Cryptography and Computer Security (CSS)

Lecture # 3

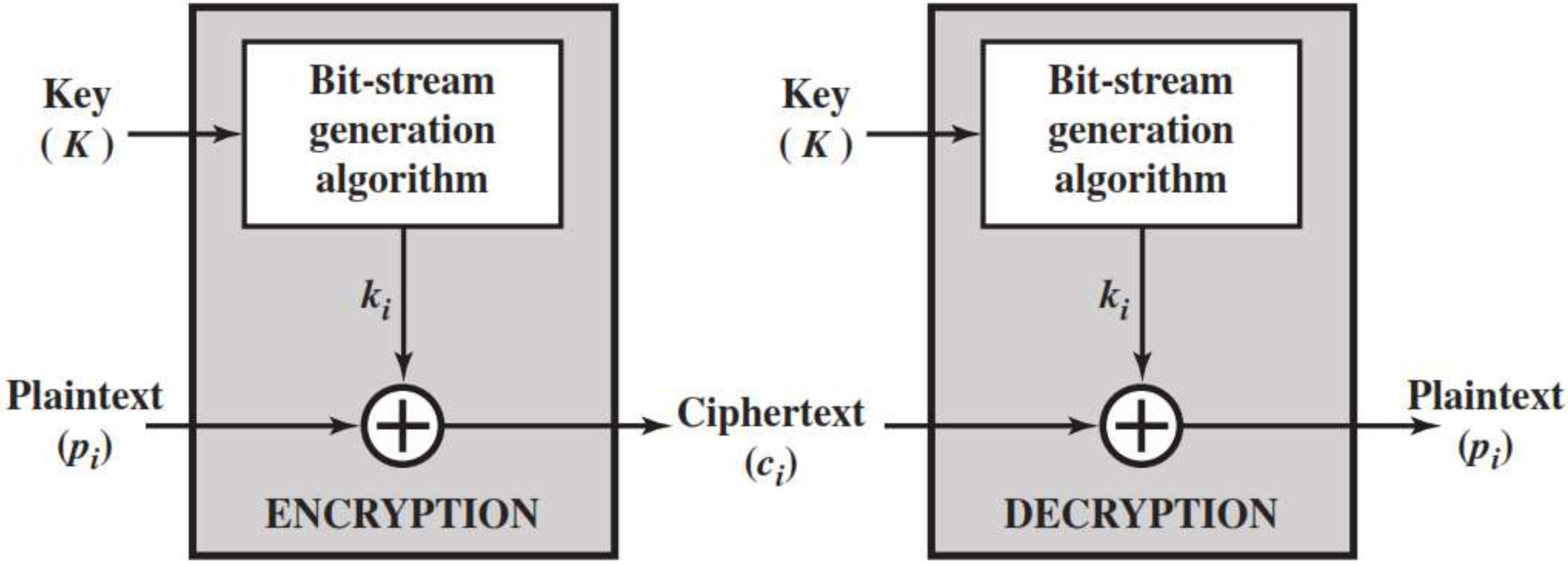
INTRODUCTION
TO
CSS COURSE
(CS401)

Unit II
Symmetric Cryptography Techniques

- Stream ciphers and block ciphers
- Block Cipher structure
- Data Encryption standard (DES)
- Design principles of block cipher
- AES with structure
- AES Transformation functions
- Key expansion

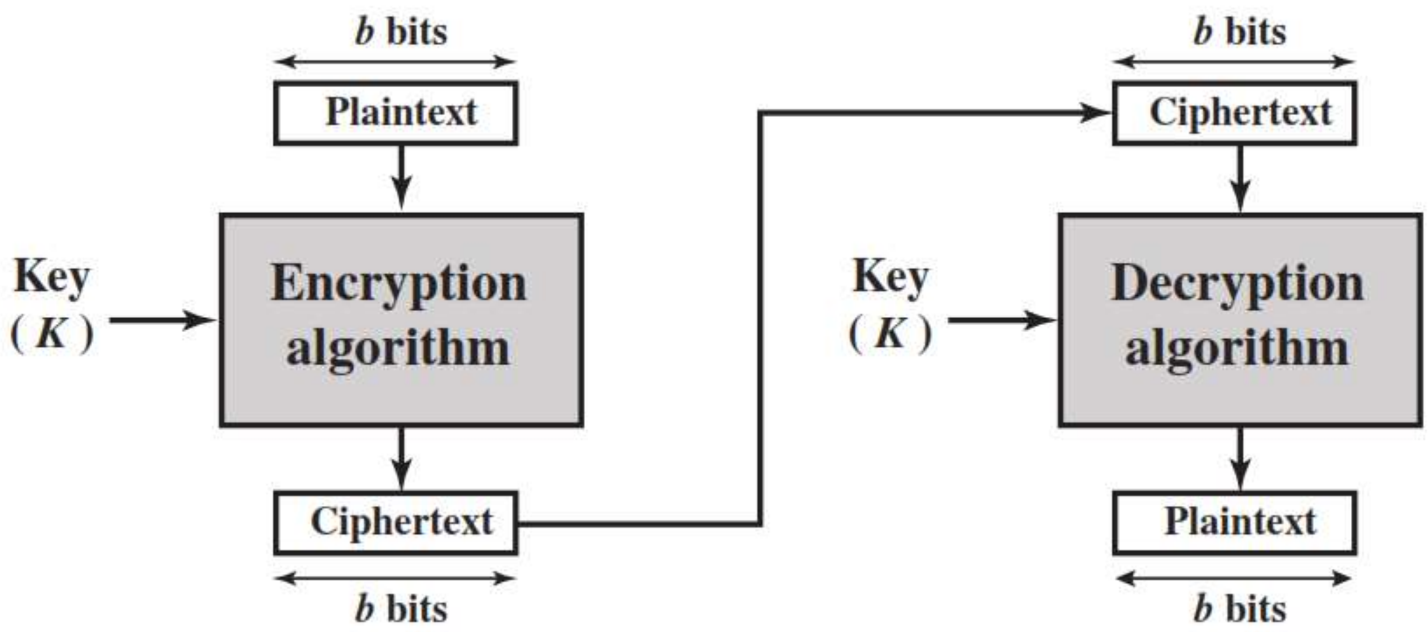
Stream Cipher

- A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time.
- Examples of classical stream ciphers are Autokeyed Vigenère cipher ,A5/1, RC4 and Vernam cipher.



Block Cipher

- A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Typically, a block size of **64 or 128** bits is used.
- Examples are Feistel Cipher, DES, Triple DES and AES



Diffusion and Confusion

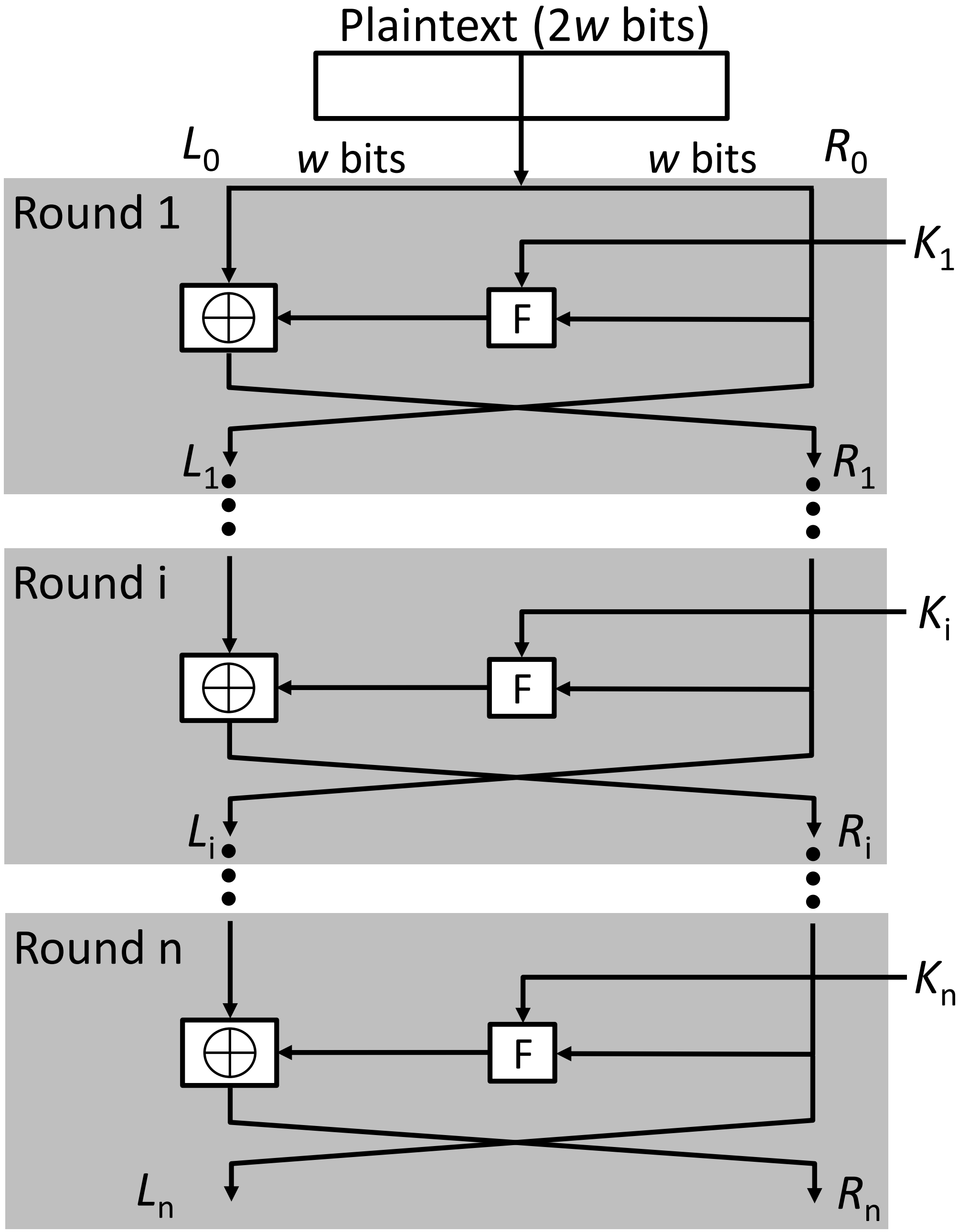
- **Diffusion** hides the relationship between the ciphertext and the plaintext.
- This is achieved by having each plaintext digit affect the value of many ciphertext digits.
- This is achieved by the use of Transposition/permutation/p-box.

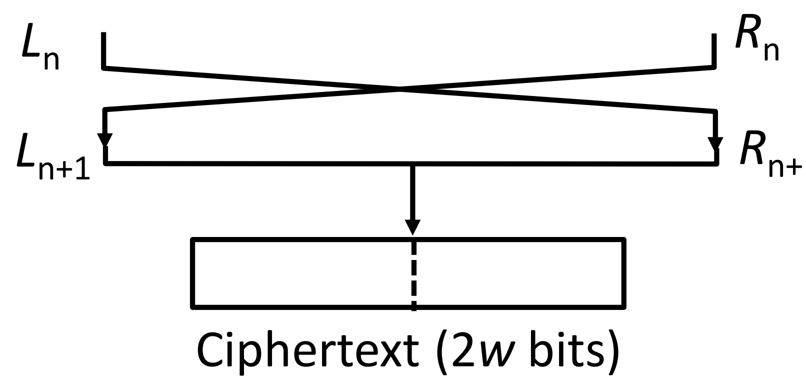
- **Confusion** hides the relationship between the ciphertext and the key.
- This is achieved by the use of a complex substitution algorithm or s-box.

Stream Cipher vs Block Cipher

	Stream Cipher	Block Cipher
Length	Bite or Byte	Block size – 64 or 128 bits
Design	Complex	Simple
Principle	Confusion	Confusion and Diffusion
Speed	Faster	Slower
Encryption	CFB (Cipher Feedback) OFB(Output Feedback)	Electronic Code Block(ECB) Cipher Block Chaining(CBC)
Decryption	XOR	Reverse of encryption
Example	Vernam	DES, AES

Feistel Cipher Structure Or Block Cipher Structure



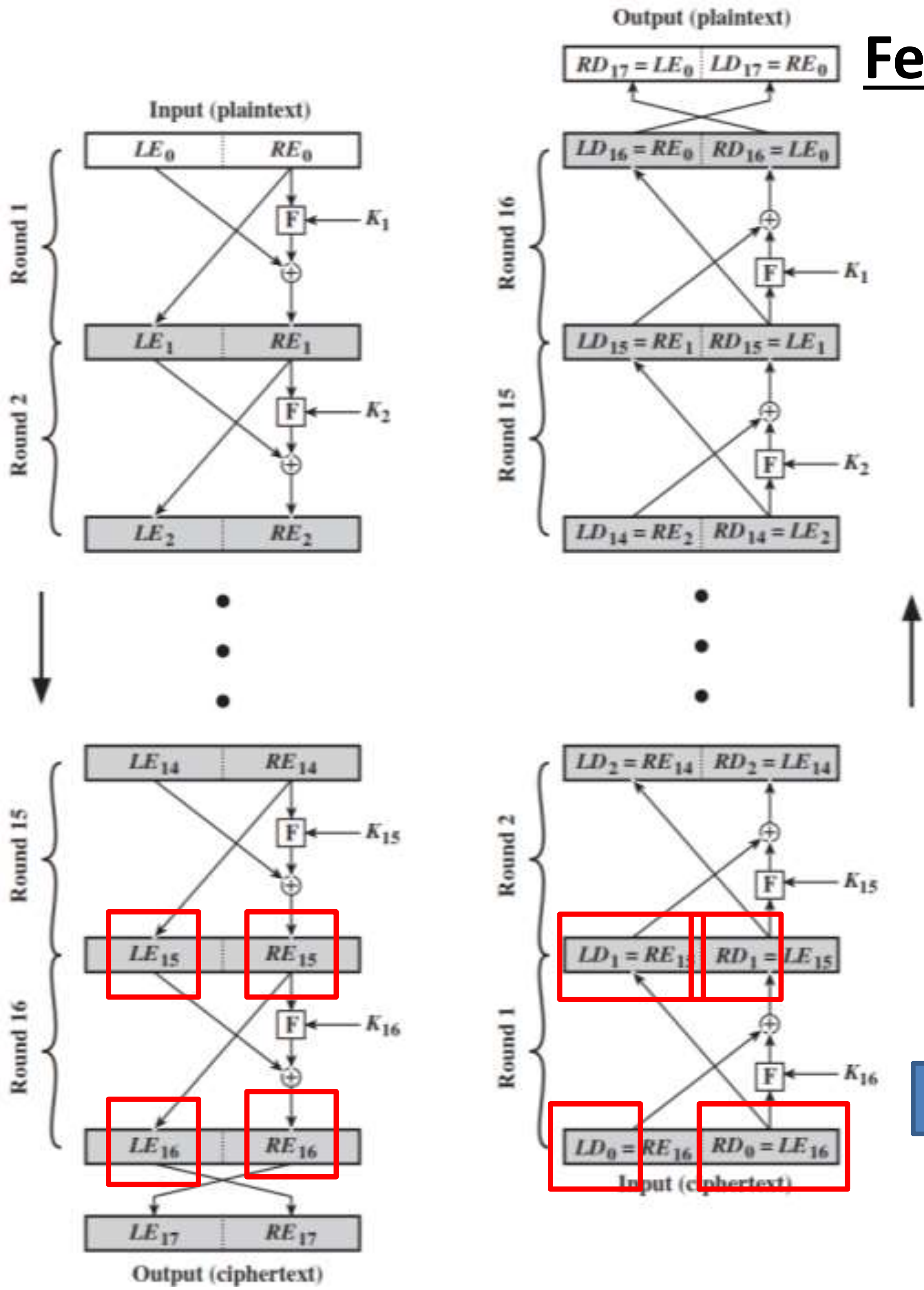


Feistel Cipher Structure

- Input plaintext block of length 2w bits
- key *K*, Sub-keys: K_1, K_2, …, K_n (Derived from *K*)
- All rounds have the same structure.
- A **substitution** is performed by taking exclusive-OR on left half(*L*i) of the data and the output of round function F which has inputs right half(*R*i) and sub key *k*i.
- A **permutation** is performed that consists of interchange of two halves of data.
- This structure is called **Substitution-Permutation Network** (SPN)

Feistel Network Factors

- **Block size:** Common block size of 64-bit. However, the new algorithms uses a 128-bit, 256-bit block size.
- **Key size:** Key sizes of 64 bits or less are now widely considered to be insufficient, These days at least 128 bit, more better, e.g. 192 or 256 bit
- **Number of rounds:** A typical size is 16 rounds.
- **Round function F:** Again, greater complexity generally means greater resistance to cryptanalysis.
- **Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.



Feistel Encryption & Decryption

- Prove that o/p of first round of Decryption is equal to 32-bit swap of i/p of 16th round of Encryption
- $LD_1 = RE_{15}$ & $RD_1 = LE_{15}$
- On Encryption Side:

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

- On Decryption Side:

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \oplus F(RD_0, K_{16})$$

$$= RE_{16} \oplus F(RE_{15}, K_{16})$$

$$= [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16})$$

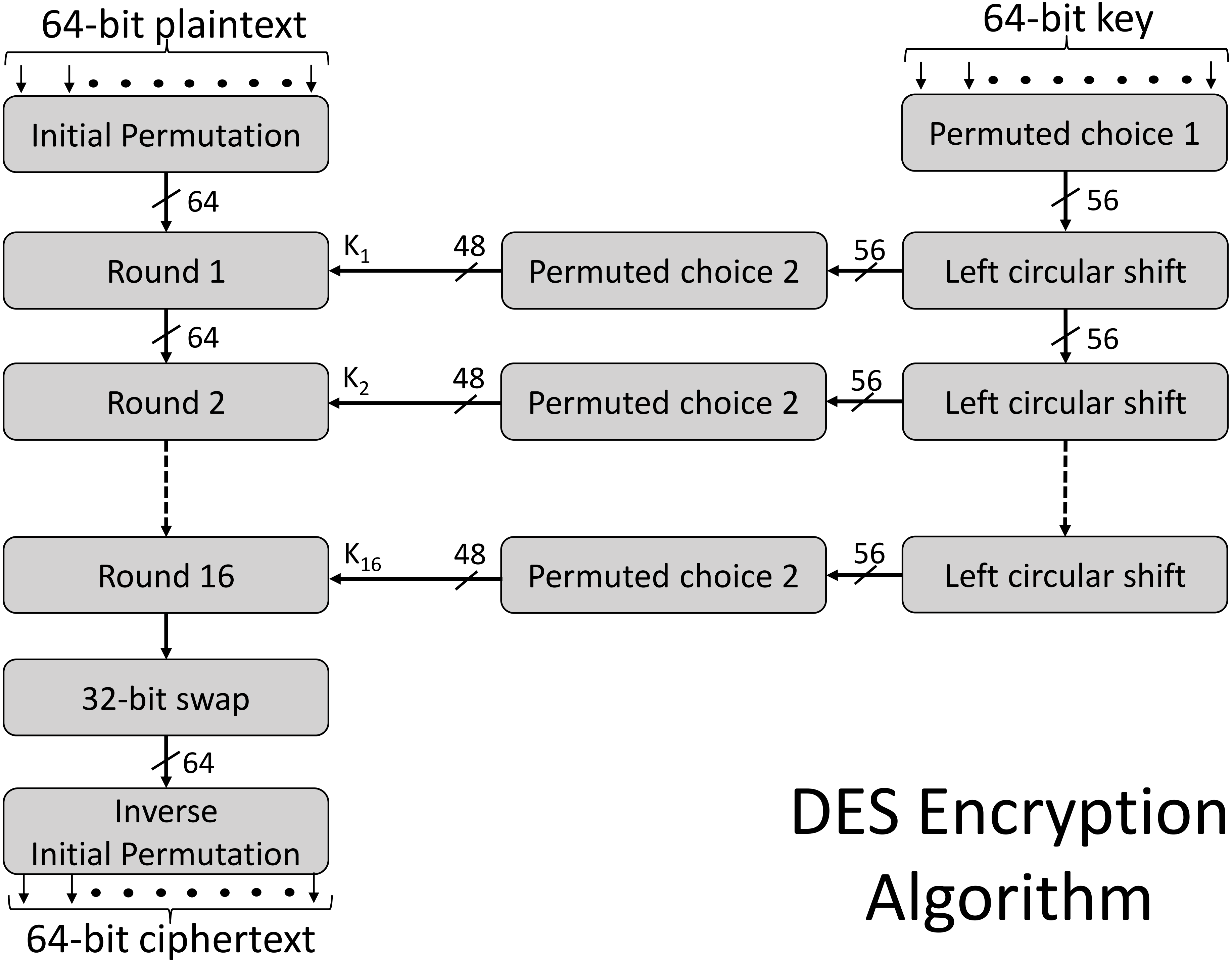
$$\oplus C]$$

Thus,

$$LD_1 = RE_{15} \,\&\, RD_1 = LE_{15}$$

Data Encryption Standard (DES)

- Symmetric Block Cipher
- A.k.a. - Data Encryption Algorithm (DEA)
- Adopted in NIST in 1977
- Input – 64 bits as block
- Output – 64 bits as block
- Main Key Size – 64-bit, with only 56-bit effective (i.e. Subkey)
- Round Key – 48 bits
- Number of Rounds: 16
- Advanced Encryption Standard (AES) in 2001



DES Encryption Algorithm

Initial Permutation

- First, the 64-bit plaintext passes through an **initial permutation** (IP) that rearranges the bits to produce the permuted input.

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

$\Rightarrow$

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	49	39	31	23	15	7

Inverse Initial Permutation

- Finally, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

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

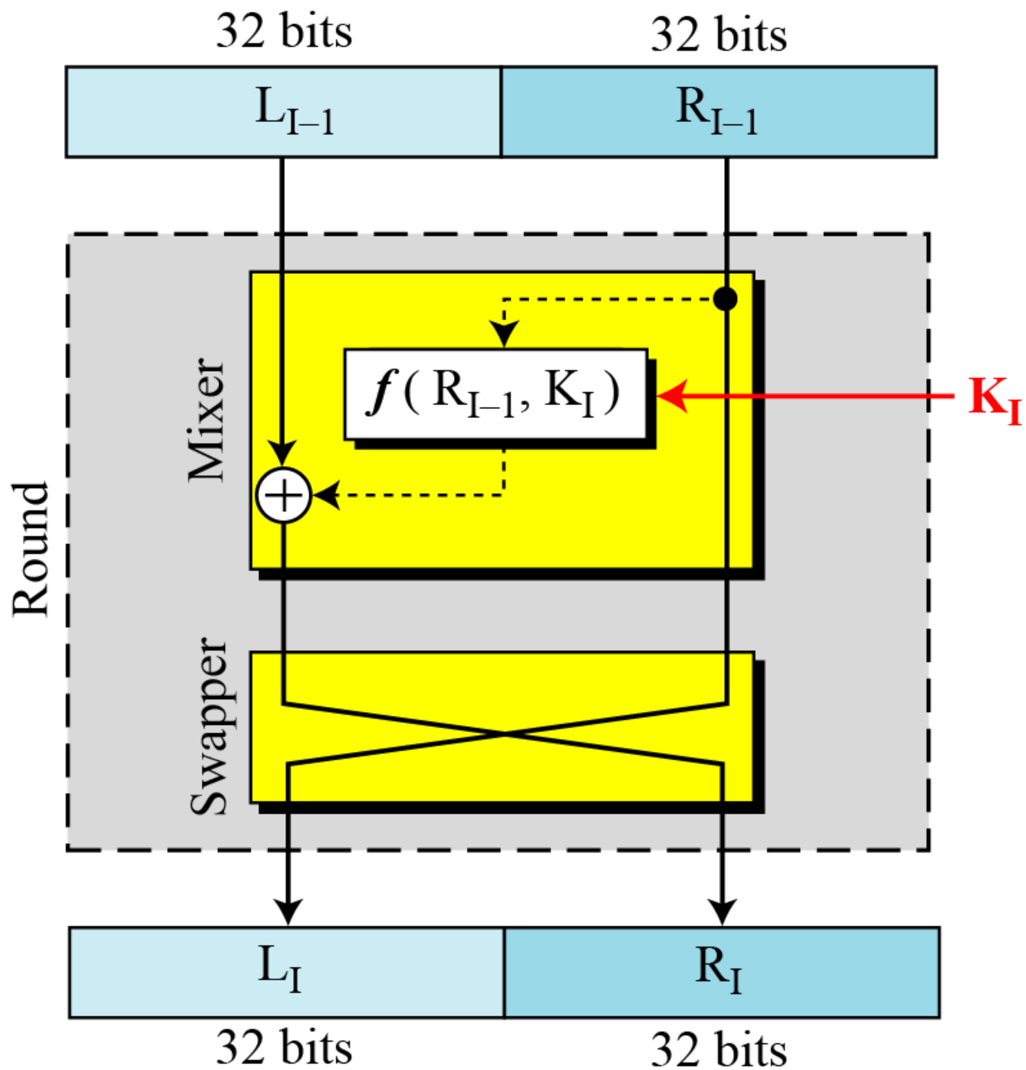
$\Rightarrow$

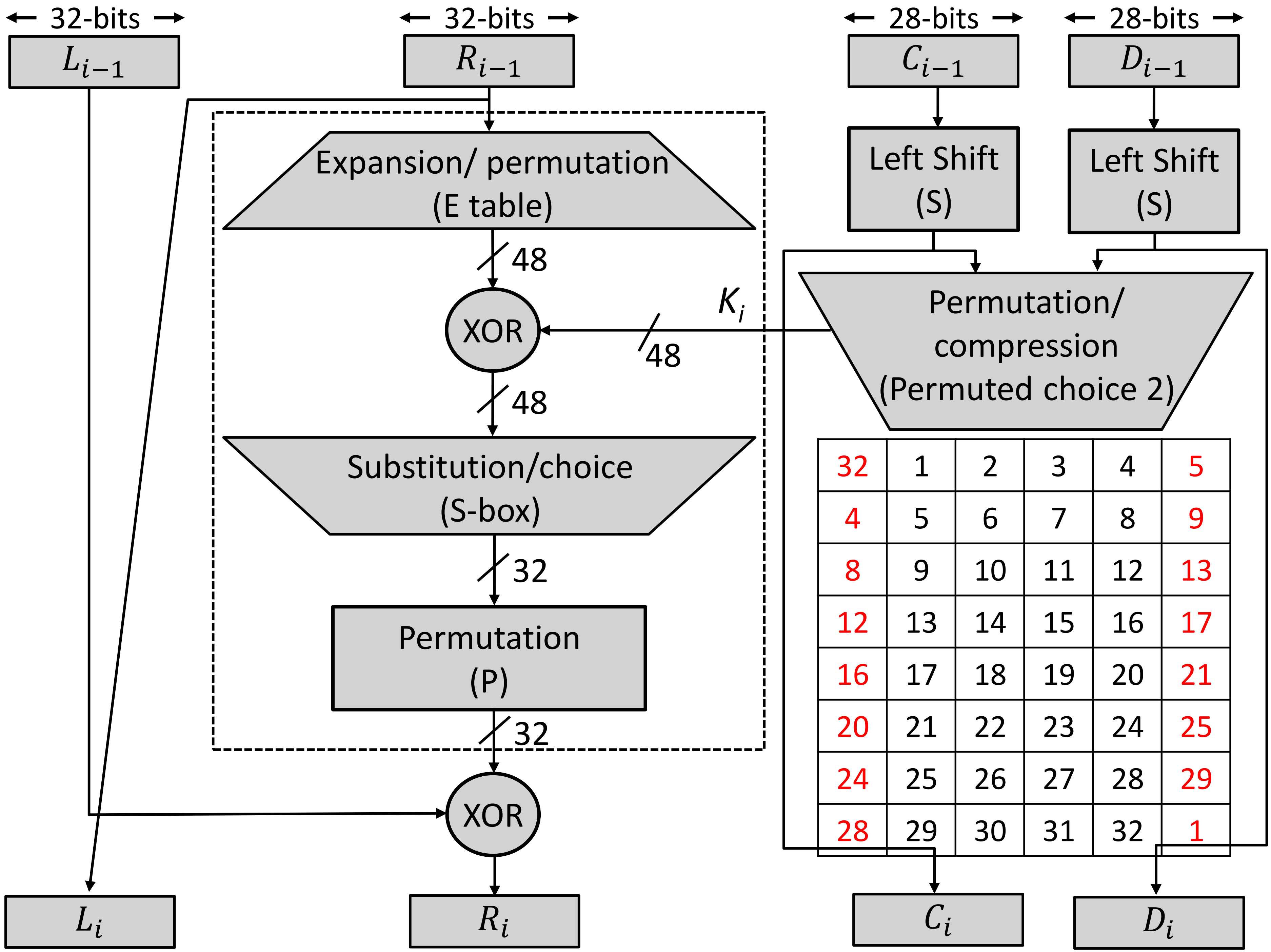
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES Summary

- First, the 64-bit plaintext passes through an **initial permutation** (IP) that rearranges the bits to produce the permuted input.
- This is followed by a phase consisting of sixteen rounds of the same function, which involves both **permutation** and **substitution** functions.
- Finally, the preoutput is passed through a permutation that is the **inverse of the initial permutation** function, to produce the 64-bit ciphertext.
- The 56-bit key is passed through a **permutation function**.
- For each of the sixteen rounds, a subkey (K_i) is produced by the combination of a **left circular shift** and a **permutation**.

DES Single Round



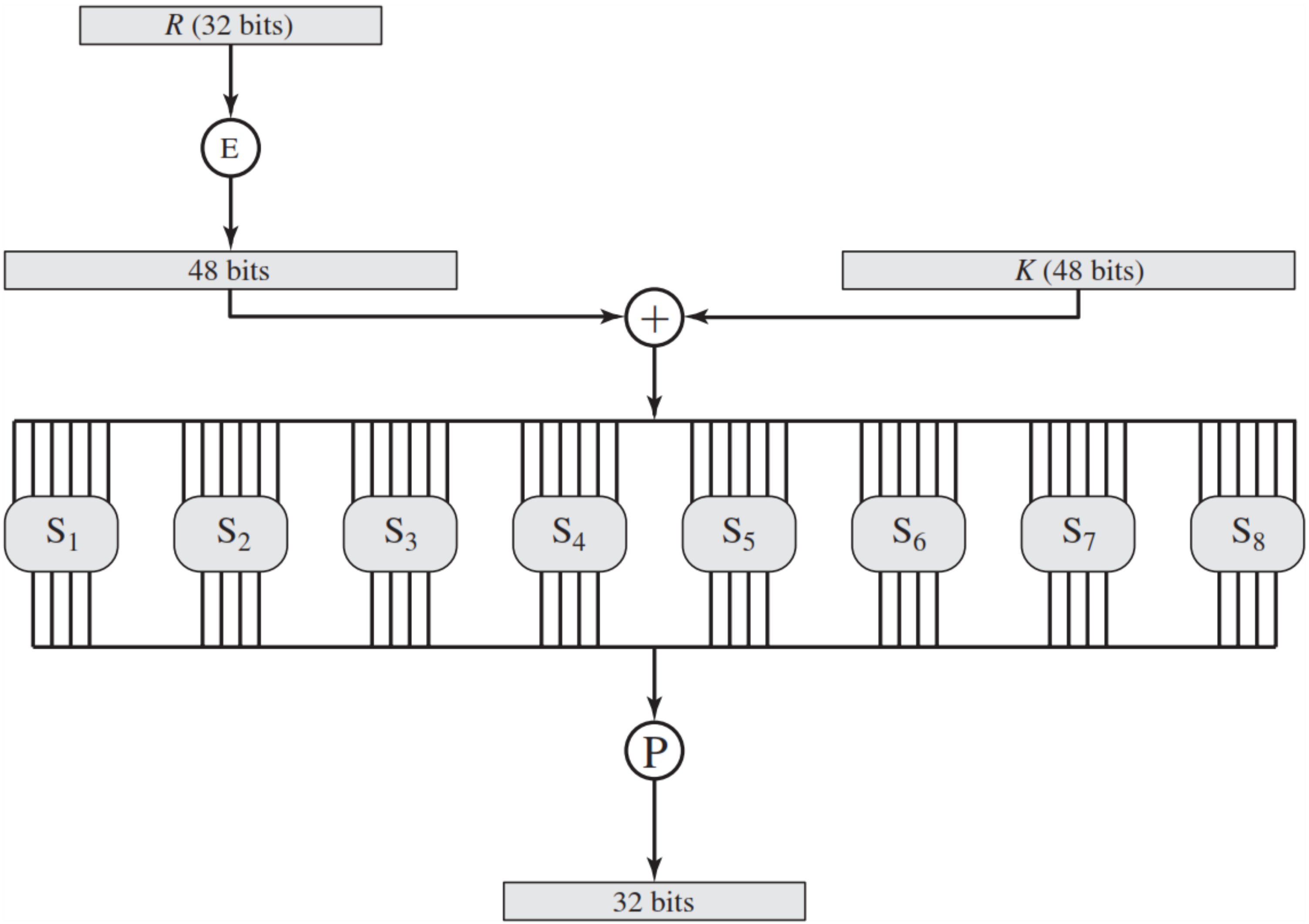


32-bits
32-bits
28-bits
28-bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/ permutation (E table)
48
XOR
K_i
48
48
Substitution/choice (S-box)
32
Permutation (P)
32
XOR
Left Shift (S)
Left Shift (S)
Permutation/ compression (Permuted choice 2)
32 1 2 3 4 5
4 5 6 7 8 9
8 9 10 11 12 13
12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 1
L_i
R_i
C_i
D_i

DES Single Round Summary

1. Key Transformation
    - Permutation of selection of sub-key from original key
2. Expansion Permutation (E-table)
    - Right half is expanded from 32-bits to 48-bits
3. S-box Substitution
    - Accepts 48-bits from XOR operation and produce 32-bits using 8 substitution boxes (each S-boxes has a 6-bit i/p and 4-bit o/p).
4. P-Box Permutation
5. XOR and Swap

Role of S-box



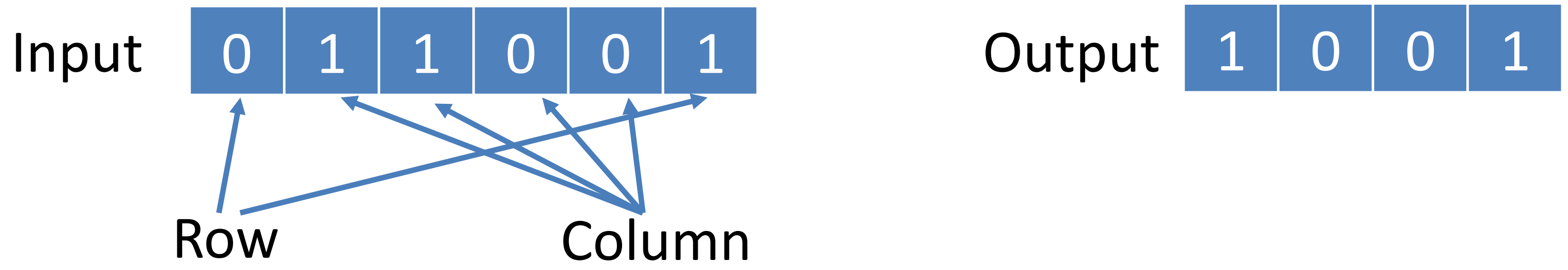
Role of S-box (Cont…)

- The outer two bits of each group select one row of an S-box.
- Inner four bits selects one column of an S-box.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-box 1

- Example:



Avalanche Effect

- Desirable property of any encryption algorithm is that a change in one bit of the plaintext or of the key should produce a change in many bits of cipher text.
- DES performs strong **avalanche effect**.

Plaintext: 0000000000000000	Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1	
Plaintext: 000000000000000<u>1</u>	Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3	

- Although the two plaintext blocks differ only in the rightmost bit, the ciphertext blocks differ in 29 bits.
- This means that changing approximately 1.5 % of the plaintext creates a change of approximately 45 % in the ciphertext.

Introduction
to
Advanced Encryption Standard (AES)
by AVN

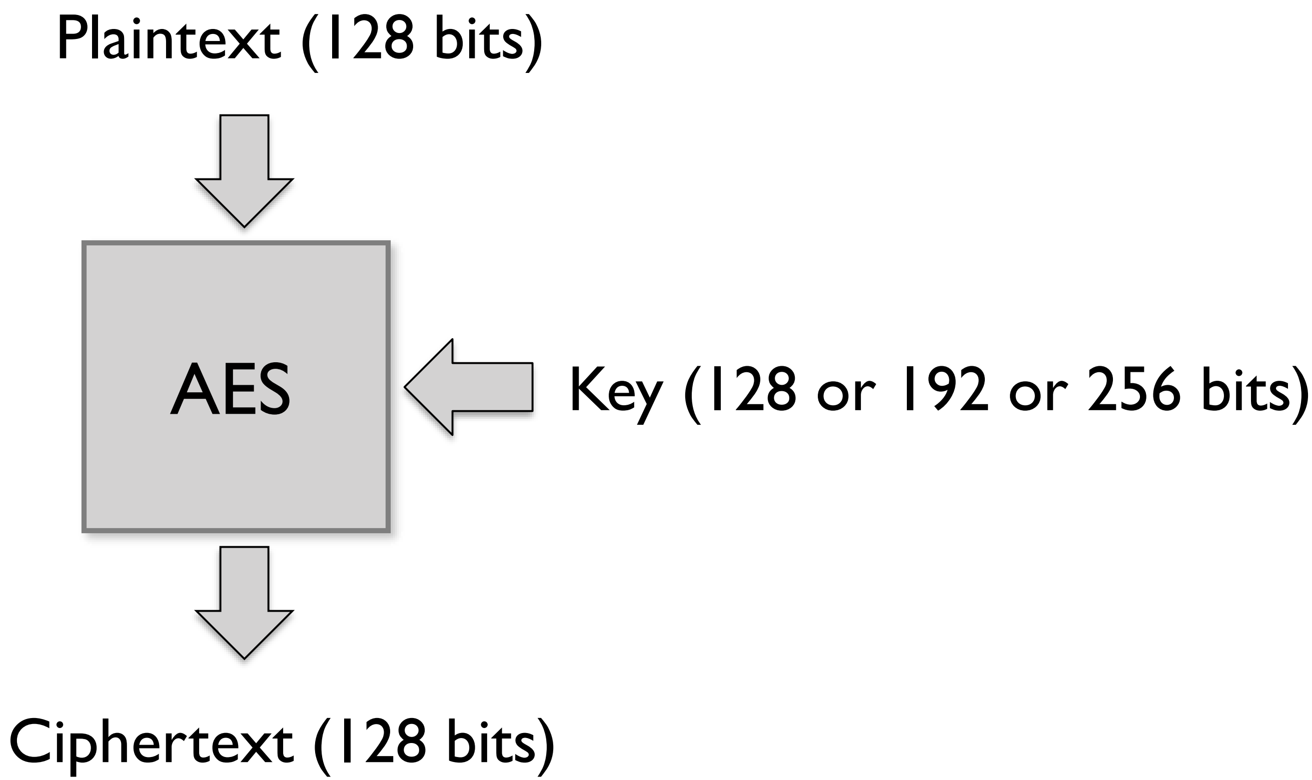
AES (Advanced Encryption Standard)

- Outline
  - Understand the basics of AES
  - AES Input and Output
  - Data Units
  - Block to State and State to Block
  - AES structure
  - AES parameters

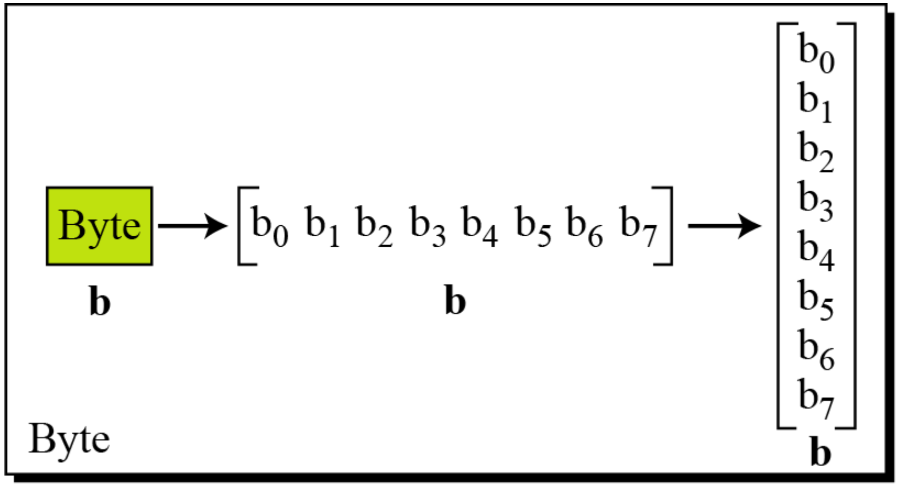
AES (Advanced Encryption Standard)

- Advanced Encryption Standard
- NIST in 2001
- Symmetric – Same key at encryption and decryption
- block cipher – consider block as input

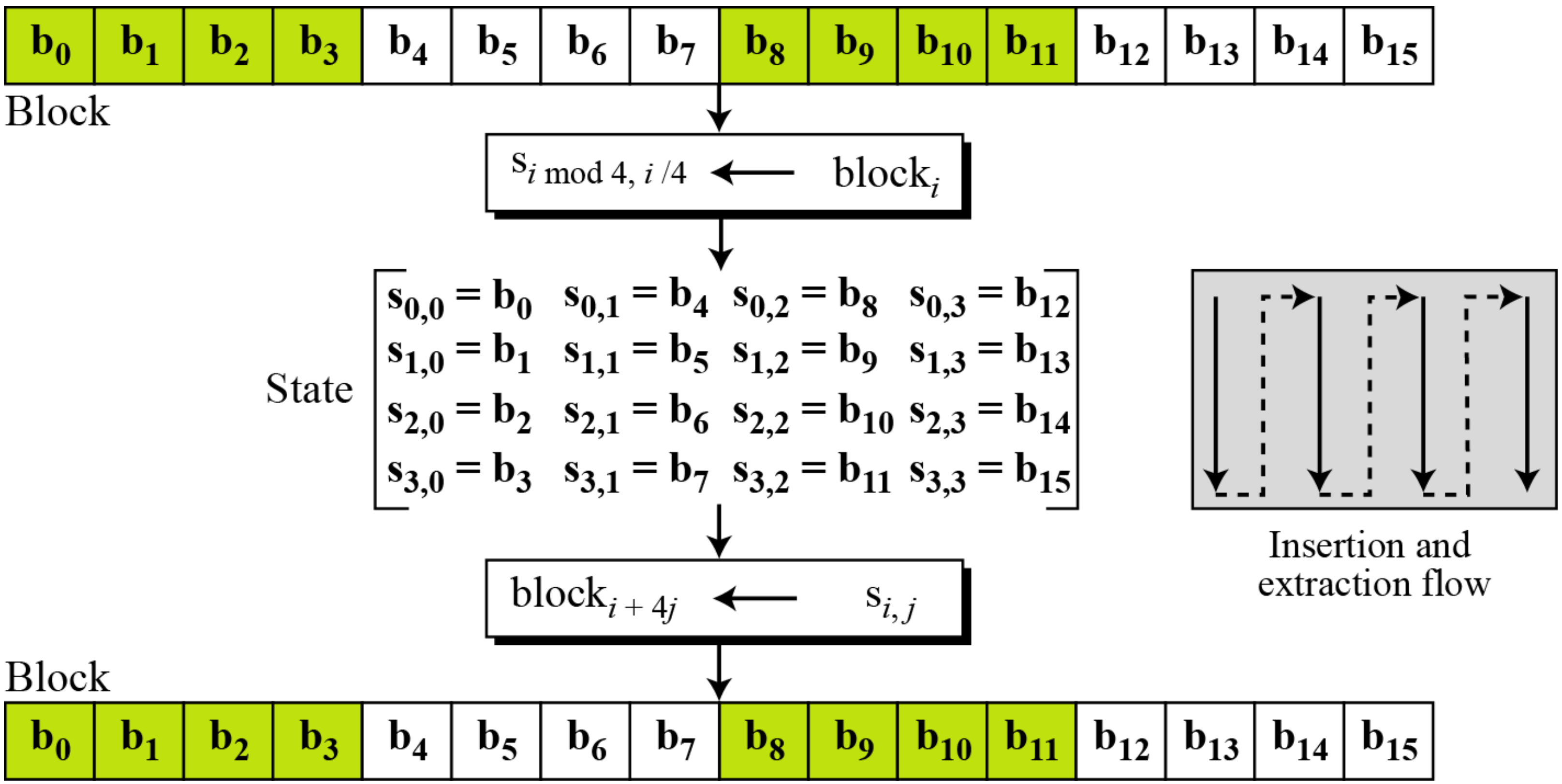
AES - I/O and O/P


Plaintext (128 bits)
AES
Key (128 or 192 or 256 bits)
Ciphertext (128 bits)

Data Units in AES



AES - Block to State & State to Block



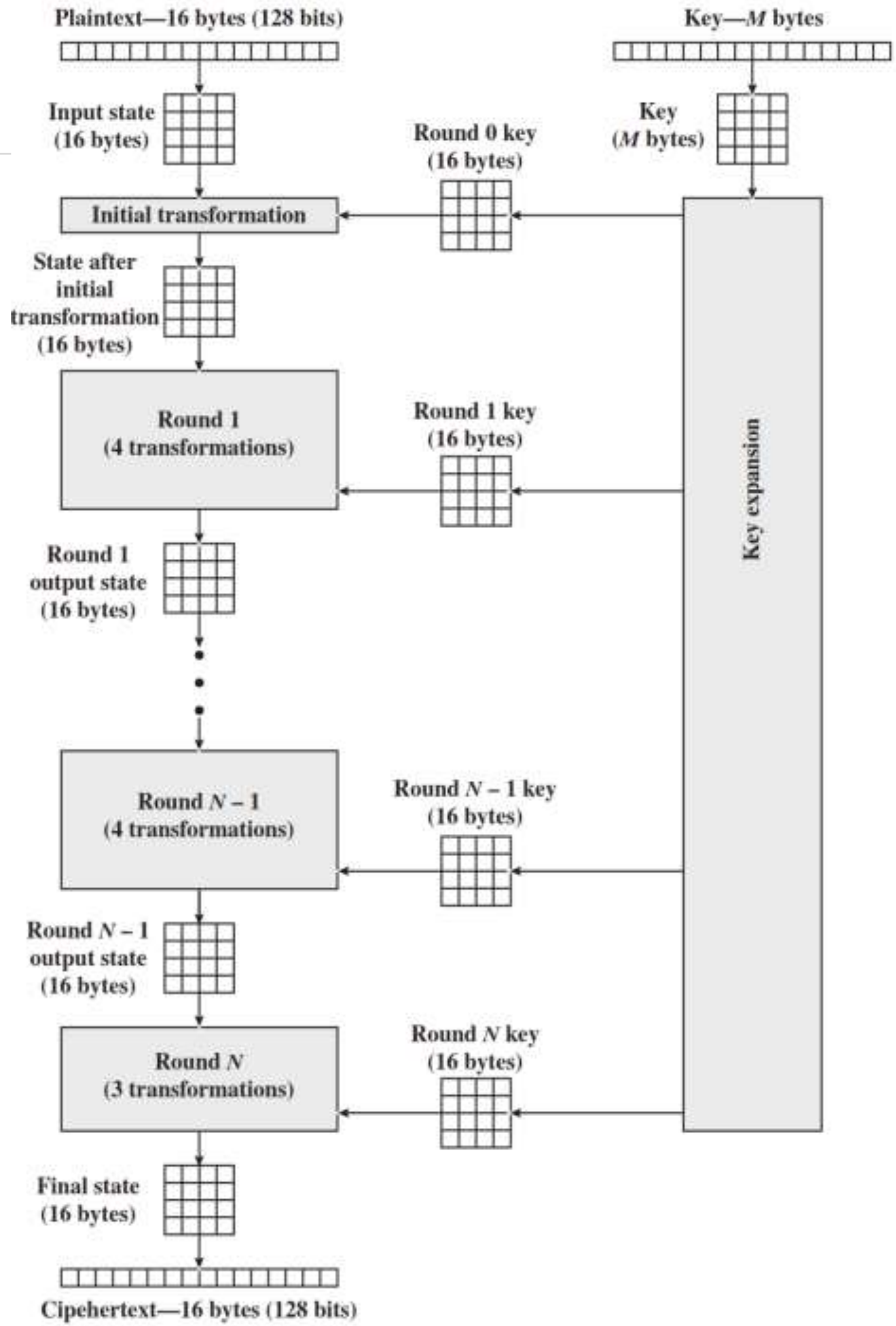
AES - Plain Text to State

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

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

AES Structure

No of rounds	Key size (in bits)
10	128
12	192
14	256



AES Parameters

	AES-128	AES-192	AES-256
Key size	128	192	256
Plainttext Size	128	128	128
No. of Rounds	10	12	14
Round Key Size	128	128	128

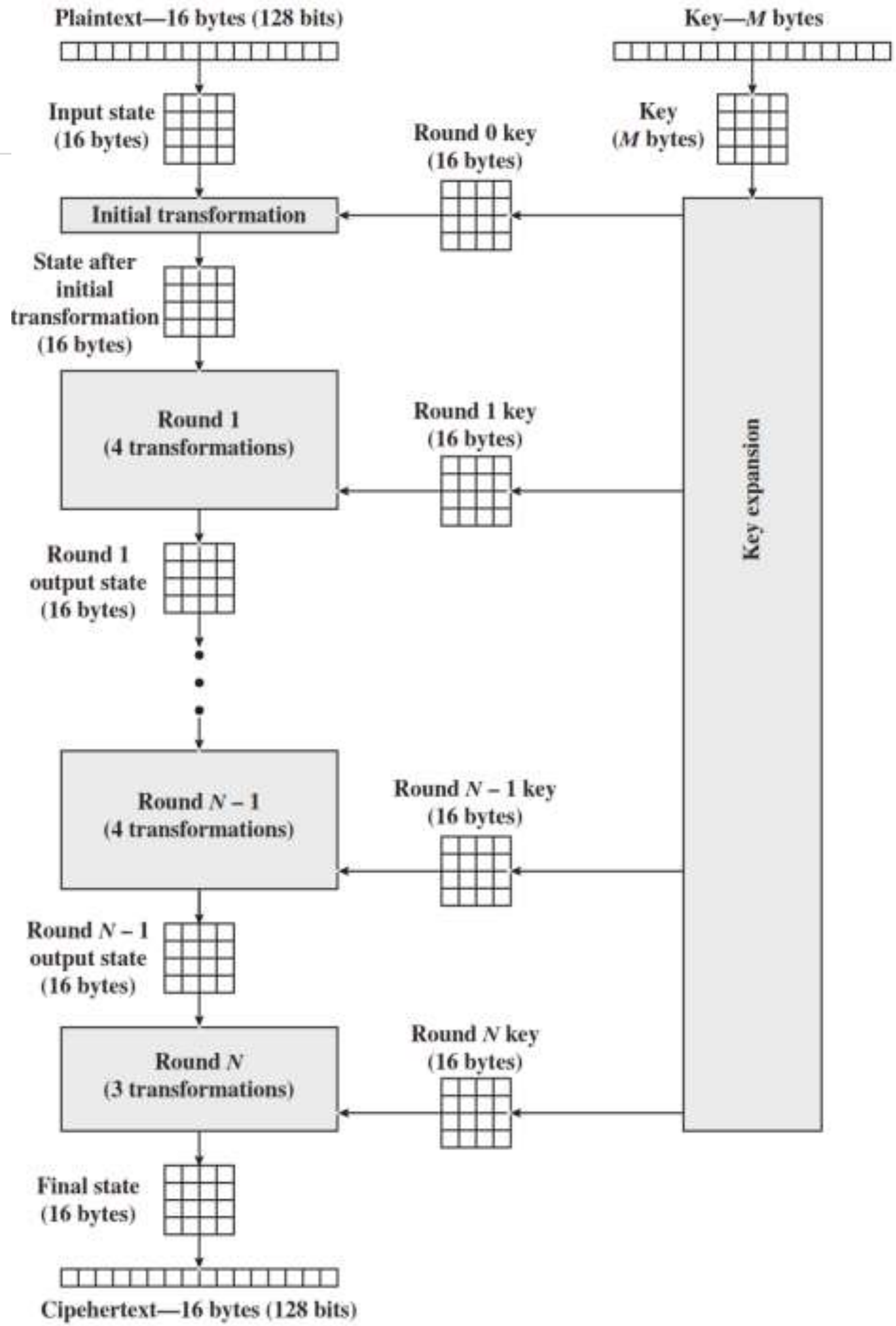
AES Encryption and Decryption

AES (Advanced Encryption Standard)

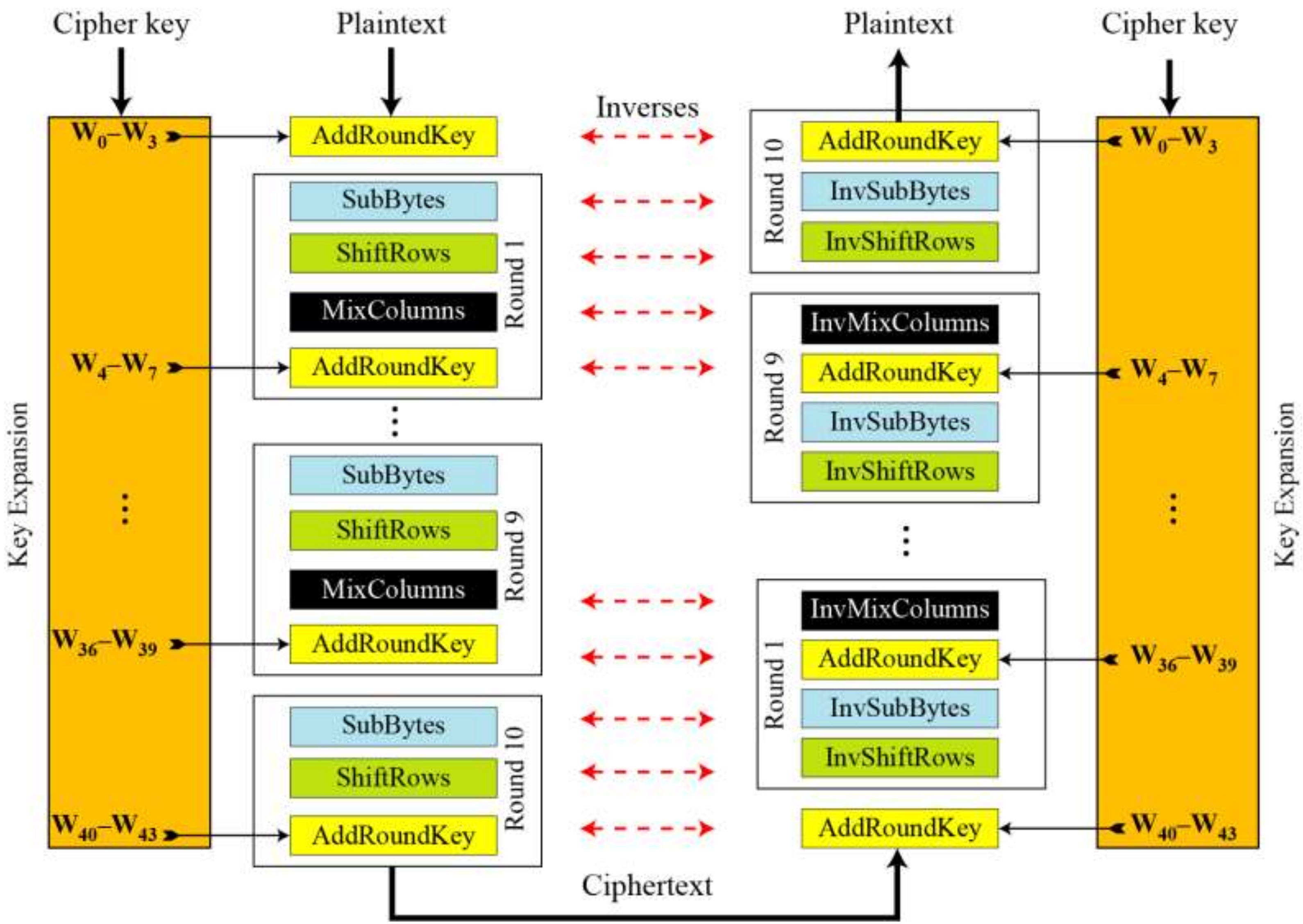
- Outline
  - Recall the AES structure and the relationship between the key size and number of rounds
  - Understand the AES encryption and decryption
  - Know the various transformations in AES encryption and decryption process

AES Structure

No of rounds	Key size (in bits)
10	128
12	192
14	256



AES Encryption and Decryption



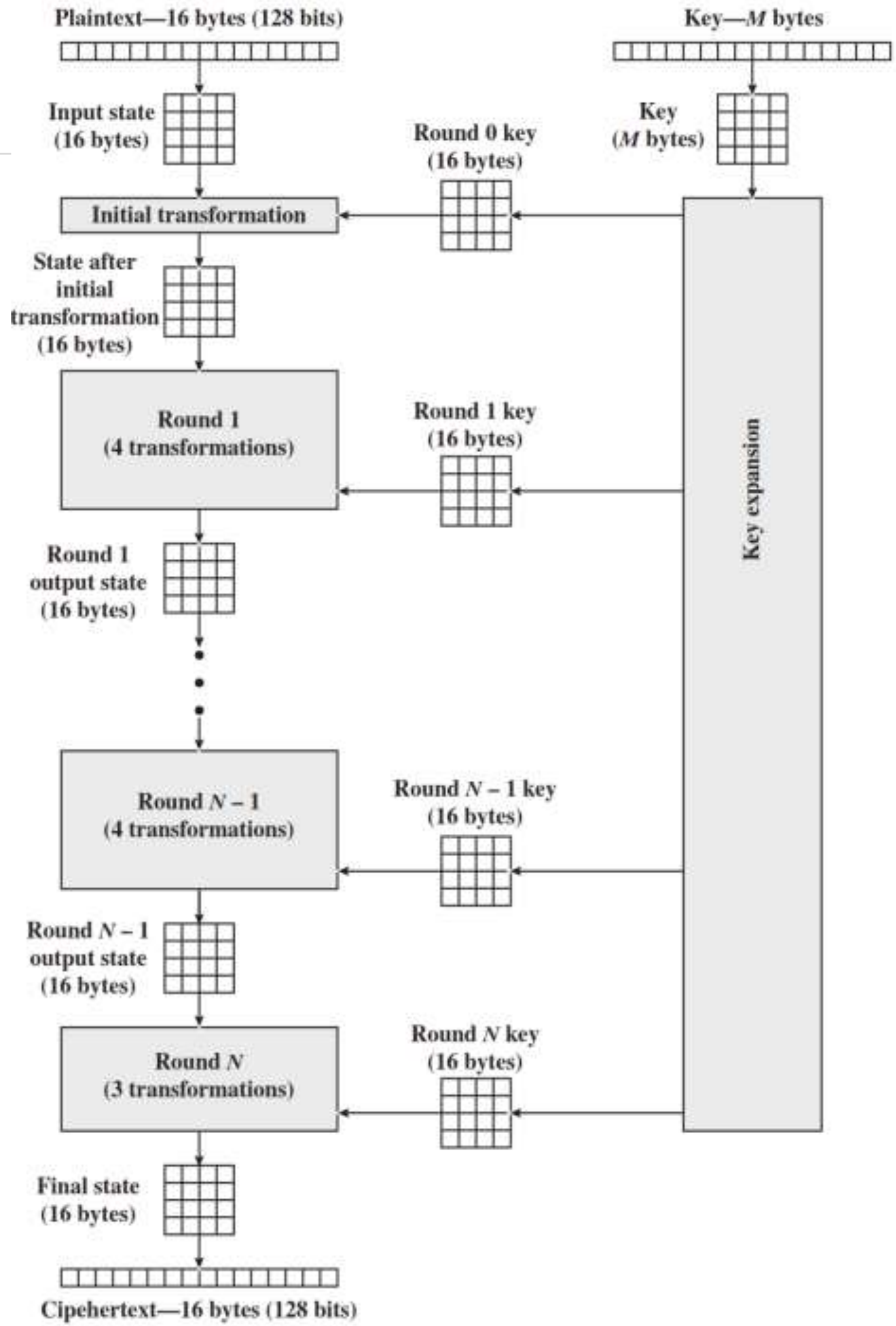
AES Round Transformation

AES Round Transformation

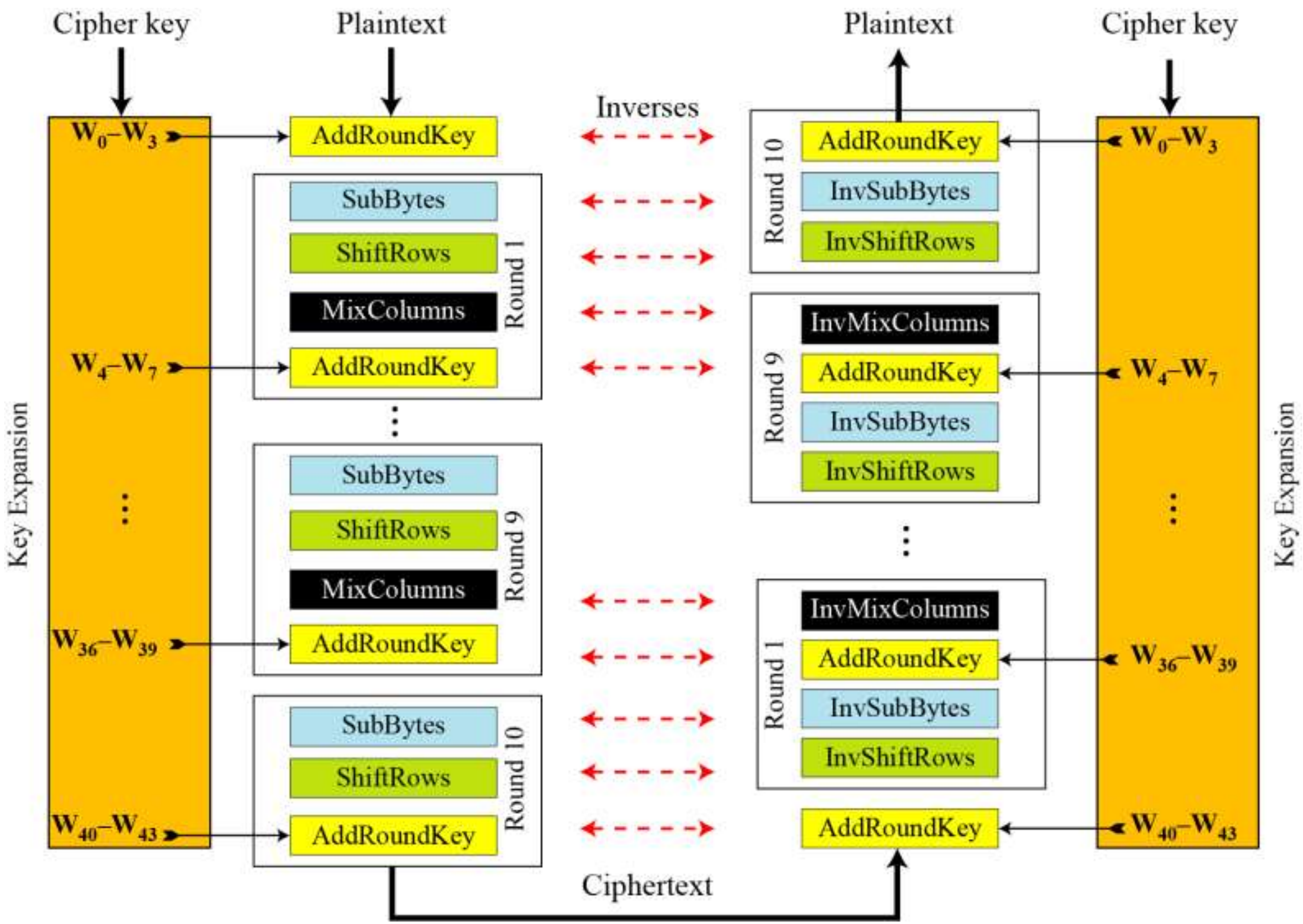
- Outline
  - Understand the four transformation in AES encryption and decryption process

AES Structure

No of rounds	Key size (in bits)
10	128
12	192
14	256



AES Encryption and Decryption



AES Transformation Functions

- Substitute Bytes ------ It is Substitution or S-box
- Shifts Rows ------ It is Permutation or P-box
- Mix Columns ------ It is Substitution or S-box
- Add Round Key ------ It is Substitution or S-box

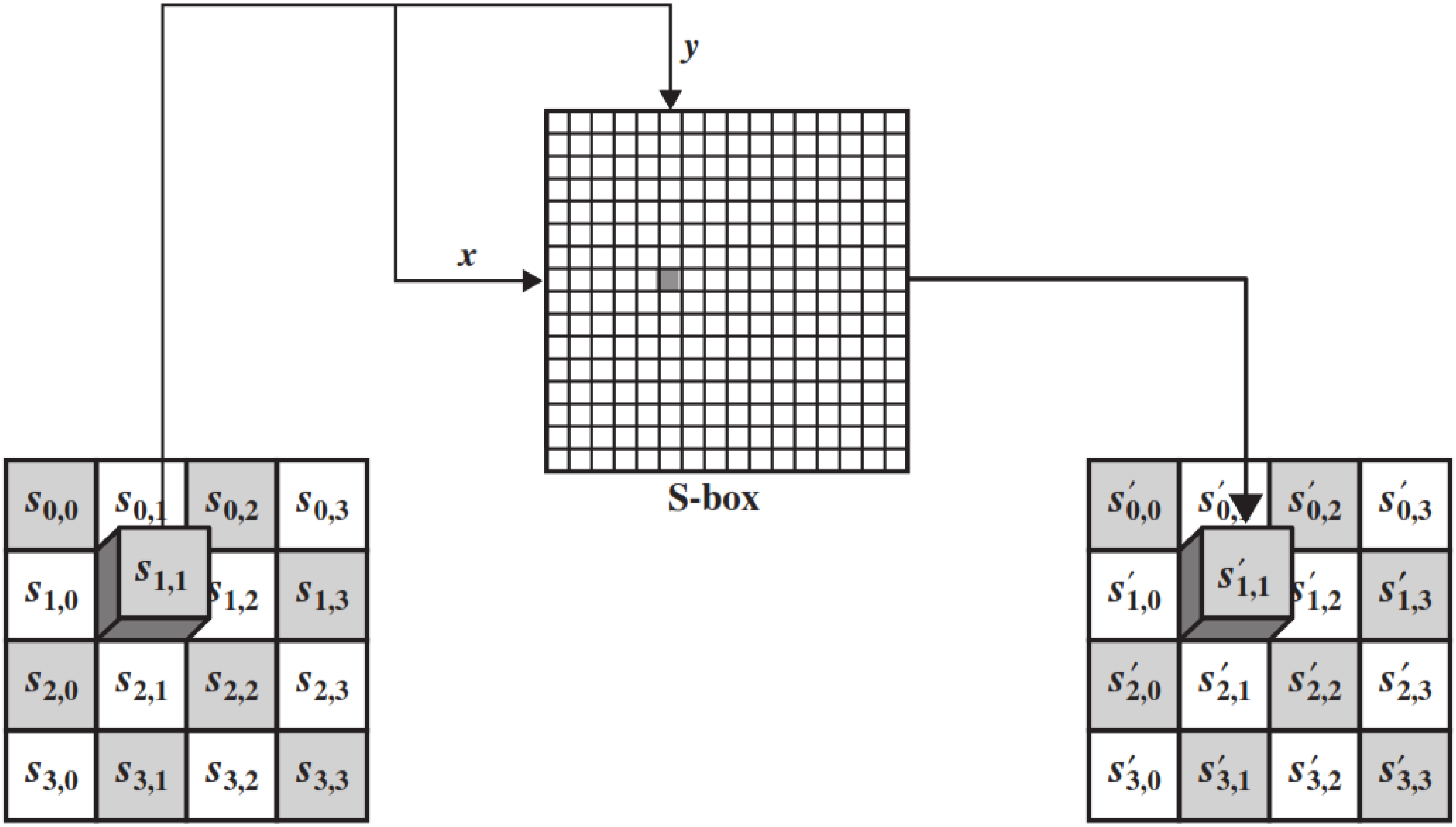
AES Structure

- The first N-1 rounds consist of four distinct transformation functions.

SubBytes	• The 16 input bytes are substituted using an **S-box**
ShiftRows	• Each of the four rows of the matrix is shifted to the left
MixColumns	• Each column of four bytes is now transformed using a special mathematical function.
AddRoundKey	• The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key.

SubByte Transformation

- The forward substitute byte transformation, called **SubBytes**, is a simple table lookup



Shift Rows

- The first row of **State is not altered**.
- For the second row, a 1-byte circular left shift is performed.
- For the third row, a 2-byte circular left shift is performed.
- For the fourth row, a 3-byte circular left shift is performed.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

→

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Mix Columns

- Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} T_{0,0} & T_{0,1} & T_{0,2} & T_{0,3} \\ T_{1,0} & T_{1,1} & T_{1,2} & T_{1,3} \\ T_{2,0} & T_{2,1} & T_{2,2} & T_{2,3} \\ T_{3,0} & T_{3,1} & T_{3,2} & T_{3,3} \end{bmatrix}$$

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Add Round Key

- In the forward add round key transformation, the 128 bits of State are bitwise XORed with the 128 bits of the round key.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$\oplus$

W_i	W_{i+1}	W_{i+2}	W_{i+3}

$T_{0,0}$	$T_{0,1}$	$T_{0,2}$	$T_{0,3}$
$T_{1,0}$	$T_{1,1}$	$T_{1,2}$	$T_{1,3}$
$T_{2,0}$	$T_{2,1}$	$T_{2,2}$	$T_{2,3}$
$T_{3,0}$	$T_{3,1}$	$T_{3,2}$	$T_{3,3}$

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

State

$\oplus$

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

Round Key

$=$

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

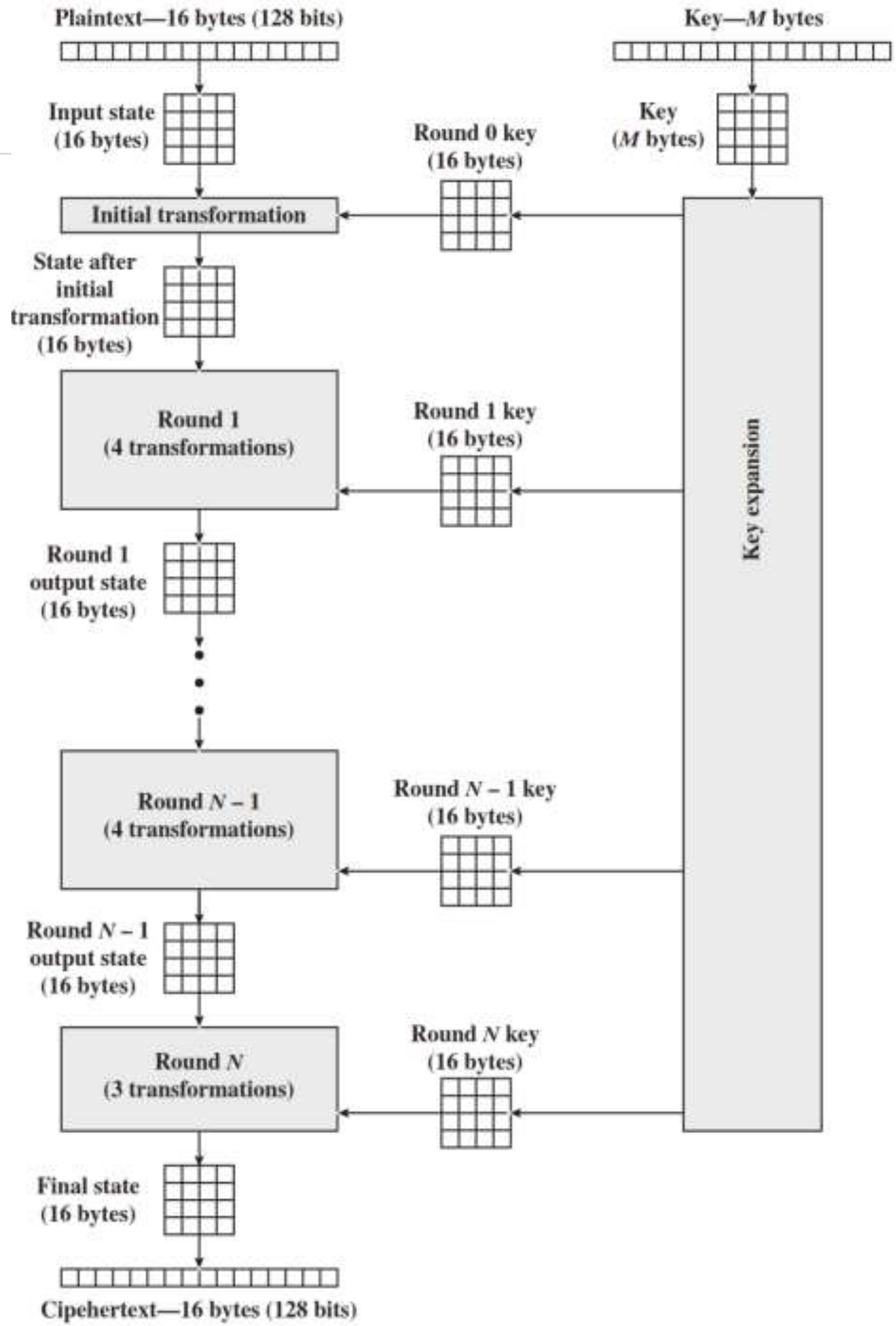
AES Key Expansion

Objectives

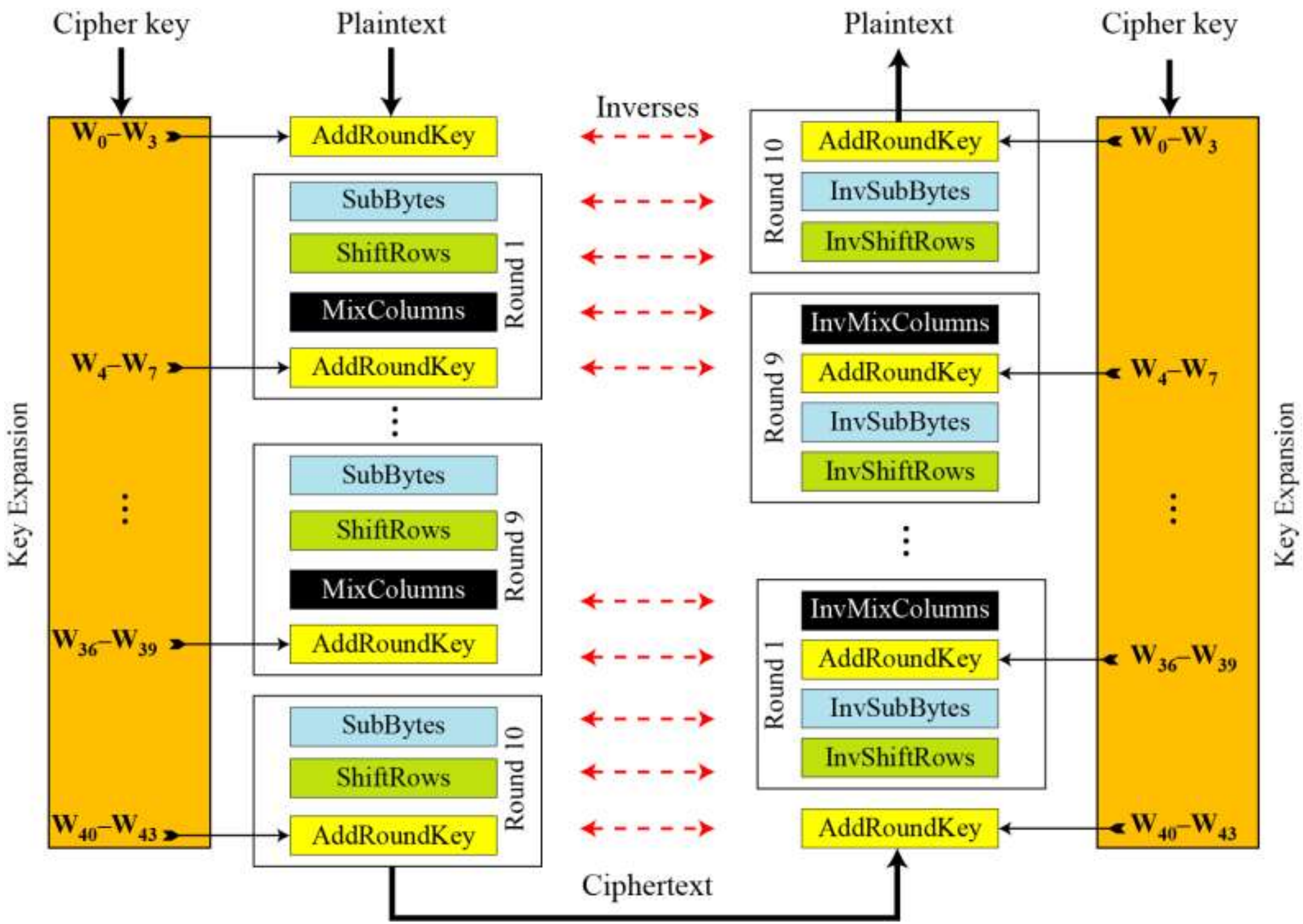
- Understand the AES key Expansion Process

AES Structure

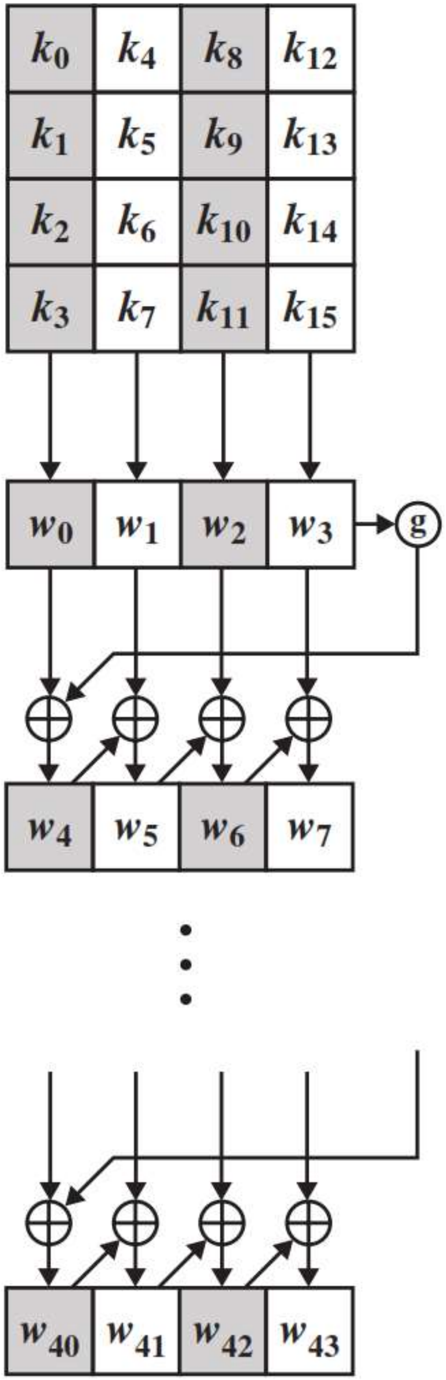
No of rounds	Key size (in bits)
10	128
12	192
14	256

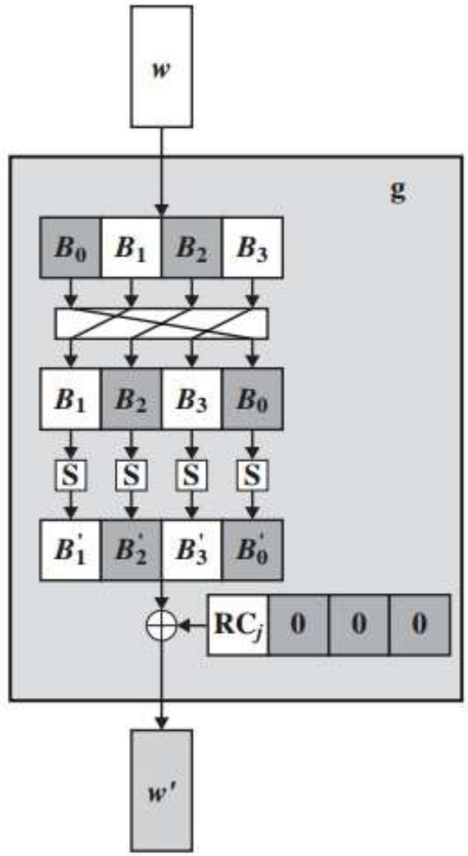


AES Encryption and Decryption



AES Key Expansion





Rcon Constants (Base 16)			
Round	Constant(Rcon)	Round	Constant(Rcon)
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

- The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of **44 words** (176 bytes).
- Each added word **w[i]** depends on the immediately preceding word, w[i - 1].
- In three out of four cases, a simple XOR is used.

Key Expansion Example

Plaintext:	0123456789abcdeffedcba9876543210
Key:	0f1571c947d9e8590cb7add6af7f6798
Ciphertext:	ff0b844a0853bf7c6934ab4364148fb9

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad d6 w3 = af 7f 67 98	RotWord(w3) = 7f 67 98 af = x1 SubWord(x1) = d2 85 46 79 = y1 Rcon(1) = 01 00 00 00 y1 ⊕ Rcon(1) = d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0 w5 = w4 ⊕ w1 = 9b 49 df e9 w6 = w5 ⊕ w2 = 97 fe 72 3f w7 = w6 ⊕ w3 = 38 81 15 a7	RotWord(w7) = 81 15 a7 38 = x2 SubWord(x2) = 0c 59 5c 07 = y2 Rcon(2) = 02 00 00 00 y2 ⊕ Rcon(2) = 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7 w9 = w8 ⊕ w5 = 49 80 b4 5e w10 = w9 ⊕ w6 = de 7e c6 61 w11 = w10 ⊕ w7 = e6 ff d3 c6	RotWord(w11) = ff d3 c6 e6 = x3 SubWord(x3) = 16 66 b4 83 = y3 Rcon(3) = 04 00 00 00 y3 ⊕ Rcon(3) = 12 66 b4 8e = z3
w12 = w8 ⊕ z3 = c0 af df 39 w13 = w12 ⊕ w9 = 89 2f 6b 67 w14 = w13 ⊕ w10 = 57 51 ad 06 w15 = w14 ⊕ w11 = b1 ae 7e c0	RotWord(w15) = ae 7e c0 b1 = x4 SubWord(x4) = e4 f3 ba c8 = y4 Rcon(4) = 08 00 00 00 y4 ⊕ Rcon(4) = ec f3 ba c8 = 4

S-box of AES key Expansion

	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
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	C8	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