Fundamentals of Information & Network Security
ECE 471/571

Lecture #11: DES

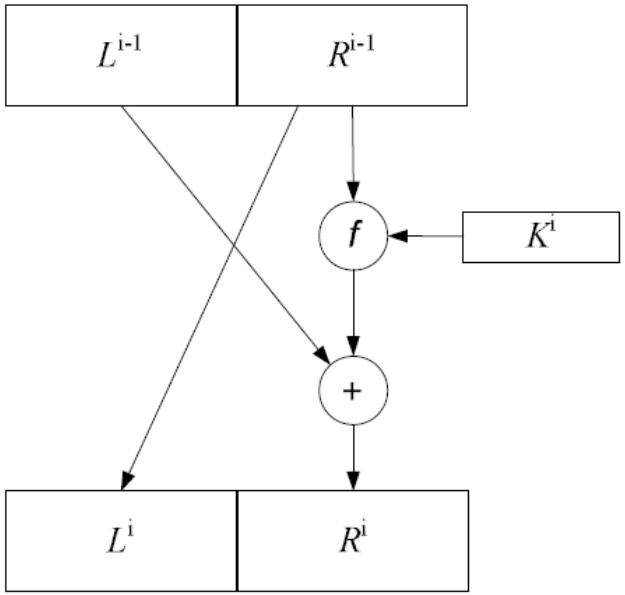
Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

The Data Encryption Standard (DES)

- Designed by IBM, publish by NIST (NBS) in 1977
- 56-bit key, mapping a 64-bit input block to a 64-bit output block
- Not secure any more
  - Keys must grow by about 1 bit every 2 years (why?)
- Triple DES, 128(112)-bit key

The Data Encryption Standard (DES)

- Description of a Feistel cipher



Question: Does the function f need to be injective?
How to decrypt?

Feistel Example

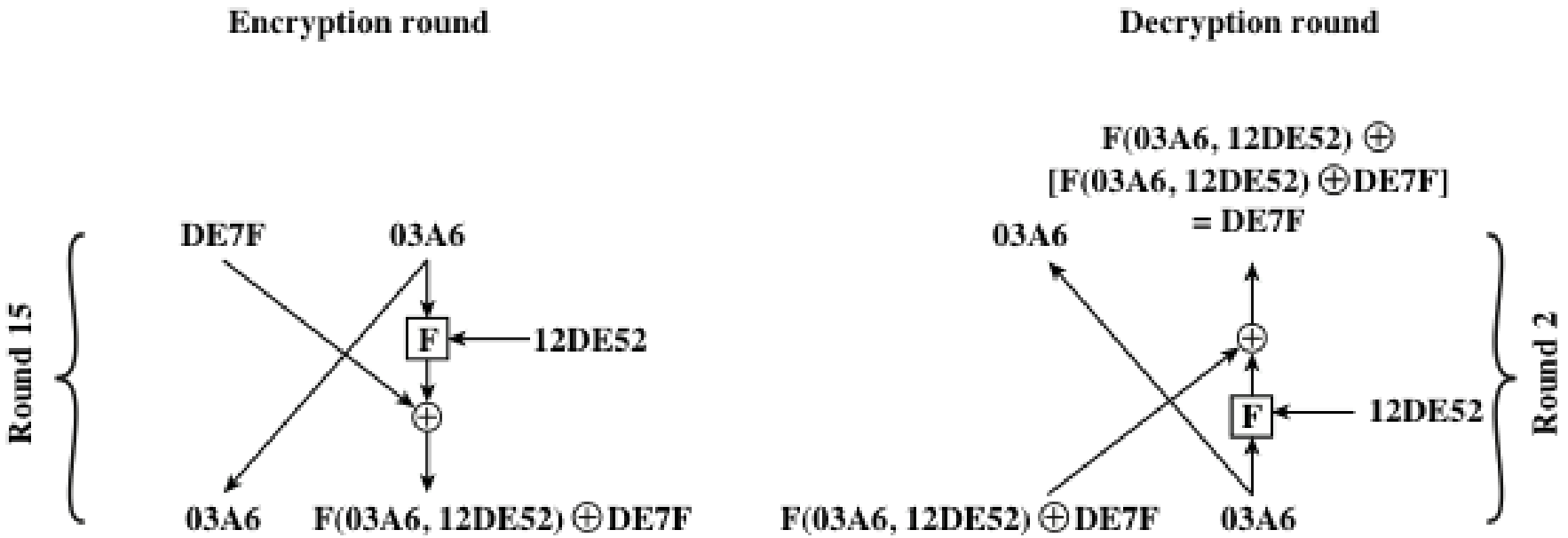
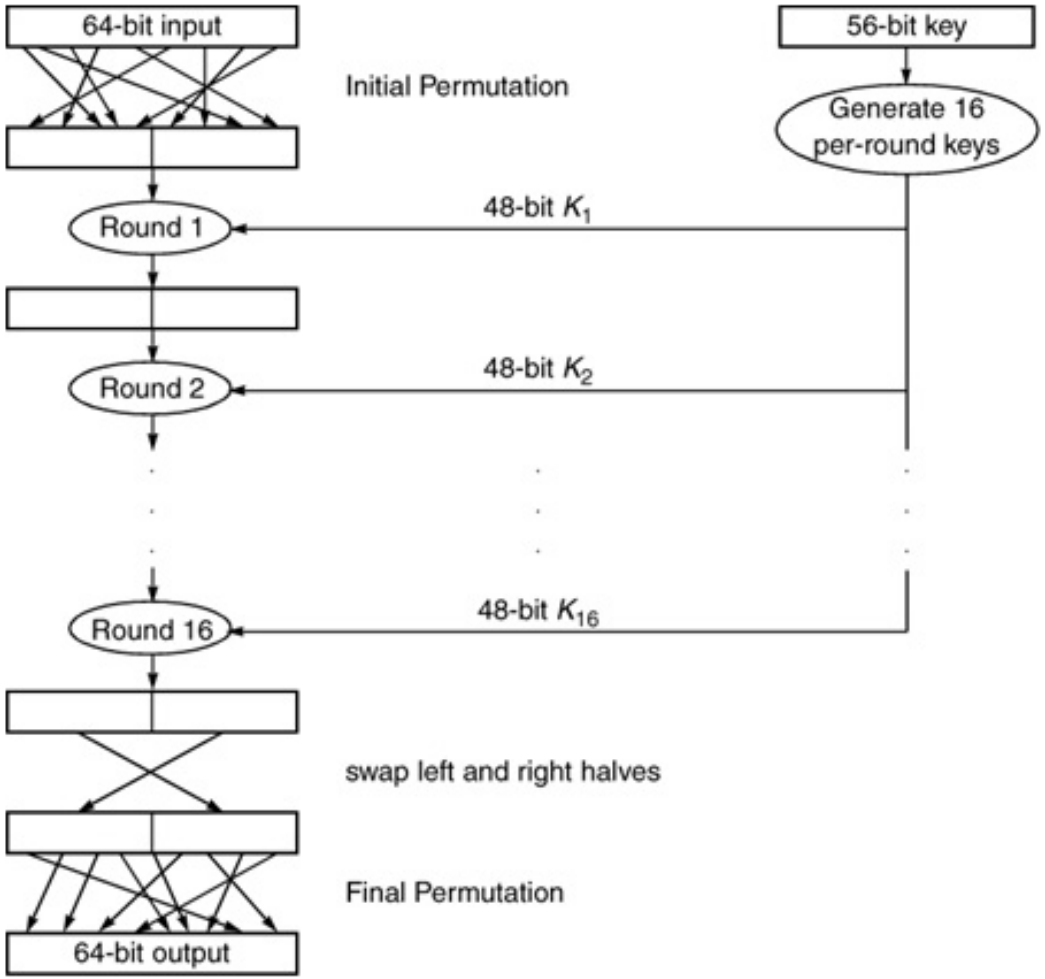


Figure 4.4 Feistel Example

DES Overview

- A 16-round Feistel cipher, with a block length of 64 bits, 56 bits key



Basic Structure of DES

Initial and Final Permutations

- Inverse of each other

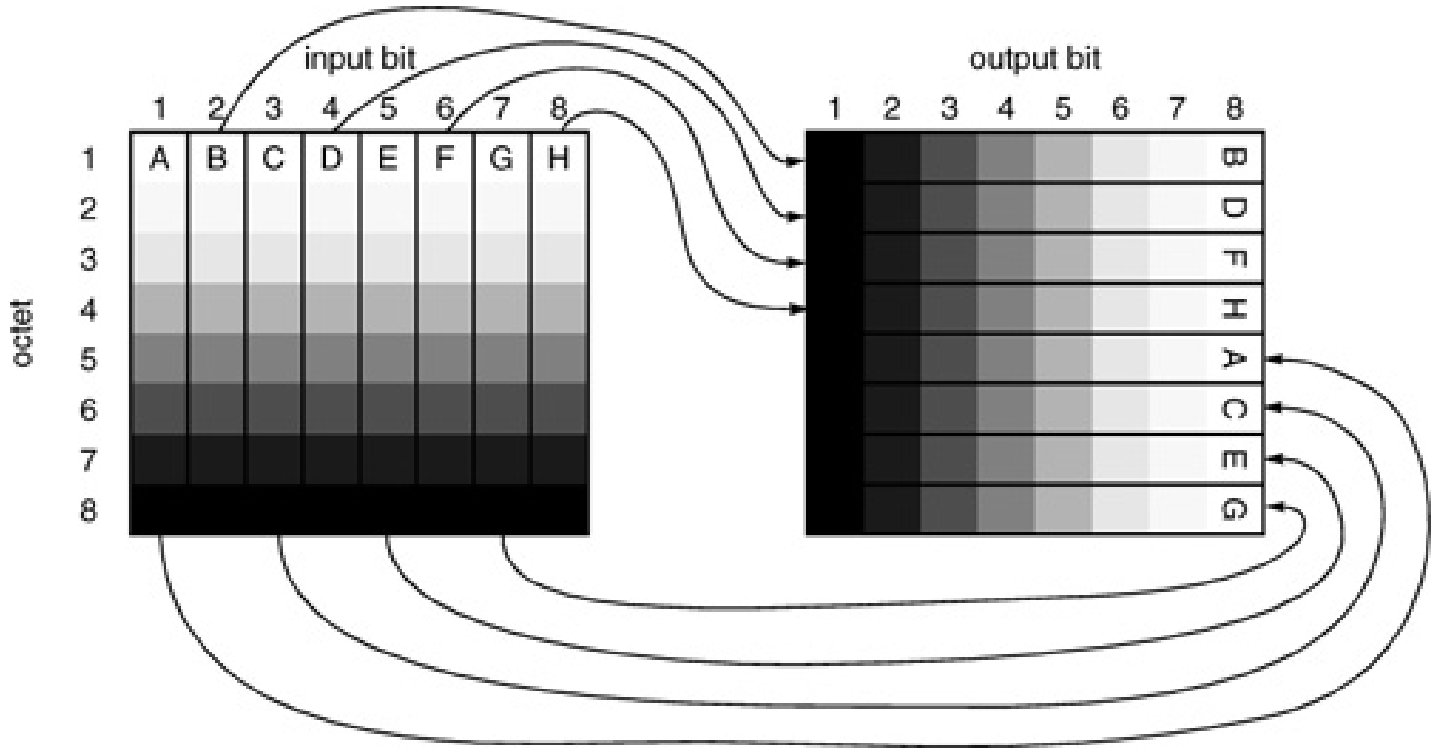
Initial Permutation (IP)

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

Final Permutation (IP^{-1})

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

Initial and Final Permutations

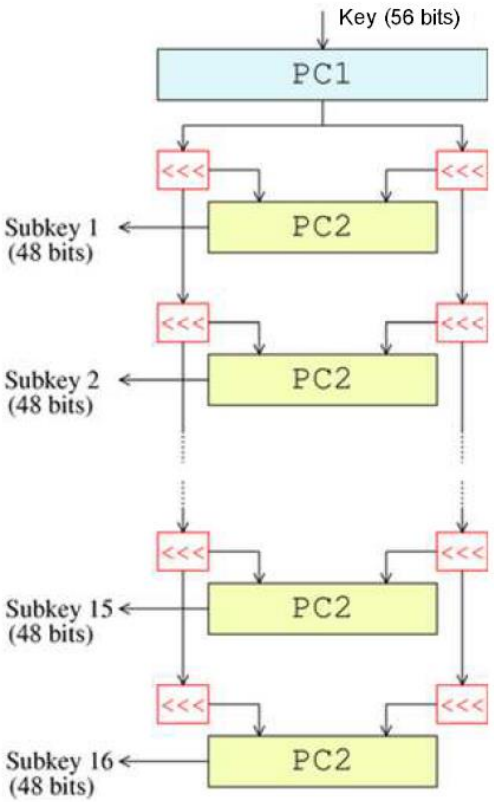


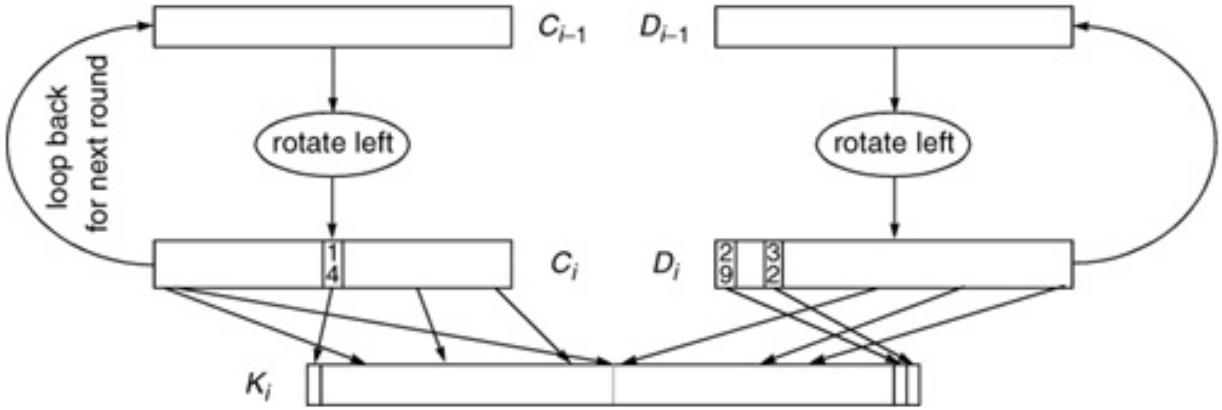
- Reverse the arrows for final permutation

Does it enhance security?

Generating the Per-Round Keys

- 16 rounds to generate 16 48-bit keys.





Round *i* for generating K_i

Generating Per-Round Keys

- Permutations for obtaining left and right halves of key

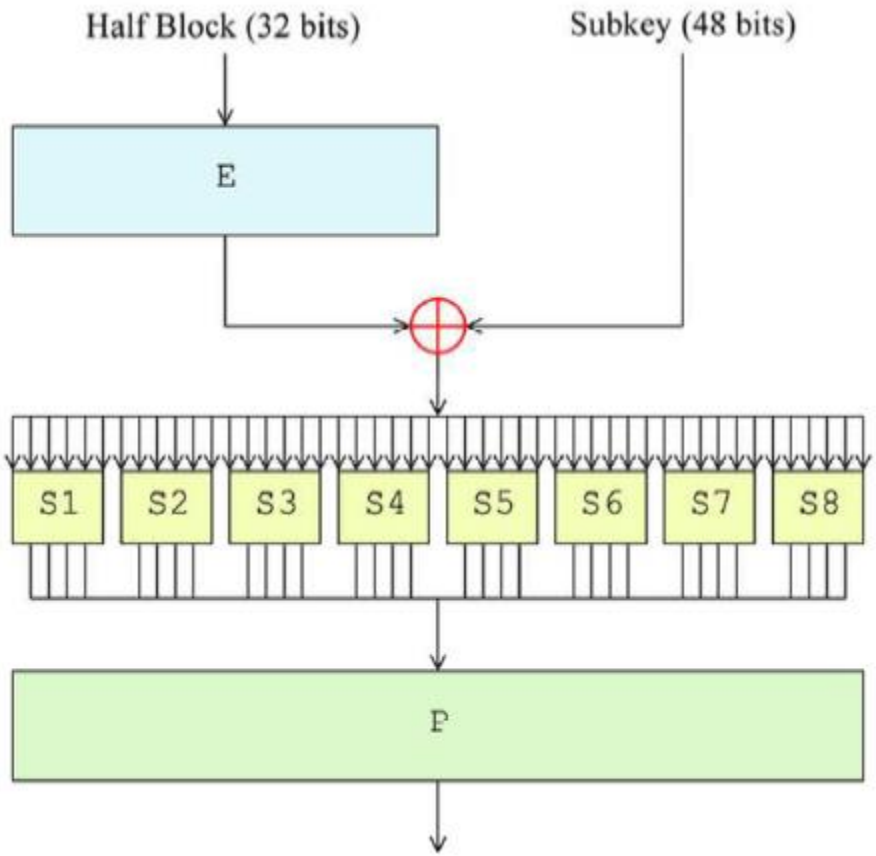
permutation to obtain the left half of K_i:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2

permutation to obtain the right half of K_i:

41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

The f (mangler) function in DES



- Each S-box is a 6-bit to 4-bit decoder, or 4 4-bit to 4-bit

S-Boxes

Figure 3-9. Table of 4-bit outputs of S-box 1 (bits 1 thru 4)

Input bits 1 and 6 ↓	Input bits 2 thru 5															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Figure 3-10. Table of 4-bit outputs of S-box 2 (bits 5 thru 8)

Input bits 7 and 12 ↓	Input bits 8 thru 11															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1111	0001	1000	1110	0110	1011	0011	0100	1001	0111	0010	1101	1100	0000	0101	1010
01	0011	1101	0100	0111	1111	0010	1000	1110	1100	0000	0001	1010	0110	1001	1011	0101
10	0000	1110	0111	1011	1010	0100	1101	0001	0101	1000	1100	0110	1001	0011	0010	1111
11	1101	1000	1010	0001	0011	1111	0100	0010	1011	0110	0111	1100	0000	0101	1110	1001

- Showing 2 S-boxes…
- There are 8 S-boxes producing 32-bit Mangle Function output
- Each S-box is a 6-bit to 4-bit decoder, or 4 4-bit to 4-bit

Permutation of the 32-bit Output

	Permutation Box P.							
Bits	Goes to Position							
1-8	9	17	23	31	13	28	2	18
9-16	24	16	30	6	26	20	10	1
17-24	8	14	25	3	4	29	11	19
25-32	32	12	22	7	5	27	15	21

- This permutation is random looking, is of some security value

- The permutation ensures: bits of the output of an S-box on one round of DES affects the input of multiple S-boxes on the next round

The Avalanche Effect

- Desired property of encryption: a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext

- Is the more the number of rounds, the better?

(a) Change in Plaintext		(b) Change in Key	
Round	Number of bits that differ	Round	Number of bits that differ
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Design Parameters

- Block size: larger - greater security, reduced encryption/decryption speed for a given algorithm

- Key size: larger key size means greater security but may decrease encryption/decryption speed

- Number of rounds: multiple rounds offer increasing security, more is not better, sufficient is good enough

- Key generation algorithm: greater complexity in this algorithm should lead to greater difficulty of cryptanalysis

- Round function: greater complexity generally means greater resistance to cryptanalysis

Cryptanalysis of DES

- Complexity of brute-force attack
- Computationally secure
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

Table 2.2 Average Time Required for Exhaustive Key Search

Key size (bits)	Number of alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Cryptanalysis of DES

- Weak keys: keys are inverse of themselves (encrypt same as decrypt)
  - E.g: when C0 and D0 are all zeros

- Cryptanalysis by exploiting weakness in S-box design
  - Differential cryptanalysis: observe the behavior of pairs of text blocks evolving along each round of the cipher, can find a DES key given 2^47 chosen plaintexts
  - Linear cryptanalysis: finding linear approximations to describe the transformations performed in DES, can find a DES key given 2^43 known plaintexts
  - Timing attacks: information about the key or the plaintext is obtained by observing how long to decrypt various ciphertexts

Design Issues for Block Ciphers

- S-Boxes:
  - Output bits of S-Box should not be close to a linear function of input bits
  - Each row of the S-Box should be a permutation of the all possible input / output values
  - Inputs that differ in one bit should generate outputs that differ in many bits

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

Design Issues for Block Ciphers

- f-Function:
  - Must be difficult to un-scramble
  - Should be non-linear
  - SAC (Strict Avalanche Criteria) – any output bit should be inverted with probability ½ when some input bit is changed.
  - BIC (Bit Independence Criteria) – any two output bits should change independently when some input bit is changed.

DES Summary

- Two techniques
  - Substitution provides the confusion
  - Transposition provides the diffusion
- Accomplish:
  - The output bits have no obvious relationship to the input bits
  - Spreading the effect of one input bit to other bits in the output.
- Implementation
  - Uses only standard arithmetic and logic operations
  - Repetitive algorithm: suitable for hardware