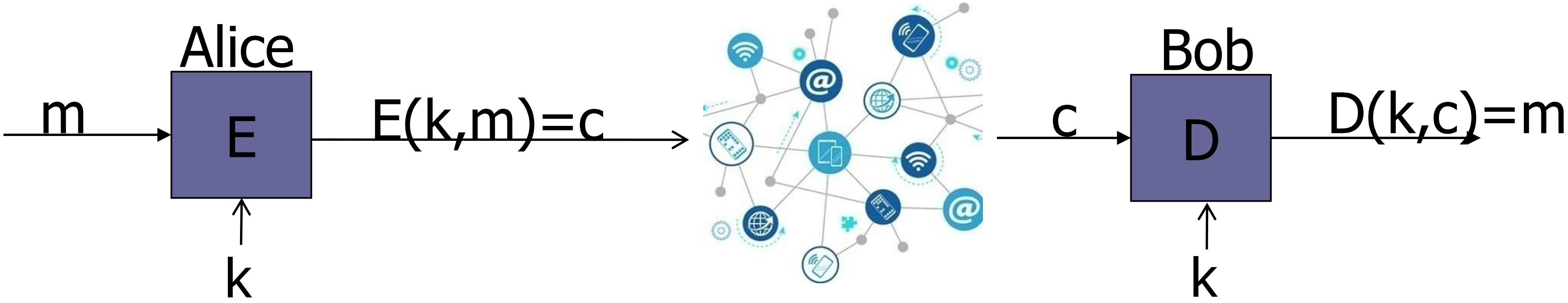
Information Security CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Symmetric Encryption



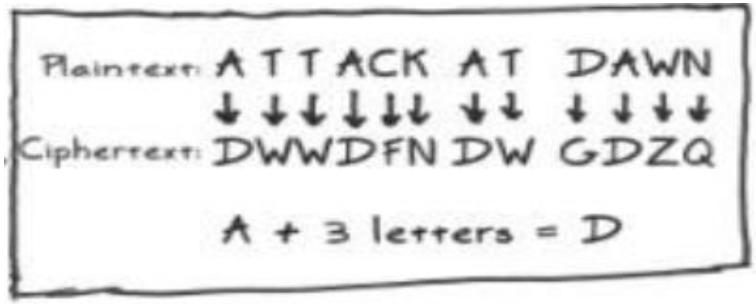
E, D: Algorithms **k: secret key**

m: plaintext **c: ciphertext**

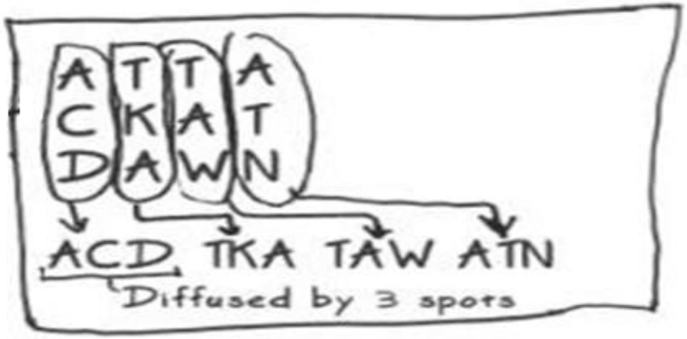
Encryption algorithm Should be publicly known

Early days techniques

- Confusion
  - Replacing of some bit strings with other bit strings
  - Also called substitution or Caesar's cipher

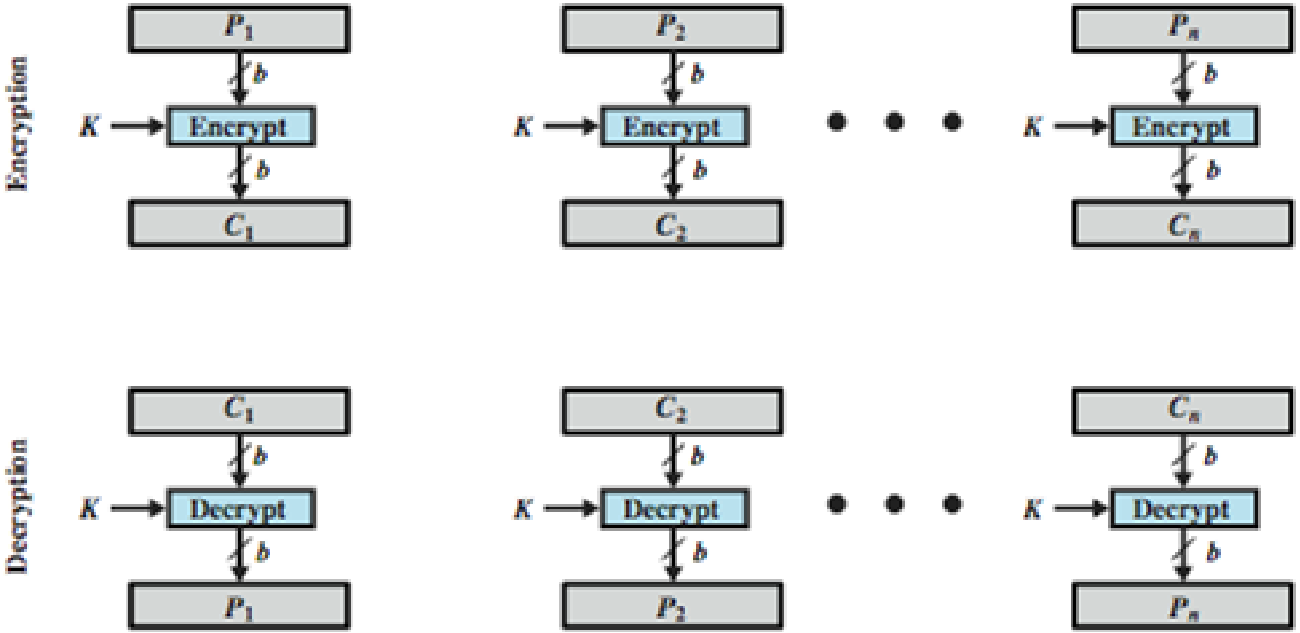


- Diffusion
  - Changing order of bit strings
  - Also called permutation/transposition



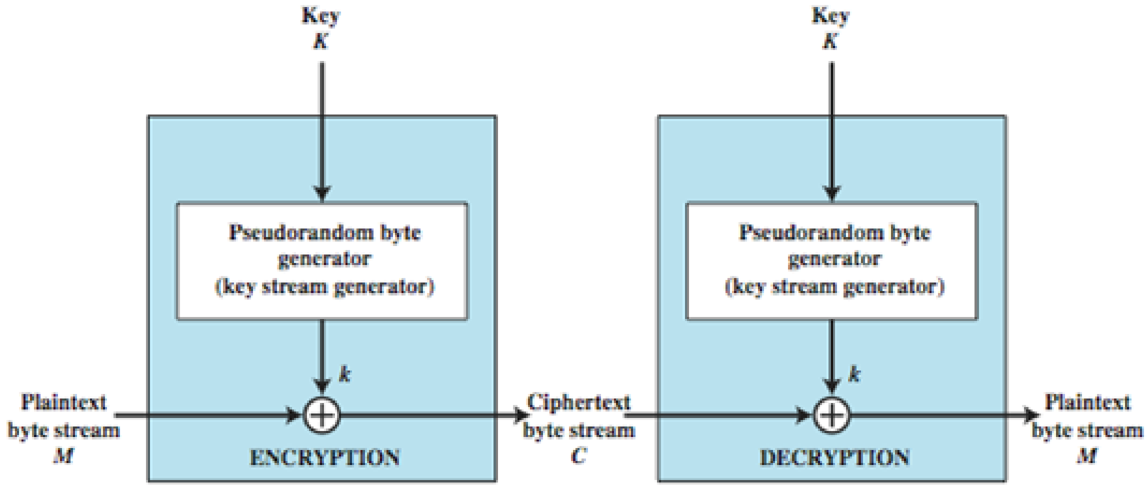
Block Cipher

- Processes the plaintext input in fixed-size blocks
- produces a block of cipher text of equal size for each plaintext block.



Stream Cipher

- Processes the input elements (typically 1 byte at a time) continuously, producing output one element at a time
- With a properly designed pseudorandom number generator, a stream cipher can be as secure as block cipher of comparable key length.
- The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers.
- The advantage of a block cipher is that you can reuse keys.


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

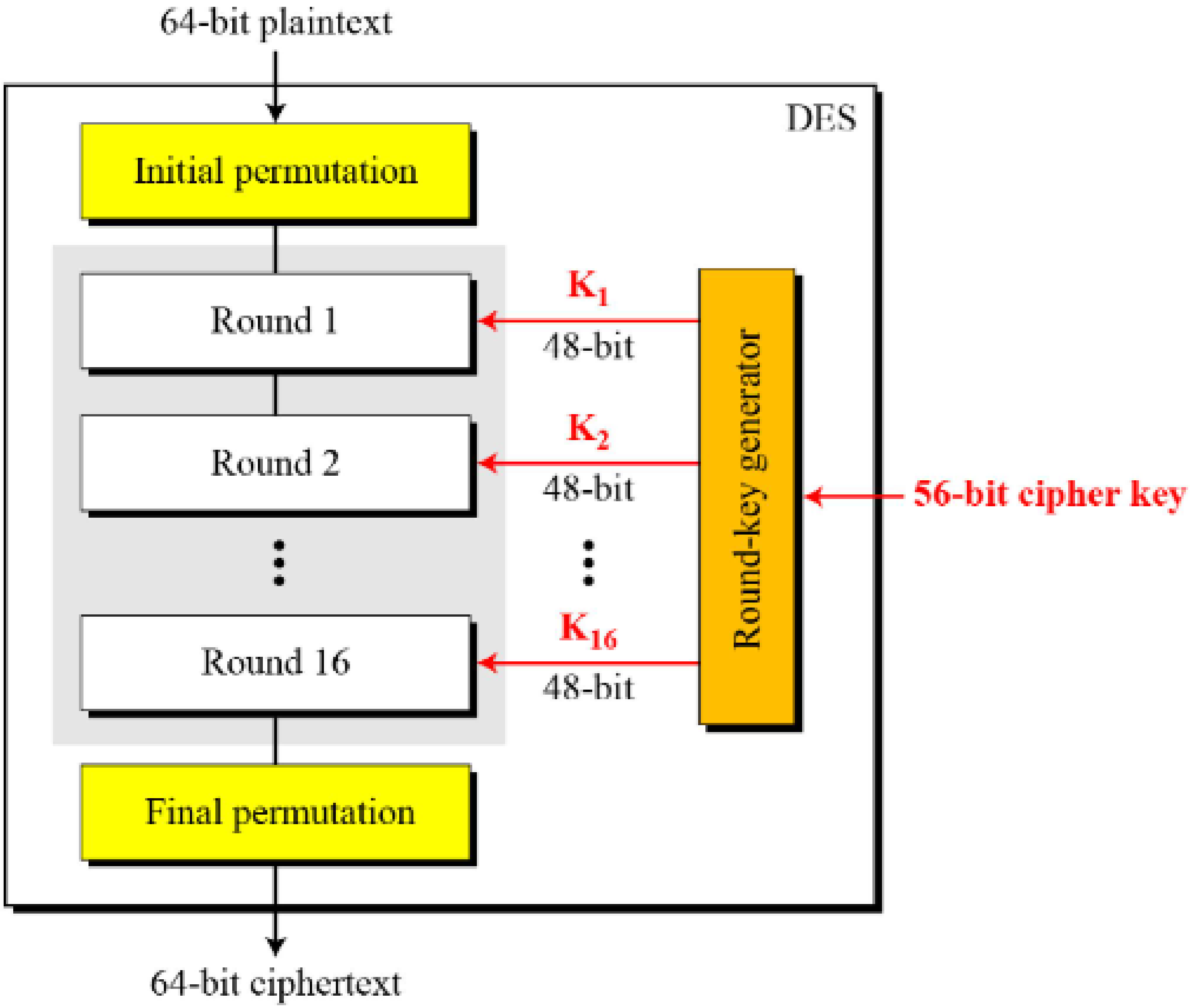
Data Encryption Standard (DES)

- Data Encryption Standard (DES) is the most widely used encryption scheme
  - uses 64 bit plaintext block and 56 bit key to produce a 64 bit cipher text block
  - concerns about algorithm & use of 56-bit key

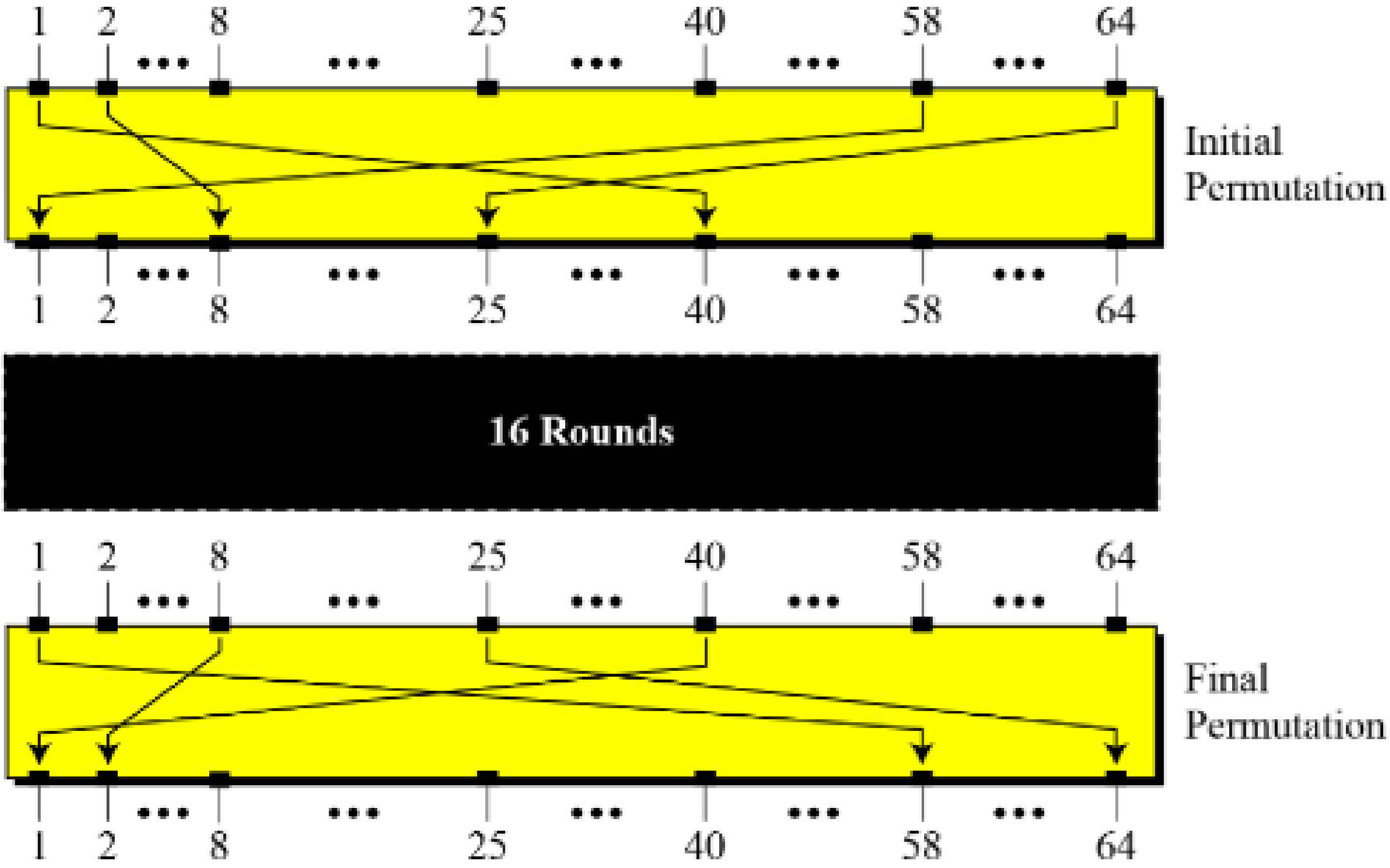
- Concerns
- The first concern refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm.

- A more serious concern is key length. With a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} keys which can be broken easily.

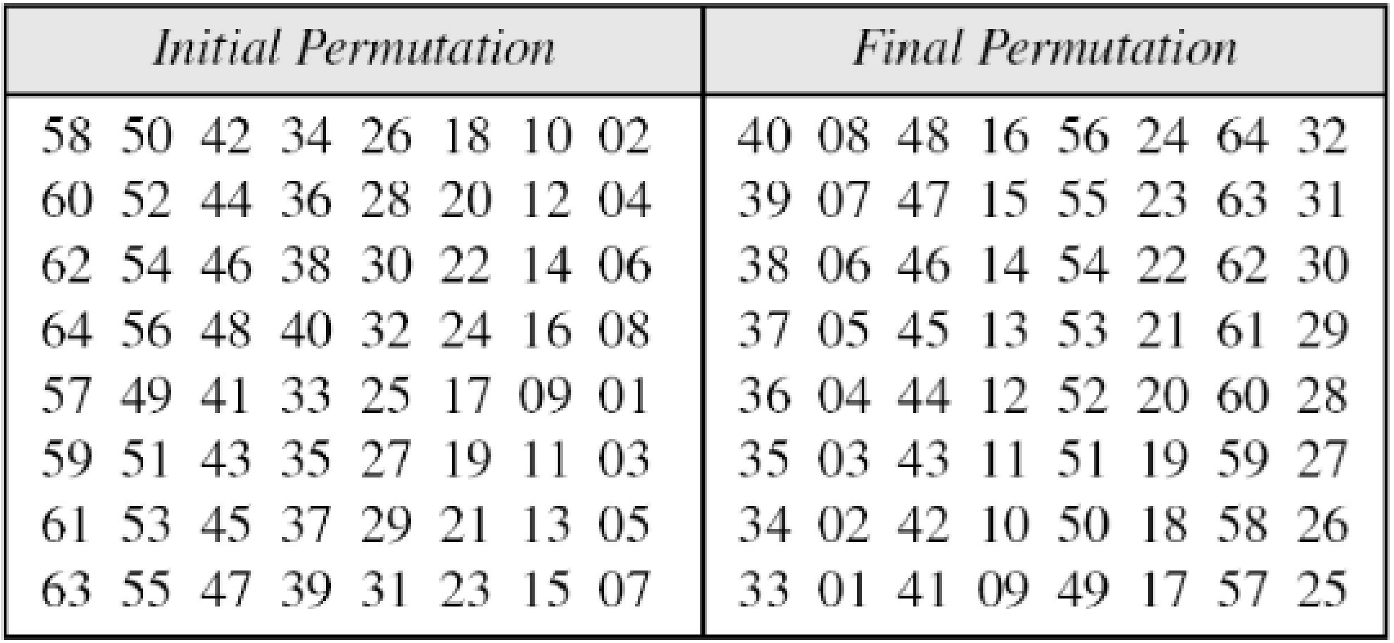
DES


64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K1
48-bit
K2
48-bit
K16
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

Initial and final permutation steps



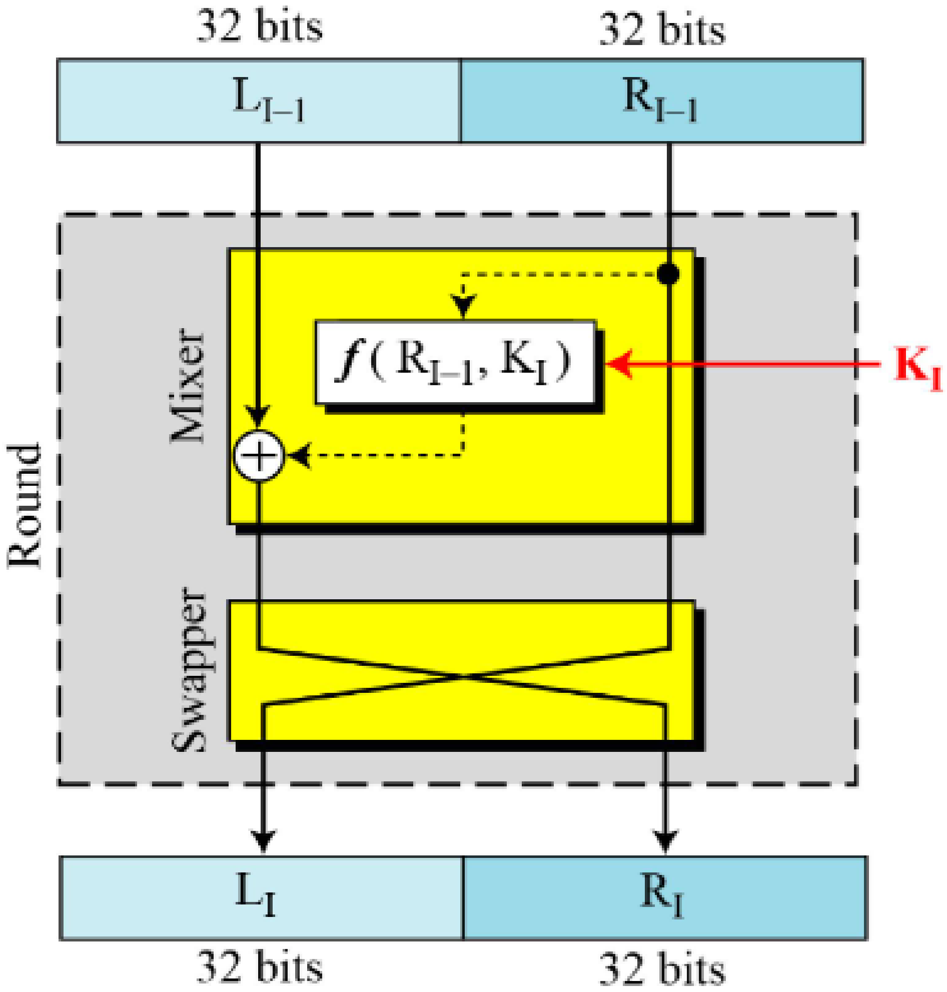
Initial and final permutation tables



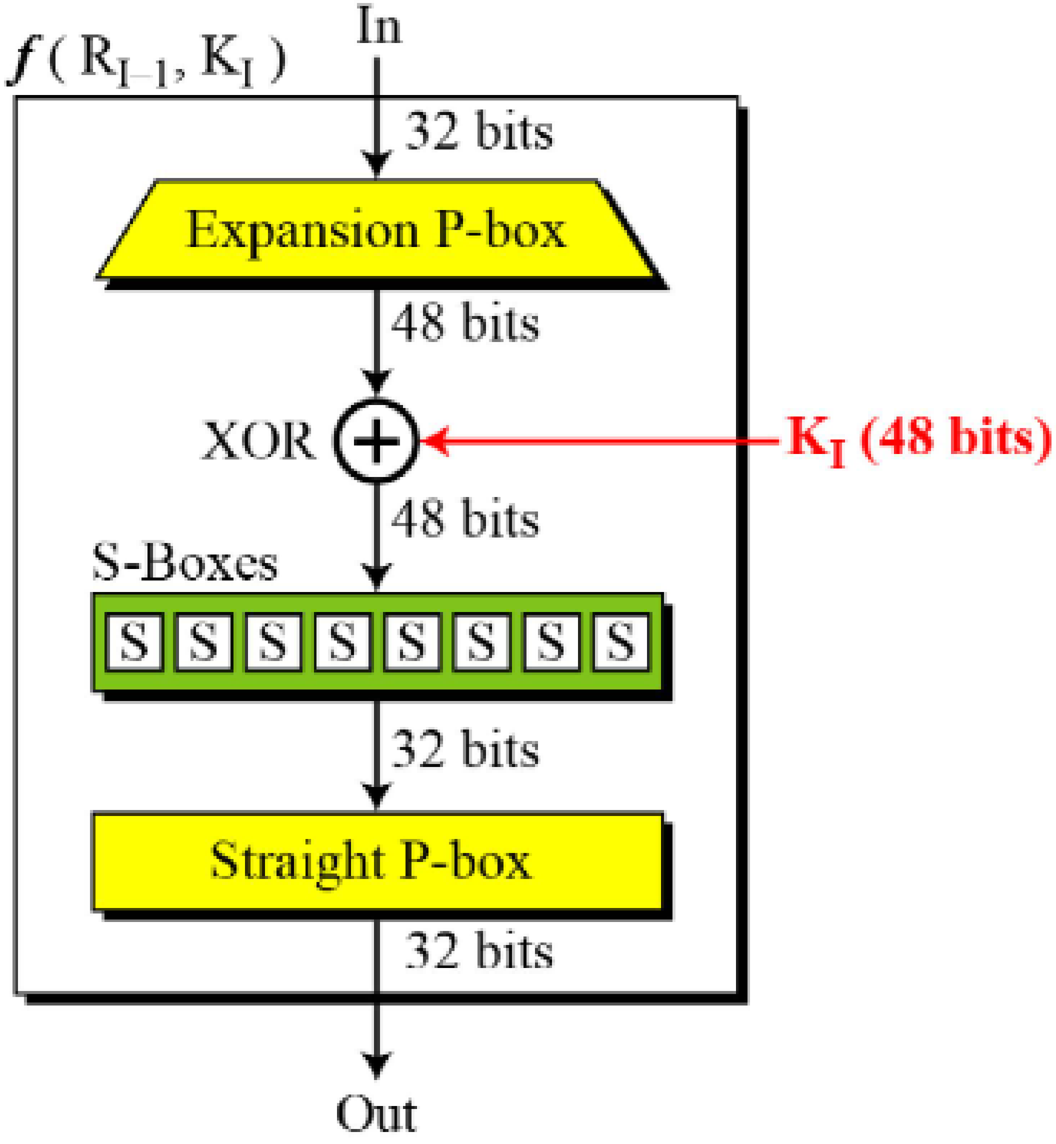
Initial Permutation								*Final Permutation*							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43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

A round in DES (Feistel cipher)

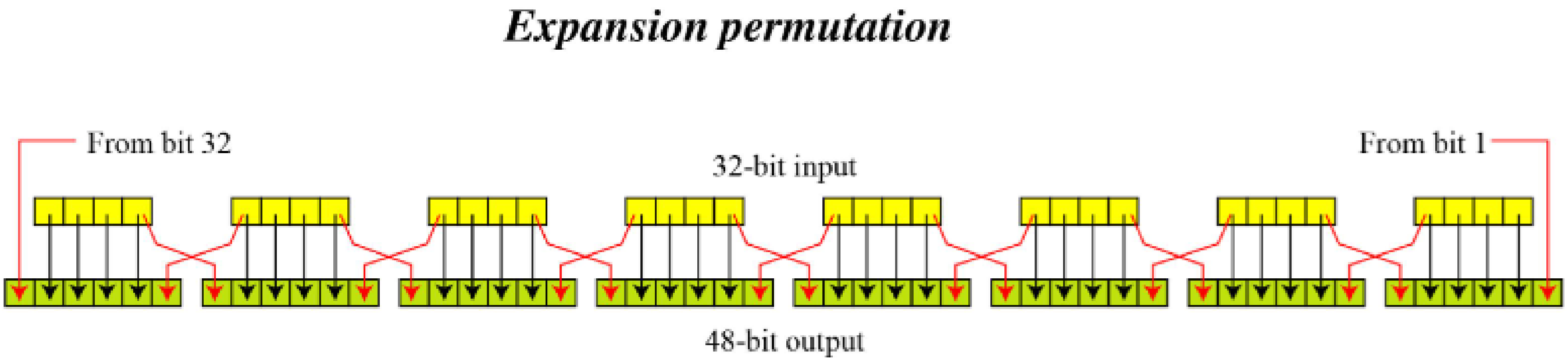
A round in DES (encryption site)



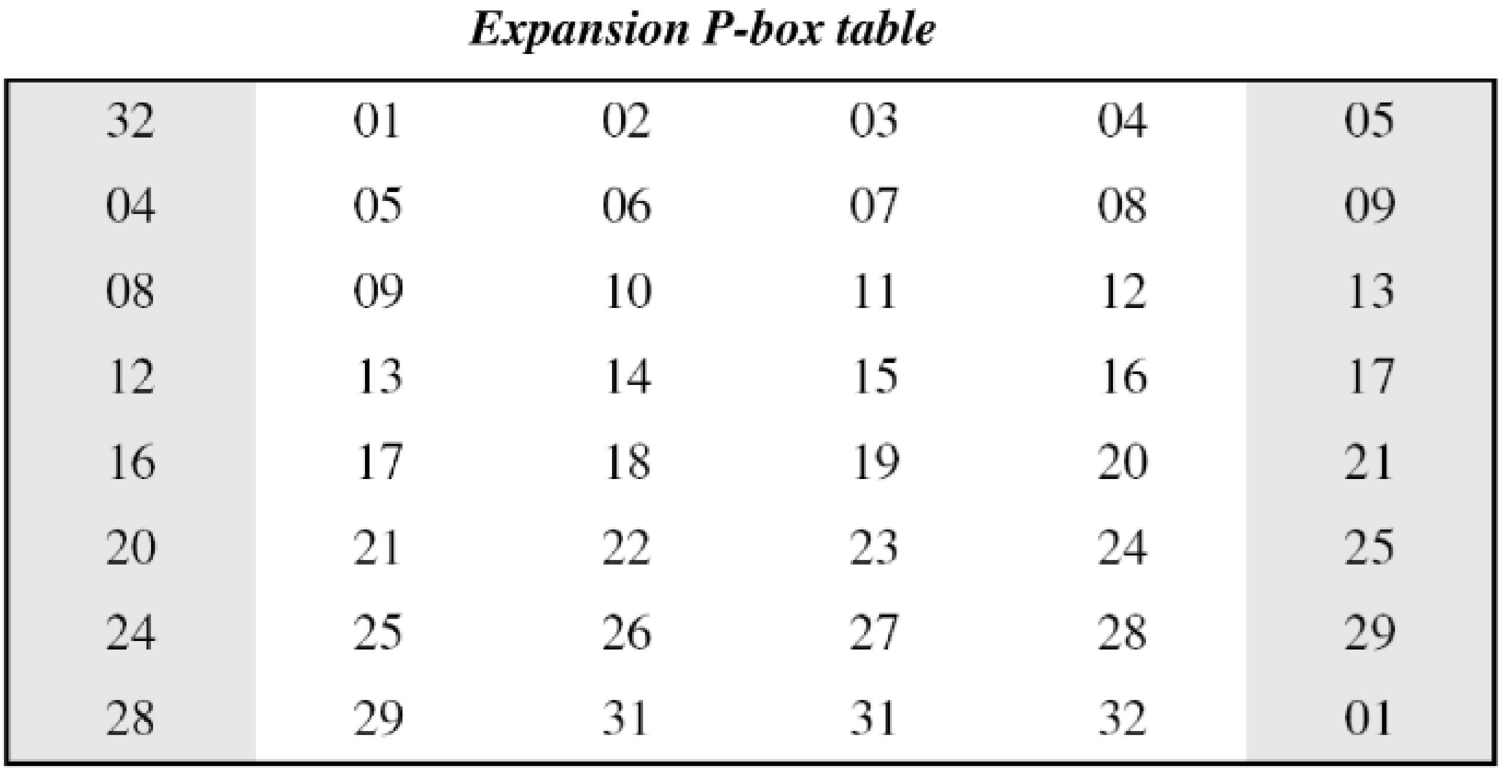
DES function



Expansion mechansim



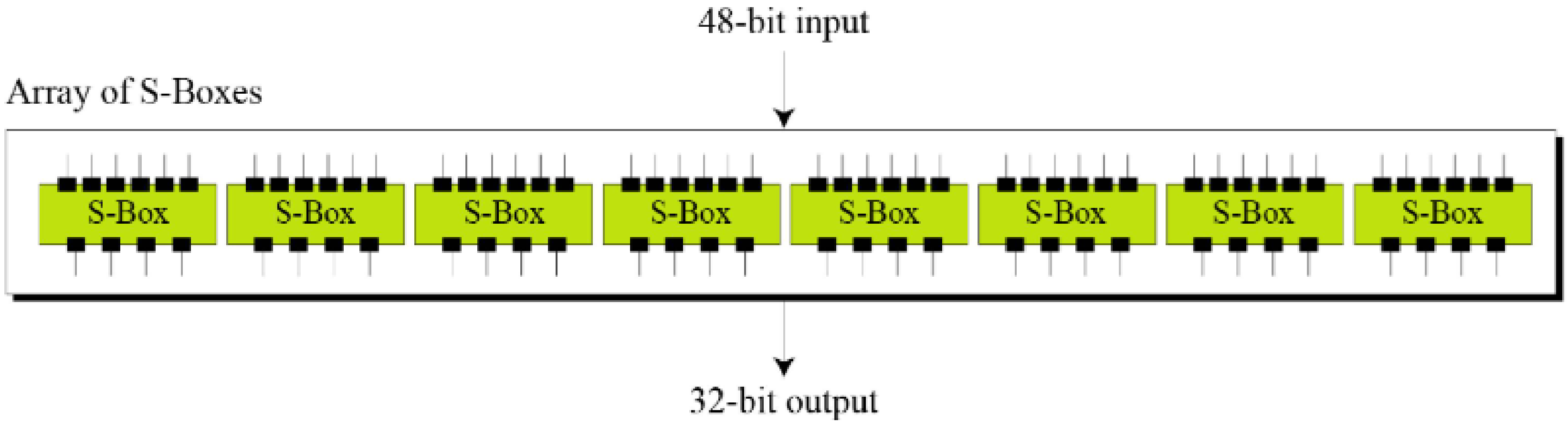
Expansion table



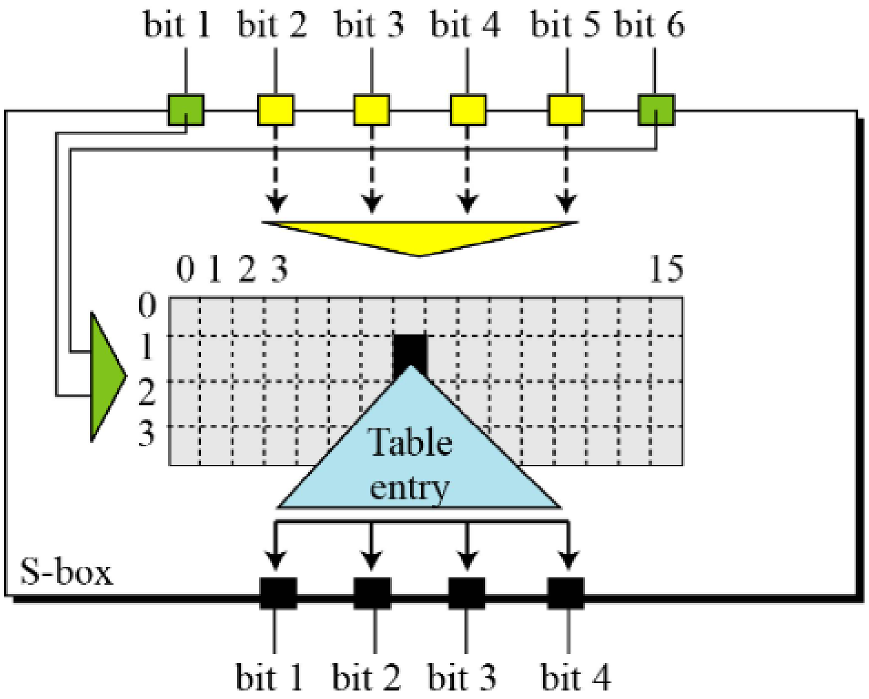
Expansion P-box table

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

S-box

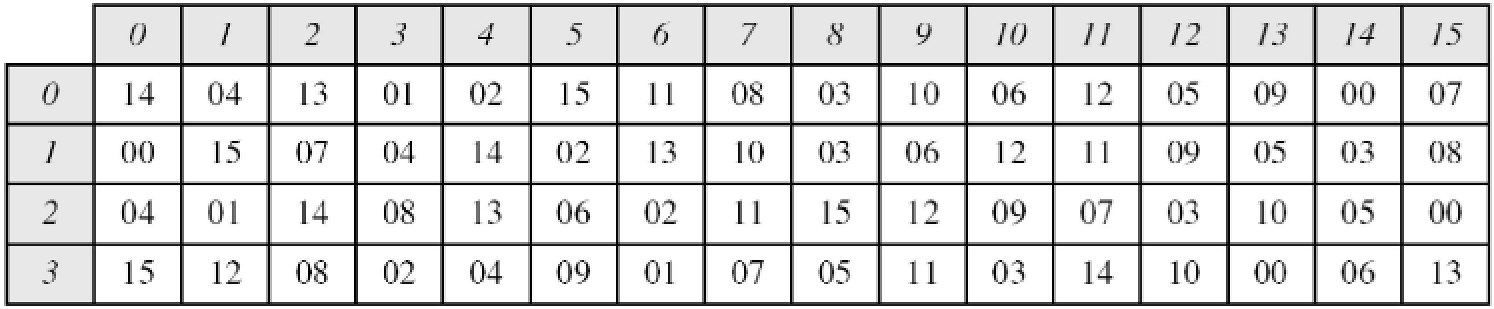


S-box rule



S-box

S-box 1

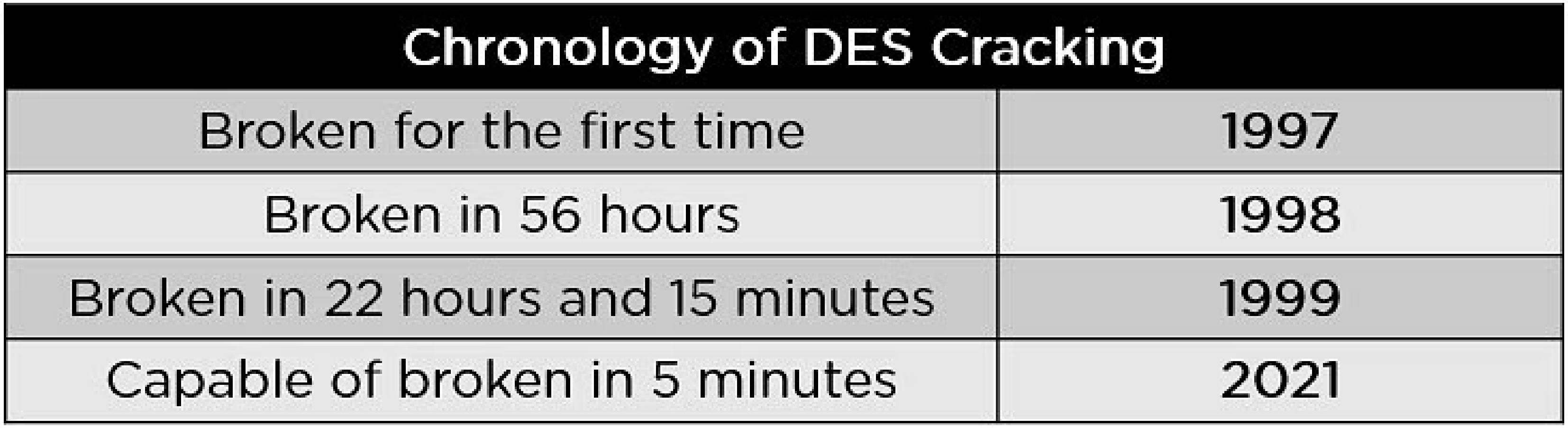


	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- **If input to s-box 1 is 100011. What would be the output?**

Strength Analysis

- Brute Force attack



Chronology of DES Cracking	
Broken for the first time	1997
Broken in 56 hours	1998
Broken in 22 hours and 15 minutes	1999
Capable of broken in 5 minutes	2021

- Weak Keys
- Semi-weak keys
- Known plaintext attack

Triple-DES

- repeats basic DES algorithm three times
- using either two or three unique keys
  - key size of 112 or 168 bits

- much more secure but also much slower
- key size of 112 or 168 bits

Advanced Encryption Algorithm (AES)

- Because of the drawbacks of 3DES, it was not a reasonable candidate for long-term use and there was need for a better replacement to DES

- NIST called for proposals in 1997
  - efficiency, security, HW/SW suitability, 128, 256, 256 keys

- selected Rijndael in Nov 2001
- symmetric block cipher
- uses 128 bit data & 128/192/256 bit keys
- now widely available commercially