Dept. of Computer Science and Engg.
Indian institute of Technology, Kharagpur

Subject: Cryptography and Network Security, Subject Code: CS60041
Full Marks: 60 Duration: 2 hrs. Date: 26.09.22 (FN)

Instruction: Answer all the questions

1.(a) Suppose that $n = pq$, where p and q are distinct odd primes. Prove that the number of involutory keys in the **Affine Cipher** over Z_n is $n + p + q - 1$.
(Note: If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an involutory key.)

(b) Encrypt the short text "IIT" by using the method of Hill cipher. Consider the keyword as "KHARAGPUR" and a key matrix of size 3 x 3 (row-wise). [Hint:Consider A=0, B=1, ... so on.]

(c) Consider the standard block cipher DES. Let S be a finite set and let f be a bijection from S to S. The function f is an involution if $f(f(x)) = x$, $\forall x \in S$. A DES key k is weak if DES_k is an involution. Exhibit four weak keys for DES.

(4+5+6 = 15)

2.(a) Let e_1, e_2, e_3, e_4 and e_5 be the bias of five random variable X_1, X_2, X_3, X_4 and X_5 respectively where, $e_1 = e_2 = ½$, $e_3 = e_4 = ¼$ and $e_5 = 1/6$. Find the bias of $(X1 \oplus X2 \oplus X3 \oplus X4 \oplus X5)$.

(b). Consider a 5-round 16-bit SPN block cipher with the S-box: $\{0, 1\}^4 \rightarrow \{0, 1\}^4$. The part of a difference distribution table for a few input-output of the S-box is as follows

		OUTPUT															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INPUT	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	8	0	0	0	0	6	0	2	0	0	0	0	2	0	2	2	2
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0

The propagation rate of the Differential Trail formed with the five active S-boxes S_2^1(1110, 1000), S_1^2(0100, 0110), S_2^3(1000, 0100), S_3^3(1000, 0100), S_2^4(0110, 0011).

(Here, S_i^k (x, y) represents ith S-box of kth round with input x and output y.)

(c) What do you mean by perfect secrecy? Prove that a cryptosystem has perfect secrecy if and only if H(P|C) = H(P).

(5+5+5=15)

3.(a) For symmetric block cipher explain "Cipher Feedback Mode (CFB)" of operation with figure. What is the disadvantage of CFB?

(b). Assume that someone sends the encrypted messages by using DES in the Output Feedback (OFB) mode of operation with a secret (but fixed) IV value

(i) Show how to perform the known-plaintext attack in order to decrypt the transmitted messages

(ii) Is it better with the Cipher Feedback (CFB) mode?

(iii) What about the Cipher Block Chaining (CBC) mode?

(6+3x3=15)

4.(a) How do you compute the constant of Inverse substitute byte transformation of AES128?

(b) Write the key expansion algorithm of AES 128.

(c) Suppose the round keys for round 7 of AES is

A0 A1 A2 A3 B0 B1 B2 B3 C0 C1 C2 C3 D0 D1 D2 D3

What are the first 4 bytes of the round key for round 8 if 8th round constant is 80. Part of AES S-Box is given below

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E

(5+5+5=15)