Indian Institute of Technology, Kharagpur

Date..... Time: 60 mins Full Marks: 25
Class Test (Autumn) Semester 2020-21 No. of Students: 56 Sub. No. MA 61027
Subject Name: Cryptography and Network Security

Instruction: The test is in open-book, open-notes mode. Answer all questions.

1. [$3 \times 2 = 6$ **mark**]

   (a) Decrypt the ciphertext "DZGIFZUOPVYYPXJYACTIXQTYGJ" that came from the Vigenere cipher with key "bluefog".

   (b) The Playfair cipher is used with keyword "barcelona" to encrypt the message "Meet agent Yullov at the Auberge Resturant". Find the ciphertext.

   (c) Suppose that π is the following permutation of $\{1, 2, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

   Decrypt the following ciphertext, for a Permutation Cipher with $m = 8$, which was encrypted using the key π:
   ETEGENLMDNTNEOORDAHATECOESAHLRMI.

2. [7 **mark**] Consider a symmetric cryptosystem with key space $\mathcal{K}$, message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$, where $\mathcal{K} = \{K_1, K_2, K_3\}$, $\mathcal{M} = \{a, b, c\}$, and $\mathcal{C} = \{1, 2, 3, 4\}$. Suppose the encryption matrix is a follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

   This means a when encrypted with key K_1 yields 1, etc. Given that the keys are chosen with equal probability and the plaintext distribution is

$$\mathsf{Pr}[a] = \frac{1}{2}, \mathsf{Pr}[b] = \frac{1}{3}, \mathsf{Pr}[c] = \frac{1}{6}.$$

   Find the probability distribution on $\mathcal{C}$. Explain with justification whether this cryptposystem provide perfect secrecy.

———-P.T.O.———

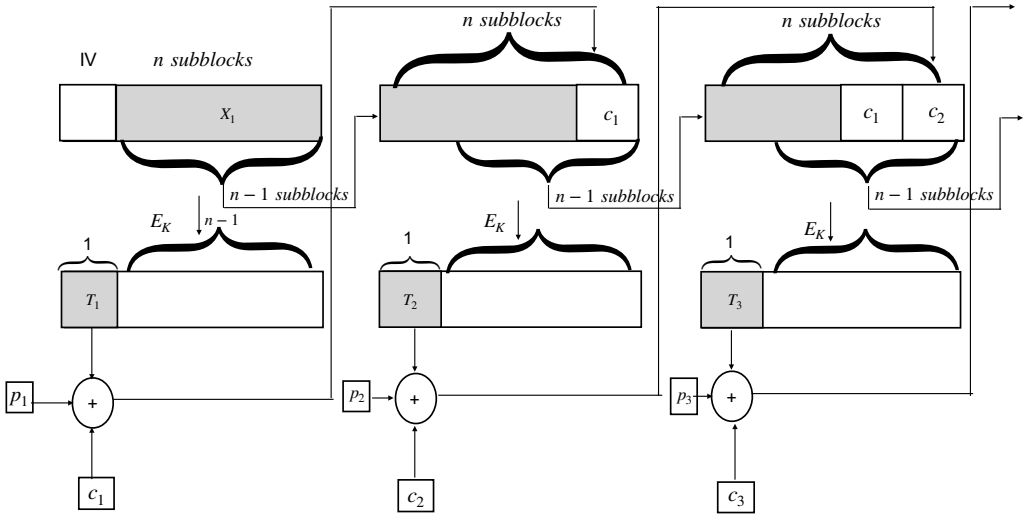
3. [$2 \times 3 = 6$ **mark**]

(a) Suppose that we are given the plaintext 101110. Determine the ciphertext that gets transmitted if the encryption function of Table 1 is used in cipher feedback mode as in Figure 1 with parameters $k = 1$ and initial vector $\mathsf{IV} = 10$. Here l is the block size, k is the subblock size, $n = l/k$ is the number of subblocks and $k|l$.

Table 1: Block Encryption Function of Question 3

P	00	01	10	11
$E(P)$	10	00	11	01

Figure 1: The cipher feedback (CFB) mode of encryption for block cryptosystems



(b) Explain the decryption algorithm for the cipher feedback mode.

(c) Apply the decryption algorithm that you obtained in part (b) to decrypt the ciphertext that you obtained in part (a).

——-P.T.O.———

4. [$2 \times 3 = 6$ **mark**] ***The Counter Mode of Operation***. The **counter (CTR) mode of operation** is another stream mode similar to the OFB mode, but with an advantage that the shift registers may be computed separately (rather than recursively), thus making it amenable to parallel processing (i.e., distributed computation). The encryption algorithm for the CTR mode is similar to that for the OFB mode, the only change is in how the shift registers S_i are updated. Recall that each S_i is an l-bit string. Such a string can be thought of as a binary expansion for a non-negative integer in the range $0 \leq x < 2^l$. The shift register updating will be by modular addition of these integers, adding 1 at each iteration : $S_{i+1} = S_i + 1 (\text{mod } 2^l)$.

   (a) Consider the following encryption mapping: $E_K = E$: {4-bit strings} $\longrightarrow$ {4-bit strings} defined by first cyclically shifting a 4-bit string one unit to the left, and then XORing the result with the fixed string 1011. For example, to compute $E(0011)$, we first shift the inputted string one unit to the left, $0011 \longrightarrow 0110$, and then we XOR the result with 1011 to produce $E(0011) = 0110 \oplus 1011 = 1101$. Suppose that we need to transmit the plaintext $P = 111000$, and we will implement one of the block cryptosystem modes of operation. Determine the resulting transmitted ciphertext if the counter mode is used with subblock size $k = 2$ and initial shift register $S_1 = 1110$.

   (b) Describe the general decryption algorithm for the counter mode.

   (c) Apply the decryption algorithm that you obtained in part (b) to decrypt the ciphertext that you obtained in part (a).

———-The End———