

GUJARAT TECHNOLOGICAL UNIVERSITY**Diploma Engineering - SEMESTER-V • Examination – WINTER • 2014****Subject Code: 3351602****Date: 26-11-2014****Subject Name: Essentials of Network 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** Answer any seven out of ten. **14**
1. What is information security?
 2. Difference between active attacks and passive attacks.
 3. What is Steganography?
 4. Explain Cryptography.
 5. Difference between symmetric and asymmetric encryption.
 6. List out five substitution techniques.
 7. List out five Block Cipher Mode of operations.
 8. What is the size of key and plaintext block in DES.
 9. List out any three active attacks.
 10. What is Brute Force Attack?
- Q.2** (a) Explain Confidentiality in Public key Cryptography. **03**
- OR
- (a) Explain Authentication in Public key Cryptography. **03**
- (b) Explain Rectangle Technique. **03**
- OR
- (b) Explain Caesar Cipher in detail. **03**
- (c) Convert plaintext to ciphertext using Playfair. **04**
- Plaintext: how r you. Key: Balloon
- OR
- (c) Convert plaintext to ciphertext using Hill Cipher. **04**
- Plaintext: MODI Key: $\begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}$
- (d) Explain Security Mechanism in detail. **04**
- OR
- (d) Explain Security Services in detail. **04**
- Q.3** (a) Write Euclidean Algorithm. **03**
- OR
- (a) Explain Groups and Rings. **03**
- (b) Explain Man in Middle Attack. **03**
- OR
- (b) Explain Double DES in detail. **03**
- (c) Explain Cipher Block Chaining Mode. **04**
- OR
- (c) Explain Counter Mode. **04**
- (d) Describe antivirus approaches in detail. **04**
- OR
- (d) Describe the importance of Operating System Updates. **04**

Q.4	(a) Explain Rail fence technique.	03
	OR	
	(a) Describe different anti malware and Clean up tools.	03
	(b) Explain Network Security Model.	04
	OR	
	(b) Explain one Round of DES in detail.	04
	(c) Explain Diffie-Hellman key exchange algorithm.	07
Q.5	(a) Explain Fiestel Structure.	04
	(b) Explain 8 S-box in detail.	04
	(c) What is passive attack? Explain any one in detail.	03
	(d) Explain four technique of Steganography.	03

ગુજરાતી

પ્રશ્ન. ૧	દશમાંથી કોઇપણ સાતના જવાબ આપો.	૧૪
૧.	ઇન્ફોર્મેશન સિક્યોરીટી શું છે?	
૨.	એક્ટીવ એટેક અને પેસીવ એટેક નો તફાવત સમજાવો	
૩.	સ્ટેગનોગ્રાફી શું છે?	
૪.	ક્રિપ્ટોગ્રાફી સમજાવો.	
૫.	સિમેટ્રિક અને એસીમેટ્રિક એનક્રિપ્શન વચ્ચે તફાવત.	
૬.	પાંચ સબ્સિટ્યુસન ની યાદી આપો.	
૭.	પાંચ બ્લોક સાઈફર મોડ ઓપરેસનની યાદી આપો.	
૮.	DES માં કી અને પ્લેન્ટેક્સ્ટ બ્લોક ની સાઈઝ શું છે.	
૯.	કોઇપણ ત્રણ એક્ટીવ એટેક ની યાદી આપો.	
૧૦	બ્રોઉટ ફોર્સ એટેક શું છે.	
પ્રશ્ન. ૨	અ પબ્લિક કી ક્રિપ્ટોગ્રાફી માં કોન્ફીડેન્સીયાલીટી સમજાવો.	૦૩
	અથવા	
અ	પબ્લિક કી ક્રિપ્ટોગ્રાફી માં ઓથેન્ટિકેસન સમજાવો.	૦૩
બ	રેક્ટેન્ગલ ટેકનીક સમજાવો	૦૩
	અથવા	
બ	સીઝર સાઈફર ટેકનીક સમજાવો.	૦૩
ક	પ્લેફર ની મદદથી પ્લેન્ટેક્સ્ટ માંથી સાઈફર મા કન્વર્ટ કરો.	૦૪
	પ્લેન્ટેક્સ્ટ: how r you. કી : Balloon	
	અથવા	
ક	હિલ સાઈફર ની મદદથી પ્લેન્ટેક્સ્ટ માંથી સાઈફર મા કન્વર્ટ કરો.	૦૪
	પ્લેન્ટેક્સ્ટ: MODI કી : $\begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}$	
ડ	સિક્યુરીટી મીકેનીસમ વિસતૃતમાં સમજાવો.	૦૪
	અથવા	
ડ	સિક્યુરીટી સર્વિસ વિસતૃતમાં સમજાવો	૦૪

પ્રશ્ન. ૩	અ	યુક્લિડીયન અલ્ગોરિધમ લખો.	૦૩
		અથવા	
	અ	ગ્રુપ અને રિંગ્સ સમજાવો.	૦૩
	બ	મેન ઇન મિડલ એટક સમજાવો.	૦૩
		અથવા	
	બ	વિગતવાર ડબલ DES સમજાવો.	૦૩
	ક	સાઈફર બ્લોક ચેઈનીંગ મોડ સમજાવો.	૦૪
		અથવા	
	ક	કાઉન્ટર મોડ સમજાવો.	૦૪
	ડ	વિગતવાર એન્ટીવાયરસ એપ્પરોચ સમજાવો.	૦૪
		અથવા	
	ડ	ઓપરેટિંગ સિસ્ટમ અપડેટ નું મહત્વ સમજાવો.	૦૪
પ્રશ્ન. ૪	અ	રેલ ફેંશ ટેકનિક સમજાવો.	૦૩
		અથવા	
	અ	અલગ અલગ એન્ટી મેલવેર અને ક્લિણિંગ ટુલ વર્ણવો	૦૩
	બ	નેટવર્ક શિકીયોરીટી મોડલ સમજાવો.	૦૪
		અથવા	
	બ	વિગતવાર DES નો એક રાઉન્ડ સમજાવો.	૦૪
	ક	ડિફી-હેલમેન કી એક્સચેન્જ અલ્ગોરિધમ સમજાવો.	૦૭
પ્રશ્ન. ૫	અ	ફીએસ્ટલ સ્ટ્રકચર સમજાવો.	૦૪
	બ	૮-એસ બોક્ષ સમજાવો.	૦૪
	ક	પેશીવ એટક શું છે? વિગતવાર કોઈ પણ એક સમજાવો.	૦૩
	ડ	સ્ટેગનોગ્રાફી ની ચાર ટેકનિક સમજાવો.	૦૩
