	Utech
Name:	
Roll No.:	A design (y'x modely) and Explains
Invigilator's Signature:	•••••

CS/M.TECH (CSE)/SEM-2/CST-1024A/2013 2013

INFORMATION SECURITY - II

Time Allotted: 3 Hours Full Marks: 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

GROUP - A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following:

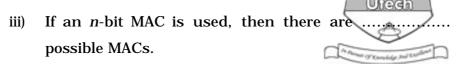
 $10 \times 1 = 10$

- i) Which of the following is not required for Kerberos?
 - a) Reliability
- b) Scalability
- c) Modularity
- d) Security.
- ii) IP security provides security at
 - a) Data link layer
- b) Transport layer
- c) Application layer
- d) Network layer.

30515 (M.Tech)

[Turn over

CS/M.TECH (CSE)/SEM-2/CST-1024A/2013



- a) 2(n-1)
- b) 2
- c) 2(n+1)
- d) 2n.
- iv) In AES, the 16 byte key is expended into
 - a) 64 bytes
- b) 128 bytes
- c) 176 bytes
- d) 78 bytes.
- $\begin{array}{ll} \mbox{v)} & \mbox{For message encryption and decryption algorithm in} \\ \mbox{SMIME is} & \mbox{} \end{array}$
 - a) Triple DES
- b) AES

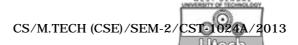
c) DES

- d) IDEA.
- vi) The number of rounds in DES is
 - a) 10

b) 8

c) 16

- d) 14.
- vii) SSL works between
 - a) Web browser, we server
 - b) Web server, application server
 - c) Application server, Database server
 - d) Web server, database server.



- viii) Authentication is maintained in public key cryptography when
 - a) Data encrypted with public key
 - b) data is not encrypted
 - c) Data encrypted with private key
 - d) Data is encrypted with encrypted key.
- ix) Has function can be applied to a block of
 - a) fixed size
- b) 512 bytes
- c) variable size
- d) 1024 bytes.
- x) In the AES encryption scheme algorithm used.
 - a) blowfish
- b) RC4

c) RCC

d) IDEA.

GROUP - B

(Short Answer Type Questions)

Answer any three of the following.

 $3 \times 5 = 15$

- 2. What are the security services provided by IPSec at the IP layer?
- 3. Briefly describe the concept of SMIME.
- 4. Discuss in detail the advanced antivirus techniques.
- 5. Describe the five principal services that Pretty Good Privacy (PGP) provides.
- 6. Describe the Cipher Feedback mode.

30515 (M.Tech)

3

[Turn over

GROUP - C

(Long Answer Type Questions)

Answer any *three* of the following. $3 \times 15 = 45$



- 7 Compare AES cipher versus RC4 encryption algorithm. Write about how PGP massages are created. 8 + 7
- 8. Write short notes on any three of the following:
 - a) Proxy server
 - b) Firewall
 - c) Authentication header
 - d) DES
 - e) Transport Layer Service
 - f) PGP
 - g) SSL.
- Describe the various Information Security Services. Briefly describe the concept of Secure Socket Layer.
 8 + 7
- 10. Describe different operational steps of PGP.
- 11. Describe the concept of public key and private key. Differentiate symmetric and asymmetric cipher. Explain DES algorithm with the help of an example. 5 + 5 + 5