Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

DIPLOMA ENGINEERING – SEMESTER –VI • EXAMINATION – WINTER 2015

Subject Code: 3361601 **Date: 21/12/2015**

Subject Name: WEB AND 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 asymmetric key cryptography?
   ૧. અસીમેટ્રીક કી ક્રીપ્ટોગ્રાફી શું છે ?
2. What is Hash function?
   ૨. હેશ ફંકશન શું છે ?
3. List out application of digital signature.
   ૩. ડીઝીટલ સીગ્નેચરની એપ્લીકેશનની યાદી આપો.
4. List out various hashing algorithm.
   ૪. અલગ અલગ હેશીંગ અલ્ગોરીધમની યાદી આપો.
5. What is IP security?
   ૫. આઈ.પી. સીક્યુરીટી શું છે ?
6. What is MIME?
   ૬. એમ.આઈ.એમ.ઈ. શું છે ?
7. Different between virus and worm.
   ૭. વાઈરસ અને વોર્મ વચ્ચેનો તફાવત શું છે ?
8. Explain Rabin scheme.
   ૮. Rabin સ્કીમ સમજાવો.
9. List out application of public key cryptosystems.
   ૯. પબ્લીક કી ક્રીપ્ટોસીસ્ટમની એપ્લીકેશનની યાદી આપો.
10. What is phishing?
    ૧૦. Phishing શું છે ?

Q.2 (a) Write down types of firewall and explain any one in detail. **03**

પ્રશ્ન. ૨ (અ) ફાયરવોલના પ્રકારો લખો અને કોઈપણ એક વિગતવાર સમજાવો. ૦૩

OR

(a) Explain types of virus. **03**

(અ) વાયરસના પ્રકારો સમજાવો. ૦૩

(b) Give difference between conventional and digital signature. **03**

(બ) કન્વેનશનલ અને ડીઝીટલ સીગ્નેચર વચ્ચેનો તફાવત આપો. ૦૩

OR

	(b)	Explain MIME content type.	**03**
	(બ)	એમ.આઈ.એમ.ઈ. કંટેન્ટ ટાઈપ સમજાવો.	૦૩
	(c)	Explain requirement of public key cryptography.	**04**
	(ક)	પબ્લીક કી ક્રીપ્ટોગ્રાફીની જરૂરીયાતો સમજાવો.	૦૪

OR

	(c)	Discuss the security of RSA algorithm.	**04**
	(ક)	આર.એસ.એ. અલ્ગોરીધમની સીક્યુરીટીની ચર્ચા કરો.	૦૪
	(d)	Give difference between SET and SSL.	**04**
	(ડ)	એસ.ઈ.ટી. અને એસ.એસ.એલ. વચ્ચેનો તફાવત આપો.	૦૪

OR

	(d)	Explain IPsec tunnel mode.	**04**
	(ડ)	IPsec ટનલ મોડ સમજાવો.	૦૪
Q.3	(a)	Explain requirements and application of digital signature.	**03**
પ્રશ્ન. 3	(અ)	ડીઝીટલ સીગ્નેચરની જરૂરીયાતો અને એપ્લીકેશન સમજાવો.	૦૩

OR

	(a)	Write difference between SHA and MD5.	**03**
	(અ)	SHA અને MD5 વચ્ચેનો તફાવત લખો.	૦૩
	(b)	Explain HTTPS connection closure.	**03**
	(બ)	એચ.ટી.ટી.પી.એસ. કનેક્શન કલોઝર સમજાવો.	૦૩

OR

	(b)	Explain HTTPS connection initiation process.	**03**
	(બ)	એચ.ટી.ટી.પી.એસ. કનેક્શન ઈનીસીયેશન પ્રોસેસ સમજાવો.	૦૩
	(c)	Explain digital signature standard.	**04**
	(ક)	ડીઝીટલ સીગ્નેચર સ્ટાન્ડર્ડ સમજાવો.	૦૪

OR

	(c)	Discuss intrusion detection techniques.	**04**
	(ક)	ઈન્ટ્રુઝન ડીટેકશન ટેકનીક વર્ણવો.	૦૪
	(d)	Explain public key cryptanalysis.	**04**
	(ડ)	પબ્લીક કી ક્રીપ્ટએનાલીસીસ સમજાવો.	૦૪

OR

	(d)	List and explain classification of intruders.	**04**
	(ડ)	ઈન્ટ્રુડર્સ ના કલાસીફીકેશનની યાદી આપો અને સમજાવો.	૦૪
Q.4	(a)	Explain malware counter measure.	**03**
પ્રશ્ન. ૪	(અ)	માલવેર કાઉન્ટર માપન સમજાવો.	૦૩

OR

	(a)	Explain firewall characteristics.	**03**
	(અ)	ફાયરવોલની લાક્ષણીકતાઓ સમજાવો.	૦૩
	(b)	Explain 3-D secure protocol in detail.	**04**
	(બ)	3-D સીક્યુર પ્રોટોકોલ વિગતવાર સમજાવો.	૦૪

OR

	(b)	Explain MD5 Hashing algorithm.	**04**
	(બ)	MD5 હેશીંગ અલ્ગોરીધમ સમજાવો.	૦૪

	(c)	Explain general format of PGP message.	**07**
	(ક)	પી.જી.પી. મેસેજની જનરલ ફોર્મેટ સમજાવો.	૦૭
Q.5	(a)	Explain RSA algorithm.	**04**
પ્રશ્ન. ૫	(અ)	આર.એસ.એ. અલ્ગોરીધમ સમજાવો.	૦૪
	(b)	Write a short note on SET.	**04**
	(બ)	એસ.ઈ.ટી. વિષે ટૂંકનોંધ લખો.	૦૪
	(c)	What are the requirements of message authentication code?	**03**
	(ક)	મેસેજ ઓથેન્ટીકેશન કોડની જરૂરીયાતો શું છે ?	૦૩
	(d)	What are the guidelines for password selection?	**03**
	(ડ)	પાસવર્ડ સીલેકશન માટેની ગાઈડલાઈન શું છે ?	૦૩

****