

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER-VI EXAMINATION – SUMMER 2025

Subject Code:3164204

Date: 28-05-2025

Subject Name: Data 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

- Q.1**
- (a) Categorize the attacks based on threatening security goals. **03**
 - (b) What is Digital signature? List out and explain the services provided by it. **04**
 - (c) Alice and Bob want to communicate with one another using public key crypto system. Generate the keys and perform encryption and decryption. **07**

- Q.2**
- (a) Compare asymmetric encryption with symmetric encryption. **03**
 - (b) Encrypt the message “Life is full of surprises” using Auto key cipher with key=7. **04**
 - (c) Why mode of operation is defined for block ciphers? Compare the block cipher modes of operation? **07**

OR

- (c) Explain the Deffie Hellman key exchange scheme in detail with an example. **07**
- Q.3**
- (a) How can we find out GCD of two numbers using Euclid algorithm? Explain with the help of example. **03**
 - (b) What problem was Kerberos designed to address? How does it work? **04**
 - (c) Briefly explain the AES encryption structure and discuss its transformation functions. **07**

OR

- Q.3**
- (a) Define Euler’s totient function $\phi(n)$ and calculate $\phi(335)$. **03**
 - (b) What characteristics are needed in a secure hash function? **04**
 - (c) Explain the single round of DES algorithm. **07**
- Q.4**
- (a) Distinguish between message integrity and message authentication. **03**
 - (b) Explain the process of symmetric key distribution using KDC. **04**
 - (c) What is MAC? Briefly discuss HMAC algorithm. **07**

OR

- Q.4**
- (a) What types of attacks are addressed by message authentication? **03**
 - (b) List out and explain the schemes for the distribution of public keys. **04**

- (c) Briefly explain the message digest generation using SHA-512. 07
- Q.5** (a) What is public key certificate? What is the purpose of the X.509 standard? 03
- (b) Briefly explain remote user authentication using symmetric key encryption. 04
- (c) Compare Elgamal and Schnorr digital signature schemes. 07
- OR**
- Q.5** (a) Compare and contrast a conventional signature and a digital signature. 03
- (b) What is the public key infrastructure? How does it work? 04
- (c) Briefly discuss the Digital Signature Algorithm (DSA). 07
