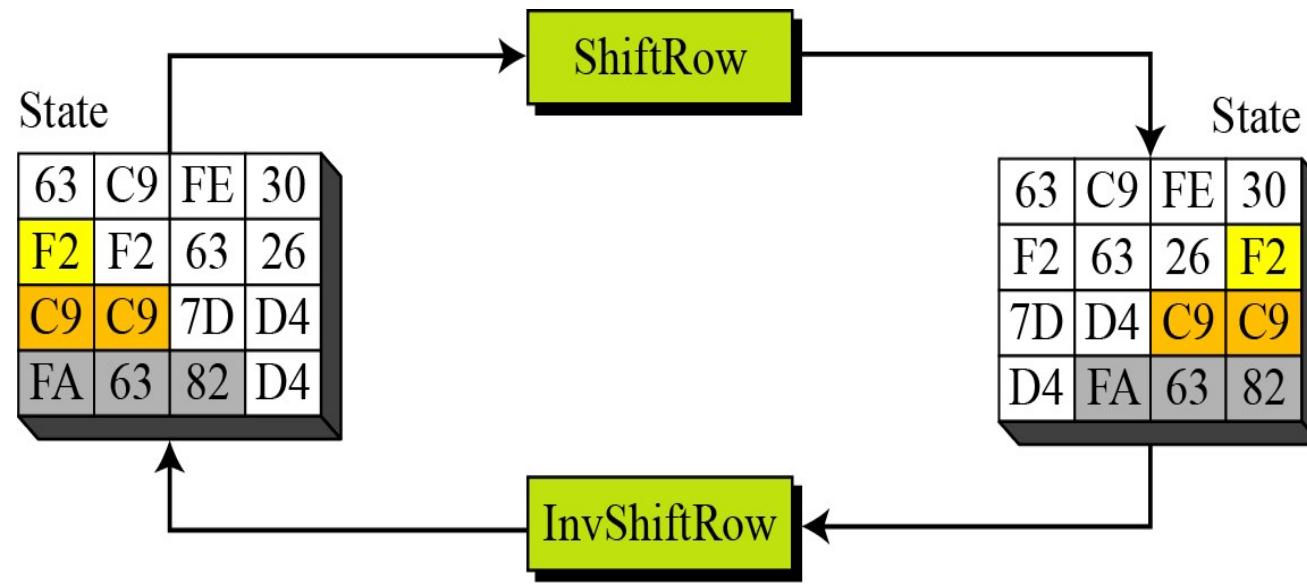
SubBytes and InvSubBytes Process



ShiftRows



ShiftRows/InvShiftRows



Mixing

- It is interbyte transformation which changes the bits inside a byte, based on the bits inside the neighboring bytes.
- Mixing bytes provide diffusion at the bit level.

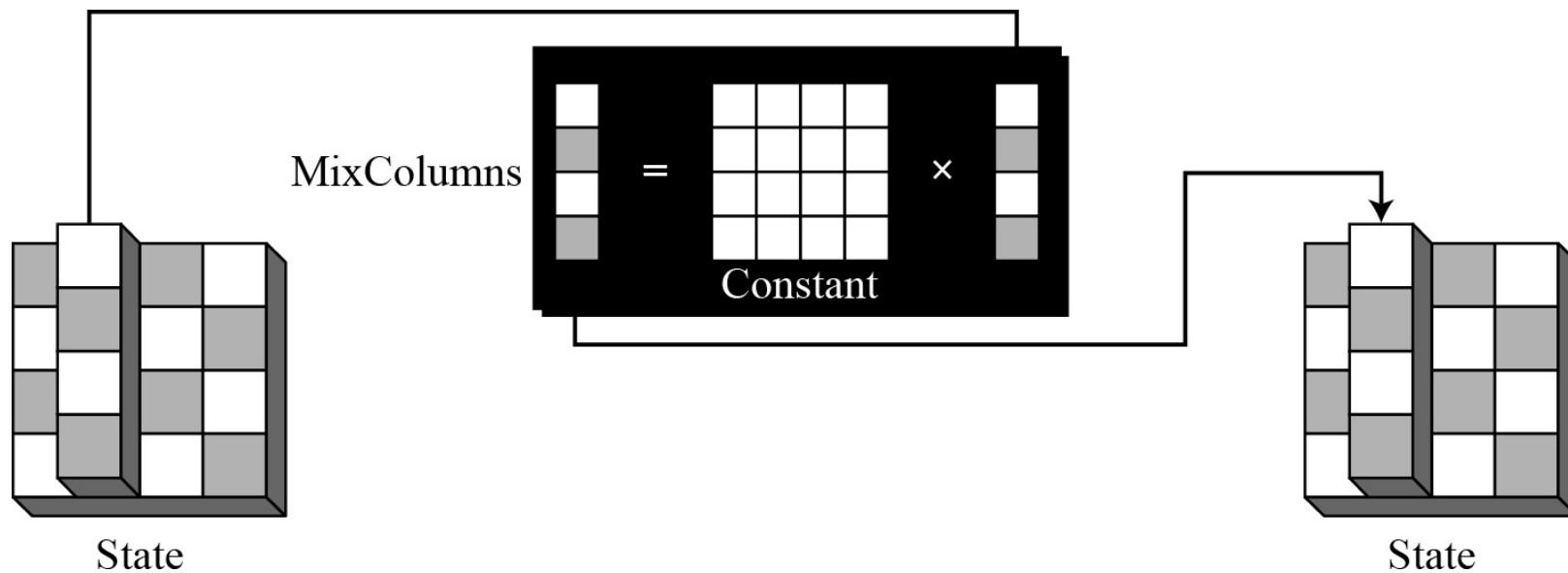
$$\begin{array}{l} ax + by + cz + dt \\ ex + fy + gz + ht \\ ix + jy + kz + lt \\ mx + ny + oz + pt \end{array} \xrightarrow{\text{New matrix}} = \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \times \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix}$$

Constant matrix

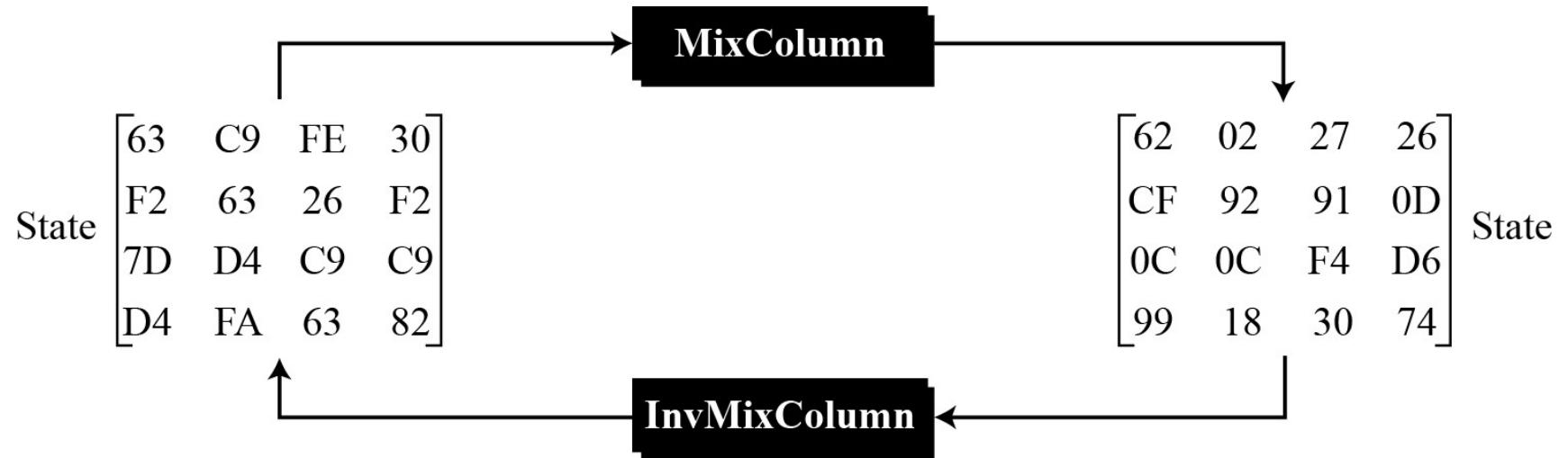
Mixing bytes using matrix multiplication

MixColumns

- It operates at the column level
- It transforms each column of the state to a new column.

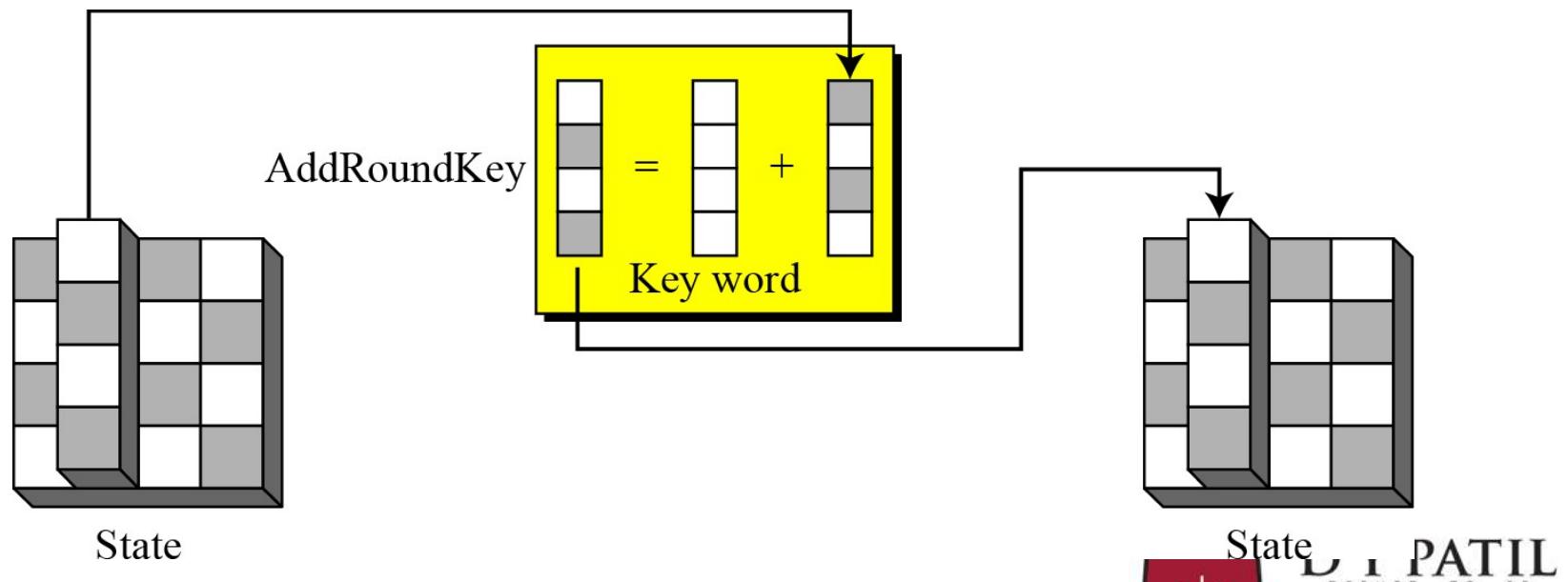


MixColumns/InvMixColumns

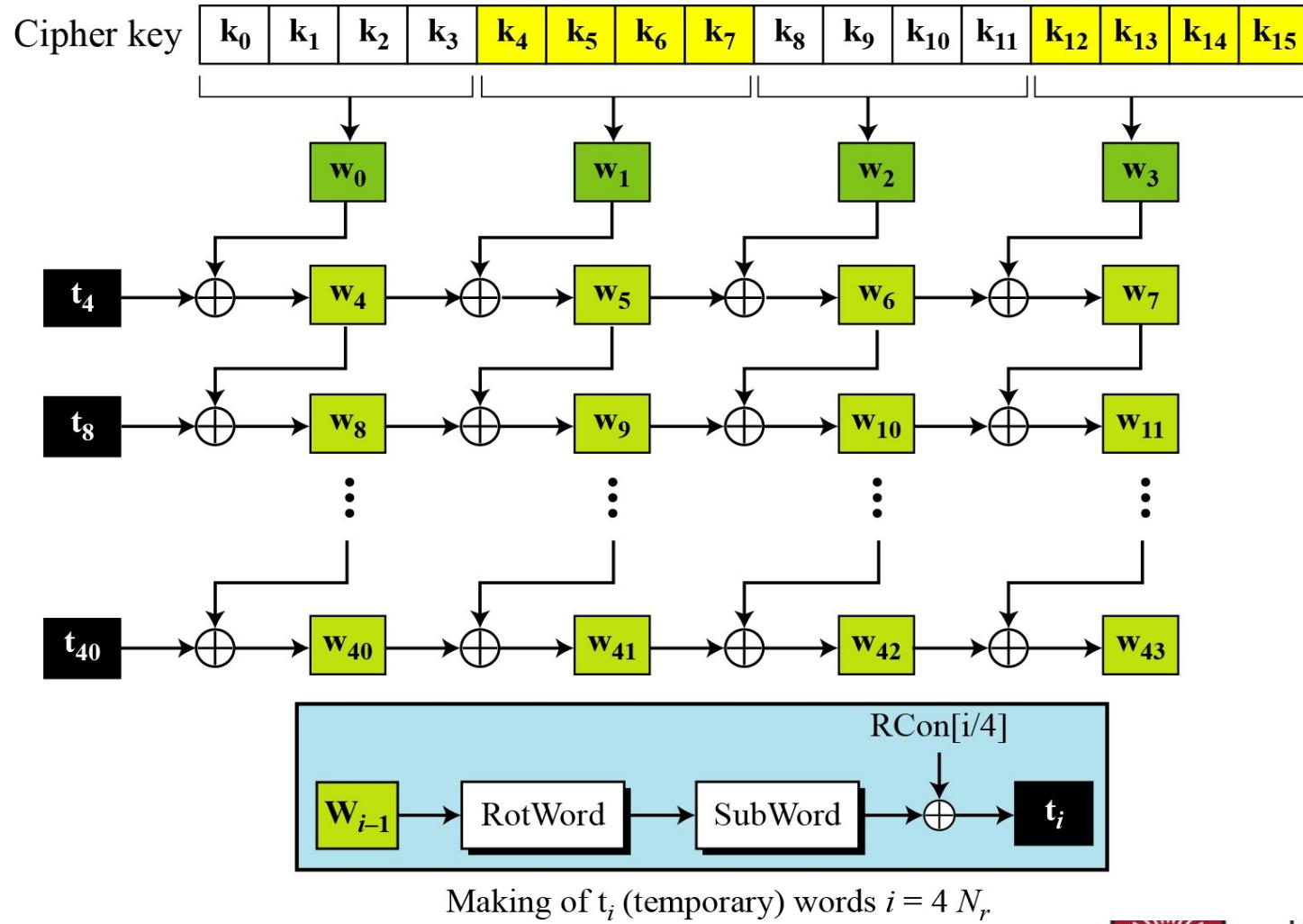


AddRoundKey

- It proceeds one column at a time.
- It adds a round key word with each state column matrix
- The operation in AddRoundKey is matrix addition.



Key Expansion in AES-128

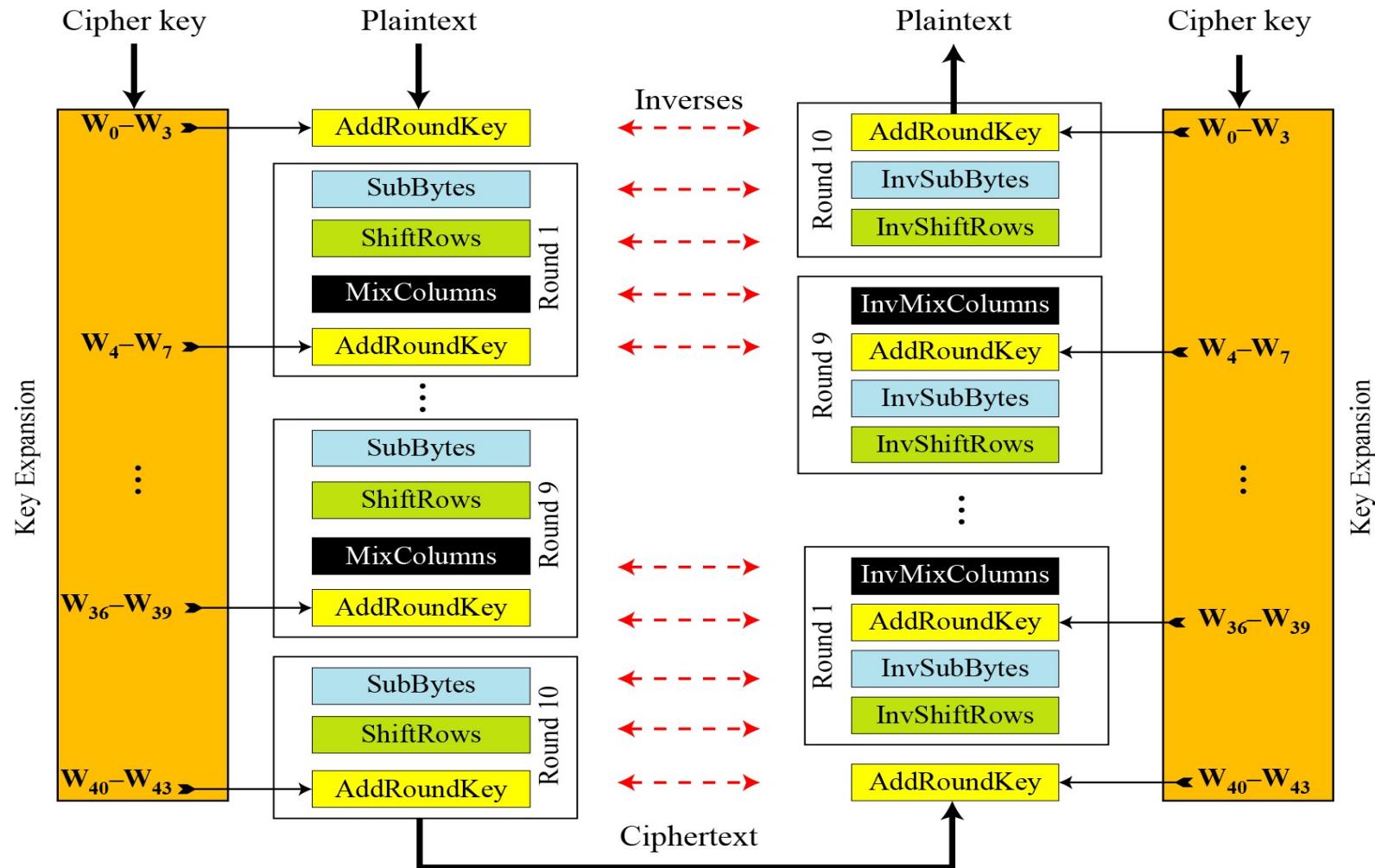


Key Expansion in AES-128

Table 7.4 *RCon constants*

Round	Constant (RCon)	Round	Constant (RCon)
1	$(\underline{01} \ 00 \ 00 \ 00)_{16}$	6	$(\underline{20} \ 00 \ 00 \ 00)_{16}$
2	$(\underline{02} \ 00 \ 00 \ 00)_{16}$	7	$(\underline{40} \ 00 \ 00 \ 00)_{16}$
3	$(\underline{04} \ 00 \ 00 \ 00)_{16}$	8	$(\underline{80} \ 00 \ 00 \ 00)_{16}$
4	$(\underline{08} \ 00 \ 00 \ 00)_{16}$	9	$(\underline{1B} \ 00 \ 00 \ 00)_{16}$
5	$(\underline{10} \ 00 \ 00 \ 00)_{16}$	10	$(\underline{36} \ 00 \ 00 \ 00)_{16}$

AES Cipher and Inverse Cipher



Thank You

