Name: **Enrolment No:**	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course: Cryptography and Network Security **Semester: VII**
Programme: B.Tech. (CSE) **Time: 03 hrs.**
Course Code: (CSEG4001) **Max. Marks: 100**
Instructions: Attempt all questions. There are internal choices in Q. No. 11 and 12.

SECTION A

Note: Answers in this section are to be typed in and each question will carry 5 marks.

Q 1	(a) Amit buys a product from a manufacturer and pays for it electronically, but the manufacturer later refuses having received the money and asks to be paid. This kind of act or attack is categorized as _____. (b) List the names of security services specified under ITU-T(X.800). (b) Which of the listed below are not security mechanisms: (i) Data Integrity (ii) Encipherment (iii) Anti-Phishing (iv) Traffic Padding (v) Non-repudiation	**1, 3, 1**	**CO1**
Q 2	(a) Which elements in the set $\mathbf{Z}_5$={0, 1, 2, 3, 4} are not members of the set $\boldsymbol{Z}_5^*$? (b) Result of –16 *mod* 13 = _____. (c) State either *true* or *false*: –3 ≡ 7 (*mod* 5)	**2, 2, 1**	**CO1**
Q 3	(a) In GF(7), the result of 5 × 4 = _____ and 6 ÷ 3 = _____. (b) The three common algebraic structures in Cryptography are ____ , _____, and _____.	**2, 3**	**CO2**
Q 4	(a) A standard DES implementation accepts _____ bits of plaintext, _____bits of secret key, and usually comprises of ____ rounds. (b) Define confusion and diffusion in the context of block ciphers.	**3, 2**	**CO2**
Q 5	(a) The result of ϕ(10) = ____. (b) The number of elements in $\boldsymbol{Z}_{15}^*$ is ____. (c) Source repudiation can be handled using public key application called _____.	**2, 2, 1**	**CO3**
Q 6	(a) Name the hash algorithms used by SSL in order to provide message integrity. (b) SSL provides four protocols in two layers. Here the *record* protocol carries messages from _____, _____, and _____ protocols as well as the data coming from application layer.	**2, 3**	**CO4**

SECTION B **Note: Answers in this section are to be scanned and uploaded. Each question will carry 10 marks.**			
Q 7	(a) A ciphertext "QTKM" has been generated by the Affine cipher using the key pair (15,2) in $\mathbf{Z}_{26}$ space. In the key pair (K_1, K_2), K_1 is the multiplicative key and K_2 is the additive key. Illustrate the decryption procedure. (b) Justify that the Vigenere' cipher is a polyalphabetic substitution cipher.	**6, 4**	**CO1**
Q 8	(a) Draw and discuss the structure of a single typical Feistel round. Does AES follow Feistel structure? (b) Compare Cipher Feedback (CFB), and Counter (CTR) modes of block cipher operation on the basis of: (i) Parallel processing capability (ii) Preprocessing of the encryption part (iii) Error propagation (iv) Usage as a stream cipher	**6, 4**	**CO2**
Q 9	(a) List all the transformations performed in a typical AES round with a brief description of each. Which of the listed operations is skipped in the last AES round? (b) Multiply $x^3 + x^2 + x + 1$ by $x^3 + 1$. Use $x^4 + x^3 + 1$ as modulus.	**6, 4**	**CO2**
Q 10	(a) Are Modification Detection Code (MDC) and Message Authentication Code (MAC) same? Justify your argument. Brief the requirements for a hash function. (b) The procedure to generate a simple hash function based on bit by bit exclusive-OR (XOR) defined as: • Divide the input message into equal sized blocks of n-bits each. • Initially set n-bit hash value to zero. • Process each successive n-bit block as follows: - Rotate the current hash value to the left (circular) by one bit. - XOR the block into the hash value Find an 8-bit hash code using this algorithm if the message obtained in the Hex format is 10 2F 1B 08. Justify whether the hash code so generated is preimage resistant.	**6, 4**	**CO3**
Q 11	(a) Define IPSec. Distinguish between the two modes of IPSec. (b) Discuss briefly the malicious software.	**6, 4**	**CO4**
	OR		
	(a) State the types of intruders. Brief intrusion detection and its mechanisms. (b) Explain the concept of firewalls.	**6, 4**	**CO4**

SECTION C **Note: Answers in this section are to be scanned and uploaded. Each question will carry 20 marks.**			
Q 12	(a) Define KDC. Discuss a protocol that involves KDC for the distribution of session keys within the communicating parties. (b) Explain the procedure to generate the session key in Diffie-Hellman key exchange algorithm. (c) In a Diffie-Hellman system, prime number p and its primitive root g are selected as 23 and 7 respectively. Further, Alice and Bob decide their private keys as 3 and 6, respectively. (i) Find the secret shared key. (ii) Show that 7 is primitive root of 23.	**7, 8, 5**	**CO3**
	OR		
	(a) Define password salting and explain the procedure of password salting. Other than fixed passwords, name two other mechanisms for entity authentication. (b) State RSA encryption and decryption as a trap-door one-way function. Explain the key generation process in RSA. (c) Perform encryption and decryption using RSA algorithm with input parameters given as $p = 3$, $q = 11$, $e = 7$, and $M = 5$.	**7, 8, 5**	**CO3**