

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) ની 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)	ક્રીપ્ટોગ્રાફીમાં 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)	૩ રેઇલ્સ સાથે રેઇલ 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 આલ્ગોરીધમ પર ઉદાહરણ સાથે શોર્ટ નોટ લખો.	૦૭
OR			
Q. 3	(a)	List principles of public key cryptosystems.	03
પ્રશ્ન.3	(અ)	public key cryptosystems ની 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 પ્રાઈવેટ અને પબ્લિક કી ની જોડી પણ શોધો.	૦૭
Q. 4	(a)	Discuss steps for obtaining a digital certificate.	03
પ્રશ્ન.4	(અ)	ડિજીટલ સર્ટીફિકેટ મેળવવાની સ્ટેપ્સ સમજાવો.	૦૩
	(b)	Describe Demilitarized Zone (DMZ) and its applications.	04
	(બ)	Demilitarized Zone (DMZ) અને તેની એપ્લિકેશન્સ સમજાવો.	૦૪
	(c)	Describe working and components of IDS.	07
	(ક)	IDS નું વર્કિંગ અને કમ્પોનન્ટ્સ વર્ણવો.	૦૭
OR			
Q. 4	(a)	Discuss steps for verifying authenticity and integrity of a certificate.	03
પ્રશ્ન.4	(અ)	સર્ટીફિકેટની authenticity અને integrity વેરીફાઇ કરવા માટેના મુદ્દાઓ લખો.	૦૩
	(b)	Describe need and working of firewall.	04
	(બ)	ફાયરવોલની 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 થ્રેટ્સની ચર્ચા કરો.	૦૭
OR			
Q.5	(a)	List types of cybercrime.	03
પ્રશ્ન.5	(અ)	જુદા જુદા પ્રકારના સાયબર ક્રાઈમની 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 ક્રાઈમ સાથે નાં traditional problems ની ચર્ચા કરો.	૦૭