No. of Printed Pages : **2**

Sl. No.

B5.3-R4 : NETWORK MANAGEMENT AND INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time : 3 Hours **Total Marks : 100**

1. Differentiate between :

(a) Plain text and cipher text

(b) Key size and key range

(c) Symmetric and asymmetric key cryptography

(d) Risk assessment and risk analysis

(e) Vulnerability and exploit

(f) Authentication and authorization

(g) RC4 and RC5 algorithm. **[7x4]**

2. For given values of p = 7, q = 11, e = 17 and m = 8 :

(a) Perform encryption using the RSA algorithm

(b) Perform decryption using the RSA algorithm **[9+9]**

3. Anita and Bobby work in a security firm. Suppose, Anita is using RSA with modulus n and public exponent e. One day they are hacked, and their private key d becomes known to the attackers. Bobby, the security consultant, suggests that instead of regenerating the new keys completely from the scratch, only the new exponents e', d' need to be re-computed, leaving the modulus n unchanged. For the above situation answer the following :

(a) Is this safe ? If yes, explain why ?

(b) If not, show how the pirates can compromise the new system ? **[8+10]**

4. (a) Why we cannot use a hash function to do encryption ?

(b) What is the main purpose of certificates used in network security ? Should we use a certificate for the key of AES ? Why ?

(c) Is SSL different from HTTPS ? How ? **[6+6+6]**

5. (a) Distinguish between modus operandi of viruses and worms.

(b) Discuss any three attacks that cannot be handled by Firewalls ?

(c) What kind of attacks is handled by captchas ? What common problem occurs with captchas ? **[6+6+6]**

6. Alice and Bob write encrypted messages to each other using a combination of Caesar and Rail Fence cipher. Specifically, each message is first encrypted using Caesar cipher with the key value K, and then such obtained ciphertext is further encrypted using Rail Fence cipher with M rails. You've managed to seize one of their messages, as shown below. The only thing that you know about this message is that it contains exactly one 3-letter word 'the'. The other words are either longer or shorter than 'the'.

zlfxwhbhzo_rth_k_qp_oquhh

For the given problem answer following :

(a) Decrypt the given message.

(b) Determine the value of K and M that Alice and Bob are using. **[12+6]**

7. Write short notes on following :

(a) ARP cache poisoning

(b) DNS spoofing

(c) IPSec **[6+6+6]**

- o 0 o -