

GUJARAT TECHNOLOGICAL UNIVERSITY**Diploma Engineering - SEMESTER-VI • EXAMINATION – SUMMER 2013****Subject Code: 361602****Date: 13/05/2013****Subject Name: Information Security****Time: 10:30 am TO 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) Explain a model for Network security. List basic tasks in designing a particular security service. **07**
- (b) Define following terms.(Any Seven) **07**
1. Cryptography
 2. Brute-force Attack
 3. Stream Cipher
 4. Permutation
 5. Asymmetric encryption
 6. Masquerader
 7. Misfeasor
 8. Firewall
 9. Malicious software
- Q.2** (a) What is firewall? List out limitations of firewall. Explain any one type of firewall in detail. **07**
- (b) What is Intruders? Explain Rule-Based Intrusion Detection. **07**
- OR**
- (b) Explain password selection strategies with Basic techniques. **07**
- Q.3** (a) Explain transposition technique with example. **07**
- (b) Explain One-Time Pad technique. List fundamental difficulties in this technique. **07**
- OR**
- Q.3** (a) Explain Steganography technique. **07**
- (b) What is Cryptanalysis? Explain the types of cryptanalytic attacks. **07**
- Q.4** (a) Explain Single-round of DES Algorithm. **07**
- (b) Explain Traffic Confidentiality. **07**
- OR**
- Q. 4** (a) Explain the use of Random Number in network security. **07**
- (b) Explain the strength of DES. **07**
- Q.5** (a) Explain RSA Algorithm. **07**
- (b) Explain Authentication protocol. **07**
- OR**
- Q.5** (a) What is Digital signature? Explain the types of Digital signature. **07**
- (b) Explain Distribution of Secret keys using public-key cryptography. **07**

પ્રશ્ન-૧	અ	નેટવર્ક સિક્યુરીટી માટેનું મોડેલ સમજાવો. સિક્યુરીટી સર્વિસીસ ડીઝાઇન કરવા માટેનાં બેઝીક કાર્યો લખો.	07
	બ	નીચેનાને વ્યાખ્યાયીત કરો..(કોઇપણ સાત)	07
		1. Cryptography 2. Brute-force Attack 3. Stream Cipher 4. Permutation 5. Asymmetric encryption 6. Masquerader 7. Misfeasor 8. Firewall 9. Malicious software	
પ્રશ્ન-૨	અ	ફાયર વોલ શું છે? ફાયર વોલની લીમીટેશન લખો. કોઇપણ એક પ્રકારની ફાયર વોલ વિગતવાર સમજાવો.	07
	બ	Intruders શું છે? Rule-Based Intrusion Detection સમજાવો.	07
		OR	
	બ	Password selection strategies Basic techniques સાથે સમજાવો.	07
પ્રશ્ન-૩	અ	Transposition technique ઉદાહરણ સાથે સમજાવો.	07
	બ	One-Time Pad technique સમજાવો. આ પદ્ધતીની પ્રાયમરી મુશ્કેલીઓ લખો.	07
		OR	
પ્રશ્ન-૩	અ	Steganography technique સમજાવો .	07
	બ	Cryptanalysis શું છે? Cryptanalytic attacks નાં પ્રકારો સમજાવો. .	07
પ્રશ્ન-૪	અ	DES અલગોરીમ. નો Single-round સમજાવો.	07
	બ	Traffic Confidentiality સમજાવો.	07
		OR	
પ્રશ્ન-૪	અ	નેટવર્ક સિક્યુરીટીમાં Random Number નો ઉપયોગ સમજાવો .	07
	બ	DES ની strength સમજાવો.	07
પ્રશ્ન-૫	અ	RSA અલગોરીમ સમજાવો.	07
	બ	Authentication protocol સમજાવો .	07
		OR	
પ્રશ્ન-૫	અ	Digital signature શું છે ? Digital signature નાં પ્રકારો સમજાવો.	07
	બ	Secret keys નું Distribution public-key cryptography ની મદદથી સમજાવો	07