*Total No. of Questions : 8]* *[Total No. of Printed Pages : 3*

**Roll No** .....

# MCSE-302(C)

## M.E./M.Tech., III Semester

Examination, December 2020

## Network Security

**(Elective-II)**

***Time : Three Hours***

***Maximum Marks : 70***

***Note:*** i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Define digital signature. List the security services provided by the digital signature.

   b) Distinguish between passive and active security attacks with suitable example.

2. a) What are the key features of Windows security architecture? How it differs from Linus security architecture.

   b) Explain Diffie Hellman key exchange protocol. List and discuss security attacks possible against the Diffie Hellman key exchange protocol.

3. a) Define affine cipher (encryption, decryption and key domain). Assume that attacker intercept the following ciphertext (by chosen-plaintext attack):
   PWUFFOGWCHFDWIWEJORSMDWRHVCMWJUPVCCG
   Attacker also very briefly obtains access to sender's computer and has only enough time to type a two-letter plaintext: "et". She then tries to encrypt the short plaintext using two algorithms, because she is not sure which one is the affine cipher:

Algorithm 1 : Plaintext: et Ciphertext: WC

Algorithm 2 : Plaintext: et Ciphertext: WF

Find out the key of affine cipher using given data.

b) Design a secure two-message authentication protocol that provides mutual authentication and establishes a session key K. Assume that Alice and Bob know each other's public keys beforehand. Does your protocol protect the anonymity of Alice and Bob from a passive attacker (i.e., an attacker who can only observe messages sent between Alice and Bob)? If not, modify your protocol so that it does provide anonymity.

4. a) SSL and IPSec are both designed to provide security over the network.
   i) What are the primary advantages of SSL over IPSec?
   ii) What are the significant differences between the two protocols?

   b) Explain why mode of operation are needed if modern block cipher are to be used for encipherment. List five modes of operation and discuss ECB mode of operation.

5. a) Define RSA cryptosystem. How does we perform factorization and chosen-plaintext attack on RSA?

   b) What is cryptographic hash function? Define cryptographic hash function criteria (preimage resistance, second preimage resistance and collision resistance).

6. a) Define pigeonhole principle and birthday problem. Assume that message in a hash function are 6 bits long and the digest are only 4 bits long. Find out how many messages are corresponding to one message digest.

   b) Define cookies, spyware, virus, logic bomb, worms, ransomware and rootkit.

7. a) Does a MAC work as an HMAC? That is, does a MAC satisfy the same properties that an HMAC satisfies?
   b) Discuss X.509 Certificates in detail. What is the role X.509 Certificates in cryptography?

8. a) Suppose that you have a message consisting of 1024 bits. Design a method that will extend a key that is 64 bits long into a string of 1024 bits, so that the resulting 1024 bits can be XORed with the message, just like a one-time pad. Is the resulting cipher as secure as a one-time pad? Is it possible for any such cipher to be as secure as a one-time pad?
   b) What is Electronic mail security? Provide the application of pretty good privacy (PGP) in transaction Authentication.

******