Name:

Enrolment No:

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

Course: Cryptography and Cryptanalysis | **Semester: II**
Program: M.TECH. | **Time: 03 hrs.**
Course Code: CSCS 7005 | **Max. Marks: 100**

Instructions: Attempt all questions.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Explain the Vigenere cipher with the help of examples.	**4**	**CO1**
Q 2	What are the differences between a block cipher and a stream cipher?	**4**	**CO4**
Q 3	a. Encrypt the message "Let us meet at our usual place" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. b. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.	**2x2=4**	**CO2**
Q 4	Perform encryption and decryption using the RSA algorithm, for the following: $p=17; q=31; e=7; M=2.$	**4**	**CO3**
Q 5	For each of the following equations, find an integer x that satisfies the equation. a. $7x \equiv 6 \pmod 9$ b. $9x \equiv 3 \pmod 7$	**2x2=4**	**CO 4**

SECTION B
(4Qx10M= 40 Marks)

S. No.		Marks	CO
Q 1	a. Define the symmetric and asymmetric cipher model with the proper structures. b. Define the terms substitution and transposition in encryption algorithms with some examples.	**2x5=10**	**CO1**
Q 2	a. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2. b. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?	**2x5=10**	**CO2**
Q 3	a. Define message authentication. b. What two levels of functionality comprise a message	**5x2=10**	**CO3**

	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.		
Q 4	In the Diffie-Hellman technique, each participant selects a secret number x and sends the other participant α^x mod q for some public number α. What would happen if the participants sent each other x^α for some public number α instead? Give at least one method A and B could use to agree on a key. Can C break your system without finding the secret numbers? Can C find the secret numbers? **OR** Suppose A (female) & B (male) use an ElGamal scheme with a common prime $q=71$ and a primitive root $\alpha=7$. a. If B has public key $K_{B1}=3$ and A chose the random integer $k=2$, what is the ciphertext of $M=30$? b. If A now chooses a different value of k so that the encoding of $M=30$ is $C=(59, C_2)$, what is the integer C_2?	**10**	**CO4**
SECTION-C **(2Qx20M=40 Marks)**			
Q 1	a. Describe the data encryption standard with each round structures. b. Explain the advanced encryption standard with all possible structures. c. Explain the international data encryption algorithm with structures. d. What are the differences in DES, AES and IDEA?	**4x5=20**	**CO1, CO2**
Q 2	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)? **OR** a. Explain Pollard's algorithm with example. b. Find a number x between 0 and 37 with x^{73} congruent to 4 modulo 37. (You should not need to use any brute-force searching.)	**2x10=20**	**CO3, CO4**