DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.

CYCLE TEST II
CSPC35 Principles of Cryptography

21/04/21 **Time**: 60 mins

ANSWER ALL THE QUESTIONS

MAX: 20 Marks

1. Consider a CFB mode of operation where the block cipher is permutation cipher and the key is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$. If the initial vector is taken as 1010 then compute the ciphertext corresponding to the plaintext 010010111100. (2)

2. In a cipher, S-boxes can be either static or dynamic. The parameters in a static S-box do not depend on the key.

   (a) State some advantages and disadvantages of static and dynamic S-boxes (3)

   (b) Are the S-boxes in AES static? Justify. (2)

3. Consider an ElGamal scheme with a common prime q = 71 and a primitive root a = 7

   a. If B has public key YB = 3 and A chose the random integer k = 2, what is the ciphertext of M = 30? (2)

   b. If A now chooses a different value of k, so that the encoding of M = 30 is C =(59, $C2$), what is the integer $C2$? (2)

4. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to an user whose public key is e = 5, n = 35. What is the plaintext M? (3)

5. In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $a^x \bmod q$ for some public number a.

(i) What would happen if the participants send each other x^a for some public number a instead? (2)

(ii) Give at least one method Alice and Bob could use to agree on a key (2)

(iii) Can Eve break your system without finding the secret numbers? (1)

(iv) Can Eve find the secret numbers? (1)