*Seat No.: _____* *Enrolment No._____*

# GUJARAT TECHNOLOGICAL UNIVERSITY

**M. E. - SEMESTER – I • EXAMINATION – WINTER • 2014**

**Subject code: 710104N** **Date: 05-12-2014**

**Subject Name: Information Security**

**Time: 10.30 am – 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.**

| | | | |
|---|---|---|---|
| **Q.1** | **(a)** | Encrypt the message 'encoding' using the double Transposition. Choose Key1 and Key2 as 'exam' and 'study'. | **03** |
| | **(b)** | Using the Euclidean algorithm, find the greatest common divisor of 2002 and 2940. | **04** |
| | **(c)** | Construct a Playfair matrix with the key *largest*. Encrypt this message "Must see you over Cadogan West" | **07** |
| **Q.2** | **(a)** | Encrypt the message "meet me at the usual place " using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result. | **07** |
| | **(b)** | (1) In what ways can a hash value be secured so as to provide message authentication? | **04** |
| | | (2) Explain the avalanche effect. | **03** |
| | | **OR** | |
| | **(b)** | (1) What is the difference between diffusion and confusion? | **04** |
| | | (2) What is the difference between a block cipher and a stream cipher? | **03** |
| **Q.3** | **(a)** | What is intrusion? What is intrusion detection system? Explain intrusion detection system types in detail. | **07** |
| | **(b)** | What is double DES? What is kind of attack on double DES makes it useless? | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | Explain a Message Authentication Code. What is the difference between a message authentication code and a one-way hash function? | **07** |
| | **(b)** | What is the S-box ? How S-Box in DES and AES are constructed and differentiate it's effect in both techniques. | **07** |
| **Q.4** | **(a)** | In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext $M$? | **07** |
| | **(b)** | Explain Diffie-Hellman key exchange. | **07** |
| | | **OR** | |
| **Q.4** | **(a)** | What is KDC? List the duties of a KDC. | **07** |
| | **(b)** | Describe the domain level threats. | **07** |
| **Q.5** | **(a)** | What are the differences between conventional signatures and digital signatures? Write a note on "Attacks on digital signature". | **07** |
| | **(b)** | Explain the server level E-mail threats. | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | Explain the three firewall technologies and compare these firewall technologies. | **07** |
| | **(b)** | "SSL differentiates a connection from a session". Elaborate through a diagram. | **07** |

**********