Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2021

Subject Code:3170720 Date:29/12/2021

Subject Name:Information security

Time:10:30 AM TO 01:00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Define the following terms: (i) Non-repudiation (ii) Data integrity (iii) Confidentiality	**03**
	(b)	Distinguish between passive and active security attacks? Define the type of Security attack in each of the following cases: (i) A student breaks into a professor's office to obtain a copy of the next day's test. (ii) A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100. (iii) A student sends hundreds of e-mails per day to another student using a phony return e-mail address.	**04**
	(c)	List and explain various block cipher modes of operation with the help of diagram.	**07**
Q.2	**(a)**	What is the purpose of S-boxes in DES? Explain the avalanche effect.	**03**
	(b)	Construct a Playfair matrix with the key "engineering". And encrypt the message "test this Balloon".	**04**
	(c)	Let K = 133457799BBCDFF1 be the key in hexadecimal. Derive K1 the first round sub key using a single round version of DES.	**07**

Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

OR

	(c)	Let M =3243F6A8885A308D313198A2E0370734 be the plain text message and K=2B7E151628AED2A6ABF7158809CF4F3C be the key in hexadecimal. Perform the following operation using AES. (a) Add round key. (b) Shift row transformation on output of (a)	**07**
Q.3	**(a)**	What is a nonce? What is the difference between a session key and a master key?	**03**

	(b)	Differentiate between hashing and encryption. What are the practical applications of hashing?	**04**
	(c)	Explain Diffie Hellman key exchange algorithm with example.	**07**

OR

Q.3	**(a)**	What is public key cryptography? What are the principal elements of a public-key cryptosystem?	**03**
	(b)	Perform encryption and decryption using the RSA algorithm for p=5, q=11, e=3, M=9.	**04**
	(c)	What do you mean by key distribution? Give at least one method for key distribution with proper illustration.	**07**
Q.4	**(a)**	Explain the triple DES scheme with two keys.	**03**
	(b)	Differentiate between Conventional encryption and Public-key encryption.	**04**
	(c)	Discuss X.509 Certificates.	**07**

OR

Q.4	**(a)**	Why not Double DES? What is a meet-in-the-middle attack?	**03**
	(b)	Discuss message digest generation using SHA-512.	**04**
	(c)	What is message authentication code? What is the difference between a Message authentication code and a one-way hash function? Write the basic uses of Message authentication code.	**07**
Q.5	**(a)**	Encrypt the message " Asymmetric key cryptography is fun" using Transposition cipher with key (3,2,6,1,5,4)	**03**
	(b)	Write difference between (i) block cipher and stream cipher (ii) monoalphabetic cipher and polyalphabetic cipher	**04**
	(c)	Discuss generic model of digital signature process.	**07**

OR

Q.5	**(a)**	Using the Viennese cipher, encrypt the word "explanation" using the key leg.	**03**
	(b)	Discuss four general categories of schemes for the distribution of public keys.	**04**
	(c)	Explain Kerberos in detail.	**07**

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2022

Subject Code:3170720 Date:10/06/2022

Subject Name:Information security

Time:02:30 PM TO 05:00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Define the following terms: (i) Security Attack (ii) Security Services (iii) Security Mechanism	**03**
	(b)	Answer following questions. (i) 15 parties want to exchange messages securely using symmetric key encryption algorithm. The number of distinct key values required will be_____. (ii) 15 parties want to exchange messages securely using asymmetric key encryption algorithm. The number of distinct key values required will be_____. (iii) Total number of s-box used in DES is_____. (iv) How many AES rounds are required for 128-bit key size?	**04**
	(c)	List and explain various types of attacks on encrypted message.	**07**
Q.2	**(a)**	Encrypt the message "CORONA" using Hill Cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	**03**
	(b)	Discuss different techniques for public-key distribution.	**04**
	(c)	Elaborate DES encryption with neat sketches.	**07**
		OR	
	(c)	Elaborate AES encryption with neat sketches.	**07**
Q.3	**(a)**	Discuss Meet-in-the-Middle Attack.	**03**
	(b)	Discuss Cipher Block Chaining (CBC) modes of operation with the help of diagram.	**04**
	(c)	What is KDC? With the help of diagram explain how KDC do key distribution.	**07**
		OR	
Q.3	**(a)**	Discuss Man-in-the-Middle Attack.	**03**
	(b)	Discuss Cipher Feedback (CFB) block cipher modes of operation with the help of diagram.	**04**
	(c)	Discuss briefly the working of KERBEROS authentication protocol.	**07**
Q.4	**(a)**	Decipher the message "KBSTZPEGBWNDGQHWQWC" Using Vigenere cipher with key "confidential"	**03**
	(b)	Explain the following properties of hash function (i) One way property (ii) Weak collision resistance	**04**
	(c)	P and Q are two prime numbers. P=17, and Q=31. Take public key E=7. If plain text value is 2, then what will be the private key and cipher text value according to RSA algorithm? Explain in detail.	**07**

OR

Q.4	**(a)**	Encrypt the message "WE ARE DISCOVERED FLEE AT ONCE" using Rail fence cipher with rail = 3	**03**
	(b)	Explain the triple DES scheme with two keys and write about proposed attacks on 3DES	**04**
	(c)	For Diffie-Hellman algorithm, two publically known numbers are prime number 23 and primitive root (g) of it is 9. A selects the random integer 4 and B selects 3. Compute the public key of A and B. Also compute common secret key.	**07**
Q.5	**(a)**	Define the following terms: (i) Cryptography (ii) Cryptanalysis (iii) Brute-force attack	**03**
	(b)	Discuss SSL protocol stack.	**04**
	(c)	Discuss Secure Hash Algorithm (SHA)	**07**

OR

Q.5	**(a)**	Illustrate variety of ways in which MAC code can be used to provide Message authentication.	**03**
	(b)	Consider ElGamal cryptosystem in Z_{17} with generator 6. If the message is 13 and the randomness chosen is 10, then find the ciphertext computed using the public key 7.	**04**
	(c)	Discuss X.509 authentication service.	**07**

****