Chapter Two

Cryptography

Basic Terminology

Plaintext: the original message or text that is used in an encryption process is called plaintext.

Cipher text: the coded message or the encrypted form of the message message that is found after encryption process has been completed.

Cipher: algorithm or process for transforming plaintext to cipher text.

Key: data (usually number(s)) used in cipher known only to sender/ receiver.

Terminology [Cont..]

Encipher (encrypt): converting plaintext to cipher text.

Decipher (decrypt) : recovering cipher text from plaintext.

Cryptography: study of encryption and decryption principles/methods.

Cryptanalysis (code breaking) : the study of principles/ methods of deciphering cipher text *without* knowing key.

Cryptology : the field of both cryptography and cryptanalysis.

Terminology [Cont..]

Cryptosystem: The system that contains both encryption and decryption processes. It includes key generation process, encryption and decryption algorithms.

Key Management: The process of generation, transmission and storage of key or keys.

Key generation process: The process or algorithm that generates the key for a cryptosystem is called key generation process. It may include one or more algorithms.

Terminology [Cont..]

Crypto analyst: The person, who conducts crypto analysis. In good intention, a crypto analyst finds the weakness of a cryptosystem and publishes it, so that the people can know it. In bad intension crypto analyst finds the weak points of break the encrypted message to know its meaning so that he can use it for beneficial purpose.

Brute-force attack: A process, the attacker attempts to obtain a plaintext using every possible key.

Terminology [Cont..]

Stream Cipher: It is a process to produce cipher text from plaintext, where key and encryption algorithm are applied in bit or byte (character) at a time.

Block Cipher: It is a process to produce cipher text from plaintext, where key and encryption algorithm are applied in a block of data such as a group of characters or a block of 64 bits.

Concept of Cryptography

There two categories of cryptography or cryptosystem. One is symmetric cryptosystem and another is asymmetric cryptosystem. Cryptography and cryptosystem are synonymous words. In future we shall use word cryptosystem in case of cryptography.

Symmetric cryptosystem: same key is used both in encryption and decryption.

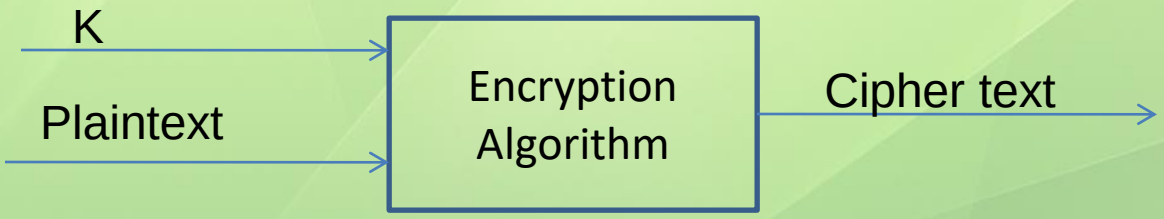
Asymmetric crypto system: one key is used for encryption and another separate key is used for decryption.

Basic Concepts of cryptography

Symmetric cryptosystem: **here only one key is used in both encryption and decryption processes.**

$$C = EA(K, P)$$

Where C-cipher text, EA- encryption algorithm, K- key, P- plain text.

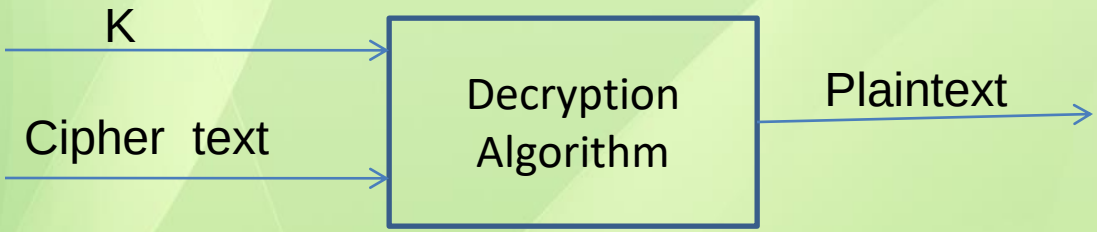


Encryption Process

Symmetric cryptosystem

P = DA(K, C)

Where DA- decryption algorithm.



Decryption Process

In symmetric cryptosystem key must be kept secret.

Asymmetric Cryptosystem

Here two keys are used. One is for encryption and another different one is for decryption. The key used for encryption is called public key and published for general use. The key used for decryption is called private or secret key. The owner will possess this (private) key and must be kept secret. In this system every one who possesses public key can encrypt the message, but only owner of the private key can decrypt the cipher text.

Asymmetric cryptosystem

$C = EA(K_{pub}, P)$

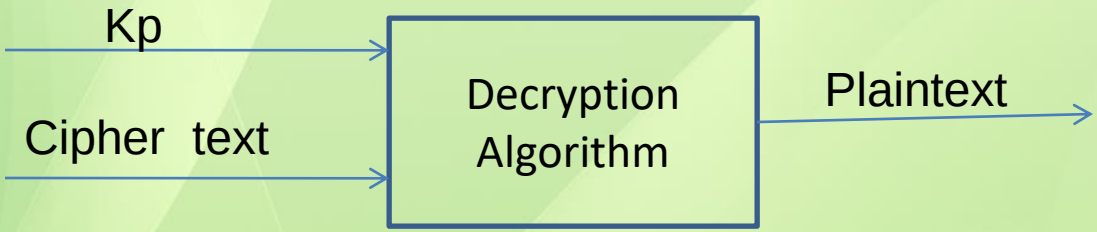
Where K_{pub} is the public key.

Encryption Process

Asymmetric cryptosystem

$$P = DA(K_p, C)$$

Where DA- decryption algorithm.



Decryption Process

In symmetric cryptosystem key must be kept secret.

Outline

- Overview of Cryptography
- Classical Symmetric Cipher
  - Substitution Cipher
  - Transposition Cipher
- Modern Symmetric Ciphers (DES)

Classical Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols
- Plaintext is viewed as a sequence of bits, then substitution replaces plaintext bit patterns with ciphertext bit patterns

Caesar cipher

- Earliest known substitution cipher
- Replaces each letter by 3rd letter on
- Example:

```
meet me after the party
PHHW PH DIWHU WKH SDUWB
```

Caesar Cipher

- Define transformation as:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Then have Caesar cipher as:

  $C = E(p) = (p + k) \bmod (26)$

  $p = D(C) = (C - k) \bmod (26)$

One-Time Pad

- If a truly random key as long as the message is used, the cipher will be secure - One-Time pad
- E.g., a random sequence of 0's and 1's XORed to plaintext, no repetition of keys
- Unbreakable since ciphertext bears no statistical relationship to the plaintext
- For **any** plaintext, it needs a random key of the same length
  - Hard to generate large amount of keys
- Have problem of safe distribution of key

Transposition Ciphers

- Now consider classical **transposition** or **permutation** ciphers
- These hide the message by rearranging the letter order, without altering the actual letters used
- Can recognise these since have the same frequency distribution as the original text

Transposition cipher

- Write message letters out diagonally over a number of rows
- Then read off cipher row by row
- E.g.,”meet me after the party” write message out as:

```
m e m a t r h p r y
e t e f e t e a t
```

- Giving ciphertext

```
MEMATRHPRYETEFETEAT
```

Block vs Stream Ciphers

- Block ciphers process messages in into blocks, each of which is then encrypted or decrypted.
- Like a substitution on very big characters
  - 64-bits or more
- Stream ciphers process messages a bit or byte at a time when encrypting or decrypted.
- Many current ciphers are block ciphers, DES (Data encryption standard) is one of the most widely used types of cryptographic algorithms.

Modern Symmetric Ciphers (DES)

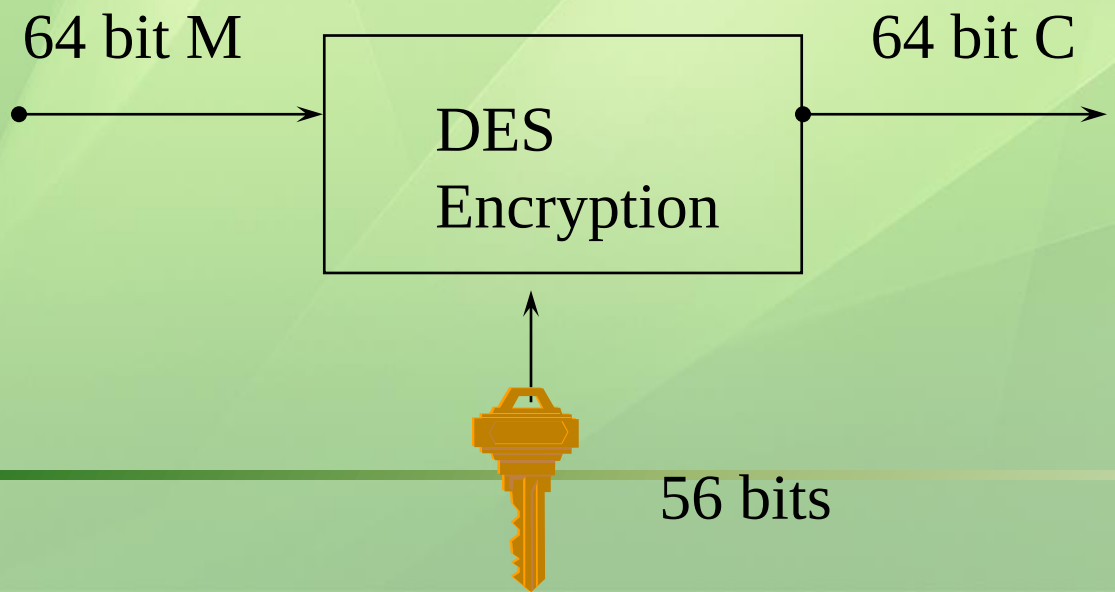
The Data Encryption Standard (DES) was published in 1977. It is the primary standard and defines the Data Encryption Algorithm (DEA).

original message is divided into block of 64 bits.

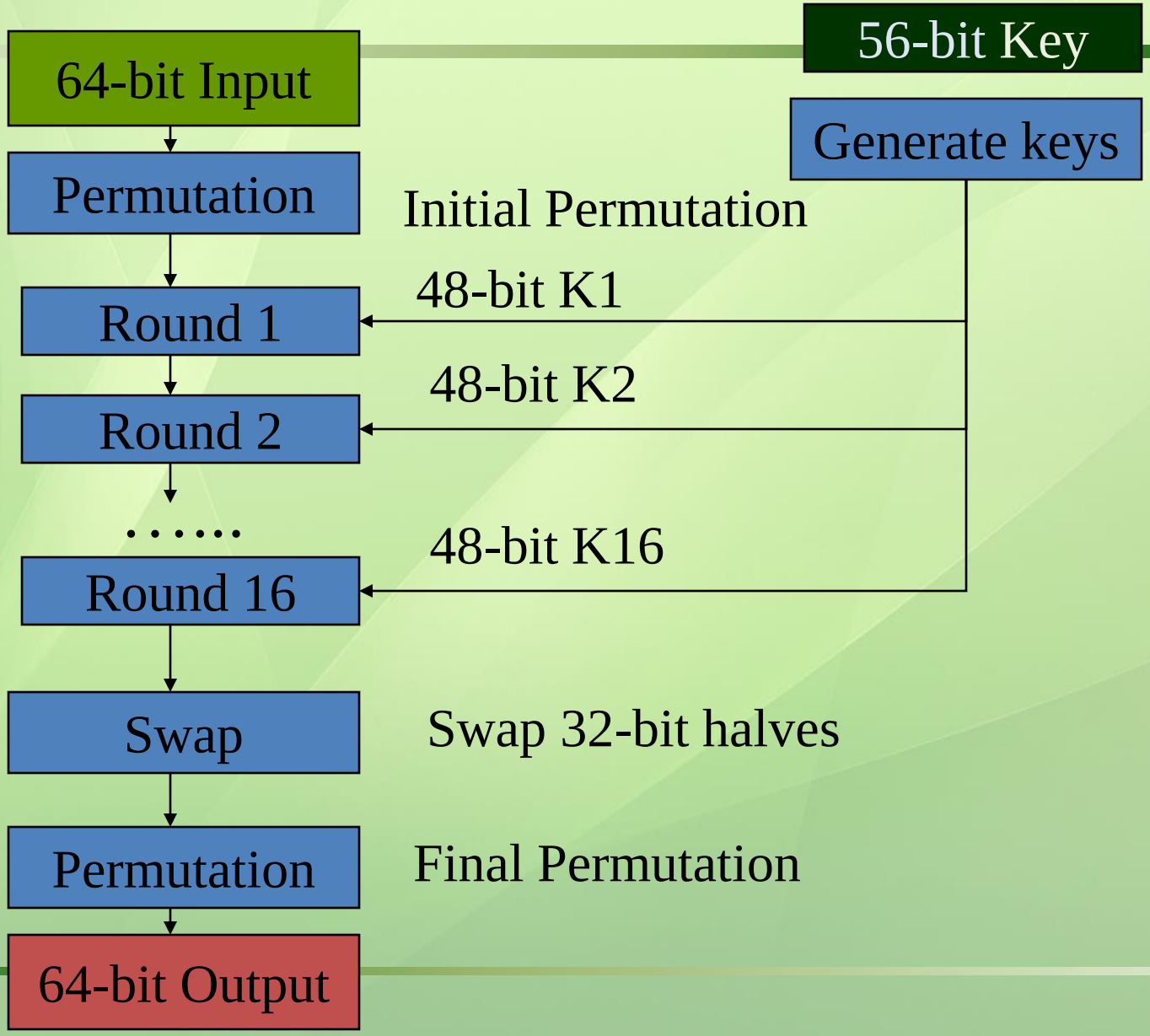
Each 64 bits block is encrypted using private or secret key.

DES (Data Encryption Standard)

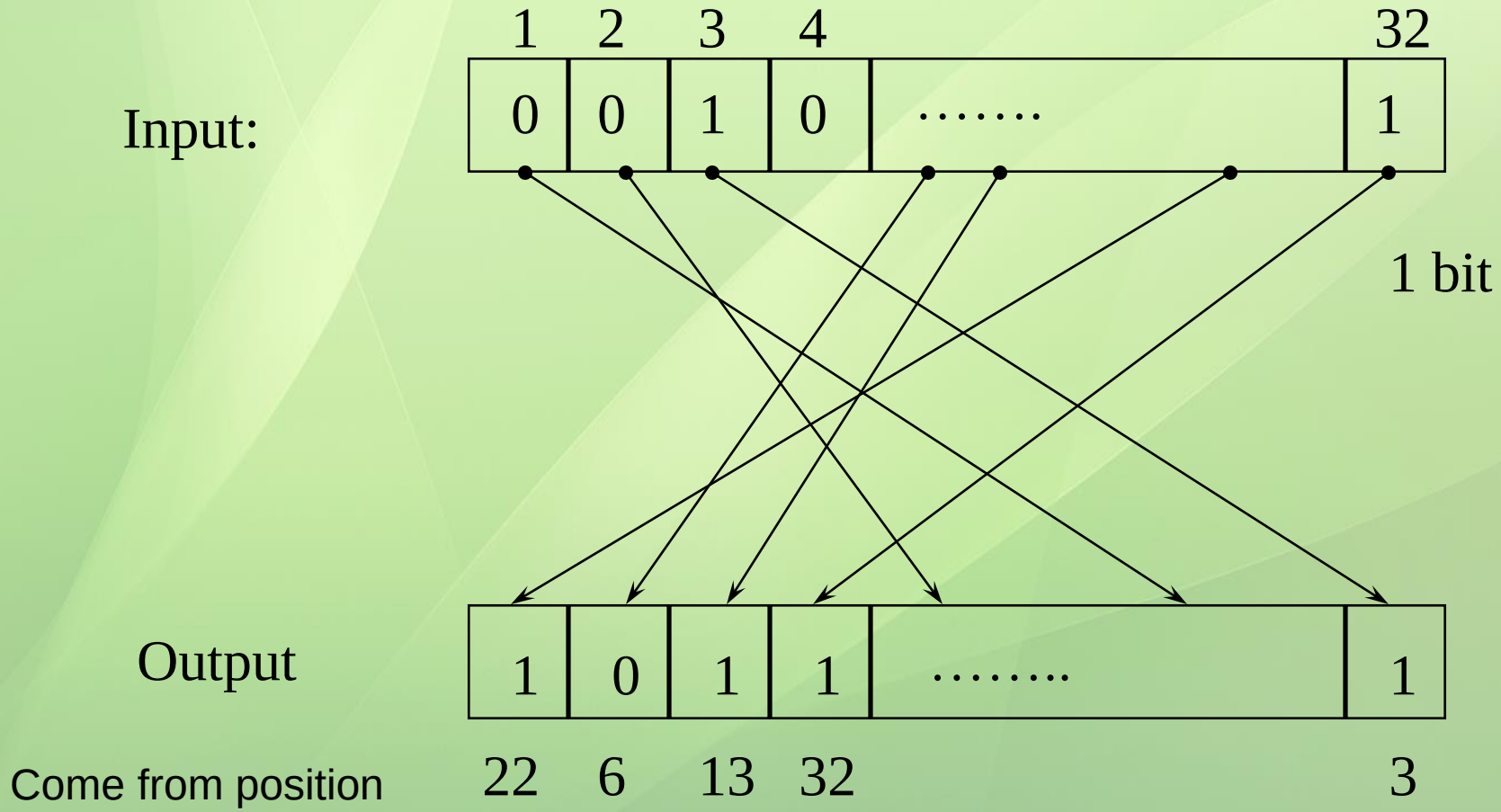
- Published in 1977, standardized in 1979.
- Key: Take 64 bit and drop the bits from the positions 8, 16, 24, 32, 40, 48, 56, 64. So key= 64 – 8 = 56-bit.
- 64 bit input, 64 bit output.



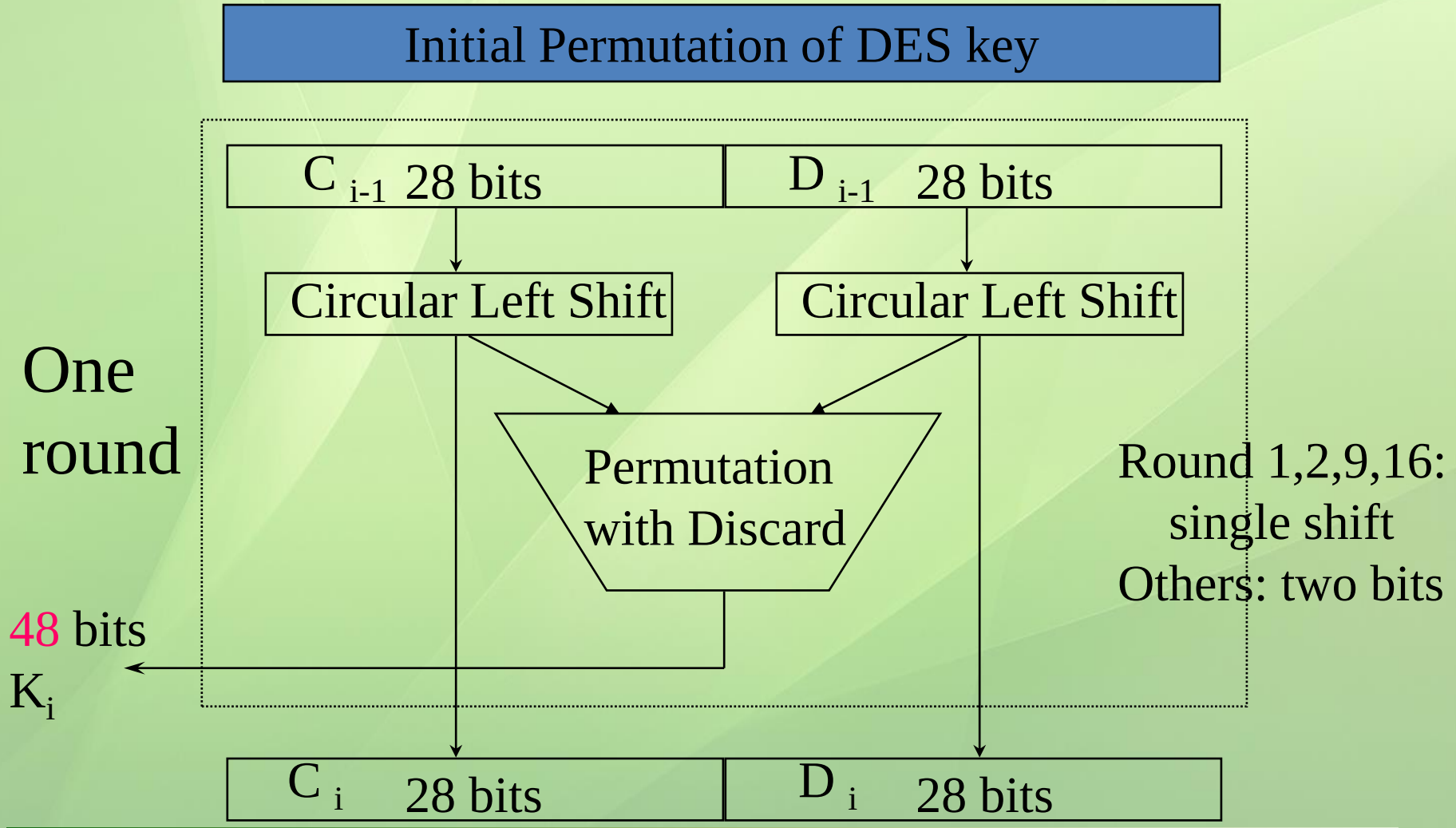
DES Top View


56-bit Key
64-bit Input
Generate keys
Permutation
Initial Permutation
48-bit K1
Round 1
48-bit K2
Round 2
.....
48-bit K16
Round 16
Swap
Swap 32-bit halves
Permutation
Final Permutation
64-bit Output

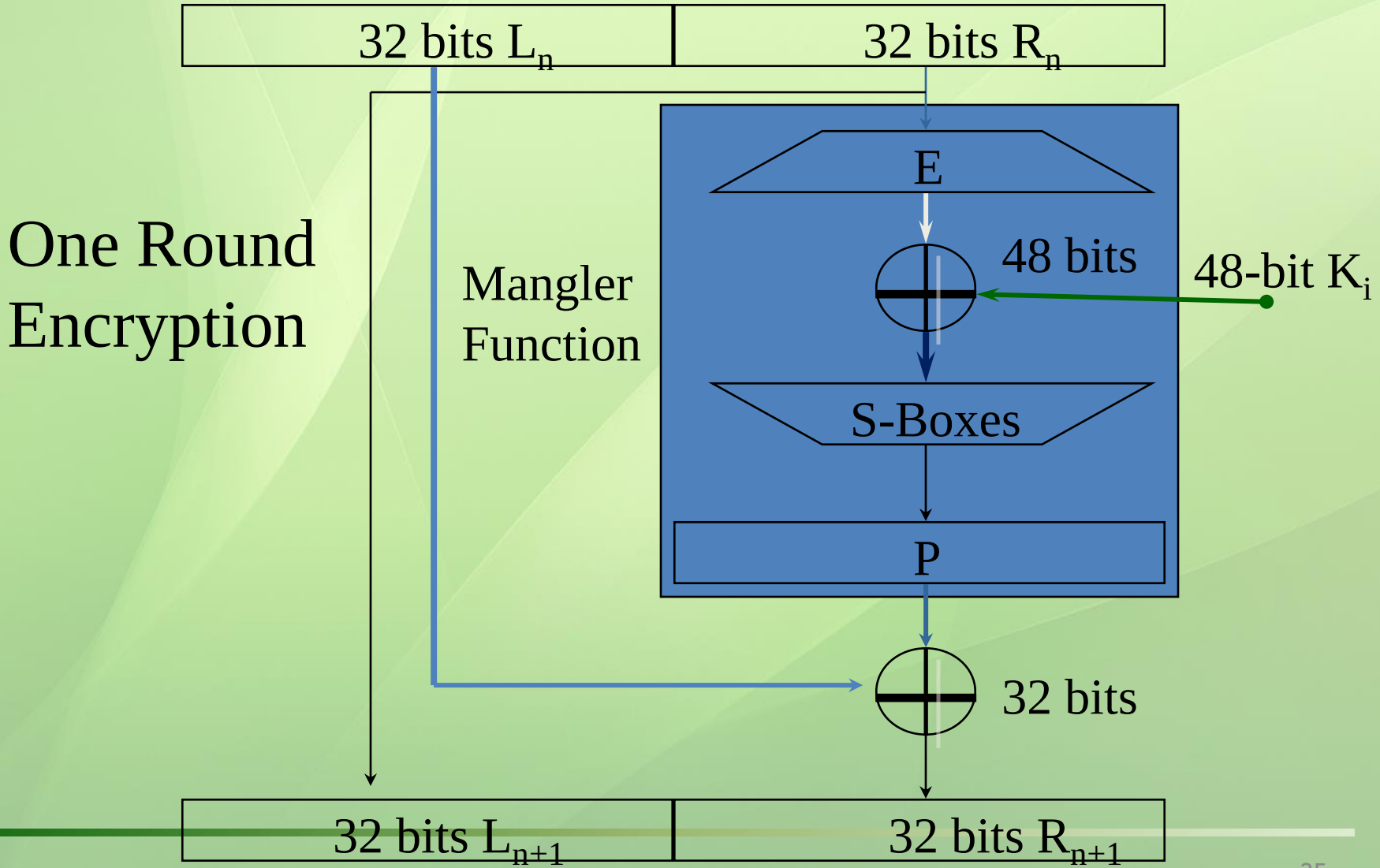
Bit Permutation (1-to-1)



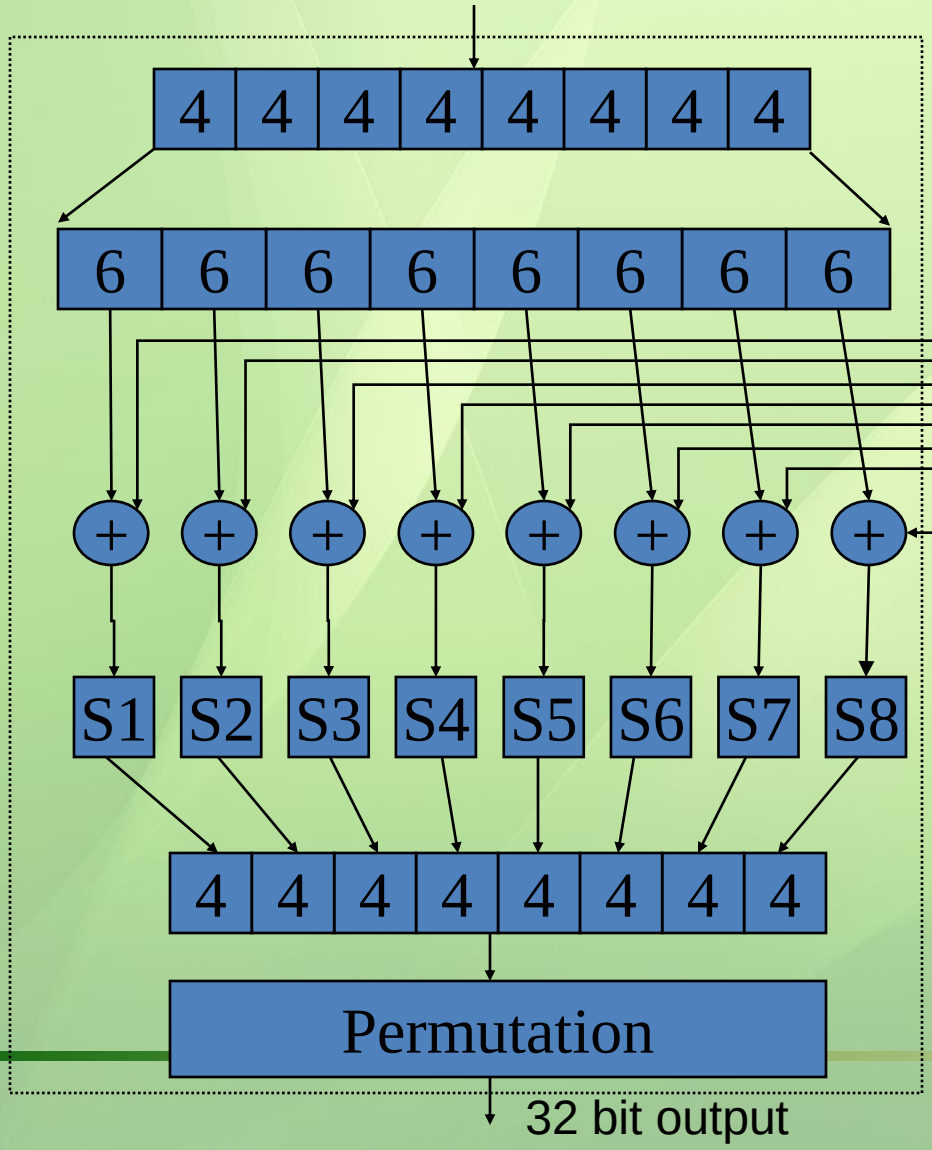
Per-Round Key Generation



A DES Round

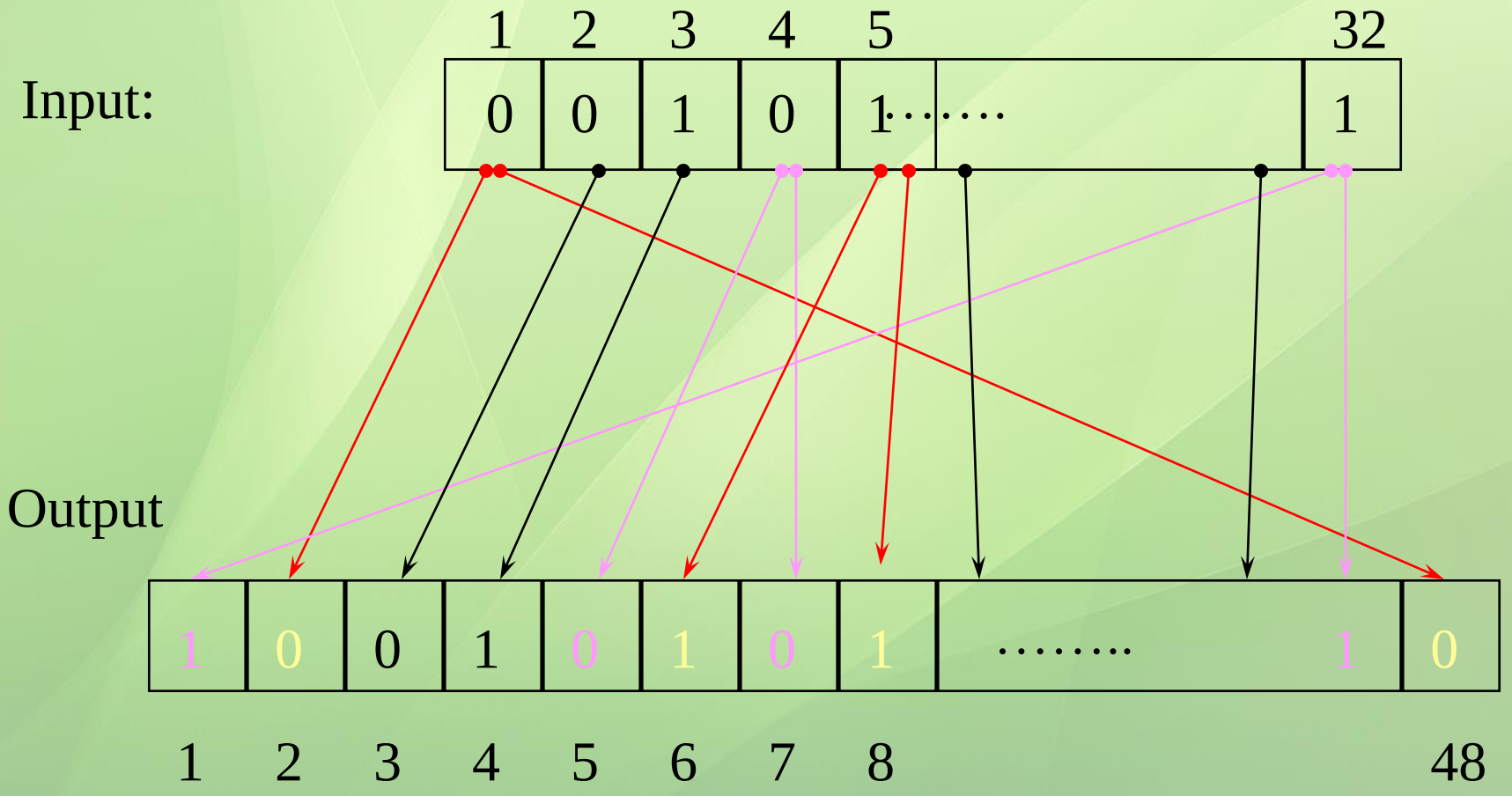

32 bits L_n
32 bits R_n
One Round Encryption
Mangler Function
E
48 bits
48-bit K_i
S-Boxes
P
32 bits
32 bits L_{n+1}
32 bits R_{n+1}

Mangler Function



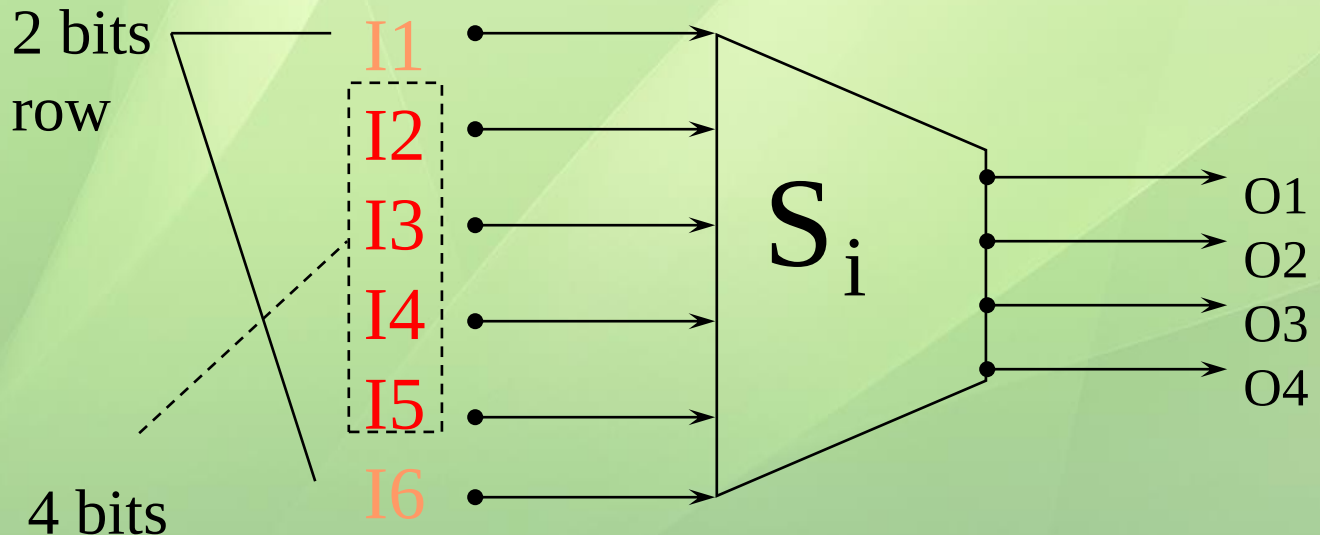
The permutation produces "spread" among the chunks/S-boxes!

Bits Expansion (1-to-m)



S-Box (Substitute and Shrink)

- 48 bits ==> 32 bits. (8*6 ==> 8*4)
- 2 bits used to select amongst 4 substitutions for the rest of the 4-bit quantity



i = 1,…,8.

S-Box Example (S-Box 1)

Each row and column contain different numbers.

	0	1	2	3	4	5	6	7	8	9…. 15
0	14	4	13	1	2	15	11	8	3	
1	0	15	7	4	14	2	13	1	10	
2	4	1	14	**8**	13	6	2	11	15	
3	15	12	8	2	4	9	1	7	5	

Example: input: 100110 output: ???

Steps of DES

1. Each block of message will be 64 bits. Do initial permutation on 64 bits data and divide it in to two halves(32bit and 32 bit).
2. Left half 32 bits and Right half 32 bits.
3. Expand **right half** up to 48 bits by expansion.
4. Take 64 bits key (reduced to 56 bits by dropping bits at positions 8, 16, 24, …, 64) and select 48 bits by permuted choice.
5. Do **EX-OR** of 48 bits right half and 48 bits key.
6. Select 32 bits from step 5 by S-box substitution choice.

Steps of DES [cont..]

7. Do P-box permutation (on 32-bits of step 6).
8. Do **EX-OR** of 32 bits left half and 32 bits right half (from step-7)
9. Result from step 8 will be new right half.
10. Old right half from step 2 will be the new lest half.

The above 10 steps make a cycle of DES.

Step 1 to 10 is for **one cycle**. There will be 16 such cycles. After completion of 16 cycles, we have to do final permutation on data bits to get decrypted data.

DES Box Summary

- Simple, easy to implement:
  - Hardware/gigabits/second, software/megabits/second
- 56-bit key DES may be acceptable for non-critical applications but triple DES (3DES) should be secure for most applications today

Strength of DES – Key Size

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- Brute force search looks hard
- Recent advances have shown is possible
  - in 1997 on a huge cluster of computers over the Internet in a few months
  - in 1998 on dedicated hardware called “DES cracker” by EFF in a few days ($220,000)
  - in 1999 above combined in 22hrs!
- Still must be able to recognize plaintext
- No big flaw for DES algorithms

DES Replacement

- Triple-DES (3DES)
  - 168-bit key, no brute force attacks
  - Underlying encryption algorithm the same, no effective analytic attacks
  - Drawbacks
    - Performance: no efficient software codes for DES/3DES
    - Efficiency/security: bigger block size desirable
- Advanced Encryption Standards (AES)
  - US NIST issued call for ciphers in 1997
  - Rijndael was selected as the AES in Oct-2000

AES

- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger & faster than Triple-DES
- Provide full specification & design details
- Evaluation criteria
  - security – effort to practically cryptanalysis
  - cost – computational
  - algorithm & implementation characteristics

This is the end

of

cryptographic concept and symmetric cryptosystem.

Thank You.