Network and Information Security
Lecture 13

B.Tech. Computer Engineering
Sem. VI.

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Transposition cipher Cryptanalysis (continue..)

- Better Approach
- Example
- Suppose that Eve has intercepted the ciphertext “EEMYNTAACTTKONSHITZG”
- The message length L=20 means that the number of columns can be 1,2,4,5,10 or 20.
- Eve ignores the first value because it means only one column and no permutation.

- If the number of column is 2, the only two permutations are (1,2), (2,1).
- (1,2) – no permutation
- (2,1) –
  - EE MY NT AA CT TK ON SH IT ZG
  - ee ym tn aa tc kt no hs ti gz (does not make sense)
  - Therefore (2! -1) trials

- Next, (4! -1) trials (24 -1) [first one is (1 2 3 4)]
- Next, (5! -1) trials (120 -1) [(1 2 3 4 5) does not make permutation]
- This has to be done till we find proper guess
- Worst case

  = (2! -1) + (4! -1) + (5! -1) +(10! -1) + (20! -1)

  Number of trials are required which are better than the bruteforce

- Pattern attack
- The cipher text created from the keyed transposition cipher has some repeated pattern

e	n	e	m	y	**a**	**t**	**t**	**a**	**c**	k	s	t	o	n	**i**	**g**	**h**	**t**	**z**
3	1	4	5	2	**3**	**1**	**4**	**5**	**2**	3	1	4	5	2	**3**	**1**	**4**	**5**	**2**
e	e	m	y	n	**t**	**a**	**a**	**c**	**t**	t	k	o	n	s	**h**	**i**	**t**	**z**	**g**

e n e m y

a t t a c

k s t o n

i g h t z

3 1 4 5 2

e e m y n

t a a c t

t k o n s

h i t z g

e t t h e a k i m a o t y c n z n t s g

3 8 13 18 1 6 11 16 4 9 14 19 5 10 15 20 2 7 12 17

Difference between 2 adjacent is 5 in all the groups

- If Eve knows/ can guess the number of columns (which is 5 in this case) she can organize the ciphertext into groups of 4 characters.
- Permuting the groups can provide clue to find the plaintext.
- In the above example
- L =20 , number of rows = L/number of columns
- Number of rows = 20/5 =4

- Fill the cipher text

Row 1 e e m y n

Row 2 t a a c t

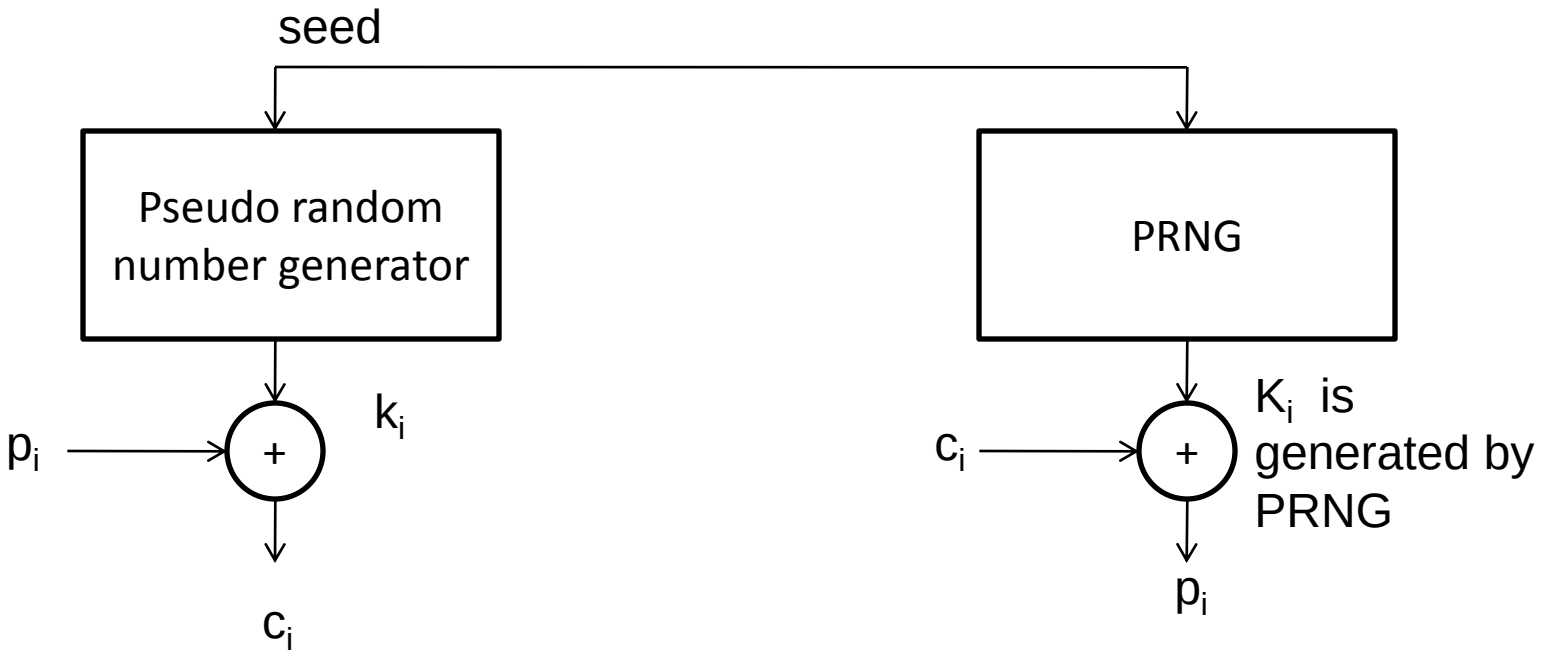
Row 3 t k o n s

Row 4 h i t z g

Find permutation which gives meaningful answer when read row by row

- Traditional ciphers
  - Block cipher (encrypts more than 1 characters at a time)
    - Hill cipher, playfair cipher
  - Stream cipher (encrypts one characters at a time)
    - Shift cipher

- How to approximate one time pad cipher?



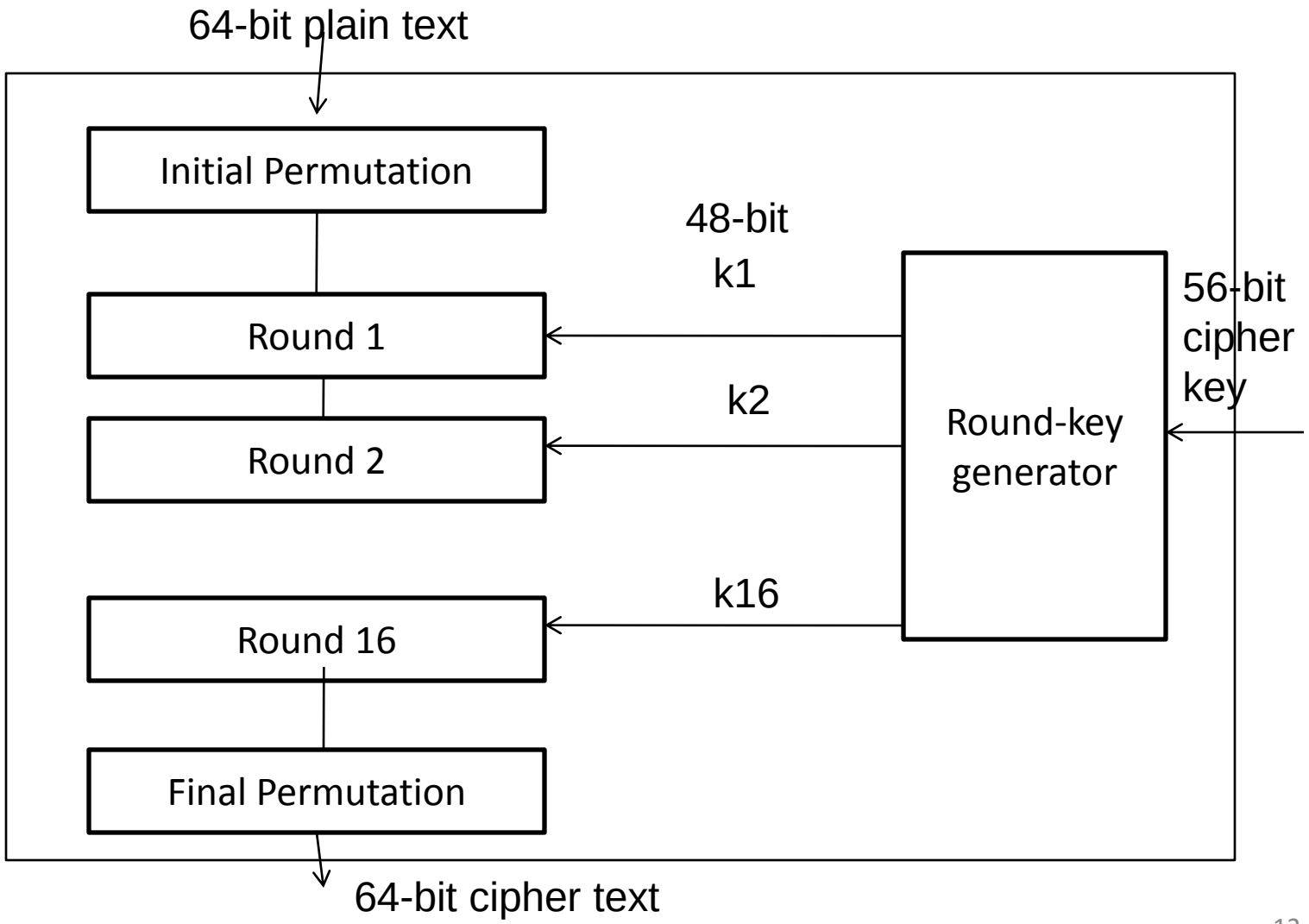
$c_i = p_i \oplus k_i$

$p_i = c_i \oplus k_i$

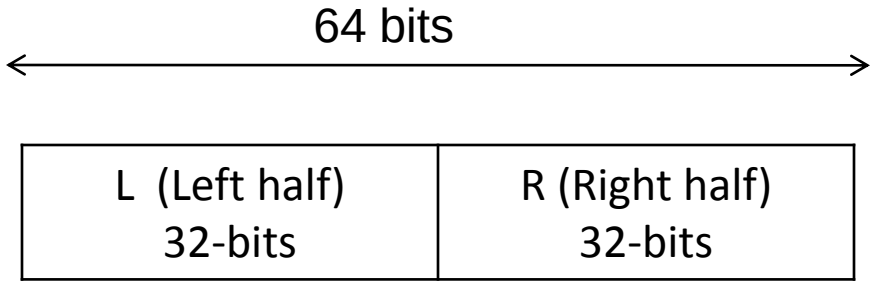
Data Encryption Standard (DES)

- It is symmetric key cipher
- It is block cipher published by NIST (National Institute of Standard and Technology)
- Block size = 64 bits
- i.e. It encrypts 64 bits at a time
- It has 16 rounds
- Structure of each round is same

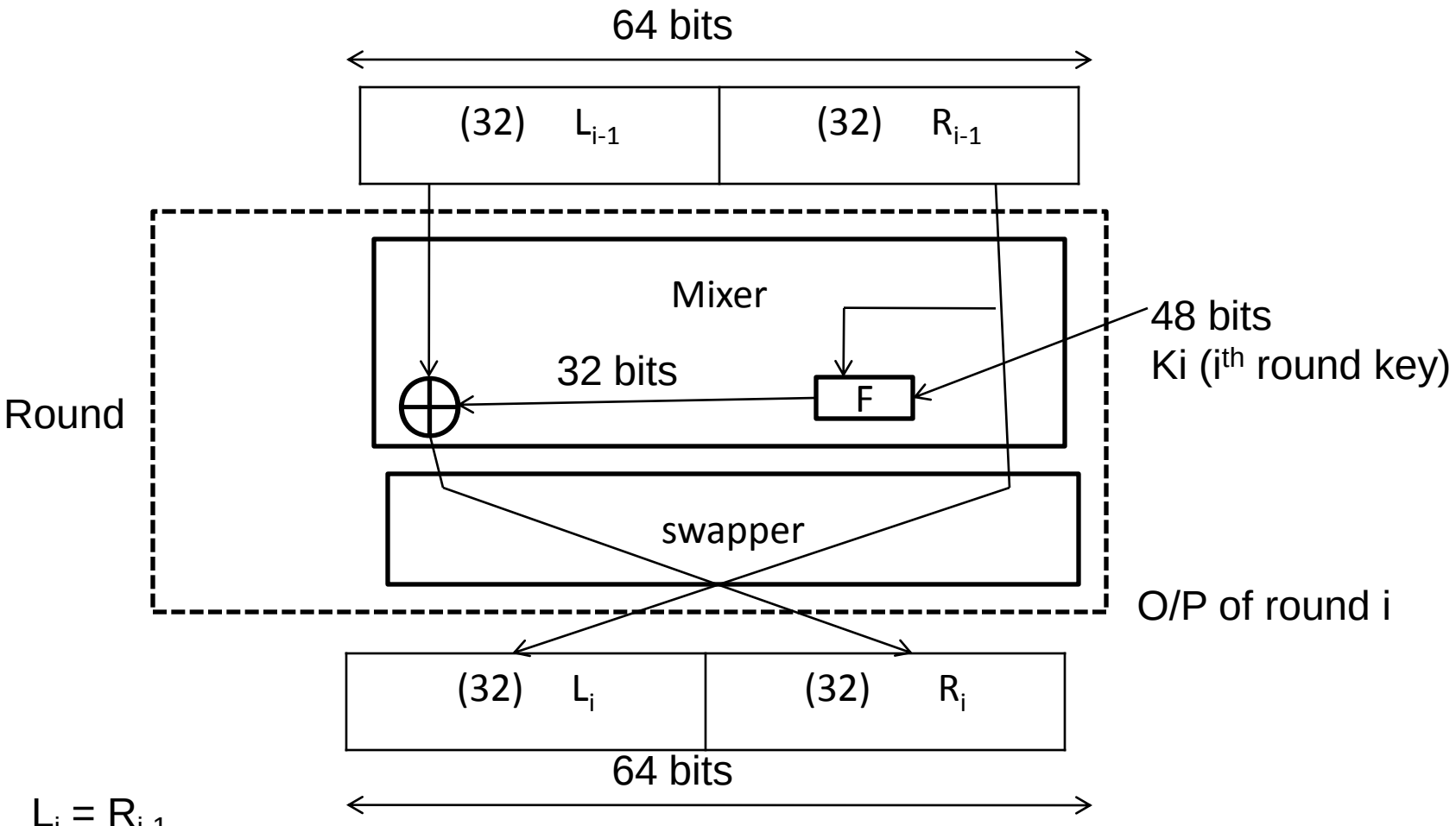
DES Structure



- Round structure
- For round number i
- 64 bits input to round i is divided into two halves each of 32 bits



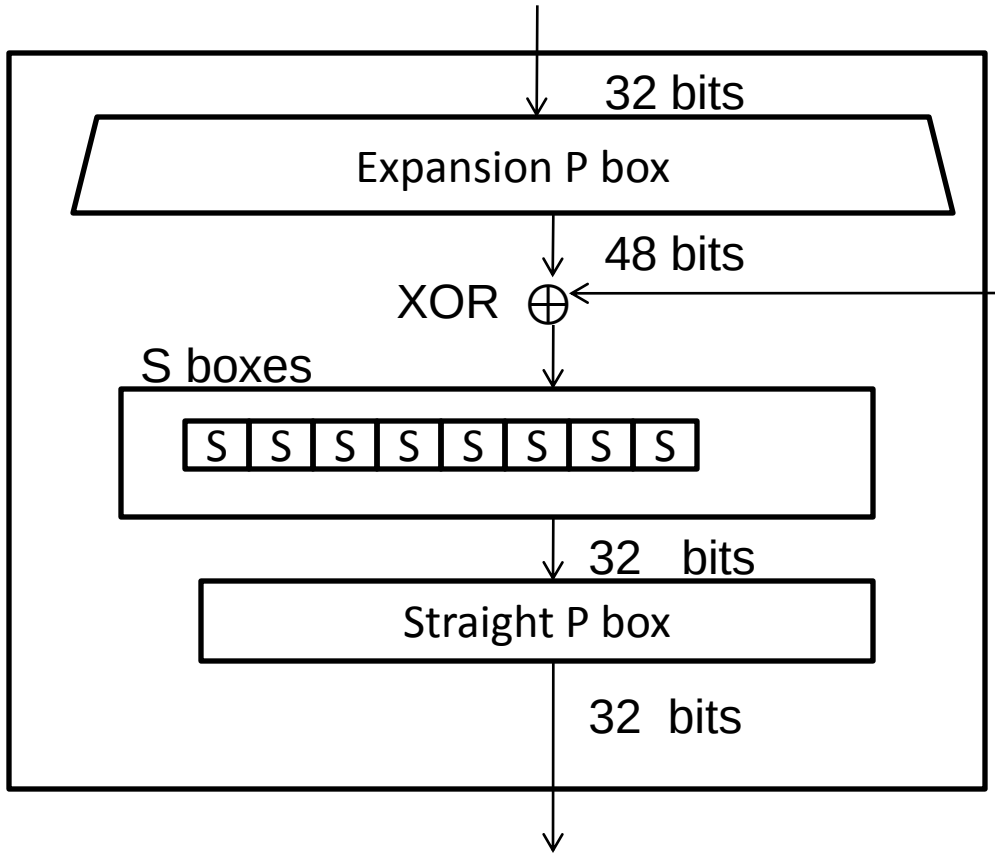
A Round in DES



$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$ F is Round function

DES Function



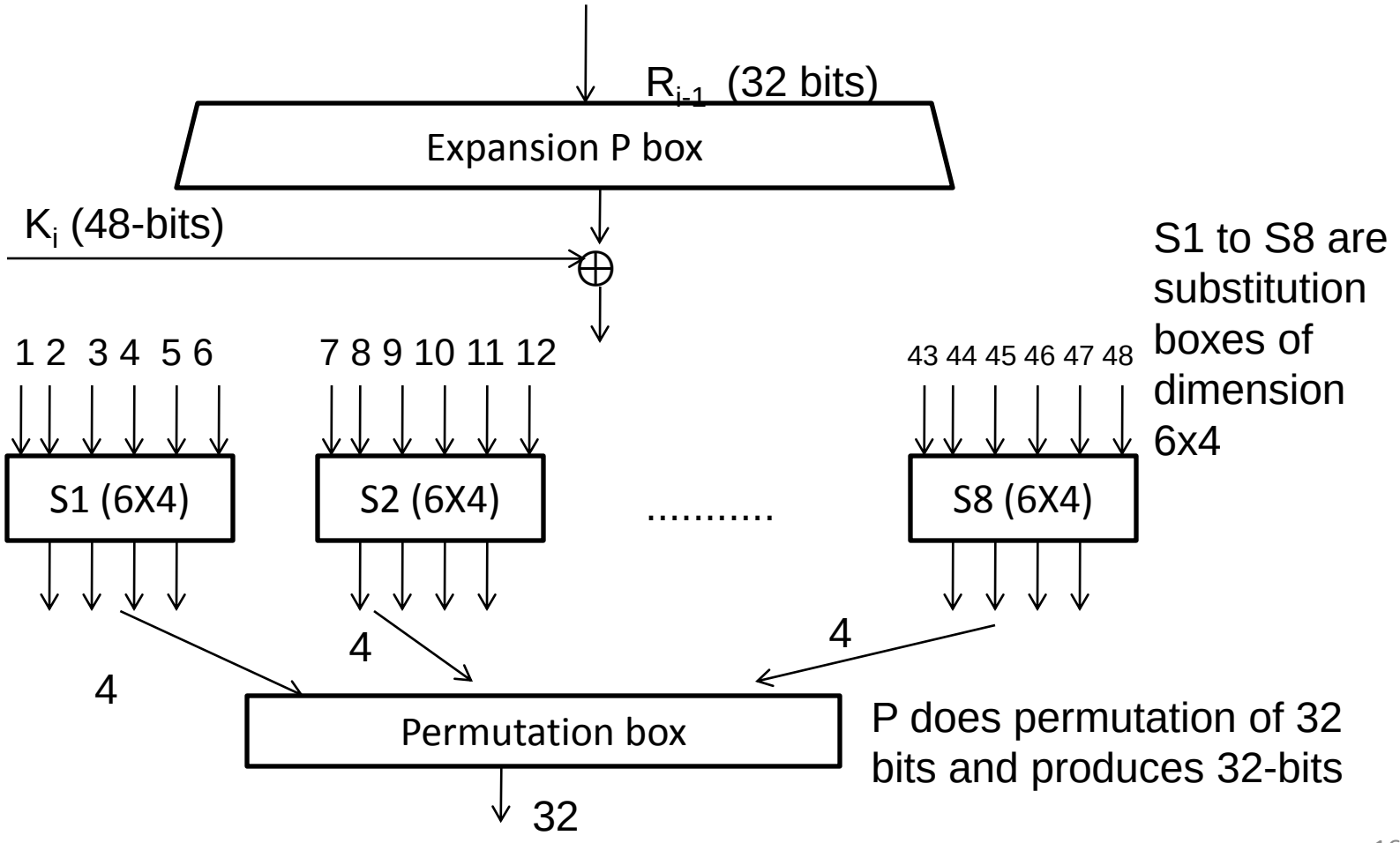
$f(R_{i-1}, K_i)$

K_i (48-bits)

An expansion P box
A whitener (that adds key)
a group of S-boxes
A straight P-box

S-boxes

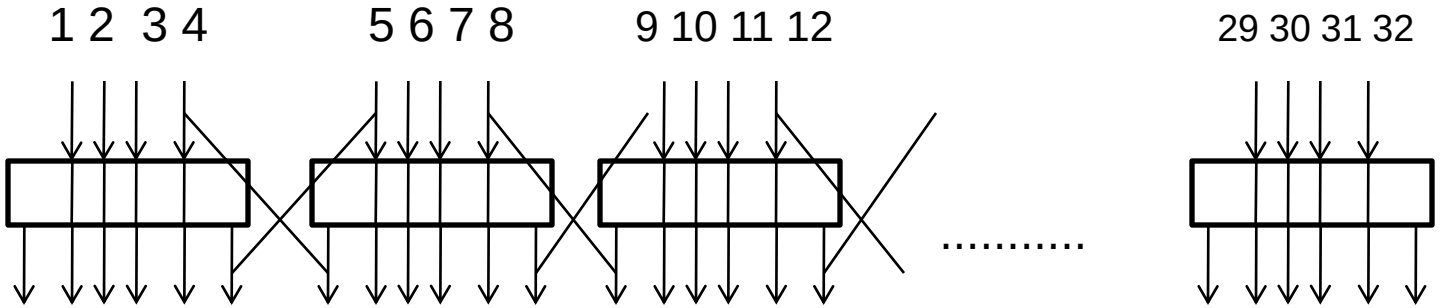
Round function, Input: R_{i-1} (32 bits), K_i (48 bits), Output: 32 bits



- Thus output of rand function F is 32 bits

1. R_{i-1} is expanded to 48- bits
2. 48-bits are ex-ored with K_i (ith round key of 48 bits)
3. Then 8 groups each of 6 bits are given to respective S-boxes to produce 8 groups of 4 bits
4. Output 32 bits are permuted

Expansion permutation



First bit is copied from last 32nd bit of input

last bit is copied from first 1st bit of input

Expansion P-box table

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

- First entry (1st row , 1st column) is 32 which indicates the index of bit from where we need to copy i.e. 1st bit of output is 32nd bit of input
- Thus by copying bits, we are able to generate 48 bits
- Basically we are adding redundancy i.e. We are creating 16 more bits by copying bits from certain position