Introduction to Information Security (IT)

Quiz-1 (Spring 2024)

International Institute of Information Technology, Hyderabad

Time: 1 Hour and 20 Minutes Total Marks: 40

Instructions: Answer *ALL* questions.
This is an open notes examination.
No query is allowed in the examination.
Use of Regular Calculator is allowed.

1 Feb 2024

1. In the Data Encryption Standard (DES) algorithm, if the key K with parity bit (64 bits) in hexadecimal is 0123 ABCD 2562 1456, find the first round key K_1. Use the following tables as shown in Figure 1. [15]

(a) Input Key

1	2	3	4	5	6	7	8
9	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

(b) Permuted Choice One (PC-1)

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
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

(c) Permuted Choice Two (PC-2)

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

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure 1: DES Key Schedule Calculation

2. Consider the following variant of DES algorithm, called Counter Mode (CTR). In this algorithm, the inputs are: a) an 64-bit counter (ctr), b) an 56-bit DES key, and c) an array of 64-bit plaintext blocks, say $P_1, P_2, \ldots, P_N$. After encryption, the outputs are the ciphertext blocks, say $C_1, C_2, \ldots, C_N$. The encryption procedure is displayed in Figure 2.

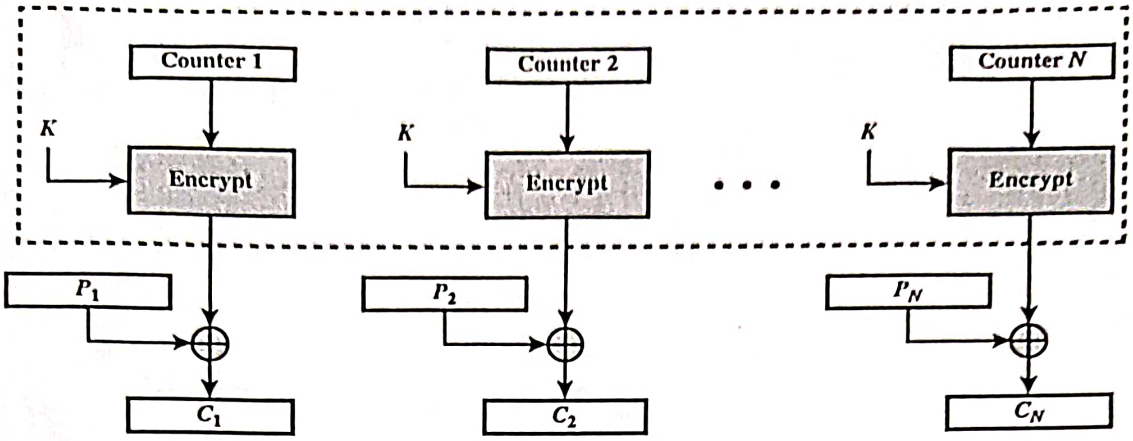

Figure 2: Encryption in Counter Mode of DES

Answer the following questions:

a) Write the encryption and decryption equations. Also, draw the decryption procedure in a figure.

b) List down all the advantages of using CTR mode with respect to 1) Hardware Efficiency, 2) Software Efficiency, 3) Pre-processing and 4) Security.

[5 + 5 = 10]

3. A *linear cipher* is defined as follows. Using the encoding technique $A = 0$, $B = 1$, $C = 2$, ..., $Z = 25$ and the blank space as 26, the encryption algorithm works as

$$C \equiv aP + b \pmod{27},$$

where P is the encoded plaintext letter and C the corresponding encrypted ciphertext letter, where a and b are integers with $\gcd(a, 27) = 1$.

(a) Design the corresponding decryption algorithm for this linear cipher.

(b) Using the linear cipher $C \equiv 5P + 11 \pmod{27}$, encrypt the plaintext message IT IS EASY.

(c) Decrypt the ciphertext message TZSVIW, which was produced using the linear cipher $C \equiv 4P + 7 \pmod{27}$.

[3 + 6 + 6 = 15]

********** **End of Question Paper** **********