

GUJARAT TECHNOLOGICAL UNIVERSITY**ME - SEMESTER– II (Old course)• REMEDIAL EXAMINATION – SUMMER 2015****Subject Code: 1722302****Date:13/05/2015****Subject Name: Advance Cryptography and Information Security****Time: 02:30 pm to 5:00 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) Using the Extended Euclidian algorithm, find the multiplicative inverse of **07**
a. 550 mod 1769
b. 24140 mod 40902
- (b) Write short-notes on: **07**
a. One Time Pad
b. Active and passive attacks
- Q.2** (a) List different ways of classifying IDS. Explain any two of them in detail. **07**
(b) Write two properties of prime numbers that are needed for Miller-Rabin algorithm. Also explain Miller óRabin algorithm. **07**
- OR**
- (b) Encrypt plaintext öGTU UNIVERSITYö with key öMONARCHYö using PlayFair cipher. Comment on the security of the PlayFair cipher. **07**
- Q.3** (a) Compare digital signature with paper signature. Also mention properties of digital signature. **07**
(b) Explain snort architecture with its components with a neat and clean diagram. **07**
- OR**
- Q.3** (a) Explain Activate and Dynamic snort rules with an example. **07**
(b) a. Explain depth and distance keywords in snort rule option. **04**
b. Write a snort rule to log TCP traffic from privileged ports less than or equal to 1024 going to ports greater than or equal to 500. **03**
- Q.4** (a) Explain Substitute bytes, Mix Columns and Add round key in AES. **07**
(b) Write RSA algorithm and explain encryption with a suitable example. **07**
- OR**
- Q.4** (a) Explain Psuedorandom number generators and Blum Blum Shub generator. **07**
(b) Explain addition and multiplication in GF (28) and find $57 + 83$ and $57 * 83$ in GF(28). **07**
- Q.5** (a) How to verify that whether a machine is connected to SMTP service or not? Explain how to spoof e-mail. Is it server level or client level threat? List other threats in this category. **07**
(b) Explain Diffie-Hellman key exchange mechanism with a suitable example. **07**
- OR**
- Q.5** (a) Write the properties that are needed for a hash function. Show how hash function can be used to achieve message authentication. **07**
(b) Draw single round of DES algorithm and explain in detail. How Avalanche effect is achieved in DES? **07**
