

Seat No.: _____

Enrolment No. _____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGG.- VIth SEMESTER-EXAMINATION – MAY/JUNE- 2012

Subject code: 361602/2361602

Date: 29/05/2012

Subject Name: Information Security

Time: 10:30 am – 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. English version is considered to be Authentic

- | | | |
|-------------|--|-----------|
| Q.1 | (a) List and briefly define categories of Passive and Active security attacks | 07 |
| | (b) Write a short note on Distributed Intrusion Detection | 07 |
| Q.2 | (a) What is Worm? Briefly explain state of Worm Technology | 07 |
| | (b) List four techniques used by firewalls to control access and enforce a security policy | 07 |
| OR | | |
| Q.3 | (b) List types of firewalls and Explain each in brief | 07 |
| | (a) Explain polyalphabetic substitution cipher with suitable example | 07 |
| | (b) Generate a cipher text from below plaintext using columnar cipher with key :- 4312567
“ATTACKPOSTPONEDUNTILTWOAM” | 07 |
| OR | | |
| Q.3 | (a) What is steganography? Discuss various techniques of steganography. | 07 |
| | (b) Differentiate the term given below
(i) Stream cipher & Block Cipher (ii) Diffusion and Confusion | 07 |
| Q.4 | (a) Briefly explain single round of DES Encryption. | 07 |
| | (b) Explain RSA algorithm | 07 |
| OR | | |
| Q. 4 | (a) Explain Any three DES Modes of Operation | 07 |
| | (b) Explain Diffie-hellman key exchange algorithm | 07 |
| Q.5 | (a) Differentiate Direct Digital Signature and Arbitrated Digital Signature. | 07 |
| | (b) List and explain four techniques used to avoid guessable passwords. | 07 |
| OR | | |
| Q.5 | (a) What is Digital Signature Standard? Discuss about Digital Signature Algorithm | 07 |
| | (b) Discuss four general categories of schemes for the distribution of public keys. | 07 |

પ્રશ્ન-૧	અ	પેસીવ અને એક્ટીવ એટેક્ની કેટેગરી લખો અને સમજાવો	07
	બ	ડીસ્ટ્રિબ્યુટેડ ઇંટુસન ડીટેક્સન પર ટુંકનોંધ લખો	07
પ્રશ્ન-૨	અ	વોર્મ શું છે? સ્ટેટ ઓફ વોર્મ ટેક્નોલોજી વિશે લખો	07
	બ	ફાયરવોલ ની કંટ્રોલ એક્સેસ અને એન્ફોર્સ સીક્યુરીટી પોલીસીની ચાર પધ્ધતિઓ લખો	07
		અથવા	
	બ	ફાયરવોલના પ્રકાર જણાવો અને દરેક વિશે સમજાવો	07
પ્રશ્ન-૩	અ	પોલીઆલ્ફાબેટીક સબ્સ્ટીટ્યુસન સાયફર ઉદાહરણ સહ સમજાવો	07
	બ	નીચેની પ્લેન ટેક્સ્ટને કોલમ્નર સાયફરમા રૂપાંતરીત કરો. કી-4312567 “ATTACKPOSTPONEDUNTILTWOAM”	07
		અથવા	
પ્રશ્ન-૩	અ	સ્ટેન્નોગ્રાફી શું છે? સ્ટેન્નોગ્રાફીના પ્રકાર વર્ણવો	07
	બ	નીચેનાનો તફાવત લખો (૧) સ્ટ્રીમ સાયફર અને બ્લોક સાયફર (૨) કંફ્યુઝન અને ડીફ્યુઝન	07
પ્રશ્ન-૪	અ	ડી.ઈ.એસ. એન્ક્રીપ્શન નો સિંગલ રાઉન્ડ સમજાવો	07
	બ	આર.એસ.એ. અલ્ગોરીધમ સમજાવો	07
		અથવા	
પ્રશ્ન-૪	અ	કોઈ પણ ત્રણ ડીઈએસ મોડ્સ ઓફ ઓપરેશન સમજાવો	07
	બ	ડેફી-હેલમેન અલ્ગોરીધમ સમજાવો	07
પ્રશ્ન-૫	અ	ડાયરેક્ટ ડીજીટલ સિગ્નેચર અને આરબીટ્રેટ ડીજીટલ સિગ્નેચર વચ્ચેનો તફાવત લખો	07
	બ	ગેસેબલ પાસવર્ડને અવોઈડ કરવાની કોઈ પણ ચાર પધ્ધતિઓ લખો અને સમજાવો	07
		અથવા	
પ્રશ્ન-૫	અ	ડીજીટલ સિગ્નેચર સ્ટાન્ડર્ડ શું છે? ડીજીટલ સિગ્નેચર અલ્ગોરીધમ સમજાવો	07
	બ	પબ્લિક કી ડીસ્ટ્રીબ્યુસનની ચાર જનરલ કેટેગરી સમજાવો	07
