Name :	
Roll No. :	Annual (V Kanadala Jud Explored
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 ?

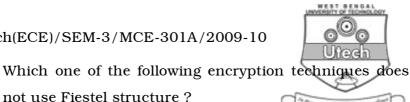
- a) Traffic analysis b) Masquerade
- c) Reply attacks d) DOS.

920568

[Turn over

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

iii)



- not use Fiestel structure? e orio
 - DES AES a) b)
 - Blowfish RC5. c) d)
- HMAC adds executions of the basic hash iv) function.

a)	3	b)	1
c)	2	d)	4.

- For Hash functions, the property to find x for any given V) value of *h* such that H(x) = h, is referred to as
 - weak collision resistance a)
 - b) one-way property
 - strong collision resistance c)
 - none of these. d)
- vi) MD 5 SHA.
 - is faster than a)
 - b) is slower than
 - has same speed as. c)
- vii) If two communicating parties use both AH and ESP, each of them requires which of the following numbers of SA?
 - a) 1 b) 2
 - 3 4. c) d)

920568

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

2.

a)

- 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

920568 3 [Turn over



- 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
- 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.

920568