2.7

(2 ½ Hours) [Total Marks: 75]

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 Attempt ANY FOUR from the following: **(20M)**

(a) Differentiate between substitution technique and transposition technique in encryption.
(b) Briefly define categories of security mechanism.
(c) State and explain steps involved in RSA Algorithm.
(d) Using a simple columnar transposition cipher, encrypt the given plaintext message. Plaintext: NETWORKSECURITY, Key: LEMON
(e) What are the components of simple symmetric cipher model? Explain with suitable diagram.
(f) Describe the Feistel Structure of encryption & decryption.

Q. 2 Attempt ANY FOUR from the following: **(20M)**

(a) Define message authentication. What are the requirements of message authentication?
(b) Describe X.509 certificate format with suitable diagram.
(c) What is the purpose of the Secure Hash Algorithm (SHA) in cryptographic applications? Explain how variants of SHA differ from one another?
(d) Explain the two approaches of Digital Signature.
(e) Write a note on Kerberos.
(f) Alice and Bob want to securely communicate using the Diffie-Hellman Key Exchange method. Given the following parameters : Prime number p = 5, Generator g = 3, Alice's private key = 3, Bob's private key = 2
Calculate Alice's public key, Bob's public key. And also compute the shared secret key using the public keys.

Q. 3 Attempt ANY FOUR from the following: **(20M)**

(a) How does Pretty Good Privacy(PGP) encryption work?
(b) Describe Secure Electronic Transaction(SET).
(c) Write a short note on Secure/Multipurpose Internet Mail Extensions (S/MIME).
(d) Explain IP security architecture.
(e) Define virus. State and explain any four types of viruses.
(f) What is Intrusion Detection System(IDS)? State and explain different types of IDS.

Q. 4 Attempt ANY FIVE from the following: **(15M)**

(a) Explain any two active attacks with suitable illusration.
(b) State design objectives of HMAC.
(c) What is packet filtering firewall?
(d) How does Electronic Code Book (ECB) encryption mode operate?
(e) Explain three charcteristics of hash function.
(f) Define the role of honeypots.

****