Candidate seat No: _____

Charotar University of Science and Technology

Sixth semester of B. Tech (IT) Examination
July 2022
IT348 Cryptography and Network Security

Date: 25/07/2022, Monday **Time: 10:00 am to 1:00 pm** **Maximum Marks: 70**

Instructions:
(i) Attempt ***all*** the questions.
(ii) Figures to the right indicate ***full*** marks.
(iii) Make suitable assumptions and draw neat figures wherever if required.

Section 1

Q-1	(a)	Define the following I. Network Security II. Differentiate cryptanalytic attacks and non-cryptanalytic attacks. III. Interception IV. Steganography	**[2]**
	(b)	Use the playfair cipher to encipher the message "The algorithm is very strong". Use the key "respective".	**[2]**
	(c)	List and explain various types to evaluate security of a cryptosystem.	**[3]**
Q-2	(a)	Draw the AES Architecture and explain its working in detail. Consider 10 rounds of AES.	**[5]**
	(b)	Use the Vigenere Cipher with the keyword "HEALTH" to encipher the message "Life is full of surprises". Find the cipher text.	**[5]**
	(c)	Find the Greatest Common Divisor of 2740 and 1760 using Euclidean Algorithm.	**[4]**
		OR	
Q-2	(a)	Explain single round of DES with figure.	**[4]**
	(b)	Explain in brief. 1. Chosen-message Attack 2. Known-message Attack 3. Key-only Attack	**[5]**
	(c)	Encrypt the message using Playfair cipher "The house is being sold tonight" with the key "MONARCHY".	**[5]**
Q-3	(a)	List and explain cryptographic hash function criteria.	**[4]**
	(b)	Describe in detail "Man-in-the-Middle" attack of Diffie Hellman algorithm.	**[5]**
	(c)	Write a short note on Broadcast Security and Multicast-Rekeying.	**[5]**
		OR	
Q-3	(a)	Explain key generation process in DES	**[4]**
	(b)	What is Kerberos? List down its servers. Define the duties of each server	**[5]**
	(c)	What is PKI? Discuss the need and future of PKI.	**[5]**

Candidate seat No: _____

Section 2

Q-4	(a)	Solve the following by applying Chinese Reminder Theorem. a1=2, a2=3, a3=3 and m1=3, m2=5, m3=7.	**[3]**
	(b)	Discuss RSA Algorithm with suitable example	**[7]**
Q-5	(a)	What is trapdoor function? What is the strength of trapdoor function in cryptography?	**[3]**
	(b)	Explain the invertible and non-invertible components used in Feistel cipher.	**[6]**
	(c)	Calculate the padding bit (SHA512) require for the messages having below-mentioned length: 1. 1 2. 896 3. 897	**[3]**

OR

Q-5	(a)	Differentiate active and passive attack.	**[3]**
	(b)	Write a short note on any TWO of the following 1. Master Key Generation in SSL 2. Trust calculation in Preety Good Privacy 3. Secure MIME	**[6]**
	(c)	Draw and explain model for network security.	**[3]**
Q-6	(a)	Find the multiplicative inverse of 23 in Z_{100}.	**[3]**
	(b)	Given p = 31, q = 23, e = 223 and m (plain text) = 439. Demonstrate the working of RSA algorithm using given values.	**[7]**
	(c)	What is cryptanalysis? What are the different ways to do cryptanalysis?	**[3]**

OR

Q-6	(a)	What is the purpose of X.509 standard? Explain the signature field of X.509 certificate format.	**[3]**
	(b)	Explain PGP and Symmetric Key Distribution.	**[7]**
	(c)	Explain Handshake protocol in SSL.	**[3]**

****