INF 638
Cryptography & Cryptosystems

Section 4: Data Encryption System

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

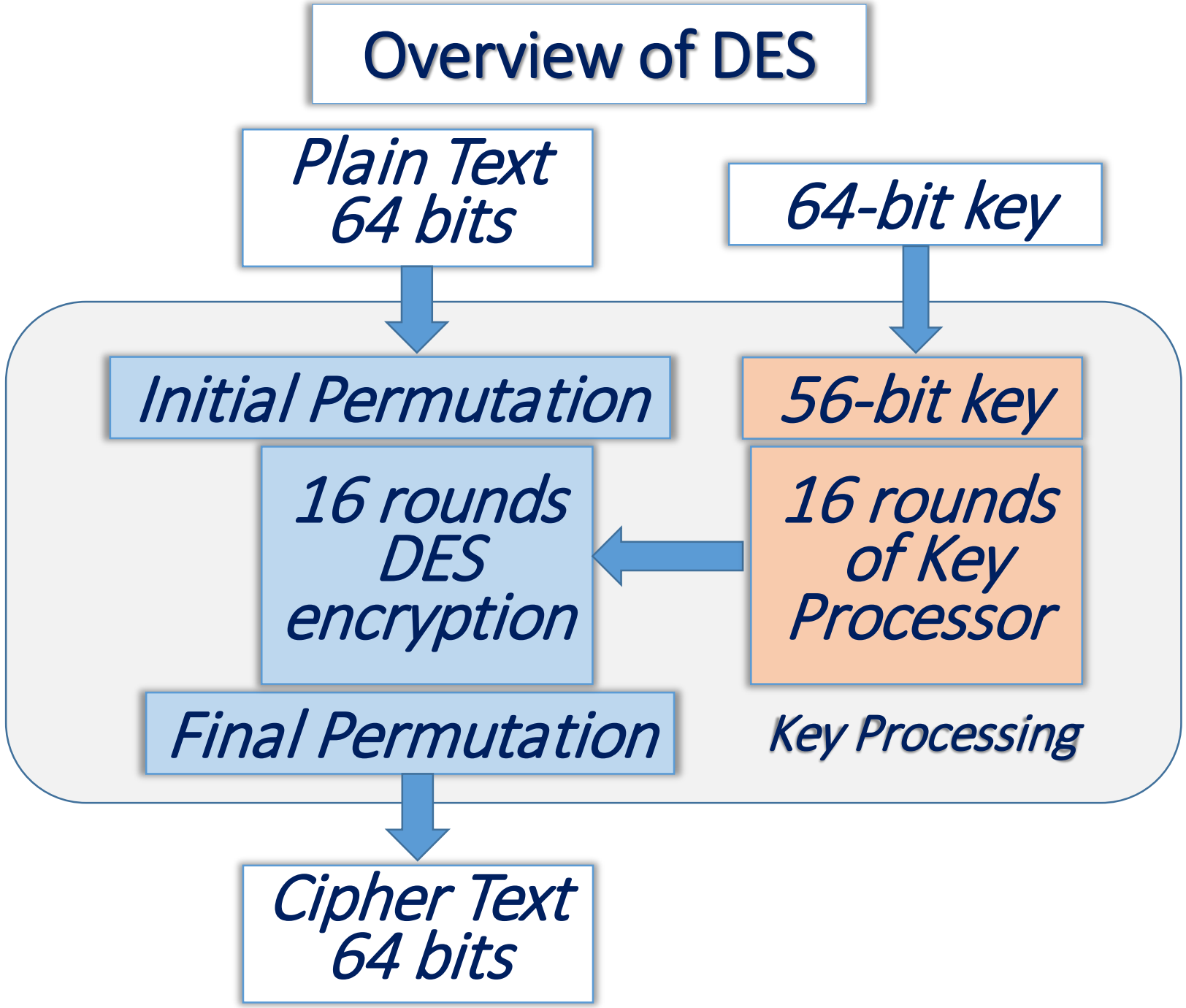
INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

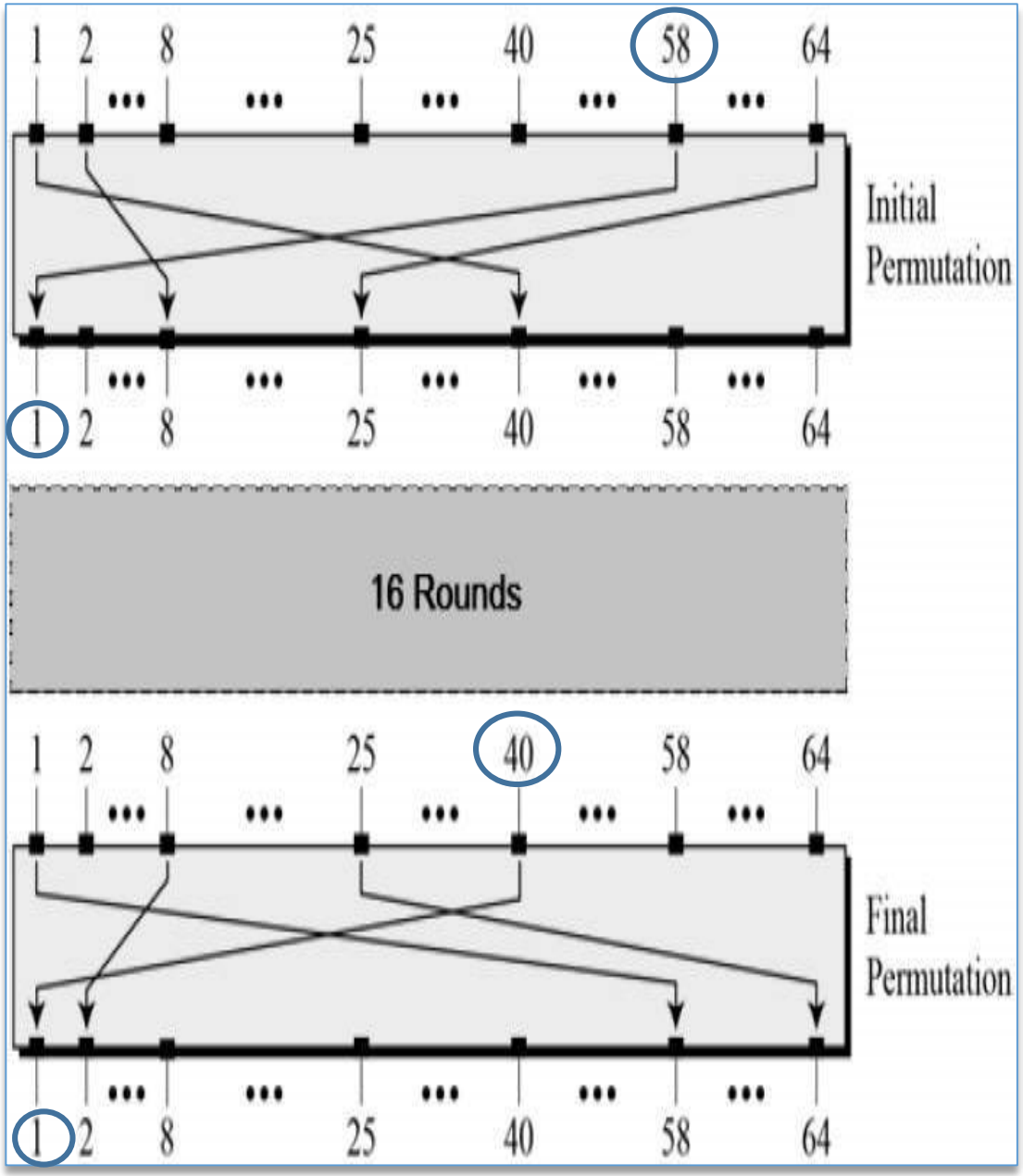
NORTHERN ARIZONA UNIVERSITY

4- Data Encryption Standard

- 4-1 History & Description
- 4-2 Encryption versus Decryption
- 4-3 The f-function
- 4-4 Key processor
- 4-5 Summary & limitations


Overview of DES
Plain Text
64 bits
64-bit key
Initial Permutation
56-bit key
16 rounds
DES
encryption
16 rounds
of Key
Processor
Final Permutation
Key Processing
Cipher Text
64 bits

1-DES: Initial and final permutation



Output IP

01	02	03	04	05	06	07	08
09	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

IP

Input 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

Input FP

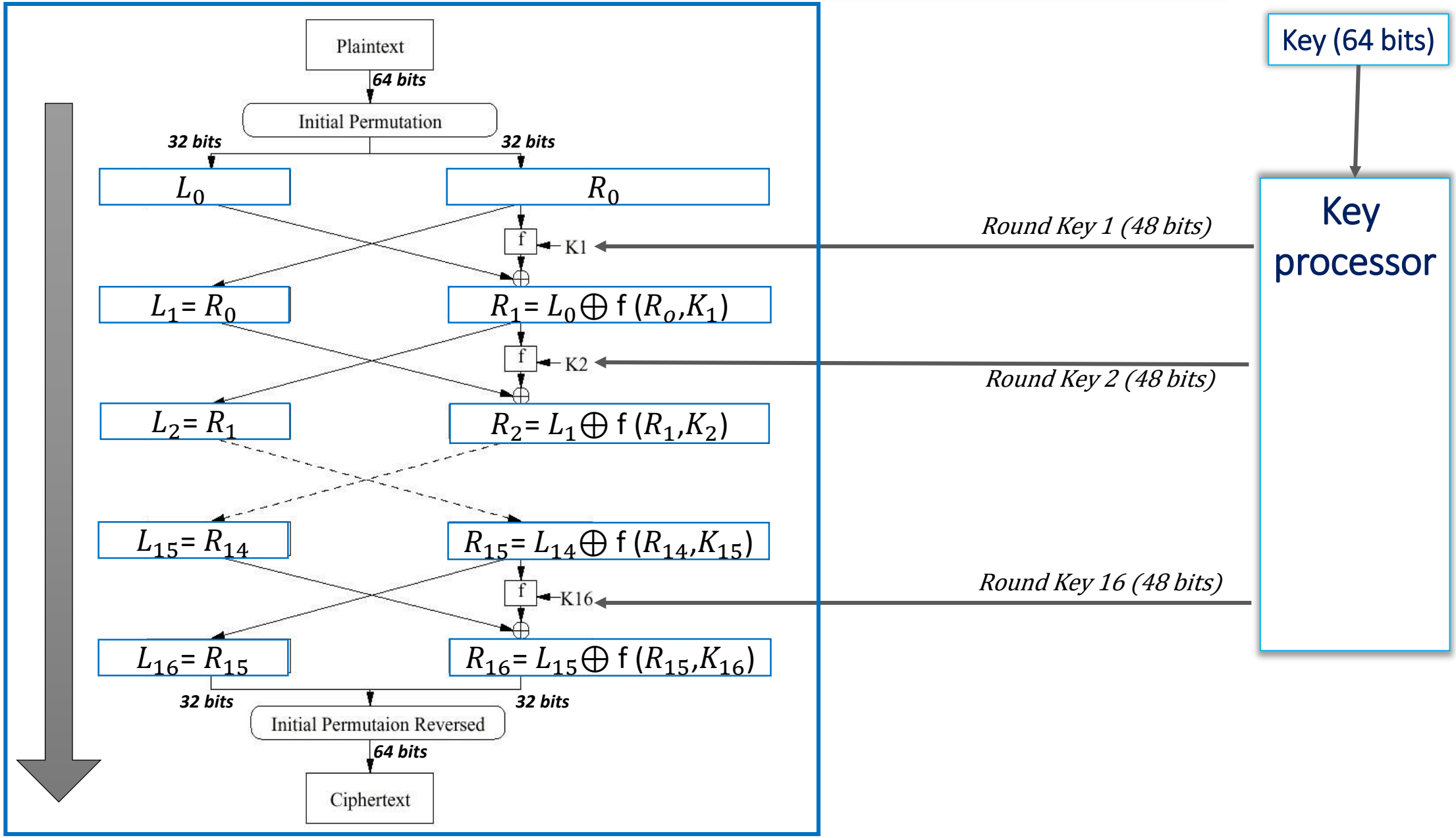
01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

FP

Input FP

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

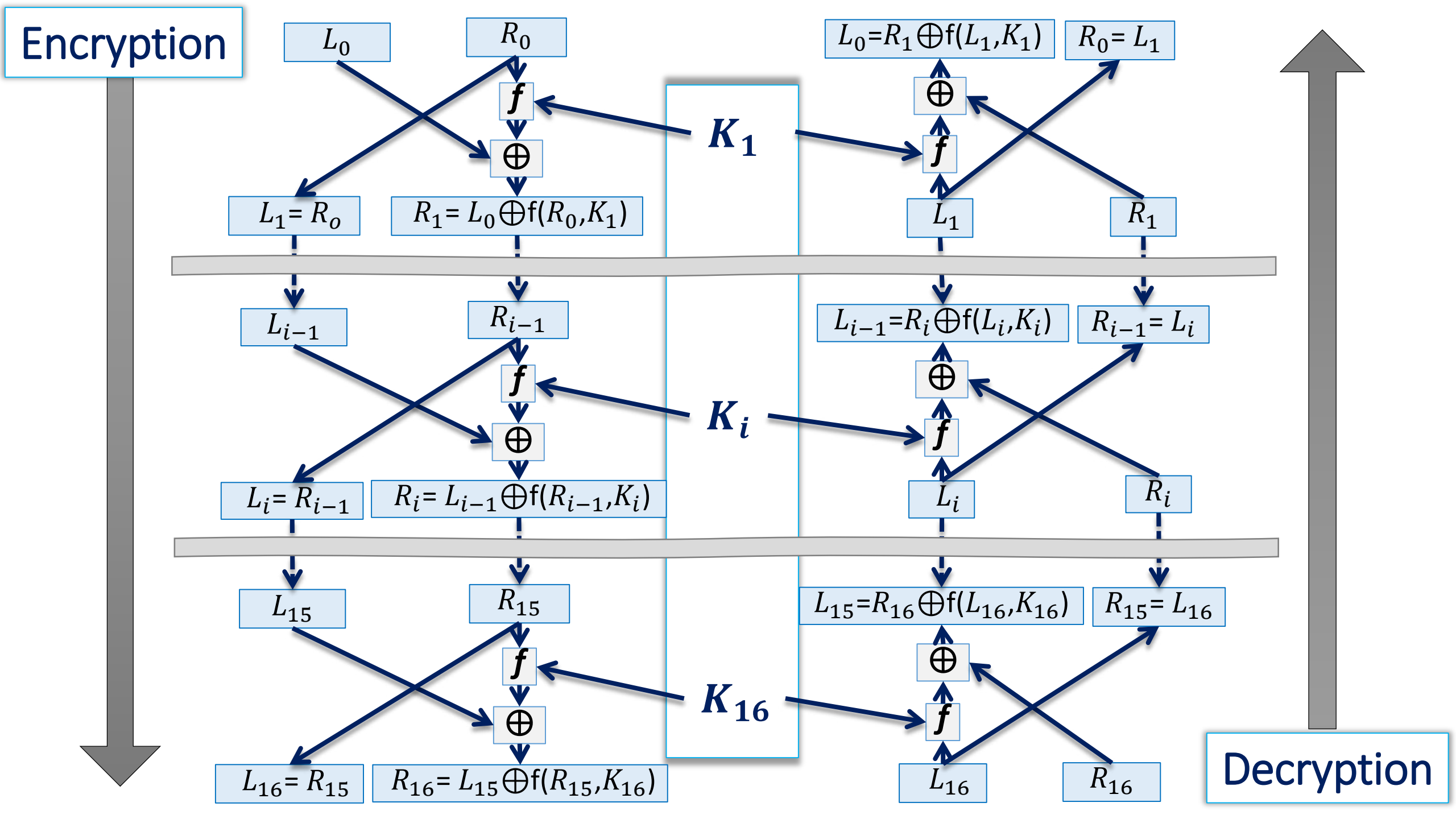
2- DES: 16 rounds of Feistel encryption



NORTHERN ARIZONA UNIVERSITY

Data Encryption Standard

- 1- History & Description
- 2- Encryption versus Decryption
- 3- The f-function
- 4- Key processor
- 5- Summary & limitations

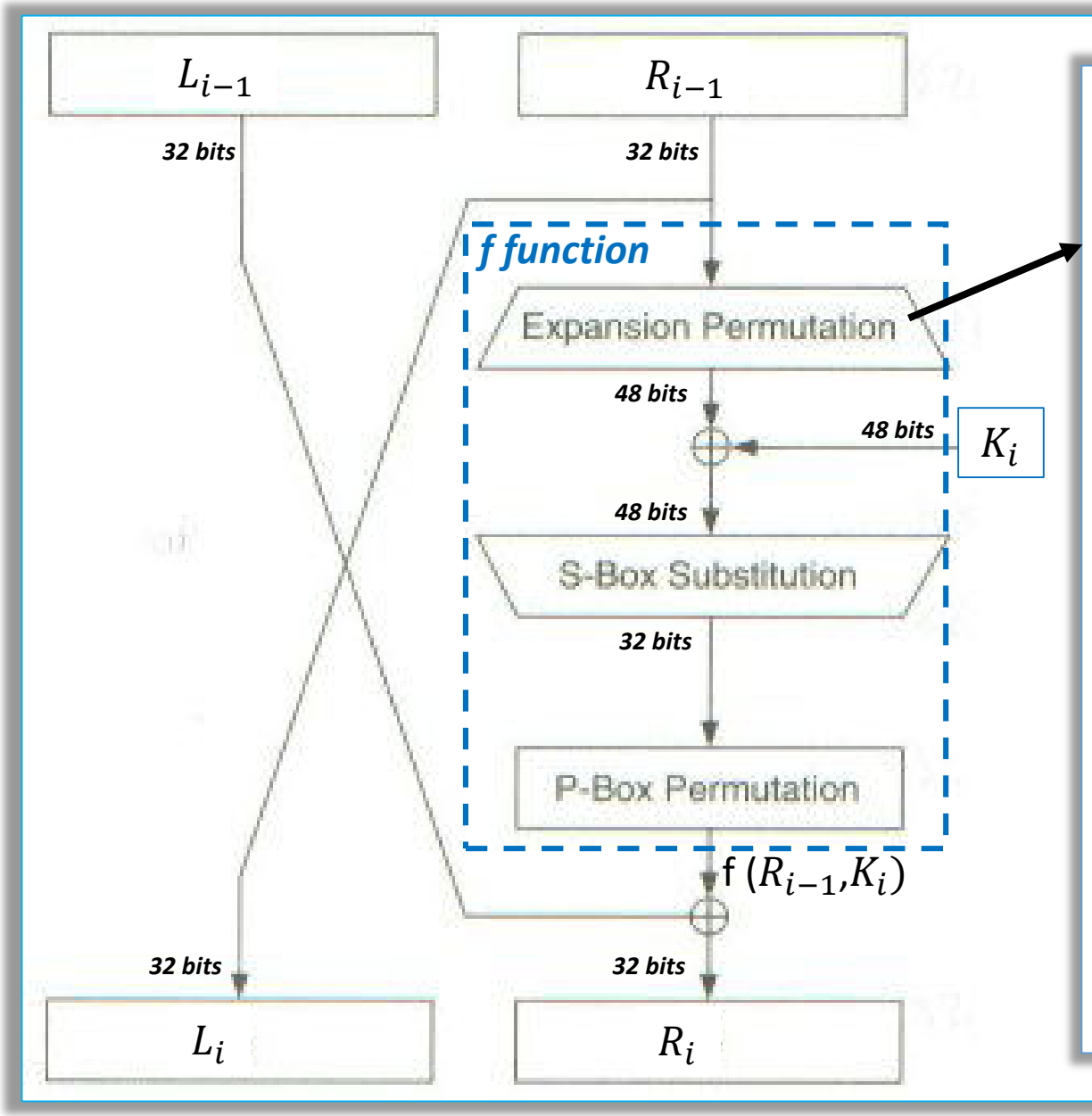

Encryption
L_0
R_0
f
$\oplus$
K_1
$L_1 = R_o$
$R_1 = L_0 \oplus f(R_0, K_1)$
L_{i-1}
R_{i-1}
K_i
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
L_{15}
R_{15}
K_{16}
$L_{16} = R_{15}$
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_0 = R_1 \oplus f(L_1, K_1)$
$R_0 = L_1$
$L_{i-1} = R_i \oplus f(L_i, K_i)$
$R_{i-1} = L_i$
$L_{15} = R_{16} \oplus f(L_{16}, K_{16})$
$R_{15} = L_{16}$
Decryption

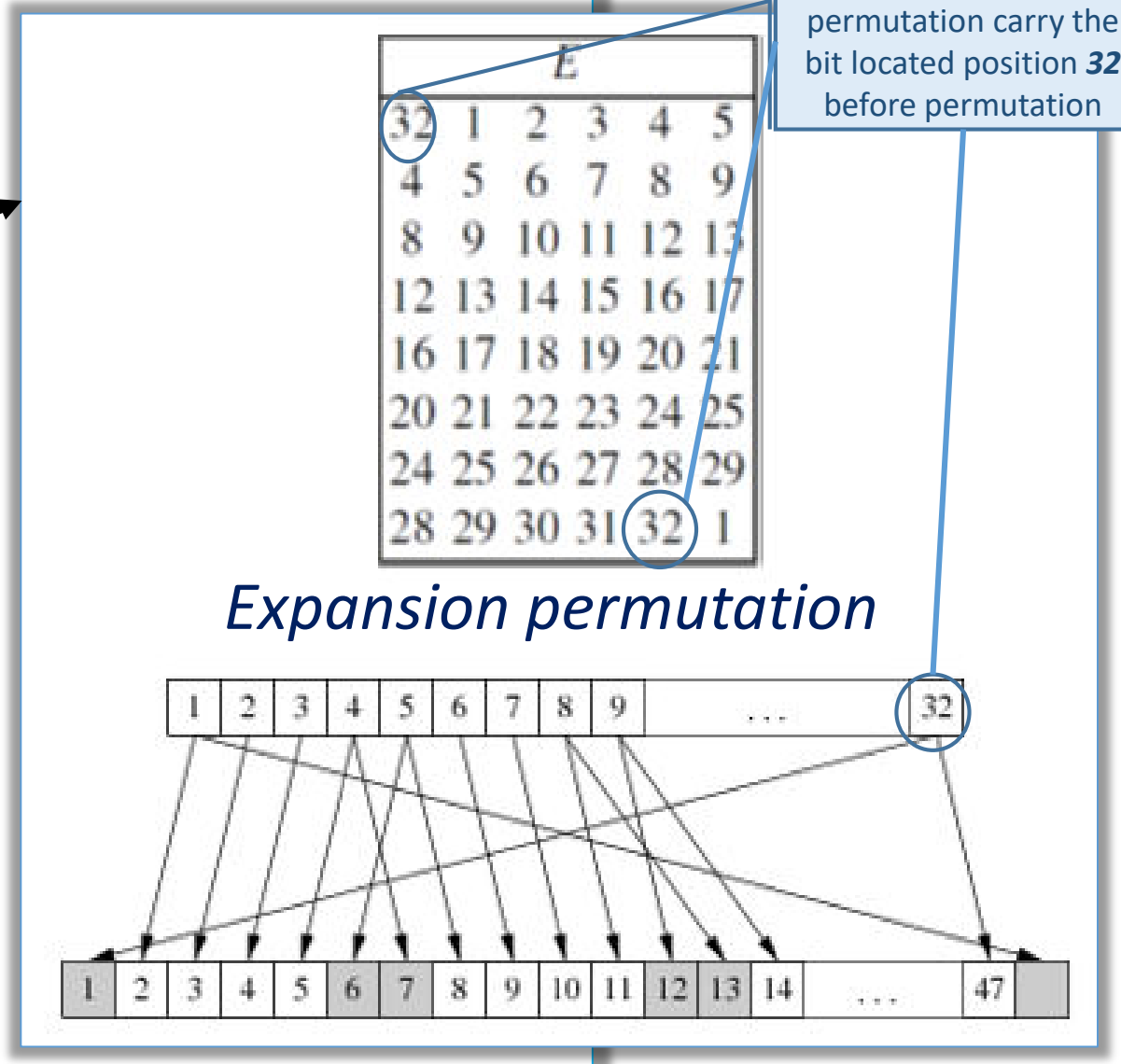
NORTHERN ARIZONA UNIVERSITY

Data Encryption Standard

- 1- History & Description
- 2- Encryption versus Decryption
- 3- The f-function
- 4- Key processor
- 5- Summary & limitations

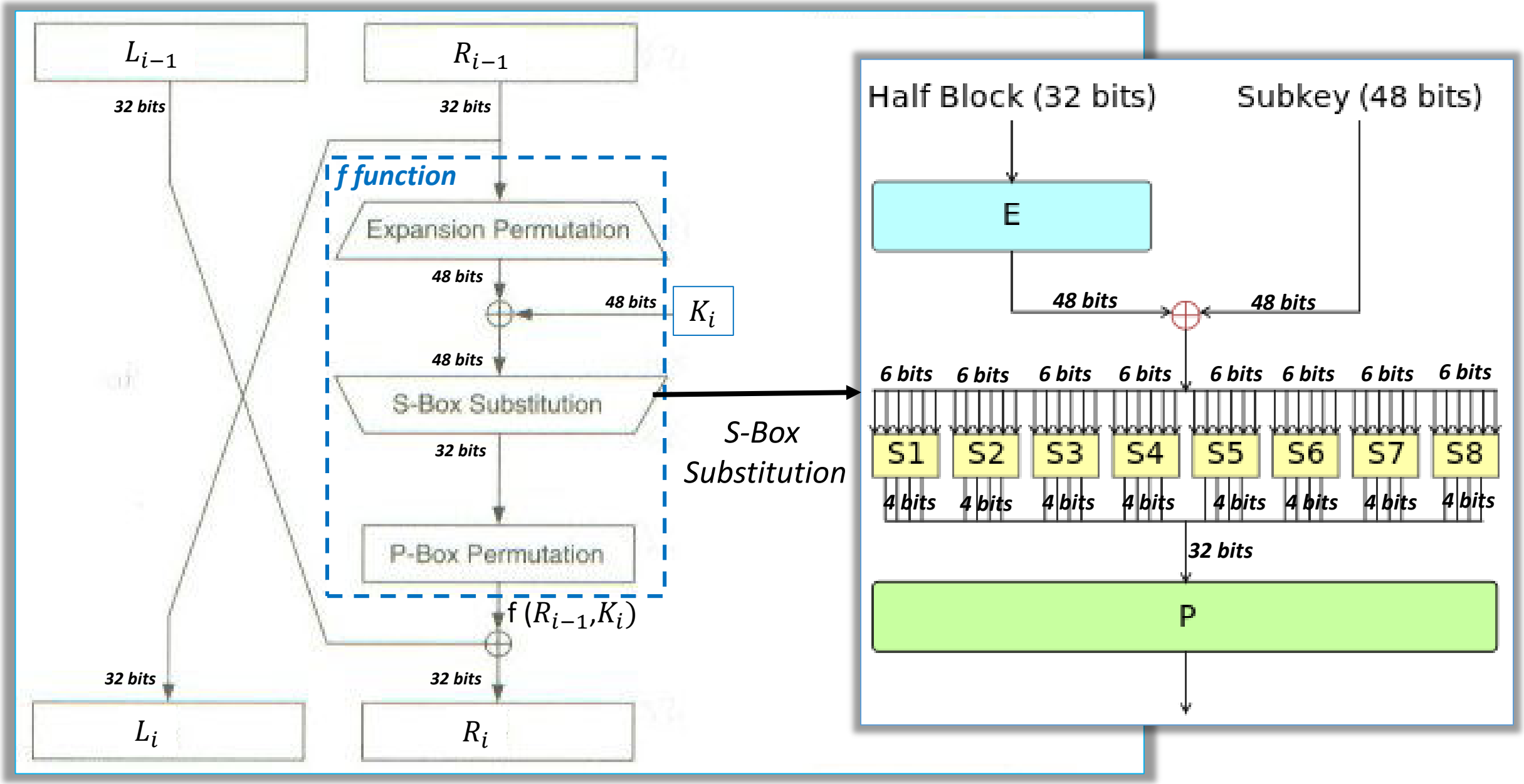
DES: f function – Expansion/Permutation



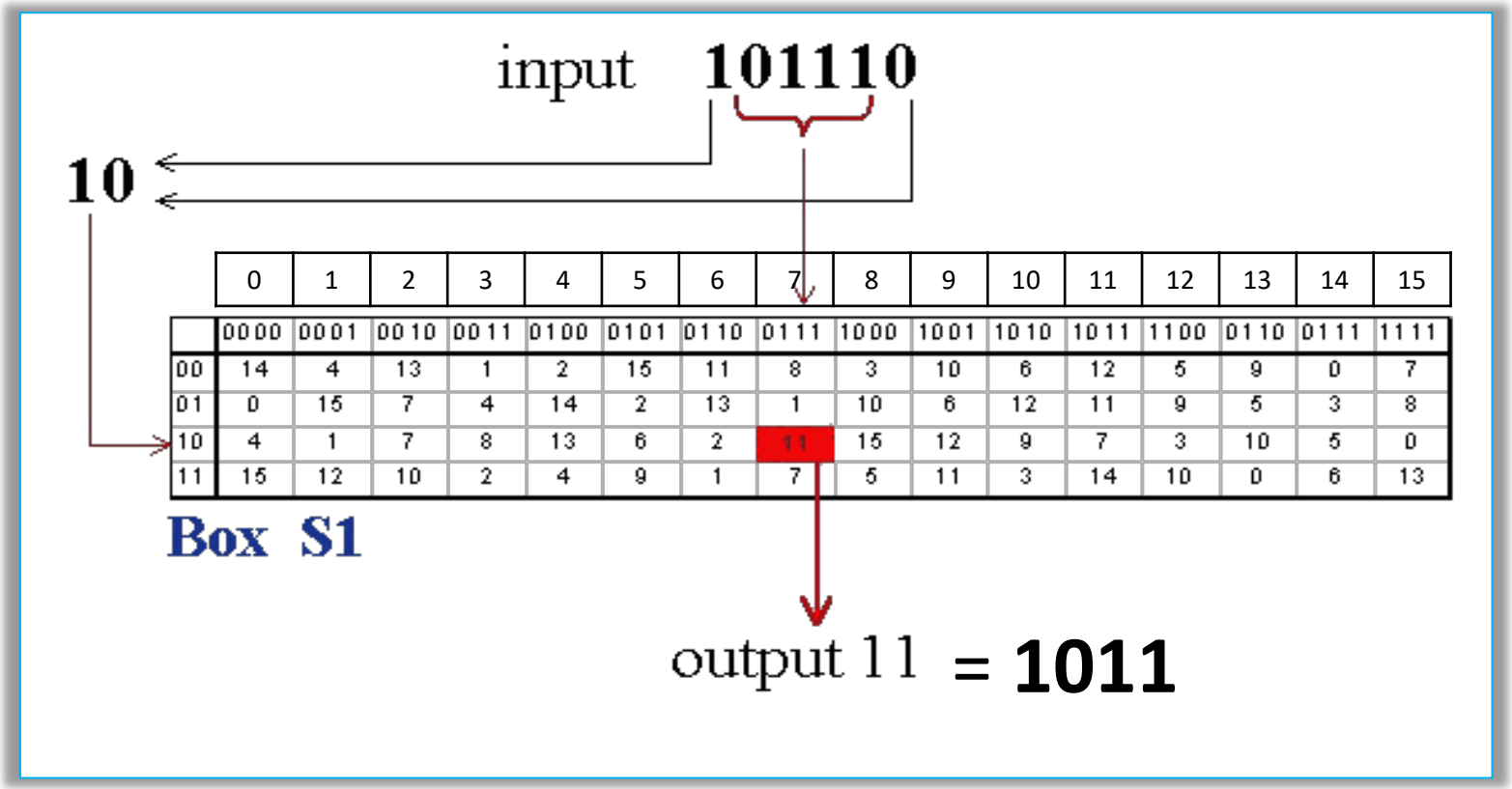


Positions ***1 & 47*** after permutation carry the bit located position ***32*** before permutation

DES: f function – S Box



DES: *description of the* S-BOX



Detail: 8 S-boxes

S_1	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0yyyy1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
0yyyy1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
1yyyy0	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1yyyy1	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
0yyyy1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
1yyyy0	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1yyyy1	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

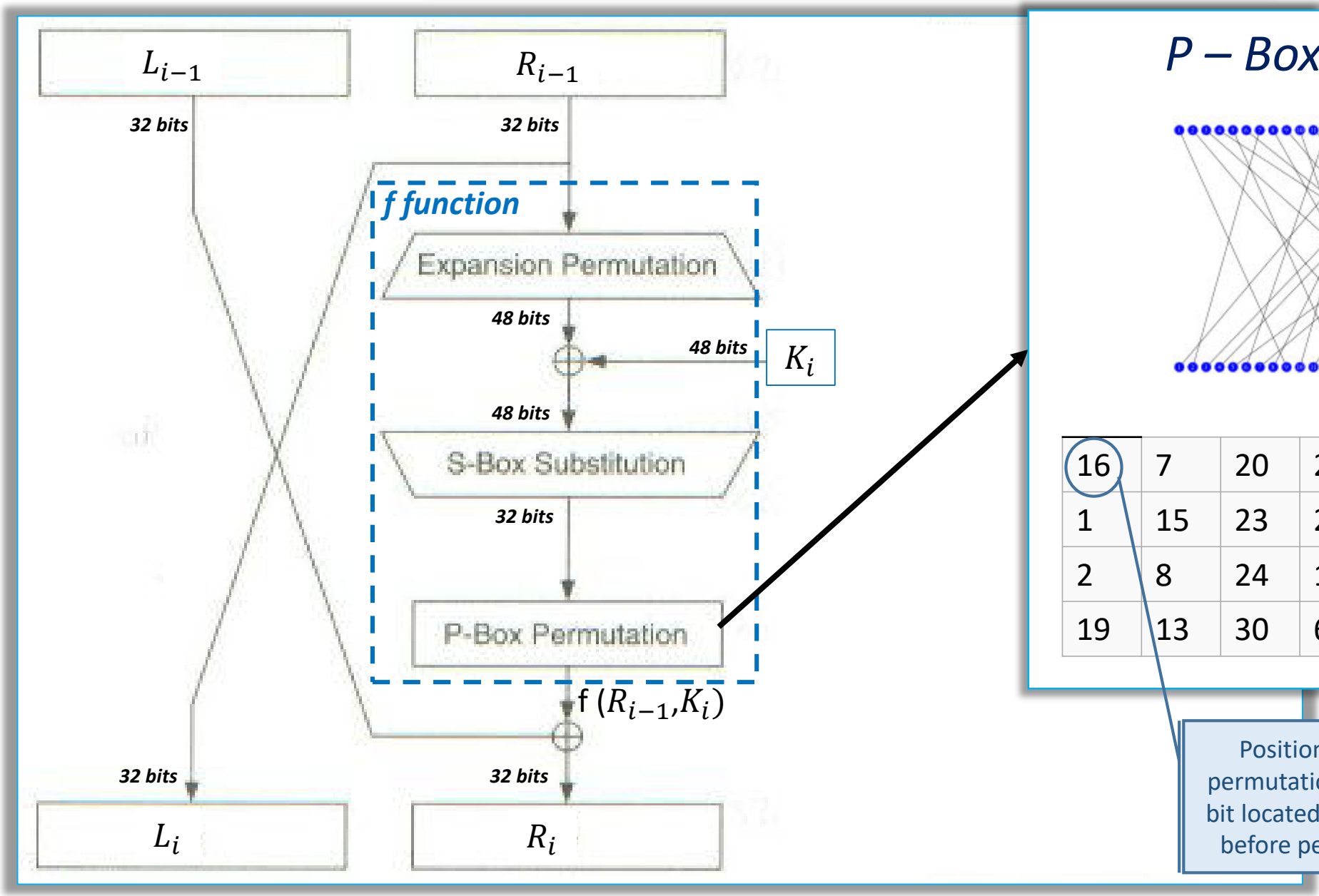
S_5	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0yyyy1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1yyyy0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1yyyy1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
0yyyy1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
1yyyy0	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
1yyyy1	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

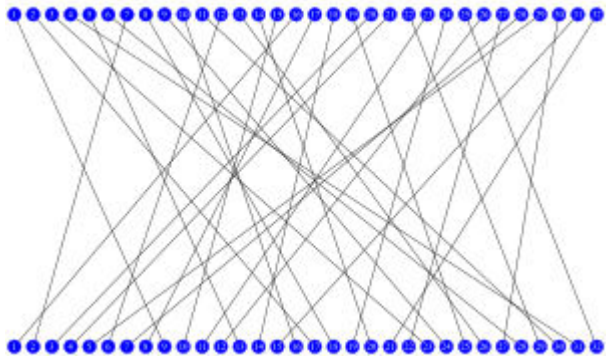
S_7	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
0yyyy1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1yyyy0	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
1yyyy1	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
0yyyy1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
1yyyy0	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
1yyyy1	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES: P-box of the f function



P – Box permutation



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

Positions ***1*** after permutation carry the bit located position ***16*** before permutation

NORTHERN ARIZONA UNIVERSITY

Data Encryption Standard

- 1- History & Description
- 2- Encryption versus Decryption
- 3- The f-function
- 4- Key processor
- 5- Summary & limitations

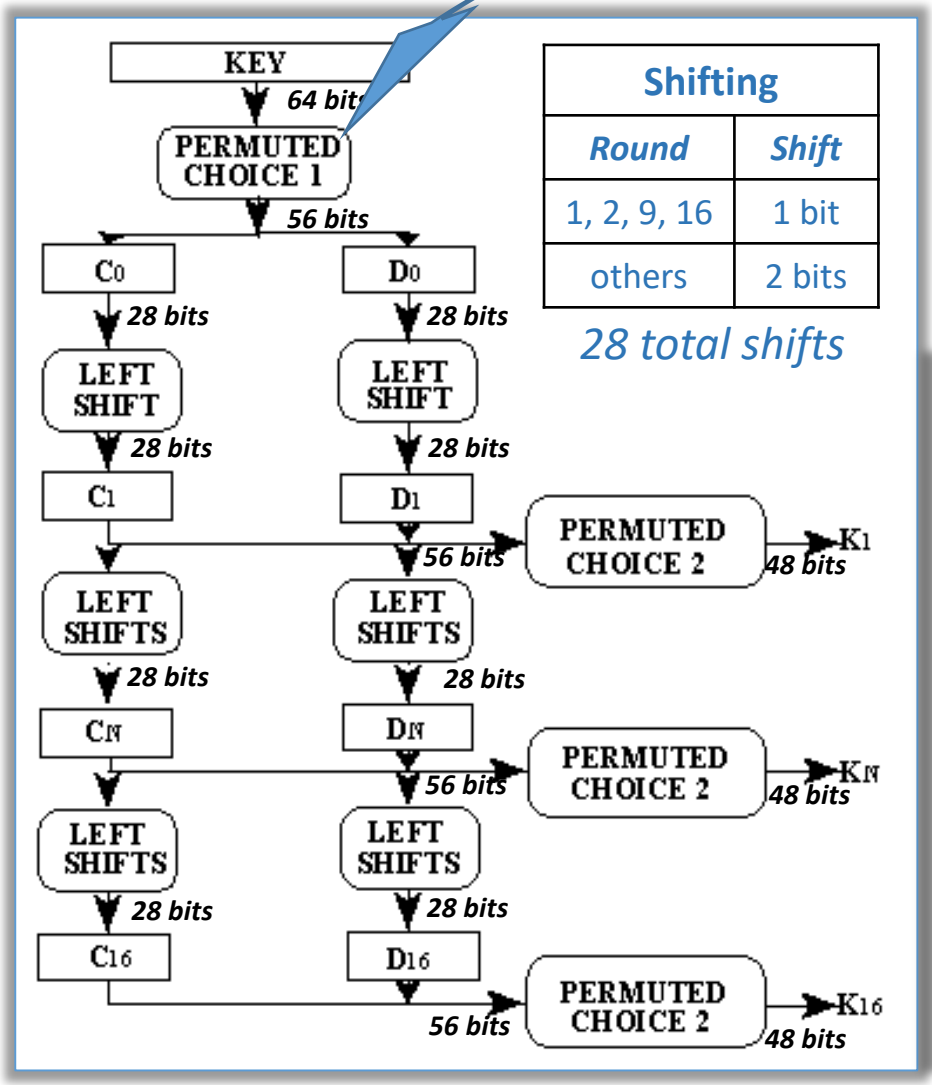
Key processing: permuted choice 1

PCI: only 56 bits of the 64 bits selected;

8, 16, 24, 32, 40, 48, 56, 64: parity bits.

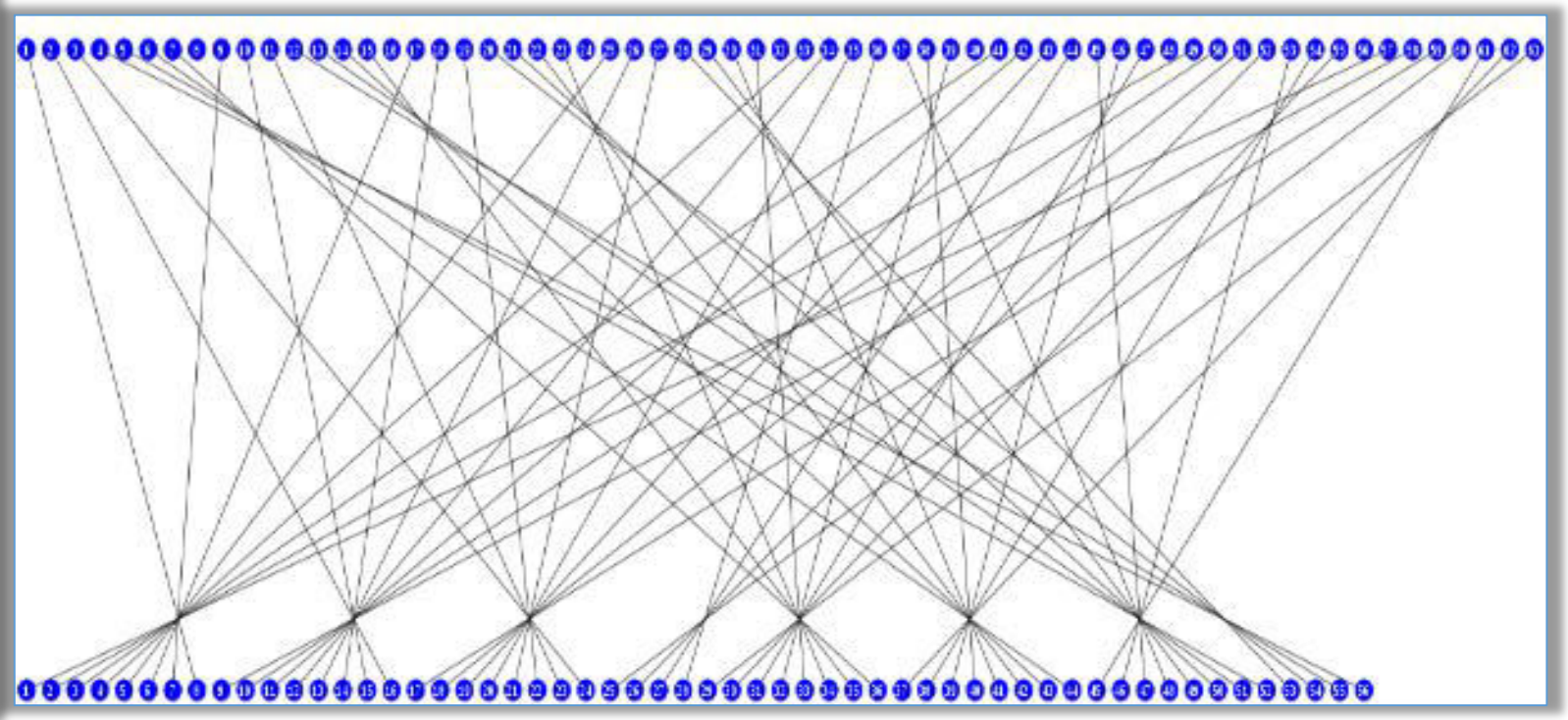
PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for C_i; below for D_i						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Positions ***1*** after permutation carry the bit located position ***57*** before permutation



Shifting	
Round	***Shift***
1, 2, 9, 16	1 bit
others	2 bits

28 total shifts



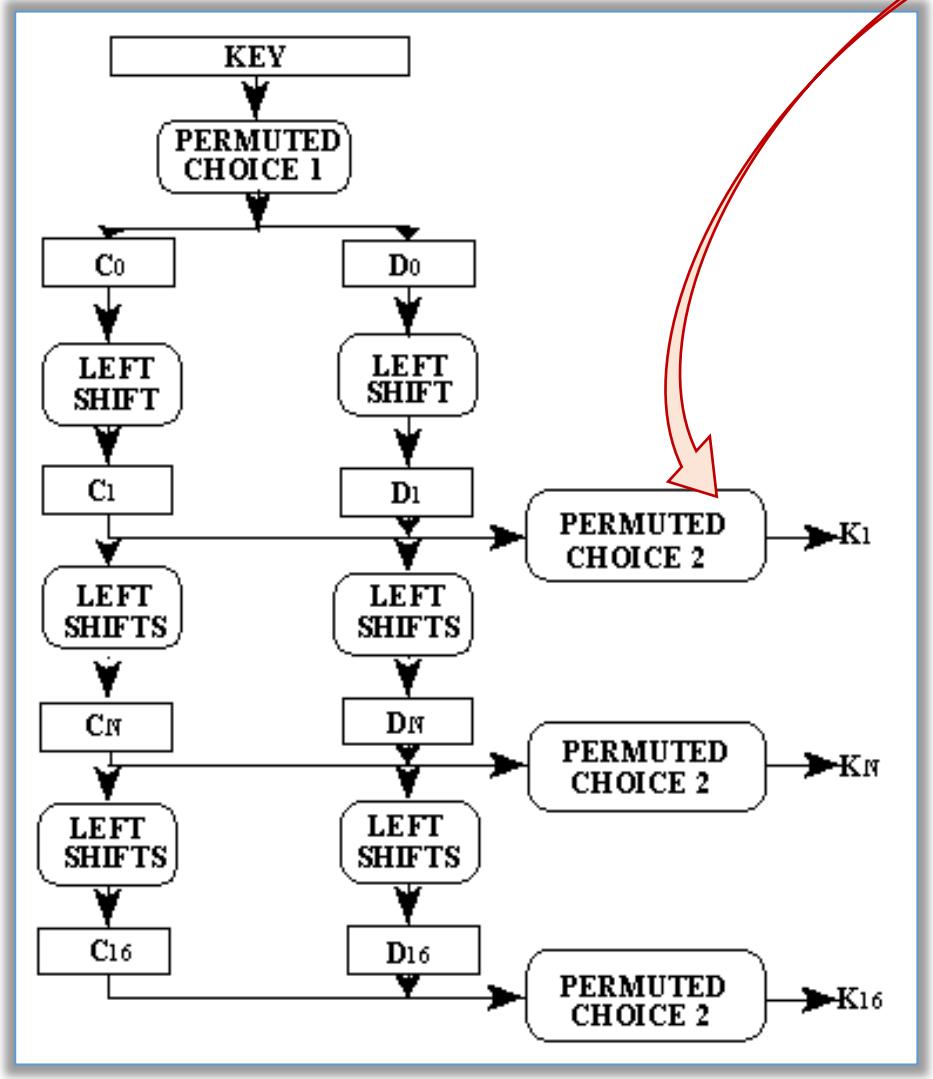
Key processing: permuted choice 2

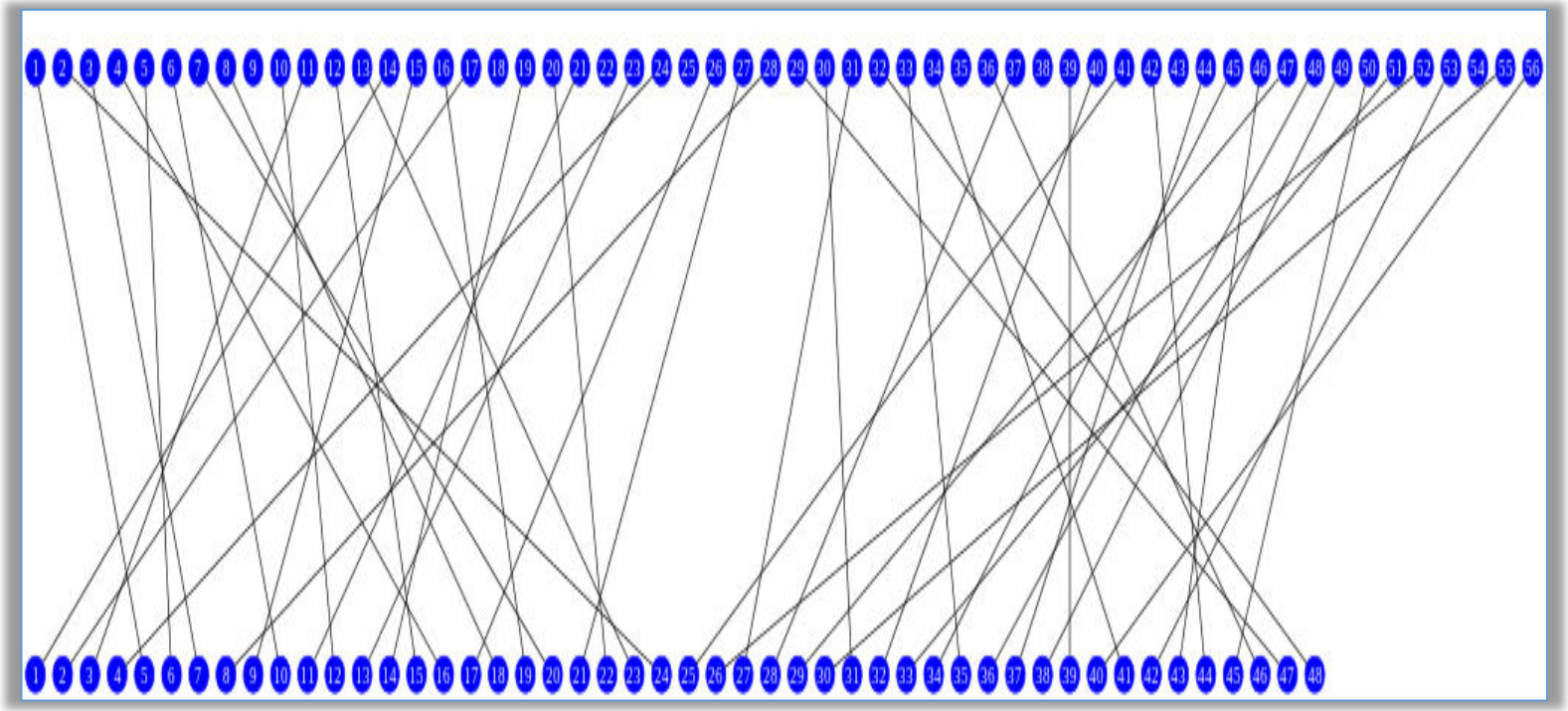
PC2: Only 48-bits of the 56-bit selected;

Left behind: 9, 18, 22, 25, 35, 38, 43, 54.

PC2					
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

Positions ***1*** after permutation carry the bit located position ***14*** before permutation





NORTHERN ARIZONA UNIVERSITY

Data Encryption Standard

- 1- History & Description
- 2- Encryption versus Decryption
- 3- The f-function
- 4- Key processor
- 5- Summary & limitations

Triple DES – Performance comparison

Method	*Properties*	*Strength*
DES	One 56-bit key	Weak
Double DES	Two 56-bit keys	2 X as strong as DES
Two-Key Triple DES	Two 56-bit keys	16 million times as strong as DES
Three-Key Triple DES	Three 56-bit keys	10^{17} as strong as DES
AES	128-bit key	$4\ 10^{21}$ as strong as DES

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu