Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER – • EXAMINATION – WINTER-2014

Subject Code: 3351602 **Date: 01/05/2014**

Subject Name: ESSENTIALS OF 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. **14**

1. Define Computer Security and Internet Security.
2. Describe OSI Security Architecture.
3. List any four types of attacks on encrypted messages.
4. Explain the avalanche effect.
5. Define Euclidean algorithm.
6. Write limitations of Symmetric Key Encryption.
7. List any four Features of ClamAV.
8. Define the term Access Control and Data Integrity.
9. List any four Security Mechanisms.
10. Explain Steganography.

Q.2 (a) Distinguish between passive and active security attacks. **04**

OR

(a) Draw Model for Network Security. **04**

(b) Describe Nonrepudiation. **02**

OR

(b) Explain Data Confidentiality. **02**

(c) Explain Polyalphabetic Cipher with example. **06**

OR

(c) Explain Playfair Cipher with example. **06**

(d) Briefly define Cryptography. **02**

OR

(d) Briefly define Cryptanalysis. **02**

Q.3 (a) Generate a cipher text from below plaintext using columnar cipher with key :- 4312567 **06**
"ATTACKPOSTPONEDUNTILTWOAMXYZ"

OR

(a) Generate a cipher text from below plaintext using Caesar cipher with key :- 3 **06**
"meetmeafterthetogaparty"

(b) Explain Key Generation of DES Encryption in brief. **04**

OR

(b) Explain Cipher Block Chaining Mode of operation of DES. **04**

(c) Differentiate between conventional encryption and public-key encryption **04**

OR

(c) Explain Secrecy provided by public key cryptosystem. **04**

Q.4	(a)	Briefly explain Groups.	**02**
		OR	
	(a)	Briefly explain Rings.	**02**
	(b)	Describe three broad categories of application of Asymmetric Key encryption.	**04**
		OR	
	(b)	Explain Authentication in Asymmetric Key Encryption using block diagram.	**04**
	(c)	Illustrate differential and liner Cryptanalysis of DES.	**08**
Q.5	(a)	Determine gcd(1970,1066) using Euclidean Algorithm	**04**
	(b)	Write steps to Disable or Delete unnecessary accounts in windows system.	**04**
	(c)	Explain operating system security assessment tools.	**04**
	(d)	Define the term confusion and diffusion.	**02**

****

ગુજરાતી

પ્રશ્ન. ૧		દશમાંથી કોઇપણ સાતના જવાબ આપો.	૧૪
	૧.	Computer Security અને Internet Security સમજાવો.	
	૨.	OSI Security Architecture સમજાવો.	
	૩.	કોઈપણ ચાર attacks on encrypted messages જણાવો.	
	૪.	Avalanche effect સમજાવો.	
	૫.	Euclidean algorithm સમજાવો.	
	૬.	Symmetric Key Encryption ની limitations લખો.	
	૭.	ClamAV ના કોઇપણ ચાર Features જણાવો.	
	૮.	Access Control અને Data Integrity સમજાવો.	
	૯.	કોઈપણ ચાર Security Mechanisms લખો.	
	૧૦	Steganography સમજાવો.	
પ્રશ્ન. ૨	અ	Passive and active security attacks વચ્ચેનો તફાવત સમજાવો.	૦૪
		અથવા	
	અ	Network Security નો મોડલ આકૃતિ દોરી સમજાવો.	૦૪
	બ	Nonrepudiation સમજાવો.	૦૨
		અથવા	
	બ	Data Confidentiality સમજાવો.	૦૨
	ક	Polyalphabetic Cipher ઉદાહરણ સાથે સમજાવો.	૦૬
		અથવા	
	ક	Playfair Cipher ઉદાહરણ સાથે સમજાવો.	૦૬
	ડ	Cryptography ટુકમાં સમજાવો.	૦૨
		અથવા	
	ડ	Cryptanalysis ટુકમાં સમજાવો.	૦૨
પ્રશ્ન. ૩	અ	નીચે જણાવેલ Plaintext અને key નો ઉપયોગ કરી columnar cipher ની મદદથી cipher text બનાવો. key :- 4312567 “ATTACKPOSTPONEDUNTILTWOAMXYZ”	૦૬
		અથવા	
	અ	નીચે જણાવેલ Plaintext અને key નો ઉપયોગ કરી Caesar cipher ની મદદથી cipher text બનાવો. key :- 3 “meetmeafterthetogaparty”	૦૬
	બ	DES Encryption નું Key Generation સમજાવો.	૦૪
		અથવા	
	બ	DES Cipher નું Block Chaining Mode of operation સમજાવો.	૦૪
	ક	Conventional encryption અને Public-key encryption વચ્ચે તફાવત સમજાવો.	૦૪

અથવા

	ક	Public key cryptosystem વડે Secrecy આપવામાં આવે છે, તે સમજાવો.	૦૪
પ્રશ્ન. ૪	અ	Groups ટુકમાં સમજાવો.	૦૨

અથવા

	અ	Rings ટુકમાં સમજાવો	૦૨
	બ	Asymmetric Key encryption ની ત્રણ broad categories of application સમજાવો.	૦૪

અથવા

	બ	Block diagram ની મદદ થી Asymmetric Key encryption વડે Authentication આપવામાં આવે છે, તે સમજાવો.	૦૪
	ક	DES ના Differential અને Liner Cryptanalysis વર્ણવો.	૦૮
પ્રશ્ન. ૫	અ	Euclidean Algorithm ની મદદ થી gcd(1970,1066) શોધો.	૦૪
	બ	Windows system માં Disable or Delete unnecessary accounts માટેના સ્ટેપ લાખો.	૦૪
	ક	Operating system ના security assessment tools સમજાવો.	૦૪
	ડ	Confusion અને diffusion વિષે સમજાવો.	૦૨

****