

GUJARAT TECHNOLOGICAL UNIVERSITY
DIPLOMA ENGINEERING - SEMESTER-VI • EXAMINATION – WINTER • 2014

Subject Code: 361602**Date: 28-11-2014****Subject Name: Information Security****Time: 02:30 pm - 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 considered to be Authentic.

- Q.1** (a) Explain model of network security **07**
(b) Explain various types of security attacks. Explain any one in detail. **07**
- Q.2** (a) What is intruders? Explain various types of intrusion detection. **07**
(b) Explain password selection strategies with basic techniques. **07**
- OR
- (b) Explain play fair cipher with example. **07**
- Q.3** (a) Explain steganography technique. **07**
(b) Explain in detail single round of DES. **07**
- OR
- Q.3** (a) Explain firewall in detail. **07**
(b) Explain s- box, p- box and strength of DES in detail. **07**
- Q.4** (a) List out block cipher mode of operations. Explain any three in detail. **07**
(b) List and explain ways of key distribution between two communicating parties. **07**
- OR
- Q. 4** (a) Explain substitution and transposition with example. **07**
(b) Write short note on virus. **07**
- Q.5** (a) Explain RSA algorithm. **07**
(b) Explain Authentication protocol. **07**
- OR
- Q.5** (a) What is digital signature? Explain direct digital signature. **07**
(b) Explain link and end to end encryption in detail. **07**

ગુજરાતી

- પ્રશ્ન. ૧ અ નેટવર્ક સિક્યોરિટી મોડેલ સમજાવો. ૦૭
બ જુદા જુદા સિક્યોરિટી અટેક સમજાવો. કોઈ પણ એક વિસ્તાર થી સમજાવો. ૦૭
- પ્રશ્ન. ૨ અ ઇન્ટ્રુડર શું છે?જુદા પ્રકાર ના ઇન્ટ્રુડર ડીટેક્શન સમજાવો. ૦૭
બ પાસવર્ડ સીલેક્શન સ્ટ્રેટેજી મુખ્ય પધ્ધતિ સાથે સમજાવો. ૦૭
- અથવા
- બ પ્લેફેર સાઈફર ઉદાહરણ સાથે સમજાવો. ૦૭
- પ્રશ્ન. ૩ અ Steganography પધ્ધતી સમજાવો. ૦૭
બ DES નો સિંગલ રાઉન્ડ વિસ્તાર થી સમજાવો. ૦૭
- અથવા
- પ્રશ્ન. ૩ અ ફાયર વોલ વિસ્તાર થી સમજાવો. ૦૭
બ S -બોક્સ અને P-બોક્સ અને DES ની સ્ટ્રેન્થ વિસ્તારથી સમજાવો. ૦૭
- પ્રશ્ન. ૪ અ બ્લોક સાઈફર મોડ ની યાદી લખો અને કોઈ પણ ત્રણ વિસ્તાર થી સમજાવો. ૦૭
બ બે કોમ્યુનિકેટિંગ પાર્ટી વચ્ચે key ડિસ્ટ્રિબ્યુશન ના જુદી જુદી રીત બતાવો. ૦૭
- અથવા
- પ્રશ્ન. ૪ અ સબ્સ્ટીટ્યુશન અને ટ્રાન્સ્પોસીશન ઉદાહરણ સાથે સમજાવો. ૦૭
બ વાઇરસ માટે ટૂંક નોંધ લખો. ૦૭
- પ્રશ્ન. ૫ અ RSA અલ્ગોરિધમ સમજાવો. ૦૭
બ ઓથેન્ટિકેશન પ્રોટોકોલ સમજાવો. ૦૭
- અથવા
- પ્રશ્ન. ૫ અ ડિજિટલ સિગ્નેચર શું છે?ડાઇરેક્ટ ડિજિટલ સિગ્નેચર સમજાવો. ૦૭
બ લિન્ક અને એન્ડ ટુ એન્ડ એક્ષિપ્શન વિસ્તાર થી સમજાવો. ૦૭
