Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Tech(ECE)/SEM-3/MCE-301A/2009-10

2009

SECURED COMMUNICATION

Time Allotted : 3 Hours | Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer question no. 1 any *four* from the rest.

1. Select the correct answers with proper justifications : $7 \times 2 = 14$

   i) Application of RSA includes

      a) Encryption / Decryption

      b) Digital Signature

      c) Key Exchange

      d) All of these.

   ii) Which one of the following is not an active attack ?

      a) Traffic analysis b) Masquerade

      c) Reply attacks d) DOS.

iii) Which one of the following encryption techniques does not use Fiestel structure ?

a) DES b) AES

c) Blowfish d) RC5.

iv) HMAC adds ..... executions of the basic hash function.

a) 3 b) 1

c) 2 d) 4.

v) For Hash functions, the property to find x for any given value of h such that $H(x) = h$, is referred to as

a) weak collision resistance

b) one-way property

c) strong collision resistance

d) none of these.

vi) MD 5 ..... SHA.

a) is faster than

b) is slower than

c) has same speed as.

vii) If two commnunicating parties use both AH and ESP, each of them requires which of the following numbers of SA ?

a) 1 b) 2

c) 3 d) 4.

2. a) What is the difference between security attack and security threat ?

   b) What are the different types of security services ?

   c) Draw a model for network security and explain its principle of operation. 2 + 3 + 9

3. a) What are the principal elements of public – key crypto system ?

   b) Explain RSA algorithm.

   c) In an RSA system, you intercept the ciphertext $C = 11$ sent to user whose public key $Pu = 7$, $N = 187$. What is the plaintext ? 3 + 5 + 6

4. a) What is the importance of studying Feistel structure ?

   b) Explain the Feistel encryption and decryption processes.

   c) Draw the details of single round function of DES algorithm. 3 + 6 + 5

5. a) What is SHA ? Explain the general principle of all SHAs.

   b) What are the basic properties of SHA ?

   c) What is the difference between MAC and one-way hash function ? 8 + 4 + 2

6. a) Briefly explain Diffie-Hellman key exchange technique.

   b) How does Man-in-the-middle attack proceed for this technique ?

   c) What are the drawbacks of HMAC ? What is the solution to these problems ? 5 + 4 + 5

7. a) What are the two modes of operation in IPSec protocols ? Explain them.

   b) What are the two main protocols of IP Security ? Why are these protocols required ?

   c) How does AH deal with reply attacks ? 4 + 5 + 5

8. Write short notes on any *two* of the following : 2 × 7

   a) MD5 algorithm

   b) Elliptic curve cryptography

   c) SSL architecture

   d) AES

   e) DSA.