IV B.Tech I Semester Examinations – November 2016

**CRYPTOGRAPHY AND NETWORK SECURITY**

Time: **3** hours (CSE/IT) Max. Marks: **60**

# SECTION – A

(Short Answer Questions)

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

1. Substitutional cipers are

a) Monoalphabatic b) Sami alphabetic c) polyalphabetic d) both a and c

1. Which one of the following algorithm is not used in asymmetric-key cryptography?

a) RSA algorithm

b) diffie-hellman algorithm

c) Electronic code book algorithm

d) none of the mentioned

1. Heart of Data Encryption Standard (DES), is the

a) Cipher b) Rounds c) Encryption d) DES function

1. Advanced Encryption Standard (AES), has three different configurations with respect to the number of rounds and

a) Data Size b) Round Size c) Key Size d) Encryption Size

1. The most commonly used MAC algorithm based on a block cipher make use of
2. Cipher block- chaining
3. Block cipher chaining
4. Both a & c
5. None of the above
6. Digital signature schemes which require the message as the input to the verification algorithm are called
7. digital signature schemes with randomized
8. digital signature schemes with appendix
9. digital signature schemes with deterministic d) All the above

7. Which one of the following is not a type of active attack?

a) Modification b) Masquerade c) Traffic analysis d) Replay

1. PGP encrypts data by using a block cipher called

a) international data encryption algorithm c) intrenet data encryption algorithm

b) private data encryption algorithm d) none of the mentioned

1. Which of the following is / are the types of firewall?
2. Packet Filtering Firewall c) Screen Host Firewall
3. Dual Homed Gateway Firewall d) All of the above
4. Which of the following is / are the types of viruses

a) Parasitic Virus b) Stealth Virus c) Boot sector Virus d) All of these

**SECTION – B**

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

1. List the types of Substitution Techniques.
2. Give four different stages of AES encryption and decryption
3. 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?
4. How is an X.509 certificate revoked?
5. Explain the common type of viruses based on their concealing techniques.

**SECTION – C**

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

1. What metrics are useful for profile-based intrusion detection?

**(OR)**

1. List and briefly define four techniques used to avoid guessable passwords.
2. The IPSec architecture document states that when two transport mode SA's are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption? Justify.

**(OR)**

1. How does PGP work and how it use the concept of trust?
2. Explain the different ways to overcome the re-blocking problem in RSA algorithm.

**(OR)**

1. Explain RSA algorithm with an example
2. What is the difference between a message authentication code and a one-way hash function? In what ways can a hash value be secured so as to provide message authentication?

**(OR)**

1. What characteristics are needed in a secure hash function? Also discuss the role of a compression function in a hash function?

**SECTION – D**

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

1. Explain six block cipher modes of operation of AES as standard (either approved or under consideration).

**(OR)**

1. Why do some block cipher modes of operation only use encryption while others use both

encryption and decryption? Also describe important design considerations for a stream

cipher.

1. Decipher the message MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B using Hill cipher with the inverse key. Show your calculations and the result.

**(OR)**

1. Using the following Playfair matrix



1. Encrypt this message: Must see you over Cadogan West. Coming at once.
2. How do you account for the results of this problem? Can you generalize your

conclusion?