

**GUJARAT TECHNOLOGICAL UNIVERSITY**  
**DIPLOMA ENGINEERING – SEMESTER –VI • EXAMINATION – SUMMER 2018**

**Subject Code:2361602****Date: 01/05/2018****Subject Name: Information 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. Each question carry equal marks (14 marks)

<b>Q.1</b>	(a)	Explain security services and security mechanism in detail.	<b>07</b>
<b>પ્રશ્ન. ૧</b>	અ	વિગતવાર સુરક્ષા સેવાઓ અને સુરક્ષા પદ્ધતિ વિસ્તારથી સમજાવો.	<b>૦૭</b>
	(b)	What is information security? Explain network security model.	<b>07</b>
	બ	Information Security શું છે? Network Security model સમજાવો.	<b>૦૭</b>
<b>Q.2</b>	(a)	Explain malicious software in brief.	<b>07</b>
<b>પ્રશ્ન. ૨</b>	અ	Malicious software ટુકમાં સમજાવો.	<b>૦૭</b>
	(b)	Define intruder and explain honeypots in detail.	<b>07</b>
	બ	Intruder ની વ્યાખ્યા આપો અને honeypots વિસ્તારથી સમજાવો.	<b>૦૭</b>
OR			
	(b)	Explain symmetric cipher model in detail.	<b>07</b>
	બ	Symmetric cipher model વિસ્તારથી સમજાવો.	<b>૦૭</b>
<b>Q.3</b>	(a)	Define cryptography. Explain types of cryptanalytic attack.	<b>07</b>
<b>પ્રશ્ન. ૩</b>	અ	Cryptography ની વ્યાખ્યા આપો. Cryptanalytic attack ના પ્રકાર સમજાવો.	<b>૦૭</b>
	(b)	Explain steganography in detail.	<b>07</b>
	બ	Steganography વિસ્તારથી સમજાવો.	<b>૦૭</b>
OR			
<b>Q.3</b>	(a)	Caesar cipher in detail.	<b>07</b>
<b>પ્રશ્ન. ૩</b>	અ	Caesar cipher વિસ્તારથી સમજાવો.	<b>૦૭</b>
	(b)	What is substitution? Explain double transposition technique.	<b>07</b>
	બ	Substitution શું છે? Double transposition technique સમજાવો.	<b>૦૭</b>
<b>Q.4</b>	(a)	Full form of DES. Explain single round DES in detail.	<b>07</b>
<b>પ્રશ્ન. ૪</b>	અ	DES નું પૂરું નામ આપો. Single round DES વિસ્તારથી સમજાવો.	<b>૦૭</b>
	(b)	Explain Diffie-Hellman key exchange algorithm.	<b>07</b>
	બ	Diffie-Hellman key exchange algorithm સમજાવો	<b>૦૭</b>
OR			
<b>Q.4</b>	(a)	Key management in public key cryptosystem in detail.	<b>07</b>
<b>પ્રશ્ન. ૪</b>	અ	Key management in public key cryptosystem વિસ્તારથી સમજાવો.	<b>૦૭</b>
	(b)	Explain any three block cipher modes of operation.	<b>07</b>
	બ	Block cipher modes of operation ના કોઈ પણ ત્રણ પ્રકાર સમજાવો.	<b>૦૭</b>

<b>Q.5</b>	(a)	What is Digital signature? Explain Digital signature in brief.	<b>07</b>
<b>પ્રશ્ન. ૫</b>	<b>અ</b>	Digital signature શું છે? Digital signature ટુકમાં સમજાવો.	<b>૦૭</b>
	(b)	Explain traffic confidentiality in detail.	<b>07</b>
	<b>બ</b>	Traffic confidentiality વિસ્તારથી સમજાવો	<b>૦૭</b>
		<b>OR</b>	
<b>Q.5</b>	(a)	RSA algorithm in detail.	<b>07</b>
<b>પ્રશ્ન. ૫</b>	<b>અ</b>	RSA વિસ્તારથી સમજાવો.	<b>૦૭</b>
	(b)	Explain DSS in detail.	<b>07</b>
	<b>બ</b>	DSS વિસ્તારથી સમજાવો.	<b>૦૭</b>

\*\*\*\*\*