Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER – V • EXAMINATION – SUMMER 2017

Subject Code: 3351602 Date: 2-05-2017

Subject Name: ESSENTIALS OF NETWORK SECURITY

Time: 2.30 PM TO 5.00PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make Suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Use of programmable & Communication aids are strictly prohibited.**
5. **Use of only simple calculator is permitted in Mathematics.**
6. **English version is authentic.**

Q.1 Answer any seven out of ten. દશમાંથી કોઇપણ સાતના જવાબ આપો. **14**

1. Define cryptography.
૧. ક્રીપ્ટોગ્રાફી વ્યાખ્યાયીત કરો.
2. Define Cryptanalysis.
૨. ક્રીપ્ટએનાલીસીસ વ્યાખ્યાયીત કરો.
3. What is firewall?
૩. ફાયરવોલ શું છે ?
4. What is OS Hardening?
૪. OS Hardening શું છે ?
5. Define a field.
૫. ફીલ્ડ વ્યાખ્યાયીત કરો.
6. What is man in the middle attack?
૬. મેન ઈન મિડલ એટેક શું છે ?
7. Give difference between stream and block cipher.
૭. સ્ટ્રીમ અને બ્લોક સાઈફર વચ્ચેનો તફાવત આપો.
8. What is asymmetric key encryption?
૮. અસીમેટ્રીક કી એનક્રીપ્શન શું છે ?
9. List out substitution techniques.
૯. સબસ્ટીટ્યુશન ટેકનીકની યાદી બનાવો.
10. Give difference between active attacks and passive attacks.
૧૦. એકટીવ એટેક અને પેસીવ એટેક વચ્ચેનો તફાવત આપો.

Q.2 (a) Explain passive attack. **03**

પ્રશ્ન. ૨ (અ) પેસીવ એટેક સમજાવો. ૦૩

OR

(a) Explain Authentication in public key cryptography. **03**

(અ) પબ્લીક કી ક્રિપ્ટોગ્રાફીમાં ઓથેન્ટીકેશન સમજાવો. ૦૩

(b) Write difference between monoalphabetic cipher and polyalphabetic cipher. **03**

(બ) મોનો આલ્ફાબેટીક સાઈફર અને પોલીઆલ્ફાબેટીક સાઈફર વચ્ચેનો તફાવત લખો. ૦૩

OR

	(b)	Explain Caesar cipher.	**03**
	(બ)	સીઝર સાઈફર સમજાવો.	૦૩
	(c)	Explain security services in detail.	**04**
	(ક)	સિક્યુરીટી સર્વિસ વિગતવાર સમજાવો.	૦૪

OR

	(c)	Explain OSI security architecture.	**04**
	(ક)	ઓ.એસ.આઈ. સિક્યુરીટી આર્કીટેકચર સમજાવો.	૦૪
	(d)	Explain Euclidean algorithm.	**04**
	(ડ)	યુક્લિડીયન અલ્ગોરિધમ સમજાવો.	૦૪

OR

	(d)	Why random numbers are important in cryptography?	**04**
	(ડ)	ક્રિપ્ટોગ્રાફીમાં રેન્ડમ નંબર કેમ મહત્વના છે ?	૦૪
Q.3	(a)	Discuss the design features of Fiestel cipher.	**03**
પ્રશ્ન. 3	(અ)	ફિએસ્ટલ સાઈફરના ડિઝાઈન ફીચર વર્ણવો.	૦૩

OR

	(a)	Explain counter mode.	**03**
	(અ)	કાઉન્ટર મોડ સમજવો.	૦૩
	(b)	What are the limitations of symmetric key encryption?	**03**
	(બ)	સિમેટ્રીક કી એન્ક્રીપ્શનની ખામીઓ શું છે ?	૦૩

OR

	(b)	Explain output feedback mode.	**03**
	(બ)	આઉટપુટ ફીડબેક મોડ સમજાવો.	૦૩
	(c)	Explain Groups and Rings.	**04**
	(ક)	ગ્રુપ અને રીંગસ સમજાવો.	૦૪

OR

	(c)	Explain antimalware and cleanup tools.	**04**
	(ક)	એન્ટી મેલવેર અને કલીનઅપ ટુલ સમજાવો.	૦૪
	(d)	Explain 8 S-box in detail.	**04**
	(ડ)	8 એસ-બોક્સ સમજાવો.	૦૪

OR

	(d)	Explain Steganography.	**04**
	(ડ)	સ્ટેગેનોગ્રાફી સમજાવો.	૦૪
Q.4	(a)	What are the key features of asymmetric encryption?	**03**
પ્રશ્ન. ૪	(અ)	અસીમેટ્રીક એનક્રીપશનની મુખ્યફ્યુચર શું છે ?	૦૩

OR

	(a)	Explain one round of DES in detail.	**03**
	(અ)	ડી.ઈ.એસ.નો એક રાઉન્ડ વિગતવાર સમજાવો.	૦૩
	(b)	Explain transposition technique with example.	**04**
	(બ)	ટ્રાન્સપોઝીસન ટેકનીક ઉદાહરણ સહિત સમજાવો.	૦૪

OR

	(b)	What are the functions of OS security assessments tools?	**04**
	(બ)	OS સિક્યુરીટી અસેસમેન્ટ ટુલ્સના ફંકશન શું છે ?	૦૪

	(c)	Explain Playfair cipher with example.	**07**
	(ક)	પ્લેફેર સાઈફર ઉદાહરણ સહિત સમજાવો.	૦૭
Q.5	(a)	Explain double DES in detail.	**04**
પ્રશ્ન. ૫	(અ)	ડબલ ડી.ઈ.એસ. વિગતવાર સમજાવો.	૦૪
	(b)	Explain any two block cipher modes of operation.	**04**
	(બ)	કોઈ પણ બે બ્લોક સાઈફર મોડસ ઓફ ઓપરેશન સમજાવો.	૦૪
	(c)	Explain rail fence technique.	**03**
	(ક)	રેલ ફેંશ ટેકનીક સમજાવો.	૦૩
	(d)	What are windows patches?	**03**
	(ડ)	વિન્ડો પેચસ શું છે ?	૦૩

****