

Seat No. / Enrolment No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

Diploma Engineering – SEMESTER – 6 (NEW) – EXAMINATION – Winter-2024

Subject Code: 4360702

Date: 21-11-2024

Subject Name: Basics of 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. Use of simple calculators and non-programmable scientific calculators are permitted.
5. English version is authentic.

		Marks
Q.1	(a) Define Security attacks and describe any two attacks in detail.	03
પ્રશ્ન.1	(અ) Security attacks ને વ્યાખ્યાયિત કરો અને કોઈપણ બે attacks નું વિગતવાર વર્ણન કરો.	૦૩
	(b) Explain data confidentiality, data integrity and data availability in terms of security.	04
	(બ) Security ની દ્રષ્ટિએ Data confidentiality, data integrity અને data availability સમજાવો.	૦૪
	(c) Describe the Rail fence method of cryptography with an example.	07
	(ક) Cryptography ની Rail fence method નું ઉદાહરણ સાથે વર્ણન કરો.	૦૭

OR

	(c) Describe the One Time Pad method of cryptography with an example.	07
	(ક) Cryptography ની One Time Pad method નું ઉદાહરણ સાથે વર્ણન કરો.	૦૭
Q.2	(a) Define Steganography and Describe any one type.	03
પ્રશ્ન.2	(અ) Steganography વ્યાખ્યાયિત કરો અને કોઈપણ એક પ્રકાર ને સમજાવો.	૦૩
	(b) Describe Caesar cipher with an example.	04

- (બ) Caesar Cipher ઉદાહરણ સાથે સમજાવો. ૦૪
- (c) Draw the key matrix for the key: UNIVERSITY and find cipher text for the plain text: GUJARAT TECHNOLOGICAL using Play fair cipher. 07
- (ક) Key: UNIVERSITY માટે Key મેટ્રિક્સ દોરો અને સાદા ટેક્સ્ટ: GUJARAT TECHNOLOGICAL માટે પ્લેફેર સાઇફરનો ઉપયોગ કરીને સાઇફર ટેક્સ્ટ શોધો. ૦૭

OR

- Q.2** (a) Differentiate between symmetric key cryptography and asymmetric key cryptography. 03
- પ્રશ્ન.2 (બ) Symmetric key cryptography અને asymmetric key cryptography ને જુદા તારવો. ૦૩
- (b) Describe Mono alphabetic cipher with an example. 04
- (બ) Mono alphabetic cipher ઉદાહરણ સાથે સમજાવો. ૦૪
- (c) Draw the key matrix for the key: GUJ and find cipher text for the plain text: HINDUSTAN using Hill cipher. 07
- (ક) Key: GUJ માટે Key મેટ્રિક્સ દોરો અને સાદા ટેક્સ્ટ: HINDUSTAN માટે હિલ સાઇફરનો ઉપયોગ કરીને સાઇફર ટેક્સ્ટ શોધો. ૦૭
- Q. 3** (a) Define public key cryptography and explain it in detail. 03
- પ્રશ્ન.3 (બ) Public key cryptography ને વ્યાખ્યાયિત કરો અને તેને સમજાવો. ૦૩
- (b) Explain the steps to verify a Digital Certificate. 04
- (બ) Digital Certificate ને verify કરવા માટેના steps સમજાવો. ૦૪
- (c) Describe the RSA algorithm with its working. 07
- (ક) RSA algorithm નું તેના કાર્ય સાથે વર્ણન કરો. ૦૭

OR

- Q. 3** (a) List out and describe three applications of public key cryptosystem. 03
- પ્રશ્ન.3 (બ) Public key cryptosystem ના ત્રણ ઉપયોગની યાદી બનાવો અને તેનું વર્ણન કરો. ૦૩

	(b) Write down the requirements of Digital Signature and List properties a Digital Signature should have.	04
	(બ) Digital Signature ની જરૂરિયાતો લખો અને Digital Signature માં જે properties હોવી જોઈએ તેની સૂચિ બનાવો.	૦૪
	(c) Describe the security of the RSA algorithm with its types in detail.	07
	(ક) RSA algorithm ની સુરક્ષાને તેના પ્રકારો સાથે વિગતવાર સમજાવો.	૦૭
Q. 4	(a) Define security zones, DMZ and VLAN.	03
પ્રશ્ન.4	(અ) Security zones, DMZ અને VLAN વ્યાખ્યાયિત કરો.	૦૩
	(b) Describe two advantages and two disadvantages of Network based Intrusion Detection System.	04
	(બ) Network based Intrusion Detection System ના બે ફાયદા અને બે ગેરફાયદાનું વર્ણન કરો.	૦૪
	(c) Describe the working of the firewall in detail with a diagram.	07
	(ક) આકૃતિ સાથે firewall ની કામગીરીનું વિગતવાર વર્ણન કરો.	૦૭
OR		
Q. 4	(a) List types of firewalls and write about needs of firewall.	03
પ્રશ્ન.4	(અ) Firewall ના પ્રકારોની યાદી આપો અને Firewall ની જરૂરિયાતો વિષયે લખો.	૦૩
	(b) Describe Network Based Intrusion Detection System.	04
	(બ) Network Based Intrusion Detection System સમજાવો.	૦૪
	(c) Describe about types of firewalls in detail.	07
	(ક) Firewall ના પ્રકારો વિશે વિગતવાર વર્ણન કરો.	૦૭
Q.5	(a) Define worms, viruses and trojans.	03
પ્રશ્ન.5	(અ) Worms, viruses અને trojans ને વ્યાખ્યાયિત કરો.	૦૩
	(b) Describe network threats with its types in detail.	04
	(બ) Network threats નું તેના પ્રકારો સાથે વિગતવાર વર્ણન કરો.	૦૪

(c) Describe traditional problems associated with cybercrime in detail. **07**

(ક) Cybercrime સાથે સંકળાયેલા traditional problems નું વિગતવાર વર્ણન કરો. ૦૭

OR

Q.5 (a) Define Cybercrime, Cybersecurity and Cyber-attack. **03**

પ્રશ્ન.5 (અ) Cybercrime, Cybersecurity and Cyber attack ને વ્યાખ્યાયિત કરો. ૦૩

(b) Describe cybercrime with its types in detail. **04**

(બ) Cybercrime નું તેના પ્રકારો સાથે વિગતવાર વર્ણન કરો. ૦૪

(c) Describe IP Spoofing, ARP spoofing and Session Hijacking in detail. **07**

(ક) IP Spoofing, ARP spoofing અને Session Hijacking નું વિગતવાર વર્ણન કરો ૦૭
