Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING - SEMESTER–VI • EXAMINATION – SUMMER • 2014

Subject Code: 361602 Date: 26-05-2014

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 types of firewalls and Explain each in brief	**07**
	(b)	Write a short note on Distributed Intrusion Detection	**07**
Q.2	(a)	List and briefly define categories of security services and security mechanisms	**07**
	(b)	List four techniques used by firewalls to control access and enforce a security policy	**07**
		OR	
	(b)	List and briefly define categories of passive and active security attacks	**07**
Q.3	(a)	Explain the difference between Block cipher and Stream cipher. Explain Playfair cipher in brief.	**07**
	(b)	What is Steganography? State the types of Steganography and explain them.	**07**
		OR	
Q.3	(a)	List and briefly define types of cryptanalytic attacks based on what is known to the attacker.	**07**
	(b)	Differentiate the term given below (i) Monoalphabetic cipher and Polyalphabetic 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**

****

ગુજરાતી

પ્રશ્ન. ૧	**અ**	Firewalls કેટલા પ્રકારના છે? દરેક પ્રકાર ટુકમાં સમજાવો.	**૦૭**
	બ	Distributed Intrusion Detection પર ટૂંકનોંધ લખો.	**૦૭**
પ્રશ્ન. ૨	**અ**	Security services અને security mechanisms ના પ્રકાર જણાવો અને ટુકમાં સમજાવો.	**૦૭**
	બ	Firewalls ની કોઇપણ ચાર control access અને enforce a security policy સમજાવો.	**૦૭**
		અથવા	
	બ	Passive અને active સિક્યુરીટી અટેકના પ્રકાર જણાવો અને સમજાવો.	**૦૭**
પ્રશ્ન. ૩	**અ**	Block cipher અને stream cipher વચ્ચે તફાવત સમજાવો. Playfair cipher ટુકમાં સમજાવો.	**૦૭**
	બ	Steganography એટલે શું? Steganography ના પ્રકાર જાણવો અને સમજાવો.	**૦૭**
		અથવા	
પ્રશ્ન. ૩	**અ**	Attacker ની જાણમાં હોય તેવા cryptanalytic attacks ના પ્રકાર જાણવો સમજાવો.	**૦૭**
	બ	તફાવત સમજાવો.	**૦૭**
		(i) Monoalphabetic cipher અને Polyalphabetic cipher	
		(ii) Diffusion અને Confusion	
પ્રશ્ન. ૪	**અ**	DES Encryption નો સીંગલ રાઉન્ડ સમજાવો.	**૦૭**
	બ	RSA અલગોરિધમ સમજાવો.	**૦૭**
		અથવા	
પ્રશ્ન. ૪	**અ**	કોઈ પણ ત્રણ DES Modes of Operation સમજાવો.	**૦૭**
	બ	Diffie-hellman key exchange અલગોરિધમ સમજાવો.	**૦૭**
પ્રશ્ન. ૫	**અ**	તફાવત સમજાવો Direct Digital Signature અને Arbitrated Digital Signature.	**૦૭**
	બ	કોઇપણ ચાર avoid guessable passwords ના પ્રકાર જણાવો અને સમજાવો.	**૦૭**
		અથવા	
પ્રશ્ન. ૫	**અ**	Digital Signature Standard શું છે? Digital Signature નો અલગોરિધમ સમજાવો.	**૦૭**
	બ	Distribution of public key ની કોઇપણ ચાર general categories of schemes સમજાવો.	**૦૭**

****