Name:

Enrolment No:



Semester: V

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2022

Course: Cryptography and Network Security

Program: B.Tech.-CSE- All Branch

Time: 03 hrs. **Course Code: CSEG3040P** Max. Marks: 100

Instructions: Attempt All Questions.

SECTION A (**5Qx4M=20Marks**)

		1	
S. No.		Marks	CO
Q 1	Define CMAC.	4	CO3
Q 2	Explain Diffie-Helman Key exchange algorithm.	4	CO2
Q 3	Elaborate Digital Signature Scheme.	4	CO3
Q 4	Describe the terms worms, virus, trojan, and spyware.	4	CO4
Q 5	Discuss the various services provided by digital signature.	4	CO3
	SECTION B		
(4Qx10M= 40 Marks)			
Q 6	Describe the key generation process of RSA. If someone applies RSA on a number 5 with p=7, q=11, and e=13. What will be the encrypted value.	10	CO2
Q 7	Explain Zero Knowledge Protocol.	10	CO4
Q 8	Illustrate IPSEC. Define the protocols under IPSEC.	10	CO3
Q 9	Describe PGP algorithm in detail. OR Differentiate between MIME and S/MIME in detail.	10	CO1
SECTION-C			
(2Qx20M=40 Marks)			
Q 10	 (a) Apply Extended Euclidean Algorithm on GCD (171, 13). (b) Differentiate between symmetric and asymmetric key cipher. Encrypt the plaintext "This is cryptography exam" using Playfair cipher with key "pascal". 	20	CO1
Q 11	Explain SHA-512 algorithm in detail. OR Explain MD-5 algorithm in detail.	20	CO2