

**GUJARAT TECHNOLOGICAL UNIVERSITY**  
**ME - SEMESTER- I (OLD course) • EXAMINATION – SUMMER 2015**

**Subject Code: 710104N****Date: 16/05/2015****Subject Name: Information Security****Time: 10:30 am to 1:00 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) Explain the key generation in DES algorithm. **07**  
 (b) Explain Data Integrity and non-repudiation security services. **07**
- Q.2** (a) What do you mean by security attack, mechanism and service? Clear all three with examples. **07**  
 (b) Decipher the message YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC **07**  
 PQTYJ using the Hill cipher with the inverse key
- |   |   |
|---|---|
| 5 | 1 |
| 2 | 7 |
- Show your calculation and the result.
- OR**
- (b) Explain the working of Hill cipher with proper example. Give its limitations. **07**
- Q.3** (a) (i) How is the S-box constructed in Advanced Encryption Standard (AES)? **07**  
 (ii) Write extended Euclidean algorithm to find multiplicative inverse.  
 (b) (i) Explain the role of key distribution center **07**  
 (ii) What is the difference between statistical randomness and unpredictability?
- OR**
- Q.3** (a) Give the Feistel cipher structure and give its design criteria. **07**  
 (b) What are the issues in effective use of IDS? Discuss some of them with examples. **07**
- Q.4** (a) (i) Explain e-mail spoofing. **07**  
 (ii) What is DNS? Which tool is used on the client to query DNS server?  
 (b) Describe the ways in which a hash code can be used to provide message authentication? **07**
- OR**
- Q.4** (a) Explain DSS signing and verifying with example. **07**  
 (b) Explain a Message Authentication Code. What is the difference between a message authentication code and a one-way hash function? **07**
- Q.5** (a) What is poly-alphabetic Cipher? How can it be broken? **07**  
 (b) What is difference between diffusion and confusion? How are they important to make algorithm strong? **07**
- OR**
- Q.5** (a) What do you mean by packet filtering? What are its limitations? **07**  
 (b) Explain the terms (i) Tampering (ii) Phishing **07**

\*\*\*\*\*