Name: **Enrolment No:**	UPES UNIVERSITY OF TOMORROW

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2022

Course: Cryptography & Network Security- Mathematical Perspectives
Semester: V
Program: B.Tech.-CSE- LLB **Time: 03 hrs.**
Course Code: CSEG 3033 **Max. Marks: 100**

Instructions: Attempt All Questions.

SECTION A
(5Qx4M=20Marks)

S. No.		**Marks**	**CO**
Q 1	Encrypt the number 3 with RSA such that p=3, q=7, and e=5.	**4**	**CO2**
Q 2	Explain the key generation process of DES.	**4**	**CO1**
Q 3	Encrypt the string “Hello World” using additive cipher with key=5.	**4**	**CO1**
Q 4	Briefly explain the terms worms, virus, trojan, and spyware.	**4**	**CO4**
Q 5	Briefly Explain HMAC.	**4**	**CO2**

SECTION B
(4Qx10M= 40 Marks)

Q 6	Explain the Encryption Steps of AES Algorithm.	**10**	**CO1**
Q 7	Explain Zero Knowledge Protocol.	**10**	**CO4**
Q 8	Define IPSEC. Define the protocols defined under IPSEC.	**10**	**CO3**
Q 9	Elaborate Elliptical Curve Cryptography. **OR** Explain Whirlpool Algorithm with all necessary steps.	**10**	**CO2**

SECTION-C
(2Qx20M=40 Marks)

Q 10	Explain Firewall in detail.	**20**	**CO4**
Q 11	Explain SHA-512 algorithm in detail. **OR** Explain MD-5 algorithm in detail.	**20**	**CO3**