Name:

Enrolment No:

UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2021

Course: Cryptography and Network Security	**Semester: VII**
Program: B. Tech. CSE	**Duration: 03 hrs.**
Course Code: CSEG 4001	**Max. Marks: 100**

Instructions: The marks for each question are given before.

SECTION A

(5Qx 4M = 20 Marks)

S. No.		**Marks**	**CO**
Q 1	Differentiate between a block cipher and a stream cipher?	**4**	**CO1**
Q 2	Distinguish between active and passive security attacks. Give some examples of both types of attacks.	**4**	**CO1**
Q 3	Describe a brute-force search and why its use as cryptographic relevance?	**4**	**CO2**
Q 4	Differentiate between Direct and Arbitrated digital signatures?	**4**	**CO3**
Q5	Elucidate different types of firewalls and their configuration.	**4**	**CO4**

SECTION B

(4Qx10M = 40 Marks)

Q 1	Explain different categories of security attacks in a computer system, clearly distinguish between security attack, security mechanism and security services.	**10**	**CO1**
Q 2	Describe public key cryptography? What is the role of the session key in public key Schemes?	**10**	**CO2**
Q 3	Describe advanced encryption standard in details with its round functions.	**10**	**CO3**
Q 4	List the various services supported by PGP. Explain how PGP supports these services.	**10**	**CO4**
	Or		
	Describe Kerberos? Describe its requirements & function in cryptosystem with an example.	**10**	**CO4**

SECTION C

(2Qx 20M= 40 Marks)

Q 1	Explain Diffie-Hellman key exchange algorithm. Let the prime number be 353 and one of its primitive root be 3. Let A and B select their secret keys X_A = 97 and X_B = 233 compute.	**10+10**	**CO2**

	(i) Public key of A and B. (ii) Common secret key.		
Q 2	Describe the role of RSA algorithm in Public key cryptography. Suppose we have a set of message blocks enclosed with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Somehow we come to know that one of the plain text block has a common factor with n. Does this help us anyway to recover plaintext without knowledge of private key? Does the RSA scheme still works even it plaintext blocks share common factor with n? Defend your answer.	**10 +10**	**CO3**
Or			
	Differentiate between Hash code and message authentication code (MAC). Consider a digital document submission center (DSC) where students of computer science have been asked to submit their assignment electronically before certain deadline. When an assignment is submitted a DSC puts a time stamp on the document and issues a digital receipt to the student. Earlier is the submission, higher is the grade awarded. Suggest a mechanisms that can be implemented for this purpose. Assume the DSC is not fully trusted by the student.	**10 +10**	**CO3**