

GUJARAT TECHNOLOGICAL UNIVERSITY
ME Semester –II Examination Dec. - 2011

Subject code: 1722302

Date: 12/12/2011

Subject Name: Advance cryptography and Information Security

Time: 02.30 pm – 05.00 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 in detail passive attacks and active attacks. **07**
 (b) (i) Explain cross-site scripting attacks with example. **04**
 (ii) Write the tricks and techniques that spammers use. **03**

- Q.2** (a) Write the three categories into which Intrusion detection system can be classified? Explain in detail. **07**
 (b) (i) Why is it that an ICMP packet does not have source and destination port numbers? How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? **04**
 (ii) Write the phases of IP assignment with DHCP(Dynamic host configuration protocol). **03**

OR

- (b) (i) What is the difference between following commands? **04**
 nslookup www.mit.edu
 nslookup -type=NS mit.edu
 nslookup www.aiit.or.kr bitsy.mit.edu
 (ii) Explain with example snort rule header and the rule options. **03**

- Q.3** (a) (i) How security of playfair cipher is improved over monoalphabetic cipher? Encrypt the text “Earth moon” with the key “playfair”. **04**
 (ii) Discuss the security of vignere cipher. **03**
 (b) (i) Explain Feistel cipher decryption. **04**
 (ii) What is the role of substitution boxes S in DES(Data Encryption standard)? **03**

OR

- Q.3** (a) (i) Define group and field. **04**
 (ii) Write the Euclidean algorithm to find greatest common divisor(a,b). **03**
 (b) (i) Explain the byte substitution in AES(Advanced Encryption standard). **04**
 (ii) Is AES(Advanced Encryption Standard) decryption identical to encryption? **03**

- Q.4** (a) Explain Psuedorandom number generators, linear congruential generator and blum blum shub generator. **07**

- (b) Explain **07**
 (i) Euler's totient function
 (ii) Fermat's theorem
- OR**
- Q.4** (a) Explain Rabin Miller algorithm.Explain probabilistic consideration of **07**
 this algorithm.
- Q.4** (b) Write the possible approaches to attack RSA. **07**
- Q.5** (a) (i) Write MAC(Message Authentication code) property. **04**
 (ii) How can we use block ciphers as Hash functions? **03**
- (b) Write the digital signature property and write digital signature **07**
 algorithm.
- OR**
- Q.5** (a) (i) Explain dual homed host, screened host. **04**
 (ii) Explain screened subnet. **03**
- (b) Explain the anomaly and pattern base intrusion detection system. **07**
