Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online Supplementary Examination, January 2021

Course: Cryptography and Network Security (RE) **Semester: VII**
Program: B. Tech. (CSE) **Time : 03 hours**
Course Code: CSEG 4001 **Max. Marks: 100**

SECTION A

1. Each Question will carry 5 Marks
2. The answers in this section are to be typed in. No explanation is expected.

Q1	The components of a symmetric key cryptosystem are _____, _____, _____, _____, and _____. (Fill up the blanks)	**CO1**
Q2	(a) The value of $\phi(18)$ = _____. (Fill up the blank) (b) Elements in the set Z_5^* are { _____ }. (Fill up the blank)	**CO1**
Q3	(a) In GF(7), the result of 6 ÷ 4 = _____. (Fill up the blank) (b) In GF(2^4), the multiplicative inverse of 1 0 1 modulo 1 0 0 1 1 = _____. (Fill up the blank)	**CO2**
Q4	A typical AES round has transformations named _____, _____, _____, and _____. Here, the substitution takes place in _____ transformation. (Fill up the blank)	**CO2**
Q5	(a) A Message Authentication Code (MAC) function accepts _____ number of inputs and gives ____ number of outputs. (Fill up the blank) (b) Define weak collision resistance in no more than two sentences.	**CO3**
Q6	(a) TLS stands for _____. (Fill up the blank) (b) Name the components in a firewall.	**CO4**

SECTION B

1. Each question will carry 10 marks
2. These answers are to scanned and uploaded.

Q7	Explain classical Transposition cipher with a suitable example.	**CO1**
Q8	Explain AES-192 (Advanced Encryption Standard – 192 bit) round key generation process with a neat diagram.	**CO2**
Q9	Discuss and differentiate between Cipher Block Chaining (CBC) and Cipher Feedback (CFB) modes of block cipher operations.	**CO2**
Q10	List and brief the requirements of a hash function. Give example of a cryptographic hash function.	**CO3**
Q11	Brief the Secure Socket Layer (SSL). Why do we need IPSec while we can encrypt data at application layer?	**CO4**

SECTION C **1. Each Question carries 20 Marks.** **2. Answer in this section is to be scanned and uploaded.**		
Q12	Explain Digital Signature Standard (DSS) algorithm with suitable example. **OR** Explain RSA algorithm for forming digital signature with suitable example.	**CO3**