Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER – V • EXAMINATION – WINTER- 2016

Subject Code:3351602 **Date: 18- 11- 2016**

Subject Name: Essentials Of 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 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. What is Cryptography ?
૧. ક્રીપ્ટોગ્રાફી શું છે ?
2. What is non repudiation ?
૨. નૉન રેપ્યુડીએશન શું છે ?
3. Define the terms Encryption and Decryption.
૩. એનક્રીપ્શન અને ડીક્રીપ્શન ની વ્યાખ્યા આપો.
4. What is CLAMAV ?
૪. CLAMAV શું છે ?
5. Define the terms CONFUSION and DIFFUSION
૫. CONFUSION અને DIFFUSION ની વ્યાખ્યા આપો.
6. State the importance of information security.
૬. ઇંન્ફોરમેશન સીક્યોરીટી ની અગત્યતા જણાવો
7. What is brute force attack ?
૭. બ્રુટ ફોર્સ એટૈક શું છે ?
8. List the different substitution techniques.
૮. જુદા જુદા સબસ્ટીટ્યુશન ટેકનીક જણાવો
9. What is a Digital Signature ?
૯. ડીજીટલ સીગનેચર શું છે ?
10. Differentiate between THREAT and ATTACK.
૧૦. THREAT અને ATTACK વચ્ચે તફાવત જણાવો.

Q.2 (a) Explain the ACTIVE attack. **03**

પ્રશ્ન. ૨ (અ) એકટીવ એટેક સમજાવો. **૦૩**

OR

(a) Explain the PASSIVE attack. **03**

(અ) પેસીવ એટેક સમજાવો. **૦૩**

(b) Explain the Euclidean Algorithm. **03**

(બ) Euclidean Algorithm સમજાવો. **૦૩**

OR

	(b)	Explain the Ring and Groups.	**03**
	(બ)	રીંગ અને ગ્રુપ સમજાવો.	૦૩
	(c)	Explain the difference between BLOCK CIPHER and STREAM CIPHER.	**04**
	(ક)	BLOCK CIPHER અને STREAM CIPHER વચ્ચે તફાવત સમજાવો.	૦૪
		OR	
	(c)	Explain Hill Cipher with an example.	**04**
	(ક)	Hill Cipher ઉદાહરણ સાથે સમજાવો.	૦૪
	(d)	In DES Encryption explain its key generation.	**04**
	(ડ)	DES એનક્રીપ્શન મા કી જનરેશ સમજાવો.	૦૪
		OR	
	(d)	Explain the 'known plaintext' and 'chosen cipher text' crypt attack .	**04**
	(ડ)	'known plaintext' અને 'chosen cipher text' ક્રીપ્ટ એટેક સમજાવો.	૦૪
Q.3	(a)	Explain asymmetric key encryption .	**03**
પ્રશ્ન. 3	(અ)	asymmetric key એનક્રીપ્શન સમજાવો.	૦૩
		OR	
	(a)	Justify how important it is to update the Operating System.	**03**
	(અ)	Operating System ને અપડેટ કરવું શા માટે જરુરી છે ?	૦૩
	(b)	Explain Steganography.	**03**
	(બ)	સ્ટીગેનોગ્રાફી સમજાવો.	૦૩
		OR	
	(b)	State the limitations of symmetric key encryption.	**03**
	(બ)	સીમેટ્રીક કી એનક્રીપ્શન ની મરીયાદા જણાવો.	૦૩
	(c)	Explain the model of nework security.	**04**
	(ક)	નેટવર્ક સીક્યોરીટી મોડેલ સમજાવો.	૦૪
		OR	
	(c)	Explain the OSI security architecture.	**04**
	(ક)	OSI સિક્યોરીટી આર્કીટેક્ચર સમજાવો.	૦૪
	(d)	Explain the Cipher Block Chaining (CBC).	**04**
	(ડ)	Cipher Block Chaining (CBC) સમજાવો.	૦૪
		OR	
	(d)	Explain the Electronic Code Book (ECB).	**04**
	(ડ)	Electronic Code Book (ECB) સમજાવો.	૦૪
Q.4	(a)	Write a short note on Fiestel structure.	**03**
પ્રશ્ન. ૪	(અ)	ફીસ્ટલ સ્ટ્રક્ચર પર ટુંકી નોંધ લખો.	૦૩
		OR	
	(a)	Explain the role of FIREWALL in a computer system.	**03**
	(અ)	કોમ્પ્યુટર સીસ્ટમ મા FIREWALL નુ કાર્ય સમજાવો.	૦૩
	(b)	Explain the Columnar Transposition Technique.	**04**
	(બ)	કોલમનર ટ્રાનસ્પોસઝીશન સમજાવો.	૦૪
		OR	
	(b)	Using the Caesar Cipher encrypt the message 'MY BOOKSHELF IS FULL OF BOOKS.'	**04**
	(બ)	Caesar Cipher વાપરી મેસેજ 'MY BOOKSHELF IS FULL OF BOOKS' ને	૦૪

		એનક્રીપ્ટ કરો.	
	(c)	Explain the Diffie-Hellman Key Exchange algorithm.	**07**
	(ક)	Diffie-Hellman Key Exchange એલ્ગોરિથમ સમજાવો.	૦૭
Q.5	(a)	Explain CONFIDENTIALITY with reference to public key cryptography.	**04**
પ્રશ્ન. ૫	(અ)	પુબ્લિક કી ક્રીપ્ટોગ્રાફી ના રેફરન્સ મા CONFIDENTIALITY સમજાવો.	૦૪
	(b)	Write a brief note on cleanup tools and anti-malware.	**04**
	(બ)	cleanup tools અને anti-malware પર ટુંકી નોંધ લખો.	૦૪
	(c)	Explain the Man in Middle Attack.	**03**
	(ક)	Man in Middle Attack સમજાવો.	૦૩
	(d)	Explain the Railfence technique with an example.	**03**
	(ડ)	ઉદાહરણ સાથે રેલ ફેન્સ ટેકનીક સમજાવો.	૦૩

****