Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER –V EXAMINATION – SUMMER 2015

Subject Code: 3350704 **Date:12 -05 - 2015**

Subject Name: COMPUTER AND NETWORK SECURITY

Time: 2:30 pm to 5:00 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 only simple calculator is permitted in Mathematics.**
6. **English version is authentic.**

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

1. Define Encryption. List out Symmetric Encryption Algorithm.

૧. વ્યાખ્યા આપો: Encryption. Symmetric Encryption અલગોરિધમ ની યાદી બનાવો.

2. Define: Backdoor.

૨. વ્યાખ્યા આપો: Backdoor.

3. Define: Sniffing.

૩. વ્યાખ્યા આપો: Sniffing.

4. List out component of good password.

૪. સારા પાસવર્ડ ના component ની યાદી બનાવો.

5. Define: Internet, Intranet.

૫. વ્યાખ્યા આપો: Internet , Intranet.

6. List out Type of Firewall.

૬. Firewall ના પ્રકારની યાદી બનાવો.

7. Write down application of hash function.

૭. Hash function ની એપ્લીકેશન લખો.

8. Which Algorithm is use for encrypt two character at time.

૮. એક સાથે બે character encrypt કરવા કયો Algorithm વપરાય છે.

9. Which key is use for encryption and decryption in Symmetric encryption Technique?

૯. Symmetric encryption Technique માં કઈ કી encryption અને decryption માટે વપરાય છે.

10. In Digital Signature which key is use for creation and verification process?

૧૦. Digital Signature માં કઈ કી creation and verification process માટે વપરાય છે.

Q.2 (a) Explain Shoulder surfing. **03**

પ્રશ્ન. ૨ (અ) Shoulder surfing સમજાવો. **03**

OR

(a) Explain password protection. **03**

(અ) Password protection સમજાવો. **03**

	(b)	Explain rail fence technique.	**03**
	(બ)	Rail fence technique સમજાવો.	૦૩
		OR	
	(b)	Explain verman cipher(one time pad).	**03**
	(બ)	verman cipher(one time pad) સમજાવો.	૦૩
	(c)	Explain passive attack in brief.	**04**
	(ક)	Passive attack ટુંકમાં સમજાવો.	૦૪
		OR	
	(c)	Explain security basic.	**04**
	(ક)	Security basic સમજાવો.	૦૪
	(d)	Explain SQL Injection in detail.	**04**
	(ડ)	SQL Injection વિસ્તારપુર્વક સમજાવો.	૦૪
		OR	
	(d)	List out steps for obtaining Digital Signature.	**04**
	(ડ)	Digital Signature મેળવવા ના steps ની યાદી બનાવો.	૦૪
Q.3	(a)	Define: hash function. Draw block diagram of hash function.	**03**
પ્રશ્ન. 3	(અ)	hash function ની વ્યાખ્યા આપી તેની આકુતી દોરો.	૦૩
		OR	
	(a)	Explain Steganography technique.	**03**
	(અ)	Steganography technique સમજાવો.	૦૩
	(b)	Draw and Explain Symmentric Encryption model.	**03**
	(બ)	Symmentric Encryption model આકુતી દોરી સમજાવો.	૦૩
		OR	
	(b)	List out type of firewall and explain any one.	**03**
	(બ)	Firewall ના પ્રકારની યાદી બનાવી કોઈ એક સમજાવો.	૦૩
	(c)	Explain Kerberos Authentication algorithm.	**04**
	(ક)	Kerberos Authentication અલગોરિધમ સમજાવો.	૦૪
		OR	
	(c)	Explain DMZ .	**04**
	(ક)	DMZ સમજાવો.	૦૪
	(d)	Explain private key protection.	**04**
	(ડ)	Private key protection સમજાવો.	૦૪
		OR	
	(d)	Explain tunneling in detail.	**04**
	(ડ)	Tunneling વિસ્તારપુર્વક સમજાવો.	૦૪
Q.4	(a)	Explain host based IDS.	**03**
પ્રશ્ન. ૪	(અ)	Host based IDS સમજાવો.	૦૩
		OR	
	(a)	Explain network based IDS.	**03**
	(અ)	Network based IDS સમજાવો.	૦૩
	(b)	Explain SSL in detail.	**04**
	(બ)	SSL વિસ્તારપુર્વક સમજાવો.	૦૪
		OR	

	(b)	Explain VLAN in detail.	**04**
	(બ)	VLAN વિસ્તારપુર્વક સમજાવો.	૦૪
	(c)	For given Plaintext=SUMMER, Key= $\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$ Find cipher text using hill cipher.	**07**
	(ક)	આપેલ Plaintext=SUMMER, Key= $\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$ માટે hill cipherનો ઉપયોગ કરી cipher text શોધો.	૦૭
Q.5	(a)	Explain Caesar cipher Algorithm with example.	**04**
પ્રશ્ન. ૫	(અ)	Caesar cipher અલગોરિધમ ઉદાહરણ આપી સમજાવો.	૦૪
	(b)	Explain Logical Component of IDS with Diagram.	**04**
	(બ)	IDS ના લોજીકલ Component આકૃતી દોરી સમજાવો.	૦૪
	(c)	Explain Secure Electronic Transaction(SET) Protocol .	**03**
	(ક)	Secure Electronic Transaction(SET) Protocol સમજાવો.	૦૩
	(d)	If Key = “computer”. Write playfair cipher key matrix.	**03**
	(ડ)	Key = “computer” માટે playfair cipher key matrix લખો.	૦૩

****