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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2021

Course: Network Security and Cryptography
Semester: VII
Program: B.Tech ECE **Time 03 hrs.**
Course Code: ECEG 4019 **Max. Marks: 100**

SECTION A

1. Each Question will carry 4 Marks
2. Instruction: Complete the statement / Select the correct answer(s)

S. No.		Marks	CO
Q 1	a) A combination of encryption and decryption algorithm is called as ________. b) Define Denial of service.	**4**	**CO1**
Q.2	Suppose that plaintext message units are single letters in the usual 26-letter alphabet with A-Z corresponding to 0-25. You receive the sequence of cipher text message units 14, 25, 89. The public key is the sequence {57, 14, 3, 24, 8} and the secret key is b = 23, m = 61. Decipher the message. Find the plain text.	**4**	**CO1**
Q.3	Dividing (11001001) by (100111). Calculate the remainder.	**4**	**CO1**
Q.4	Determine the quotient for Division of (HAPPY) 26 by (SAD) 26.	**4**	**CO1**
Q.5	a) Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique. b) List out the components of encryption algorithm.	**4**	**CO1**

SECTION B

1. Each question will carry 10 marks

2. Instruction: Write short / brief notes

Q.1	a) Differentiate Message Authentication Code and Hash function. b) How Digital signature differs from authentication protocols?	**10**	**CO2**
Q.2	Perform encryption and decryption using RSA Alg. for the following. P=17; q=11; e=7; M=88.	**10**	**CO2**
Q.3	Differentiate the following: a) Stream Cipher and Block Cipher b) Symmetric and Asymmetric Encryption c) Threat and Attack d) Active attack and Passive attack	**10**	**CO3**

	e) AES decryption algorithm and the equivalent inverse cipher		
Q.4	Explain the architecture of IP security in detail.	**10**	**CO3**
SECTION-C **1. Each Question carries 20 Marks.** **2. Instruction: Write long answer.**			
Q.1	a)Discuss authentication header and ESP in detail with their packet format. b)Explain all the different phases a virus go through his lifetime? Or a) Explain Intrusion Detection System (IDS) in detail with suitable diagram. b) Explain the concepts of Digital Signature algorithm with key generation and verification in detail.	**20**	**CO4**
Q.2	a) Describe client server Mutual authentication, with example of flow diagram. b) Explain the reasons for using PGP? or a) Discuss technical details of firewall and describe any three types of firewalls with neat diagram. b) What are the services provided by PGP?	**20**	**CO5**