


Name:			
Enrolment No:			
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, May 2022			
Course: Cryptography and Network Security Program: B.Tech. Course Code: CSEG-4001		Semester: VI Time: 03 hrs. Max. Marks: 100	
Instructions: Attempt all questions.			
SECTION A (5Qx2M=10Marks)			
S. No.		Marks	CO
Q 1	How is steganography different from cryptography, and what are the two general approaches to attacking a cipher?	2x1=2	CO1
Q 2	In the context of Kerberos, what is a principal?	2	CO5
Q 3	Define the RSA algorithm stepwise.	2	CO3
Q 4	List the layers in OSI security architecture.	2	CO4
Q 5	How much key space is available when a monoalphabetic substitution cipher is used to replace plaintext with ciphertext?	2	CO2
SECTION B (4Qx5M= 20 Marks)			
Q 1	Show that data encryption standard (DES) decryption is, in fact, the inverse of data encryption standard (DES) encryption.	5	CO1
Q 2	a. Define a nonsingular transformation with example. b. Define a product cipher with example.	3+2=5	CO2
Q 3	Define a one-way function, and Perform encryption and decryption using the RSA algorithm, for the following: $p=11; q=13; e=11; M=7$.	1+4=5	CO3
Q 4	List and define the fundamental security design principles.	5	CO4
SECTION-C (2Qx10M=20 Marks)			
Q 1	For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES. <ol style="list-style-type: none"> XOR of subkey material with the input to the f function XOR of the f function output with the left half of the block f function permutation P swapping of halves of the block 	5x2=10	CO1, CO2
Q 2	a. Define message authentication.	5x2=10	CO4,

	<ul style="list-style-type: none"> b. What two levels of functionality comprise a message authentication or digital signature mechanism? c. What are some approaches to producing message authentication? d. In what ways can a hash value be secured so as to provide message authentication? e. List and briefly describe the design objectives for HMAC. 		CO5
SECTION-D (2Qx25M=50 Marks)			
Q 1	<ul style="list-style-type: none"> a. Explain the symmetric cipher model with example. b. Explain substitution techniques with example. c. Define monoalphabetic ciphers with example. d. Explain transposition techniques with example. e. What are the drawbacks of a Playfair cipher? 	5x5=25	CO1, CO2, CO3
Q 2	<ul style="list-style-type: none"> a. What are the two types of protocols used for transferring email (explain both the protocols)? What are the PGP and S/MIME standards (explain both)? b. Describe the S/MIME message content types. How compression of messages is achieved in S/MIME (needs proper explanation)? c. Describe the role of a compression function in a hash function. 	9+10+6=25	CO4, CO5