IV B.Tech II Semester Examination – April\May 2018

**CRYPTOGRAPHY AND NETWORK SECURITY**

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

# SECTION – A

(Short Answer Questions)

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

1. Peer entity authentication can be provided by using \_\_\_\_\_authenticate exchange\_\_\_\_\_\_\_\_\_\_\_\_\_\_ mechanism**.**
2. The length of the key in one-time pad is
3. less than the length of the message
4. greater than the length of the message
5. Equal to the length of the message
6. DES can be used to encrypt \_\_\_\_\_\_\_\_\_\_\_\_\_\_ bits of message at a time with a key size of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ bits.
7. The number of ciphertext blocks that needs to be sent using *Cipher-Block Chaining Mode* for encrypting *n* message blocks is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
8. The security of RSA cryptosystem relies on computationally hard \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ problem.
9. Digital signature can be used to provide
10. Data integrity b) Authentication c) Non-repudiation d) All of the above
11. Which of the following are not optional in X.509 certificate format?
12. Name of the user b) Public key of the user

c) Signature of the CA d) Name of the CA

1. The Authentication Only Exchange is used to perform \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ without a key  
   exchange.
2. \_\_\_\_\_\_\_\_\_\_\_\_\_ssl\_\_\_\_\_\_provides security services between TCP and applications that use TCP.
3. \_\_\_\_\_\_\_\_ip spoofing\_\_\_\_\_\_\_\_\_\_\_\_uses forged IP addresses to fool a host into accepting bogus data.

**SECTION – B**

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

1. What is SSL protocol stack, explain.
2. Explain Handshake protocol action.
3. What is need of authentication header?
4. Explain PGP? and it’s working principles
5. Always as a cryptographer my aim is to design a cipher with perfect secrecy. It seems, I cannot have block cipher with perfect secrecy. Why?

**SECTION – C**

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

1. Describe the security architecture for OSI model.

**(OR)**

1. Explain any one substitution encryption techniques with example.
2. Based on the adversarial capabilities, there are several attacks that a designed cryptosystem  
   should withstand. Brief the possible adversarial attacks that are to be taken care of while  
   designing a cryptosystem.

**(OR)**

1. In a transposition cipher the two parts have the key 213, i.e, the message is written in 3 columns with last row stopped with X for completion. Find the ciphertext for the message “MEET ME AT KIM IN BELGIUM”.
2. For encrypting a message to the user or verifying the signature of the user requires authentic public key. There is a need to manage the public key and need of public key infrastructure. With respect to public key infrastructure, explain certificates, the tasks of certificate authority, creation, storing, usage and revocation of certificates.

**(OR)**

1. Kerberos is designed to authenticate clients who try to get access to servers in a network. Elaborate Kerberos protocol that provides both entity authentication and key establishment, by use of symmetric cryptography and a trusted third party.
2. Write a short notes on a) Traffic confidentiality b) Intrusion detection

**(OR)**

1. Write a short notes on a) Viruses and threats b) Firewalls

**SECTION – D**

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

1. a) Why “modes of operations” are important to encrypt the messages using block ciphers?

b) How *Electronic Code-Book Mode* is used to encrypt large messages? Does ECB mode reveal any information about the message encrypted? Suppose there is a transmission bit error in block *ci*, how many blocks of the message are affected during decryption?

c) How *Cipher-Block Chaining Mode* is used to encrypt large messages? Does CBC mode has advantages over ECB mode? Suppose there is a transmission bit error in block *ci*, how many blocks of the message are affected during decryption and precisely which are those blocks? **(5)**

**(OR)**

1. Discuss the various strengths of DES. Briefly explain the ways of cryptanalysis of DES.
2. Diffie-Hellman key exchange protocol enables Alice and Bob to exchange a secret key over an insecure channel. Explain the protocol. Is man in the middle attack possible in the protocol? The security of Diffie-Hellman key exchange is based on which assumption? Show that an adversary can obtain the secret key if he/she able to solve the hard problem on which the security of the protocol depends. Suppose, if primitive root is 2 and prime is 11. And, if user A has public key 9, and user B has public key 3, what is the shared key?

**(OR)**

1. a) Suppose there are three users *u*1*, u*2 and *u*3 using RSA cryptosystem. The public keys  
   of *u*1*, u*2 and *u*3 are (*n*1*, e*1 = 3), (*n*2*, e*2 = 3) and (*n*3*, e*3 = 3) respectively (the modulus  
   *ni, i* = 1*,* 2*,* 3 are more likely pair wise relatively prime). Suppose user A sends the same message *m* to all three users by encrypting with their corresponding public keys. Can an adversary mount an attack to get the plaintext? Justify.

b) Is the basic RSA cryptosystem secure against chosen-cipher text attack? Justify.