Assignment-2
Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Note that you need to solve Question 1 and verify its solution using the program as mentioned in Question 2. Please submit the assignment (pdf of Question 1, programs (C/C++), output files) to both **MS team** and email id: **cryptomathsiitkgp@gmail.com** by **19/10/2020**. Your **Roll No.** and **Name** must be mentioned. No marks will be awarded without detailed solution.]

1. [5 mark] Suppose that Bob uses the Merkle-Hellman knapsack cryptosystem with superincreasing sequence

$$[a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9] = [1, 2, 6, 10, 25, 55, 105, 205, 505],$$

$m = 999$ (which is greater than $\sum a_i$), and $w = 334$ (which is relatively prime to m).

   (a) What is Bob's public key?

   (b) If Alice uses Bob's public key to encrypt each of the following plaintexts:

      (i) 111000111

      (ii) 101010101

      (iii) 110011001

      determine the resulting ciphertexts.

   (c) Perform the decryption process that would need to be done when Bob receives each of the ciphertexts of part (b).

2. [15 mark] ***Program for Merkle-Hellman Encryption***. Write a program with syntax C=MerkleHellmanEncrypt(PublicWeights, xPlaintext) that will use Merkle-Hellman knapsack cryptosystem. The inputs are: PublicWeights, the public key vector object weights (positive integers), and xPlaintext=a binary vector representing the plaintext. The output is a non-negative integer C that is the corresponding ciphertext. Run your program on the encryptions of Question 1.