Name:

**Enrolment No:** 



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

Course: B Tech
Program: CSE (All IBM + Xebia)
Course Code: CSEG4001
Semester: VII
Time : 03 hrs.
Max. Marks: 100

**Instructions:** Answer all the Questions

SECTION A				
S. No.		Marks	СО	
Q 1	What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?	4	CO1	
Q 2	What entities constitute a full-service Kerberos environment?	4	CO3	
Q 3	What is the difference between weak and strong collision resistance?	4	CO2	
Q 4	What is the difference between direct and arbitrated digital signatures?	4	CO3	
Q 5	What is the sum of three points on an elliptic curve that lie on a straight line?	4	CO2	
	SECTION B			
Q 6	Differentiate between symmetric and asymmetric cipher. Encrypt the plaintext using this Play fair cipher having key "Sunil" and message is: "cryptography is a secret writing".	10	CO1	
Q 7	List four techniques used by firewalls to control access and enforce a security policy.	10	CO4	
Q 8	What are the different services provided by IPsec? How AH and ESP are used in the architecture of IPsec.	10	CO3	
Q 9	Decipher the message YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ using the Hill cipher with the inverse $\ker = \begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$ . Show your calculations and the result.  OR  Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the $\ker = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ . Show your calculations and the result.	10	CO1	

## SECTION-C

Q 10	Why do we use public key cryptography? Describe the role of the RSA algorithm and perform encryption and decryption using the RSA algorithm for the following:  (a) $p = 3$ , $q = 11$ , $e = 7$ , $M = 5$ (b) $p = 11$ , $q = 13$ , $e = 11$ , $M = 7$ OR  Explain public key management in cryptography. Whether Diffie-Hellman supports in public key management, also solve the following example and show your calculations and the result:  Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 2$ 3 and a primitive root $\alpha = 5$ .  a. If Bob has a public key $Y_B = 10$ , what is Bob's private key $Y_B$ ?  b. If Alice has a public key $Y_A = 8$ , what is the shared key K with Bob?  c. Show that 5 is a primitive root of 23.	20	CO2
Q 11	Explain the following:  a) Intrusion Detection System b) Trusted Systems c) Zero Knowledge Protocol d) Biometric Authentication	20	CO4