SECOND ASSIGNMENT
SEPTEMBER/OCTOBER SEMESTER 2020

BACHELOR OF COMPUTER SCIENCE (HONS.)
(IN COLLABORATION WITH IUKL)

NETWORK AND DATA SECURITY
(CSC 2735)

LECTURER'S NAME : MANOJ GAUTAM

GENERAL INSTRUCTIONS

1. This question booklet consists of 2 pages including this page.
2. There is one **SECTION** in this question booklet.
3. Please submit assignment solution in **SOFT COPY FORMAT in A4 size paper.**
4. **The Deadline for Submission is on 5th January.**

1. Write a program to implement a rail fence cipher algorithm. A program must implement encryption and decryption algorithm inside encrypt and decrypt function. Verify the implementation of an algorithm by passing a plain text as your name in encrypt function and decipher the generated cipher text using decryption function.

(10 marks)

2. In a public key system using RSA you intercept a cypher text C:10 sent to a user whose public key is e:5, n:35. What is the plaintext M?

(10 marks)

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n),e) = 1$: $1<e<\phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public Key	$KU = \{e,n\}$
Private Key	$KR = \{d,n\}$
Encryption	
Plaintext:	$M<n$
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

3. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.

(10 marks)

*****End of Questions*****