

**GUJARAT TECHNOLOGICAL UNIVERSITY**  
**DIPLOMA ENGINEERING – SEMESTER – VI• EXAMINATION – SUMMER 2016**

**Subject Code: 3361601****Date: 11/05/2016****Subject Name: Web and Network Security****Time: 10:30 AM to 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. 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 encryption?
૧. Asymmetric encryption શું છે?
2. Define: SSL
૨. SSL ની વ્યાખ્યા આપો
3. List out Application of Hash function
૩. Hash function ની અપ્લિકેસન લખો.
4. Define: Hashing
૪. Hashing વ્યાખ્યા આપો
5. Define :MAC
૫. MAC વ્યાખ્યા આપો
6. List out PGP services
૬. PGP services ની યાદી લખો
7. Define: Digital Signature
૭. Digital Signature ની વ્યાખ્યા આપો.
8. List out steps of MD-5 hashing
૮. MD-5 hashing ના સ્ટેપ્સ લખો
9. Define : MIME
૯. MIME ની વ્યાખ્યા આપો
10. What is IPSec?
૧૦. IPSec શું છે?

**Q.2**

(a) Explain Rabin Scheme.

**03****પ્રશ્ન. ૨**

(અ) Rabin Scheme સમજાવો

**03****OR**

(a) Explain IPSec Services.

**03**

(અ) IPSec Services સમજાવો

**03**

(b) What are the advantages of asymmetric cryptography?

**03**

(બ) asymmetric cryptography ના ફાયદા કયા કયા છે તે લખો

**03**

		OR	
	(b)	Explain SSL protocol stack?	03
	(બ)	SSL protocol stack સમજાવો.	03
	(c)	Describe SHA in detail.	04
	(ક)	SHA વર્ણન કરી સમજાવો.	04
		OR	
	(c)	Explain any two operational description of PGP .	04
	(ક)	PGP ની કોઈ પણ બે operational description સમજાવો.	04
	(d)	Explain in detail SET works.	04
	(ડ)	SET કેવી રીતે કાર્ય કરે છે તે સમજાવો	04
		OR	
	(d)	Explain timing attack in brief.	04
	(ડ)	Timing attack સમજાવો.	04
<b>Q.3</b>	(a)	Explain MAC in detail.	03
<b>પ્રશ્ન. 3</b>	(અ)	MAC સમજાવો	03
		OR	
	(a)	Explain S/MIME functionality in brief.	03
	(અ)	S/MIME functionality સમજાવો	03
	(b)	What is Message authentication? Explain its requirements.	03
	(બ)	Message authentication શું છે? અને તેની જરૂરીયાતો લખો.	03
		OR	
	(b)	Explain Web Traffic Security approaches.	03
	(બ)	Web Traffic Security approaches સમજાવો	03
	(c)	Explain Digital Signature Standard (DSS).	04
	(ક)	Digital Signature Standard (DSS) સમજાવો	04
		OR	
	(c)	Explain benefits of IP Sec.	04
	(ક)	IP Sec ની લાભ જણાવો.	04
		OR	
	(d)	Explain application of Digital Signature .	04
	(ડ)	Digital Signature ની એપ્લિકેશન સમજાવો.	04
		OR	
	(d)	Explain Message components and Signature components of PGP	04
	(ડ)	PGP ની Message components અને Signature components સમજાવો	04
<b>Q.4</b>	(a)	Describe applications of IPSec.	03
<b>પ્રશ્ન. 4</b>	(અ)	IPSec ની એપ્લિકેશન સમજાવો.	03
		OR	
	(a)	Explain Davies-Meyer Scheme.	03
	(અ)	Davies-Meyer Scheme સમજાવો	03
	(b)	Describe Security of RSA.	04

(બ) RSA ની સીક્યુરીટી નું વર્ણન કરો . 0૪

OR

(b) Explain in brief Intrusion and Classification of Intruders. 04

(બ) Intruders ની Intrusion and Classification સમજાવો 0૪

(c) Explain RSA algorithm with an example. 07

(ક) RSA અલ્ગોરીધમ દાખલા સાથે સમજાવો 0૭

**Q.5**

(a) What is firewall? Explain the need of firewall in detail. 04

**પ્રશ્ન. ૫**

(અ) Firewall શું છે? અને તેની જરૂરીયતો સમજાવો 0૪

(b) Write differentiate between Conventional encryption and Public-key encryption 04

(બ) Conventional encryption અને Public-key encryption વચ્ચે નો તફાવત લખો 0૪

(c) Explain Malicious Software. 03

(ક) Malicious Software સમજાવો. 03

(d) Describe Virus. 03

(ડ) Virus નું વર્ણન કરો. 03

\*\*\*\*\*