Seat No. / Enrolment No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

Diploma Engineering – SEMESTER – 6 (NEW) – EXAMINATION – Summer-2025

Subject Code: 4360702 **Date: 12-05-2025**

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

			Marks
Q.1	**(a)**	Explain Confidentiality, Integrity and Availability with neat diagram.	**03**
પ્રશ્ન.1	**(અ)**	Confidentiality, Integrity અને Availability ને આકૃતિ સાથે સમજાવો.	૦૩
	(b)	Differentiate Active Attack and Passive Attack.	**04**
	(બ)	Active Attack અને Passive Attack નો તફાવત લખો.	૦૪
	(c)	Explain PING command. Describe Caesar Cipher and One Time Pad Cipher encryption technique with example.	**07**
	(ક)	PING કમાન્ડ સમજાવો. ઉદાહરણ સાથે સીઝર સાઇફર અને One Time Pad સાઇફર એન્ક્રિપ્શન ટેકનિક સમજાવો.	૦૭
		OR	
	(c)	Explain IPCONFIG command. Explain Play Fair Cipher encryption technique with example.	**07**
	(ક)	IPCONFIG કમાન્ડ સમજાવો. ઉદાહરણ સાથે પ્લે ફેર સાઇફર એન્ક્રિપ્શન ટેકનિક સમજાવો.	૦૭
Q.2	**(a)**	Compare substitution and Transposition Technique.	**03**
પ્રશ્ન.2	**(અ)**	Substitution and Transposition Technique **ની તુલના કરો.**	**૦૩**
	(b)	Describe Symmetric cryptography with advantage and disadvantage.	**04**
	(બ)	Symmetric cryptography લાભ અને ગેરલાભ સાથે સમજાવો.	૦૪
	(c)	Explain Data Encryption Standard with advantage and disadvantage.	**07**
	(ક)	ડેટા એન્ક્રિપ્શન સ્ટાન્ડર્ડ લાભ અને ગેરલાભ સાથે સમજાવો.	૦૭
		OR	
Q.2	**(a)**	Define: Cryptanalysis, Encryption, Decryption.	**03**
પ્રશ્ન.**2**	**(અ)**	વ્યાખ્યાયિત કરો: ક્રિપ્ટએનાલિસિસ, એન્ક્રિપ્શન, ડિક્રિપ્શન.	૦૩
	(b)	What is Steganography? Classify Steganography.	**04**
	(બ)	સ્ટેગનોગ્રાફી શું છે? સ્ટેગનોગ્રાફીનું વર્ગીકરણ કરો.	૦૪
	(c)	Explain Hill Cipher encryption and decryption technique steps with example.	**07**

	(ક)	હિલ સાઇફર એન્ક્રિપ્શન અને ડિક્રિપ્શન ટેકનિક સ્ટેપ્સ ઉદાહરણ સાથે સમજાવો.	૦૭
Q. 3	**(a)**	Explain Public Key Infrastructure.	**03**
પ્રશ્ન.3	(અ)	Public Key Infrastructure સમજાવો.	૦૩
	(b)	Write full form of CA, RA. What are the steps for verifying authenticity and integrity of a certificate?	**04**
	(બ)	CA, RAનું full form લખો. પ્રમાણપત્રની authenticity and integrity ચકાસવા માટેના પગલાં શું છે?	૦૪
	(c)	Explain the RSA algorithm with advantage and disadvantage.	**07**
	(ક)	RSA અલ્ગોરિધમ લાભ અને ગેરલાભ સાથે સમજાવો.	૦૭
		OR	
Q. 3	**(a)**	Describe Public-Key Cryptography and list out its applications.	**03**
પ્રશ્ન.3	(અ)	પબ્લિક-કી ક્રિપ્ટોગ્રાફીનું વર્ણન કરો અને તેની એપ્લિકેશનોની યાદી બનાવો.	૦૩
	(b)	Draw and explain how digital signature works.	**04**
	(બ)	ડિજિટલ સિગ્નેચર કેવી રીતે કાર્ય કરે છે તે દોરો અને સમજાવો.	૦૪
	(c)	Why do we trust a digital certificate? Name the four key steps in the creation of a digital certificate and explain each step.	**07**
	(ક)	શા માટે આપણે ડિજિટલ પ્રમાણપત્ર પર વિશ્વાસ કરીએ છીએ? ડિજિટલ સર્ટિફિકેટ બનાવવાના ચાર મુખ્ય પગલાઓને નામ આપો અને દરેક પગલાને સમજાવો.	૦૭
Q. 4	**(a)**	Explain Packet Filtering Firewall.	**03**
પ્રશ્ન.4	(અ)	પેકેટ ફિલ્ટરિંગ ફાયરવોલ સમજાવો.	૦૩
	(b)	Explain DMZ in detail.	**04**
	(બ)	DMZ ને વિગતવાર સમજાવો.	૦૪
	(c)	What is a Host Intrusion Detection System (HIDS)? Explain it's working with advantage and disadvantage.	**07**
	(ક)	હોસ્ટ ઈન્ટ્રુઝન ડિટેક્શન સિસ્ટમ (HIDS) શું છે? તેના કામ ની સાથે તેના ફાયદા અને ગેરફાયદા સમજાવો.	૦૭
		OR	
Q. 4	**(a)**	Explain Logical components of IDS.	**03**
પ્રશ્ન.4	(અ)	IDS ના Logical components સમજાવો.	૦૩
	(b)	Explain VLAN in detail.	**04**
	(બ)	VLAN ને વિગતવાર સમજાવો.	૦૪
	(c)	What is a Network Intrusion Detection System (NIDS)? Explain it's working with advantage and disadvantage.	**07**
	(ક)	નેટવર્ક ઈન્ટ્રુઝન ડિટેક્શન સિસ્ટમ (NIDS) શું છે? તેના કામ ની સાથે તેના ફાયદા અને ગેરફાયદા સમજાવો.	૦૭
Q.5	**(a)**	Describe Session Hijacking briefly.	**03**
પ્રશ્ન.5	(અ)	સેસન હાઇજેકિંગનું ટૂંકમાં વર્ણન કરો.	૦૩
	(b)	Explain Tunneling with diagram.	**04**
	(બ)	ટનલીંગ ડાયાગ્રામ સાથે સમજાવો.	૦૪
	(c)	Differentiate Virus and Worms. List out traditional problems associated with Computer Crime.	**07**
	(ક)	વાઇરસ અને વોર્મ્સને અલગ પાડો. Computer Crime સાથે સંકળાયેલી પરંપરાગત સમસ્યાઓની યાદી બનાવો.	૦૭
		OR	
Q.5	**(a)**	Explain working of IP Spoofing.	**03**
પ્રશ્ન.5	(અ)	IP સ્પુફિંગની કામગીરી સમજાવો.	૦૩

	(b)	Define: Internet, intranet, Firewall, IDS.	**04**
	(બ)	વ્યાખ્યાયિત કરો: ઇન્ટરનેટ, ઇન્ટ્રાનેટ, ફાયરવોલ, IDS.	૦૪
	(c)	Explain Intruders and Hackers with its types.	**07**
	(ક)	ઈનટ્રૂડર અને હેકર્સને તેના પ્રકારો સાથે સમજાવો.	૦૭

Seat No.: Enrolment No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 4360702 **Date: 16-05-2024**

Subject Name: Basics of 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. **Use of programmable & Communication aids are strictly prohibited.**
5. **Use of non-programmable scientific calculator is permitted.**
6. **English version is authentic.**

Q.1	**(a)**	Describe confidentiality, integrity and availability.	**03**
પ્રશ્ન.1	(અ)	Confidentiality, integrity અને availability સમજાવો.	૦૩
	(b)	Describe security services and security mechanism.	**04**
	(બ)	સિક્યુરિટી સર્વિસીસ અને સિક્યુરિટી મિકેનીઝમ સમજાવો.	૦૪
	(c)	Write short note on structure of Data Encryption Standard (DES) with advantages and disadvantages.	**07**
	(ક)	ફાયદા અને ગેરફાયદા સાથે ડેટા એન્ક્રિપ્શન સ્ટાન્ડર્ડ (DES) ના બંધારણ પર ટૂંકી નોંધ લખો.	૦૭
		OR	
	(c)	Construct a PlayFair Matrix with the key “TRUST” and encrypt the message “BE CONFIDENT IN YOURSELF”.	**07**
	(ક)	“TRUST” કી વડે પ્લેફેર મેટ્રિક્સ બનાવો અને “BE CONFIDENT IN	૦૭
Q.2	**(a)**	List substitution and transposition techniques.	**03**
પ્રશ્ન.2	**(અ)**	Substitution અને transposition techniques ની યાદી લખો.	**૦૩**
	(b)	Describe plain text, cipher text, encryption and decryption in cryptography.	**04**
	(બ)	ક્રીપટોગ્રાફીમા plain text, cipher text, encryption અને decryption સમજાવો.	૦૪
	(c)	Write a short note on Hill Cipher with example.	**07**
	(ક)	ઉદાહરણ સાથે હિલ સાઇફર પર ટૂંકી નોંધ લખો.	૦૭
		OR	
Q.2	**(a)**	List types of Steganography.	**03**
પ્રશ્ન.**2**	(અ)	Steganography ની યાદી લખો.	૦૩
	(b)	Describe symmetric cryptography with example.	**04**
	(બ)	Symmetric cryptography ઉદાહરણ આપી સમજાવો.	૦૪
	(c)	Encrypt the plain text “THIS IS A SECRET MESSAGE” using a Rail Fence with 3 rails.	**07**
	(ક)	3 રેઇલ્સ સાથે રેઈલ ફેન્સ નો ઉપયોગ કરીને સાદા ટેક્સ્ટ " THIS IS A SECRET MESSAGE " ને એનક્રિપ્ટ કરો.	૦૭

Q. 3	**(a)**	List applications of public key cryptosystems.	**03**
પ્રશ્ન.3	(અ)	public key cryptosystems applications ની યાદી લખો.	૦૩
	(b)	Describe basics of digital signatures and digital certificates	**04**
	(બ)	digital signatures અને digital certificates ને મૂળભૂત રીતે સમજાવો.	૦૪
	(c)	Write short note on RSA Algorithm with example.	**07**
	(ક)	RSA આલ્ગોરીધામ પર ઉદાહરણ સાથે શોર્ટ નોટ લખો.	૦૭
		OR	
Q. 3	**(a)**	List principles of public key cryptosystems.	**03**
પ્રશ્ન.3	(અ)	public key cryptosystems નાં principles ની યાદી લખો.	૦૩
	(b)	Describe certificate authorities and registration authorities.	**04**
	(બ)	certificate authorities અને registration authorities સમજાવો.	૦૪
	(c)	Perform encryption using RSA Algorithm for following Parameters : p=3, q=11 (p and q are prime numbers), e=7 and M = 2 (e-public and M-message) and also find private and public key pair.	**07**
	(ક)	નીચેના પરિમાણો માટે RSA અલ્ગોરિધમનો ઉપયોગ કરીને એન્ક્રિપ્શન કરો: p=3, q=11 (p અને q એ અવિભાજ્ય સંખ્યાઓ છે), e=7 અને M = 2 (e-પબ્લિક અને M-સંદેશ) અને પ્રાઇવેટ અને પબ્લિક કી ની જોડી પણ શોધો.	૦૭
Q. 4	**(a)**	Discuss steps for obtaining a digital certificate.	**03**
પ્રશ્ન.4	(અ)	ડીઝીટલ સર્ટીફીકેટ મેળવવાની સ્ટેપ્સ સમજાવો.	૦૩
	(b)	Describe Demilitarized Zone (DMZ) and its applications.	**04**
	(બ)	Demilitarized Zone (DMZ) અને તેની એપ્લીકેશન્સ સમજાવો.	૦૪
	(c)	Describe working and components of IDS.	**07**
	(ક)	IDS નું વર્કિંગ અને કમ્પોનન્ટસ વર્ણવો.	૦૭
		OR	
Q. 4	**(a)**	Discuss steps for verifying authenticity and integrity of a certificate.	**03**
પ્રશ્ન.4	(અ)	સર્ટીફીકેટની authenticity અને integrity વેરીફાય કરવા માટેના મુદાઓ લખો.	૦૩
	(b)	Describe need and working of firewall.	**04**
	(બ)	ફાયરવોલણી જરૂરિયાત અને કામગીરી સમજાવો.	૦૪
	(c)	Describe different types of firewall.	**07**
	(ક)	જુદા જુદા પ્રકારની ફાયરવોલ સમજાવો.	૦૭
Q.5	**(a)**	List types of cyber attacks.	**03**
પ્રશ્ન.5	(અ)	જુદા જુદા પ્રકારના સાયબર એટેક્સની યાદી લખો.	૦૩
	(b)	Describe Virtual LAN (VLAN) security topology.	**04**
	(બ)	Virtual LAN (VLAN) security topology સમજાવો.	૦૪
	(c)	Discuss different types of threats.	**07**
	(ક)	જુદા જુદા પ્રકારના થ્રેટસની ચર્ચા કરો.	૦૭
		OR	
Q.5	**(a)**	List types of cybercrime.	**03**
પ્રશ્ન.5	(અ)	જુદા જુદા પ્રકારના સાયબર ક્રાઇમની યાદી લખો.	૦૩
	(b)	Discuss advantages and disadvantages of Host based IDS (HIDS).	**04**
	(બ)	Host based IDS (HIDS) નાં ફાયદા અને ગેરફાયદા લખો.	૦૪
	(c)	Discuss traditional problems associated with computer crime.	**07**
	(ક)	કોમ્પ્યુટર ક્રાઇમ સાથે ના traditional problems ની ચર્ચા કરો.	૦૭