Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VII (NEW) EXAMINATION – WINTER 2020

Subject Code:2170709 Date:21/01/2021

Subject Name:Information and Network Security

Time:10:30 AM TO 12:30 PM Total Marks: 56

Instructions:

1. **Attempt any FOUR questions out of EIGHT questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			MARKS
Q.1	**(a)**	Define: Confidentiality, Authenticity and Integrity.	**03**
	(b)	Discuss Avalanche effect and Completeness property of a block cipher.	**04**
	(c)	Explain Playfair cipher technique in detail. Find cipher text for plain text 'GTUINSEXAM' using 'STUDY' as key.	**07**
Q.2	**(a)**	Compare and contrast symmetric key cryptography and asymmetric key cryptography.	**03**
	(b)	Explain the process of key generation in DES.	**04**
	(c)	Draw a detailed block diagram of encryption process in DES. Add appropriate description.	**07**
Q.3	**(a)**	Briefly explain Triple DES with two keys.	**03**
	(b)	Explain public key cryptosystem with neat diagram.	**04**
	(c)	Calculate all the values of RSA assuming two primes p=17 and q=11. Assume other values appropriately.	**07**
Q.4	**(a)**	State the differences between *chosen plain text* and *chosen cipher text* attack.	**03**
	(b)	Write a short note on Man-in-the-middle attack.	**04**
	(c)	Calculate all the values for Diffie-Hellman key exchange, consider two primes q=353 and a=3. Assume other values appropriately.	**07**
Q.5	**(a)**	Enlist various web security threats. Explain any one.	**03**
	(b)	Explain how Birthday attack is carried out.	**04**
	(c)	Define message authentication code and its characteristics. Discuss MAC based on any standard block cipher.	**07**
Q.6	**(a)**	What are different ways for distribution of public keys?	**03**
	(b)	Write a short note on PGP.	**04**
	(c)	Justify the characteristics needed for a hash function. Explain Secure Hash Algorithm-1 in brief.	**07**
Q.7	**(a)**	What is defined by X.509 certificate? Write the process of authentication in X.509.	**03**
	(b)	What is TGT? Explain its use in Kerberose.	**04**
	(c)	Write a detailed note on SSL architecture and protocol.	**07**
Q.8	**(a)**	How does secure socket layer protocol work?	**03**
	(b)	Explain key distribution process using Key Distribution Center (KDC).	**04**
	(c)	Explain digital signature schemes Elgamal and Schnorr.	**07**

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER– VIII EXAMINATION – SUMMER 2020

Subject Code: 2170709 Date:27/10/2020

Subject Name: Information and Network 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.**

			MARKS
Q.1	**(a)**	Define the terms: Confidentiality, Data integrity, Non-repudiation	**03**
	(b)	Construct a Playfair matrix with the key "engineering". And encrypt the message "impossible".	**04**
	(c)	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.	**07**
Q.2	**(a)**	Write the differences between conventional encryption and public key encryption.	**03**
	(b)	Write a note on Hill Cipher.	**04**
	(c)	Explain the key generation in DES algorithm.	**07**
		OR	
	(c)	Explain the key generation in AES algorithm.	**07**
Q.3	**(a)**	What is the purpose of the S-boxes in DES? Explain the avalanche effect.	**03**
	(b)	Explain Cipher Block Chaining (CBC) and Electronic Code Book (ECB) block cipher modes of operation with the help of diagram.	**04**
	(c)	Explain X.509 authentication service.	**07**
		OR	
Q.3	**(a)**	What is the difference between a session key and a master key?	**03**
	(b)	Explain Cipher Feedback (CFB) and Output Feedback mode (OFB) block cipher modes of operation with the help of diagram.	**04**
	(c)	Explain authentication mechanism of Kerberos.	**07**
Q.4	**(a)**	What characteristics are needed in a secure hash function?	**03**
	(b)	In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?	**04**
	(c)	What do you mean by key distribution? Give at least one method for key distribution with proper illustration.	**07**
		OR	
Q.4	**(a)**	What is the purpose of the State array? How many bytes in State are affected by ShiftRows?	**03**
	(b)	Is message authentication code same as encryption? How message authentication can be done by message authentication code?	**04**
	(c)	Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.	**07**
Q.5	**(a)**	Using the Vigenère cipher, encrypt the word "ATTACKATDAWN" using the key "LEMON".	**03**
	(b)	Write a note on HTTPS.	**04**
	(c)	Write a short note on "Digital Signature Algorithm".	**07**
		OR	
Q.5	**(a)**	Explain basic Hash code generation.	**03**
	(b)	How public keys can be distributed.	**04**
	(c)	Explain SSL architecture.	**07**

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER– VII (New) EXAMINATION – WINTER 2019

Subject Code: 2170709 **Date: 26/11/2019**

Subject Name: Information and Network 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.**

Q.1	**(a)**	Define following principles of security: 1) Confidentiality 2) Integrity 3) Availability	**03**
	(b)	Describe Rail-fence cipher algorithm with example.	**04**
	(c)	Explain cryptanalytic attacks with example of any encryption algorithm.	**07**
Q.2	**(a)**	Explain one time pad algorithm with example and mention its strength and weakness.	**03**
	(b)	What is the difference between a mono alphabetic cipher and a polyalphabetic cipher?	**04**
	(c)	Encrypt the message “GTU Examination” using the Hill cipher algorithm with the key matrix $\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$. Show your calculations and the result.	**07**
		OR	
	(c)	Perform encryption in Playfair Cipher algorithm with plain text as “INFORMATION AND NETWORK SECURITY”, Keyword is “MONARCHY”. (Note: 1.Put j and i both combine as a single field in 5*5 matrix).	**07**
Q.3	**(a)**	Explain CFB algorithm mode with diagram.	**03**
	(b)	Describe the Diffie Hellman key exchange Algorithm with example.	**04**
	(c)	Draw block diagram to show Broad level steps in DES and also give steps of one round in DES with another diagram.	**07**
		OR	
Q.3	**(a)**	Explain Counter (CTR) algorithm mode with diagram.	**03**
	(b)	Differentiate block cipher and stream cipher algorithm with example	**04**
	(c)	Explain process of encryption in RSA Algorithm with suitable example. (Prime Number P,Q and Encryption Key E is given for reference) P=7, Q=17, E=7	**07**
Q.4	**(a)**	What are the principal elements of a public-key cryptosystem?	**03**
	(b)	What is a meet-in-the-middle attack in double DES?	**04**
	(c)	Briefly describe Mix Columns and Add Round Key in AES algorithm.	**07**
		OR	
Q.4	**(a)**	What is the role of a compression function in a hash function?	**03**
	(b)	What is the main difference between HTTP and HTTPS protocol. When HTTPS is used, which elements of the communication are Encrypted?	**04**

	(c)	Explain working of Secure Hash Algorithm, with basic arithmetical and logical functions used in SHA.	**07**
Q.5	**(a)**	Draw Generic Model of Digital Signature Process.	**03**
	(b)	Explain Elgamal Digital Signature Scheme.	**04**
	(c)	Describe MAC with its security implications.	**07**

OR

Q.5	**(a)**	What problem was Kerberos designed to address?	**03**
	(b)	Explain Schnorr Digital Signature Scheme.	**04**
	(c)	Explain use of Public-Key Certificate with diagram and draw X.509 certificate format.	**07**

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII(NEW) EXAMINATION – SUMMER 2019

Subject Code:2170709 Date:14/05/2019

Subject Name:Information and Network 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**

				MARKS
Q.1	**(a)**		Which two methods are used to frustrate statistical cryptanalysis?	**03**
	(b)		In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key , find out decryption key. What will be the ciphertext, if the plaintext is 2?	**04**
	(c)	(i)	Explain working of ECB.Why ECB (Electronic code book) is rarely used to encrypt message?	**07**
		(ii)	Why CFB(Cipher feedback mode) encrypted messages are less subject to tampering than OFB(Output feedback mode)?	
Q.2	**(a)**		Is a message authentication code(MAC) function is similar to encryption. Does MAC provide authentication or confidentiality? Justify your answer	**03**
	(b)		For Diffie-Hellman algorithm, two publicaly known numbers are prime number 353 and primitive root of it is 3. A selects the random integer 97 and B selects 233. Compute the public key of A and B. Also compute common secret key.	**04**
	(c)		Explain four different stages of AES(Advance Encryption standard) structure.	**07**
			OR	
	(c)		Explain how DES(Data Encryption standard) algorithm observes Fiestel structure. Explain key generation and use of S-box in DES algorithm.	**07**
Q.3	**(a)**		Explain the three approaches to attack RSA mathematically.	**03**
	(b)		What is the difference between weak and strong collision resistance? Consider the hash functions based on cipher block chaining, What kind of attack can occur on this?	**04**
	(c)		Given key K= $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ and plaintext =”ney”. Find out the ciphertext applying Hill Cipher. Is Hill cipher strong against ciphertext only attack or known plaintext attack? Justify the answer.	**07**
			OR	
Q.3	**(a)**		For what purpose Secure Shell(SSH) is useful? Briefly define SSH protocol.	**03**
	(b)		How meet in the middle attack is performed on double DES?	**04**

	(c)	How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key "hidden" and encrypt the message "Message" using playfair cipher.	**07**
Q.4	**(a)**	Explain the rail fence cipher. Why a pure transposition cipher is easily recognized?	**03**
	(b)	What is the difference between a session key and a master key? List four general categories of schemes for the distribution of public keys.	**04**
	(c)	Explain the logic of SHA(Secure Hash Algorithm).	**07**
		OR	
Q.4	**(a)**	Why Transport Layer Security makes use of a pseudo random function?	**03**
	(b)	What is the purpose of X.509 standard? How is an X.509 certificate revoked?	**04**
	(c)	Write the algorithm for message authentication code(MACs) based on HASH functions.	**07**
Q.5	**(a)**	Define the parameters that define SSL session state and session connection.	**03**
	(b)	What problem was Kerberos designed to address? What are the three threats associated with user authentication over a network or Internet?	**04**
	(c)	Describe Elgamal digital signature.	**07**
		OR	
Q.5	**(a)**	Which types of security threats are faced by user while using the web?	**03**
	(b)	List three approaches to secure user authentication in a distributed environment.	**04**
	(c)	What is the principle of digital signature algorithm(DSA). How a user can create a signature using DSA? Explain the signing and verifying function in DSA.	**07**

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2018

Subject Code: 2170709 **Date: 19/11/2018**

Subject Name: Information and Network 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.**

			MARKS
Q.1	**(a)**	Differentiate block cipher and a stream cipher.	**03**
	(b)	Encrypt the Message "Surgical Strike" with key "GUJAR" using PLAYFAIR technique.	**04**
	(c)	Discuss in detail encryption and decryption process of DES.	**07**
Q.2	**(a)**	Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.	**03**
	(b)	Describe the term: Authentication, Authorization, Integrity and Non – repudiation.	**04**
	(c)	Discuss in detail encryption and decryption process of AES.	**07**
		OR	
	(c)	Encrypt the message "meet me at the usual place " using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$	**07**
Q.3	**(a)**	Explain Avalanche Effect.	**03**
	(b)	Discuss Man in Middle Attack.	**04**
	(c)	Explain in detail RSA algorithm, highlighting its security aspect.	**07**
		OR	
Q.3	**(a)**	Explain the VERNAM Cypher method.	**03**
	(b)	Explain the difference between diffusion and confusion.	**04**
	(c)	Briefly explain Diffie Hellman Key exchange with an example	**07**
Q.4	**(a)**	What is MAC ? How it useful in Crypto System.	**03**
	(b)	Briefly explain Digital Signature algorithm	**04**
	(c)	Described briefly the Authentication process covered by X.509.	**07**
		OR	
Q.4	**(a)**	Discuss HASH function and its application in Crypto System.	**03**
	(b)	Explain Different type of Attacks on Crypto System.	**04**
	(c)	Explain PGP with its Authentication and Confidentiality Operation.	**07**
Q.5	**(a)**	List out the various web security threats.	**03**
	(b)	What is meant by message digest? Give an example.	**04**
	(c)	Discuss clearly Secure Hash Algorithm with its real time application.	**07**
		OR	
Q.5	**(a)**	Explain HAND SHAKE protocol in SSL.	**03**
	(b)	What is KDC? List the duties of a KDC.	**04**
	(c)	Explain digital signature schemes Elgamal and Schnorr.	**07**

****

Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) - EXAMINATION – SUMMER 2018

Subject Code:2170709 **Date:01/05/2018**

Subject Name:Information and Network 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.**

			MARKS
Q.1	**(a)**	Explain data confidentiality, data authentication and data integrity.	**03**
	(b)	Describe mono alphabetic cipher.	**04**
	(c)	Explain playfair cipher with example.	**07**
Q.2	**(a)**	Explain one time pad cipher with example.	**03**
	(b)	Explain columnar transposition Cipher technique.	**04**
	(c)	Write a short note on DES.	**07**
		OR	
	(c)	Describe various steps of AES.	**07**
Q.3	**(a)**	Explain key pair generation using RSA algorithm.	**03**
	(b)	Explain encryption and decryption using RSA.	**04**
	(c)	What is digital signature? Explain hash code base digital signature.	**07**
		OR	
Q.3	**(a)**	Explain Diffie Hellman key exchange algorithm.	**03**
	(b)	Explain man in middle attack in Diffie Hellman key exchange	**04**
	(c)	Explain HMAC algorithm.	**07**
Q.4	**(a)**	Explain digital public key certificate format.	**03**
	(b)	Explain double and triple DES.	**04**
	(c)	Explain authentication mechanism of Kerberos.	**07**
		OR	
Q.4	**(a)**	Explain DSA (Digital Signature Algorithm).	**03**
	(b)	Explain various public key distribution techniques.	**04**
	(c)	Write a short note on SSL.	**07**
Q.5	**(a)**	Explain basic Hash code generation.	**03**
	(b)	Explain cipher feedback mode of DES operation.	**04**
	(c)	Write a short note on public key infrastructure.	**07**
		OR	
Q.5	**(a)**	Explain MAC code generation using block cipher.	**03**
	(b)	Explain counter mode of DES operation.	**04**
	(c)	Explain HTTPS and SSH.	**07**

****

Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) - EXAMINATION – SUMMER 2017

Subject Code: 2170709 **Date: 02/05/2017**

Subject Name: Information and Network 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.**

Q.1	**(a)**	(1) Briefly explain any two active security attacks. (2) Discuss the following terms in brief: - brute force attack - cryptography	**04** **03**
	(b)	Explain single round of DES algorithm. Support your answer with neat sketches.	**07**
Q.2	**(a)**	Elaborate AES encryption with neat sketches.	**07**
	(b)	Discuss Electronic code book and cipher feedback mode with neat diagrams.	**07**
		OR	
	(b)	Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. Key = ENGINEERING Plaintext=COMPUTER	**07**
Q.3	**(a)**	(1) Write differences between substitution techniques and transposition techniques. (2) Explain triple DES with two keys.	**03** **04**
	(b)	Write requirements for hash function and briefly explain simple hash function.	**07**
		OR	
Q.3	**(a)**	(1) Discuss the following terms in brief. - authentication - data integrity (2) Explain avalanche effect in DES and discuss strength of DES in brief.	**03** **04**
	(b)	Explain RSA algorithm in detail with suitable example.	**07**
Q.4	**(a)**	Explain any one approach to Digital Signatures.	**07**
	(b)	Discuss Diffie-Hillman key exchange algorithm in detail.	**07**
		OR	
Q.4	**(a)**	(1) Give differences between hash function and message authentication codes. (2) What are the principal elements of public-key cryptosystem? Explain in brief.	**03** **04**
	(b)	Write a detailed note on : Kerberos.	**07**
Q.5	**(a)**	Write a note on : Message Authentication Codes	**07**
	(b)	(1) Briefly explain web security threats. (2) Discuss SSL architecture in brief.	**03** **04**
		OR	
Q.5	**(a)**	Explain various general categories of schemes for the distribution of public keys.	**07**
	(b)	Write a note on : X.509 Certificate Format.	**07**

****