

Seat No.: _____

Enrolment No. _____

GUJARAT TECHNOLOGICAL UNIVERSITY
DIPLOMA ENGINEERING – SEMESTER – V• EXAMINATION – SUMMER 2016

Subject Code: 3351602

Date: 07/05/2016

Subject Name: Essential of Network Security

Time: 02:30 PM to 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. 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. What is Windows OS Hardening?
૧. Windows OS Hardening શું છે?
2. List out application of Asymmetric Key Cryptography.
૨. Asymmetric Key Cryptography ના ઉપયોગ જણાવો.
3. What is Traffic Padding?
૩. Traffic Padding શું છે?
4. Which type of attack is difficult to detect? Why?
૪. કયા પ્રકારનાં એટેકની જાણ થતી નથી. શા માટે?
5. Explain Caesar cipher with suitable example.
૫. Caesar cipher યોગ્ય ઉદાહરણની મદદથી સમજાવો
6. Discuss the three dimension of Cryptographic System.
૬. Cryptographic System ના ત્રણ ડાઇમેન્શન સમજાવો
7. List out the properties of Group.
૭. Group ની properties જણાવો
8. Lists block cipher modes of operation.
૮. block cipher modes of operation નું લિસ્ટ લખો.
9. What is Firewall?
૯. Firewall શું છે?
10. What do you mean by DoS Attack?
૧૦. DoS Attack શું છે?

Q.2

- (a) Explain OSI Security Architecture.

03

પ્રશ્ન. ૨	(અ) OSI Security Architecture સમજાવો.	03
	OR	
	(a) Explain Network Security Model.	03
	(અ) Network Security Model સમજાવો.	03
	(b) Compare Symmetric key and Asymmetric key Cryptography.	03
	(બ) Symmetric key and Asymmetric key Cryptography કંપેર કરો.	03
	OR	
	(b) Discuss the type of attacks of encrypted message.	03
	(બ) encrypted message પર ના એટેકની ચર્ચા કરો.	03
	(c) Explain Playfair cipher using following data. PlainText="Why don't you?" KeyWord="KEYWORD"	04
	(ક) Playfair સમજાવો. PlainText="Why don't you?" KeyWord="KEYWORD"	04
	OR	
	(c) Explain Diffie-Hellmen Key Exchange Algorithm with Suitable example.	04
	(ક) Diffie-Hellmen Key Exchange Algorithm યોગ્ય ઉદાહરણની મદદથી સમજાવો.	04
	(d) Discuss Various Transposition Techniques.	04
	(ડ) Transposition Techniques સમજાવો.	04
	OR	
	(d) Explain Briefly Steganography.	04
	(ડ) Steganography સમજાવો.	04
Q.3	(a) Explain Euclidean Algorithm using suitable example.	03
પ્રશ્ન. ૩	(અ) Euclidean Algorithm યોગ્ય ઉદાહરણની મદદથી સમજાવો.	03
	OR	
	(a) Find GCD of 1066 and 904.	03
	(અ) 1066 અને 904 ના GCD શોધો.	03
	(b) Explain one time pad using suitable example.	03
	(બ) one time pad યોગ્ય ઉદાહરણની મદદથી સમજાવો.	03
	OR	
	(b) List All Active Attack. Explain any one with example.	03
	(બ) બધા એક્ટીવ એટેક લખો. કોઈ એક સમજાવો.	03
	(c) Define Ring. Discuss its properties also.	04
	(ક) Ring સમજાવી તેની પ્રોપર્ટી ની ચર્ચા કરો.	04
	OR	
	(c) Define Field. Discuss its properties also.	04
	(ક) Field સમજાવી તેની પ્રોપર્ટી ની ચર્ચા કરો.	04

	(d)	Draw modular arithmetic table of 8 for addition, multiplication, additive and multiplicative inverse.	04
	(S)	modular arithmetic table of 8 for addition, multiplication, additive and multiplicative inverse ડ્રો કરો.	04
		OR	
	(d)	Draw modular arithmetic table of 7 for addition, multiplication, additive and multiplicative inverse.	04
	(S)	modular arithmetic table of 7 for addition, multiplication, additive and multiplicative inverse ડ્રો કરો.	04
Q.4	(a)	Compare Block cipher with Stream Cipher.	03
પ્રશ્ન. ૪	(અ)	Block cipher with Stream Cipher કમ્પેર કરો.	03
		OR	
	(a)	Discuss the limitation of Symmetric Key Encryption.	03
	(અ)	Symmetric Key Encryption ની મર્યાદાઓ લખો.	03
	(b)	How can we achieve Confidentiality using Asymmetric Key Cryptography?	04
	(બ)	Asymmetric Key Cryptography માં Confidentiality કેવી રીતે પ્રાપ્ત કરશો.	04
		OR	
	(b)	How can we achieve Authentication using Asymmetric Key Cryptography?	04
	(બ)	Asymmetric Key Cryptography માં Authentication કેવી રીતે પ્રાપ્ત કરશો.	04
	(c)	Briefly explain DES Algorithm	07
	(ક)	DES Algorithm વિસ્તારથી સમજાવો.	07
Q.5	(a)	Discuss CBC.	04
પ્રશ્ન. ૫	(અ)	CBC સમજાવો.	04
	(b)	Explain design criteria of block cipher mode.	04
	(બ)	design criteria of block cipher mode સમજાવો.	04
	(c)	List All Passive Attack. Explain any one with example.	03
	(ક)	બધા પેસીવ એટેક લખો. કોઈ એક સમજાવો.	03
	(d)	Explain patches, updates, upgrades.	03
	(ડ)	patches, updates, upgrades સમજાવો.	03
