Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER –VI • EXAMINATION – WINTER 2015

Subject Code: 361602 **Date: 21/12/2015**

Subject Name: Information Security

Time: 02:30 PM TO 05:00 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 Authentic**.

Q.1	(a)	What is firewall? Explain each type of firewall in detail	**07**
	(b)	Explain Security Services.	**07**
Q.2			
	(a)	What is virus? Explain different types of virus.	**07**
	(b)	Write short note on Distributed Intrusion Detection.	**07**
		OR	
	(b)	What is Worm? Briefly explain state of Worm Technology.	**07**
Q.3			
	(a)	What is monoalphabetic cipher? Explain cryptanalysis of monoalphabetic cipher with suitable example.	**07**
	(b)	Explain Playfair Cipher with an Example	**07**
		OR	
Q.3	(a)	Explain One-Time Pad technique.List fundamental difficulties in this technique.	**07**
	(b)	Explain Caesar Cipher with an example.	**07**
Q.4			
	(a)	Explain RSA Algorithm with example.	**07**
	(b)	Explain Authentication protocol.	**07**
		OR	
Q. 4	(a)	Differentiate Direct Digital Signature and Arbitrated Digital signature.	**07**
	(b)	Explain Diffle Hellman Key Exchange Algorithom.	**07**
Q.5			
	(a)	Explain single round of DES Encryption.	**07**
	(b)	Discuss four general categories of schemes for the distribution of public keys.	**07**
		OR	
Q.5	(a)	Explain DSS approach.	**07**
	(b)	Write the comparison between Link and End to End Encryption.	**07**

****

Q.1	(a)	ફાયરવોલ એટલે શુ? દરેક પ્રકારની ફાયરવોલ વિગતવાર સમજાવો.	**07**
	(b)	સીકયુરિટી સર્વિસ સમજાવો.	**07**
Q.2			
	(a)	વાયરસ એટલે શુ? જુદા જુદા પ્રકાર નાં વાયરસ્ સમજાવો.	**07**
	(b)	ડીસ્ટ્રીબુટેડ ઇન્ટ્રુસન ડીટેકશન પર ટુંક નોંધ લખો.	**07**
		OR	
	(b)	"Worm" એટલે શુ? Worm ટેકનોલોજીના સ્ટેટ સમજાવો.	**07**
Q.3			
	(a)	" Monoalphabetic cipher" એટલે શુ? " Monoalphabetic cipher" નું ક્રીપ્ટએનાલીસિસ ઉદાહરણ આપી સમજાવો.	**07**
	(b)	પ્લેફેર સાયફર ઉદાહરણ આપી સમજાવો.	**07**
		OR	
Q.3	(a)	"One-Time Pad" ટેકનિક સમજાવો. આ ટેકનિક ની પ્રાથમીક મુશ્કેલીઓ લખો.	**07**
	(b)	"Caesar Cipher" ઉદાહરણ આપી સમજાવો.	**07**
Q.4			
	(a)	RSA અલગોરિથમ ઉદાહરણ આપી સમજાવો.	**07**
	(b)	Authentication પ્રોટોકોલ સમજાવો.	**07**
		OR	
Q. 4	(a)	Direct Digital Signature અને Arbitrated Digital signature વચ્ચેનો તફાવત લખો.	**07**
	(b)	"Diffle Hellman Key Exchange" અલગોરિથમ સમજાવો.	**07**
Q.5			
	(a)	"DES Encryption" નો સિંગલ રાઉન્ડ સમજાવો.	**07**
	(b)	Public keys ની વહેંચણી માટે ચાર પ્રકારની જનરલ કેટેગરી સ્કીમની ચર્ચા કરો.	**07**
		OR	
Q.5	(a)	DSS એપ્રોચ સમજાવો.	**07**
	(b)	Link અને End to End Encryption વચ્ચેની સરખામણી કરો.	**07**

****