

GUJARAT TECHNOLOGICAL UNIVERSITY
DIPLOMA ENGG.- SEMESTER-VI EXAMINATION – OCTOBER 2012

Subject code: 361602**Date: 29-10-2012****Subject Name: Information Security****Time: 2:30 pm – 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. English version is considered to be Authentic

Q.1	(a)	Explain model for network security.	07
	(b)	What is honeypots? Explain briefly.	07
Q.2	(a)	Write short note : Digital Immune System	07
	(b)	List and Briefly explain types of viruses.	07
		OR	
	(b)	List and Briefly explain types of firewalls.	07
Q.3	(a)	What is cryptanalysis? Explain types of attacks on encrypted messages.	07
	(b)	Explain playfair cipher.	07
		OR	
Q.3	(a)	What is monoalphabetic cipher? Explain cryptanalysis of monoalphabetic cipher with suitable example.	07
	(b)	Briefly explain single round of DES encryption.	07
Q.4	(a)	Explain any three block cipher modes of operations.	07
	(b)	List and briefly explain ways in which secret keys can be distributed to two communicating parties.	07
		OR	
Q. 4	(a)	Differentiate between link and end-to-end encryption?	07
	(b)	Explain RSA algorithm with example.	07
Q.5	(a)	Write short note: Diffie-Hellman key Exchange.	07
	(b)	Differentiate between direct and arbitrated digital signature.	07
		OR	
Q.5	(a)	What is Digital signature? Explain digital signature algorithm.	07
	(b)	Briefly explain public-key distribution using public-key authority.	07

પ્રશ્ન-૧	અ	નેટવર્ક સિક્યુરિટી નો મોડેલ સમજાવો.	07
	બ	હનીપોટ શું છે ? વિસ્તૃતમાં સમજાવો.	07
પ્રશ્ન-૨	અ	ટુંક નોંધ લખો : ડીજીટલ ઈમ્યુન સિસ્ટમ.	07
	બ	વાઇરસના પ્રકાર જાણવો અને વિસ્તૃતમાં વર્ણવો.	07
		અથવા	
	બ	ફાયરવોલના પ્રકાર જાણવો અને વિસ્તૃતમાં વર્ણવો.	07
પ્રશ્ન-૩	અ	ક્રપ્ટોનાલીસીસ શું છે ? એન્ક્રિપ્ટ મેસેજ પર અટેક ના પ્રકાર જણાવો.	07
	બ	પ્લેયફેર સિફર સમજાવો.	07
		અથવા	
પ્રશ્ન-૩	અ	મોનોઆલ્ફાબેટીક સિફર શું છે? મોનોઆલ્ફાબેટીક સિફરનો ક્રપ્ટોનાલીસ ઉદાહર આપી સમજાવો.	07
	બ	DES એન્ક્રિપ્શન નો એક રાઉન્ડ વિસ્તાર થી સમજાવો.	07
પ્રશ્ન-૪	અ	કોઇપણ ત્રણ બ્લોક સિફર મોડ ઓફ ઓપરેશન સમજાવો.	07
	બ	બે પાર્ટી વચ્ચે સિક્રેટ કીય ડ્રીસ્ટીબ્યુટ કરવાના પ્રકાર જણાવો અને સમજાવો.	07
		અથવા	
પ્રશ્ન-૪	અ	લીંક અને એન્ડ-ટુ-એન્ડ વચ્ચે તફાવત સમજાવો.	07
	બ	RSA અલગોરિધમ ઉદાહરણ સાથે સમજાવો.	07
પ્રશ્ન-૫	અ	ટુંક નોંધ લખો : ડેફી-હેલ્મેન કીય એક્ચેન્જ	07
	બ	ડાયરેક્ટ અને આર્બિટ્રેટેડ ડીજીટલ સિગ્નેચર વચ્ચે તફાવત સમજાવો.	07
		અથવા	
પ્રશ્ન-૫	અ	ડીજીટલ સિગ્નેચર શું છે? ડીજીટલ સિગ્નેચરનો અલગોરિધમ સમજાવો.	07
	બ	પબ્લીક-કીય ડીસ્ટ્રીબ્યુશન પબ્લીક-કીય ઓથોરીટીનો ઉપયોગ કરી સવિસ્તાર સમજાવો	07
