Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER – V-EXAMINATION – WINTER 2015

Subject Code: 3351602 **Date: 19/12/2015**

Subject Name: Essentials of Network Security

Time: 10:30 AM TO 1:00 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. Describe Security Mechanism.

૧. સેક્યુરીટી મેકેનીસમ સમજાવો.

2. Define Information Security.

૨. ઇન્ફોર્મેશન સેક્યુરીટી ની વ્યાખ્યા આપો.

3. What is Cryptography? Briefly Explain.

૩. Cryptography શું છે? ટુકમાં સમજાવો.

4. What are the two General Approaches to Attacking a Cipher? Briefly Explain.

૪. સિફર પર અટેક કરવા માટે ના બે જનરલ અપ્રોચ કયા છે? ટુકમાં સમજાવો.

5. Define Groups and Rings.

૫. Groups અને Rings ની વ્યાખ્યા આપો.

6. Describe Limitation of Symmetric Key Encryption.

૬. Symmetric Key Encryption ની લીમીટેશન સમજાવો.

7. List Any Three Anti Malware and Cleanup Tools.

૭. કોઈ પણ ત્રણ Anti Malware અને Cleanup Tools ના નામ આપો.

8. Define Data Confidentiality and Data Integrity.

૮. Data Confidentiality અને Data Integrity ની વ્યાખ્યા આપો.

9. Define Access Control of Security Services.

૯. સેક્યુરીટી સર્વિસીસ ના Access Control ની વ્યાખ્યા આપો.

10. Describe Nonrepudiation.

૧૦. Nonrepudiation સમજાવો.

Q.2 (a) Differentiate Between Block Cipher and Stream Cipher. **03**

પ્રશ્ન. ૨ (અ) Block Cipher અને Stream Cipher વચ્ચે નો તફાવત સમજાવો. **૦૩**

Or

	(a)	Differentiate Between Symmetric Encryption and Asymmetric Encryption.	**03**
	(અ)	Symmetric Encryption અને Asymmetric Encryption વચ્ચે નો તફાવત સમજાવો.	૦૩
	(b)	Discuss Caeser Cipher With Example.	**03**
	(બ)	Caeser Cipher વિષે ઉદાહરણ આપી લખો.	૦૩
		Or	
	(b)	Explain Playfair Cipher.	**03**
	(બ)	Playfair Cipher સમજાવો.	૦૩
	(c)	Discuss Fiestel Structure.	**04**
	(ક)	Fiestel Structure વિષે લખો.	૦૪
		Or	
	(c)	Explain First Round Of DES.	**04**
	(ક)	DES નું ફસ્ટ રાઉન્ડ સમજાવો.	૦૪
	(d)	Write the steps the way Firewall Protect our system when Malware Attack Occurs in Windows7?	**04**
	(ડ)	Windows7 માં Malware Attack અટેક થાય ત્યારે Firewall કઈ રીતે સિસ્ટમ ને પ્રોટેક્ટ કરે તેના સ્ટેપ લખો.	૦૪
		Or	
	(d)	Discuss Four Features of Calmav.	**04**
	(ડ)	Calmav ના ચાર ફીચર્સ લખો.	૦૪
Q.3	(a)	Generate a Cipher text from below Plaintext using Caesar Cipher with Key :- 3 "Meetmeafterthetogaparty"	**03**
પ્રશ્ન. 3	(અ)	નીચેની Plaintext નો ઉપયોગ કરી Caesar Cipher ની મદદ થી સીફેર બનાવો. કી : 3 "Meetmeafterthetogaparty"	૦૩
		Or	
	(a)	Using The Vigenere Cipher, Encrypt The Word "Explanation" Using The Key Leg.	**03**
	(અ)	Vigenere Cipher ની મદદથી "Explanation" વાક્યને એનક્રિપ્ટ કરો કી : Leg	૦૩
	(b)	"56 Bit Key is not Secure for DES " Justify It.	**03**
	(બ)	"56 Bit Key is not Secure for DES " સાબિત કરો.	૦૩
		Or	
	(b)	Illustrate Any One Cryptanalysis Of DES	**03**
	(બ)	DES ની કોઇપણ એક Cryptanalysis વર્ણવો.	૦૩
	(c)	Explain Key Generation Of DES Encryption In Brief.	**04**
	(ક)	DES Encryption નું કી જનરેશન સમજાવો	૦૪
		Or	

	(c)	Explain Cipher Block Chaining Mode Of Operation Of DES.	**04**
	(ક)	DES નું Cipher Block Chaining મોડ ઓફ ઓપેરેશન સમજાવો.	૦૪
	(d)	Differentiate Between Active And Passive Security Attacks.	**04**
	(ડ)	Active અને Passive Security Attacks વચ્ચે તફાવત સમજાવો.	૦૪
		Or	
	(d)	Explain Security Services.	**04**
	(ડ)	સેક્યુરીટી સર્વિસીસ સમજાવો.	૦૪
Q.4	(a)	Draw Model For Network Security.	**03**
પ્રશ્ન. ૪	(અ)	નેટવર્ક સેક્યુરીટી નો મોડલ દોરો.	૦૩
		Or	
	(a)	Define The Term : Threat And Attack	**03**
	(અ)	નીચેની વ્યાખ્યા આપો : Threat અને Attack	૦૩
	(b)	Explain Authentication in Asymmetric Key Encryption Using Block Diagram.	**04**
	(બ)	બ્લોક ડાયાગ્રામ ની મદદથી Asymmetric Key Encryption નું Authentication સમજાવો.	૦૪
		Or	
	(b)	Explain Confidentiality in Asymmetric Key Encryption Using Block Diagram.	**04**
	(બ)	બ્લોક ડાયાગ્રામ ની મદદથી Asymmetric Key Encryption નું Confidentiality સમજાવો.	૦૪
	(c)	Generate a Cipher Text From Below Plaintext Using Columnar Cipher With Key :- 4312567 "ATTACKPOSTPONEDUNTILTWOAMXYZ".	**07**
	(ક)	નીચેની Plaintext નો ઉપયોગ કરી Columnar Cipher ની મદદ થી સીફેર બનાવો. કી : 3 "Meetmeafterthetogaparty"	૦૭
Q.5	(a)	Determine Gcd(1970,1066) Using Euclidean Algorithm.	**04**
પ્રશ્ન. ૫	(અ)	Euclidean અલ્ગોરીધમ ની મદદથી Gcd(1970,1066) શોધો.	૦૪
	(b)	Write Steps to Disable or Delete Unnecessary Accounts in System.	**04**
	(બ)	Windows સિસ્ટમની અંદર Unnecessary Accounts Disable અથવા Delete કરવા માટેના સ્ટેપ લખો.	૦૪
	(c)	Define the term Confusion and Diffusion.	**03**
	(ક)	Confusion અને Diffusion વિષે સમજાવો	૦૩
	(d)	Describe Any one Operating System Security Assessment Tools.	**03**
	(ડ)	કોઇપણ એક Operating System ના Security Assessment Tools સમજાવો.	૦૩