

GUJARAT TECHNOLOGICAL UNIVERSITY**BE- SEMESTER-VII (NEW) EXAMINATION – WINTER 2024****Subject Code:2170709****Date:07-12-2024****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.
4. Simple and non-programmable scientific calculators are allowed.

		Marks
Q.1	(a) Define: Cryptography, Cryptanalysis and Cryptanalytic attacks.	03
	(b) Discuss <i>Avalanche Effect</i> and <i>Completeness</i> property of a block cipher with appropriate example.	04
	(c) Explain Playfair cipher technique in detail. Find cipher text for plain text 'GTUEXAMMODE' using 'OFFLINE' as key.	07
Q.2	(a) Compare and contrast symmetric key cryptography and asymmetric key cryptography.	03
	(b) Explain the steps of key generation in Data Encryption Standard.	04
	(c) Draw a detailed block diagram of encryption process in DES. Add appropriate description.	07
	OR	
	(c) Draw a detailed block diagram of encryption process in AES. 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
	OR	
Q.3	(a) State the differences between <i>chosen plain text</i> and <i>chosen cipher text</i> 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.4	(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
	OR	
Q.4	(a) List out different ways for distribution of public keys? Briefly explain one.	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.5** (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 Kerberos. **04**
(c) Write a detailed note on SSL architecture and protocol. **07**
- OR**
- Q.5** (a) Define the parameters that define SSL session state and session connection. **03**
(b) Explain key distribution process using Key Distribution Center (KDC). **04**
(c) Explain digital signature schemes Elgamal and Schnorr. **07**
