III B.Tech II Semester Examination – May 2017

**CRYPTOGRAPHY AND NETWORK SECURITY**

**(ECM)**

Time: **3** hours Max. Marks: **60**

# SECTION – A

(Short Answer Questions)

**Answer all ten questions 10×1M=10M**

1. An asymmetric-key cipher uses \_\_\_\_\_\_\_\_\_\_ keys
2. In Message Confidentiality, transmitted message must make sense to only intended

(i) Receiver (ii) Sender (iii) Third Party (iv) Translator.

1. Date Encryption Standard (DES) is a type \_\_\_\_\_\_\_\_\_\_\_\_ cipher.
2. Triple DES
   1. is a symmetric key encryption method
   2. guarantees excellent security
   3. a public key encryption method with three keys
   4. is implementable as a hardware VLSI chip
3. Which of the following are used to generate a message digest by the network security protocols?
4. RSA b) SHA -1 c) DES d) MD5
   1. a and c only
   2. b and c only
   3. b and d only
   4. c and d only
5. A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

(i) Sender encrypts using receiver’s public key

(ii) Sender encrypts using his own public key

(iii) Receiver decrypts using sender’s public key

(iv) Receiver decrypts using his own public key

7. \_\_\_\_\_\_\_\_\_ uniquely identifies the MIME entities uniquely with reference to multiple contexts.

1. Content description
2. Content –id
3. Content type

(iv) Content transfer encoding

* + - 1. Pretty good privacy (PGP) is used in
  1. browser security
  2. email security
  3. FTP security
  4. none of the mentioned

9. SET provides an authentication with the help of \_\_\_\_\_\_\_\_\_\_\_\_.

* 1. dual signature.
  2. digital certificate.
  3. payment’s public key.
  4. payment’s private key.

10. Which type of virus uses computer to reproduce itself?

1. Trojan horse
2. Worm
3. Melissa Virus
4. Logic bomb

**SECTION – B**

**Answer all five questions 5×2M= 10M**

1. How to achieve data integrity during transmission?
2. What is the purpose of the S- boxes in DES?
3. What is meet – in – the middle attack?
4. List out the different ways of key distribution between two parties.
5. Compare weak collision resistance and strong collision resistance.

**SECTION – C**

**Answer all four questions 4×5M = 20M**

1. List the different types of security attacks and explain in detail.

**(OR)**

1. Define One - Time Pad and Convert the plaintext “Hello World” into cipher text using Caesar Cipher substitution technique.
2. Define stegenography and explain the types of stegenography techniques.

**(OR)**

1. How rotor machines used for encryption?
2. Illustrate Feistel encryption and decryption.

**(OR)**

1. What is the need for AES? Write about features of AES and its evaluation criteria.
2. Perform encryption and decryption using the RSA algorithm, for the following,
   1. p = 3; q = 11; e = 7 and M = 5
   2. p = 5; q = 11; e = 3 and M = 9

**(OR)**

1. Explain how the MACs are affected by Birthday attacks?

**SECTION – D**

**Answer all two questions 2×10M= 20M**

1. What are the requirements for Kerberos? Explain Kerberos Version 4 with Kerberos realms in detail.

**(OR)**

1. Explain IP security architecture and IP security protocols in detail.
2. Elaborate the operations of SET and Compare SSL with SET.

**(OR)**

1. Describe about the characteristics and types of firewall.