Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.TECH (CSE)/SEM-3/MCSE-302F/2011-12

2011
NETWORK SECURITY

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 any *Five* Question.

1. What is cryptanalysis ? Explain different types of cryptanalysis with examples. What are the differences between security mechanism and security services ? Explain different types of theoretical and practical attacks.

   1 + 4 + 2 + 7

2. What is multiplicative inverse ? Find the multiplicative inverse of 8 in Z_{10}. Critically comment how algebraic structures are useful in cryptography. What is Galois field ?

   1 + 4 + 7 + 2

3. What are the differences between symmetric-key and asymmetric-key cryptography ? Explain different types of symmetric-key with examples. Explain different attacks on block cipher. 2 + 7 + 5

4. Explain RSA algorithm with proof. What different attacks are possible in RSA cryptosystem ? Explain Diffie-Hellman shared key exchange algorithm. What is man in middle attack ?

4 + 6 + 3 + 1

5. Explain DES algorithm. What are the drawbacks of DES algorithm ? What is Double DES ? What is meet in middle attack ? Briefly explain AES algorithm. 6 + 1 + 2 + 1 + 4

6. What is authentication ? How can authentication be implemented in security system ? What is message digest ? What are the differences between MD5 and SHA-1 ? What is HMAC ? 1 + 5 + 1 + 5 + 2

7. Explain different features of IPsec and SSL. What is SHTTP ? Write short note on PGP. 10 + 1 + 3