

GUJARAT TECHNOLOGICAL UNIVERSITY

Diploma Engineering – SEMESTER – 5 (OLD) – EXAMINATION – Winter-2023

Subject Code: 3350704

Date: 08-12-2023

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

Q.1 Answer any seven out of ten. દશમાંથી કોઇપણ સાતના જવાબ આપો. **14**

- પ્રશ્ન ૧**
1. Define: Data security, Network security.
 ૧. Data security અને Network security ની વ્યાખ્યા આપો.
 2. Write the full form of: MALWARE, SHA, PKI, HIDS
 ૨. પૂર્ણ નામ લખો: MALWARE, SHA, PKI, HIDS
 3. Write the full form of: INTERNET, FTP, NIDS, IPSec
 ૩. પૂર્ણ નામ લખો: INTERNET, FTP, NIDS, IPSec
 4. Define symmetric key encryption and give its examples.
 ૪. symmetric key encryption ની વ્યાખ્યા આપી તેના ઉદાહરણ આપો.
 5. Define: hashing.
 ૫. વ્યાખ્યા આપો: hashing.
 6. Write the full form of: OTP, SET, SSL, NIDS
 ૬. પૂર્ણ નામ લખો: OTP, SET, SSL, NIDS
 7. Draw the neat figure of 'conventional encryption system'.
 ૭. 'conventional encryption system' ની સ્વચ્છ આકૃતિ દોરો.
 8. Define physical security.
 ૮. physical security ની વ્યાખ્યા આપો.
 9. Write the full form of: MITM, IDS, KDC, CA
 ૯. પૂર્ણ નામ લખો: MITM, IDS, KDC, CA
 10. During the lifetime of a virus, it goes from which four phases?
 ૧૦. વાઇરસ તેના સમયકાળ દરમિયાન કયા ચાર તબક્કા માંથી પસાર થાય છે?

Q.2 (a) Write a short note on TLS. **03**

પ્રશ્ન. ૨ (અ) TLS પર ટૂંકનોંધ લખો. **૦૩**

OR

(a) Write a short note on sniffing attack. **03**

(અ) sniffing attack પર ટૂંકનોંધ લખો. **૦૩**

(b) Explain data confidentiality, data integrity and data availability **03**

(બ) data confidentiality, data integrity અને data availability સમજાવો. **૦૩**

(b) Define cryptography and explain asymmetric key cryptography. **03**

(બ) Cryptography ની વ્યાખ્યા લખો અને asymmetric key cryptography ટૂંકમાં સમજાવો. **૦૩**

(c) Write a short note on steganography. **04**

	(ક) steganography પર ટૂંકનોંધ લખો.	૦૪
	OR	
	(c) Explain TCP/IP hijacking.	04
	(ક) TCP/IP hijacking સમજાવો.	
	(d) Explain DOS attack with diagram.	04
	(S) આકૃતિ દોરી DOS attack સમજાવો.	૦૪
	OR	
	(d) Explain SSL.	04
	(S) SSL સમજાવો.	૦૪
Q.3	(a) Write a short note on cryptanalysis.	03
પ્રશ્ન. ૩	(અ) Cryptanalysis પર ટૂંકનોંધ લખો.	૦૩
	OR	
	(a) Explain spoofing in brief.	03
	(અ) Spoofing ને ટૂંકમાં સમજાવો.	૦૩
	(b) Write a short note on finger print bio metric.	03
	(બ) finger print bio metric પર ટૂંકનોંધ લખો.	૦૩
	OR	
	(b) Write a short note on NIDS.	03
	(બ) NIDS પર ટૂંકનોંધ લખો.	૦૩
	(c) Write a short note on IPSec.	04
	(ક) IPSec પર ટૂંકનોંધ લખો.	૦૪
	OR	
	(c) Write a short note on email security.	04
	(ક) email security પર ટૂંકનોંધ લખો.	૦૪
	(d) List different trust models. Explain any one in brief.	04
	(S) trust models ની પ્રકાર લખો અને કોઈ પણ એક ટૂંકમાં સમજાવો.	૦૪
	OR	
	(d) Write a short note on OTP.	04
	(S) OTP પર ટૂંકનોંધ લખો.	૦૪
Q.4	(a) Write a short note on centralized and decentralized infrastructure.	03
પ્રશ્ન. ૪	(અ) centralized and decentralized infrastructure પર ટૂંકનોંધ લખો.	૦૩
	OR	
	(a) Define firewall. Explain its limitations.	03
	(અ) Firewall ની વ્યાખ્યા આપો. તેની મર્યાદાઓ લખો.	૦૩
	(b) Write a short note on password selection strategies.	04
	(બ) password selection strategies પર ટૂંકનોંધ લખો.	૦૪
	OR	
	(b) List and explain web security threats.	04
	(બ) web security threats ની પ્રકારો જણાવો અને વર્ણવો.	૦૪
	(c) Explain SHA-1 with neat figure.	07
	(ક) સ્વચ્છ આકૃતિ દોરી SHA-1 સમજાવો.	૦૭
Q.5	(a) Write a short note on VLAN.	04
પ્રશ્ન. ૫	(અ) VLAN પર ટૂંકનોંધ લખો.	૦૪
	(b) Write the definition of cipher text and write key matrix for the plaintext “BHAGYA” using playfair method.	04
	(બ) cipher text ની વ્યાખ્યા લખો અને આપેલ plaintext “BHAGYA” માટે playfair મેથડનો ઉપયોગ કરી key matrix તૈયાર કરો.	૦૪
	(c) Explain retinal scan biometric.	03
	(ક) retinal scan biometric સમજાવો.	૦૩

(d) Convert a plaintext 'CAT' into ciphertext using Hill cipher method. **03**

Key is: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

(S) 'CAT' plaintext to ciphertext by Hill cipher method. **03**

Key is: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$
