

(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 All**

- (A) \_\_\_\_\_ takes place when one entity pretends to be a different entity. (10M)
- (1) i) Replay ii) Masquerade iii) Denial of service iv) Traffic analysis
- (2) \_\_\_\_\_ is not a security service.  
i) Authentication ii) Digital Signature iii) Data Confidentiality iv) Non Repudiation
- (3) In \_\_\_\_\_ cipher, a single cipher alphabet is used per message.  
i) Poly alphabetic ii) Mono alphabetic iii) Playfair cipher iv) Hill cipher
- (4) DES follows \_\_\_\_\_.  
i) Hash Algorithm ii) Caesar Cipher iii) Feistel Structure iv) Networks
- (5) One commonly used public-key cryptography method is the \_\_\_\_\_ algorithm.  
i) RSS ii) RSA iii) RAA iv) RAS
- (6) A \_\_\_\_\_ attack does not depend on the specific algorithm but depends only on bit length.  
i) MIM ii) brute-force iii) worm iv) ransom
- (7) \_\_\_\_\_ the value of ipad in the HMAC structure.  
i) 111110 ii) 110010 iii) 10110110 iv) 1110110
- (8) IPsec is designed to provide security at the \_\_\_\_\_.  
i) Transport layer ii) Network layer iii) Application layer iv) Session layer
- (9) \_\_\_\_\_ is a person who attempts to gain unauthorized access to a network.  
i) Intruder ii) Hacker iii) Developer iv) Tester
- (10) Packet filtering firewalls are deployed on \_\_\_\_\_.  
i) routers ii) switches iii) hubs iv) repeaters
- (B) Fill in the blanks (5M)
- (Ticket, Digital Signature, MAC, DES, PGP, IP packet)
- (a) \_\_\_\_\_ is an authentication algorithm.
- (b) For a client-server authentication, the client requests from the KDC a \_\_\_\_\_ for access to a specific asset.
- (c) \_\_\_\_\_ is a mathematical technique used to produce authenticity of digital documents.
- (d) In tunnel mode, IPsec protects the \_\_\_\_\_.
- (e) \_\_\_\_\_ was invented by Phil Zimmerman.

**Q. 2 Attempt the following (Any THREE)**

- (a) What is OSI? Explain the following terms in OSI security architecture: (15M)  
i) Security Attack ii) Security Mechanism iii) Security Service
- (b) Explain Active Attacks.
- (c) Write a short note on Caesar Cipher.
- (d) Explain DES with a Diagram.
- (e) Discuss Cipher Block Chaining Mode.

- (f) Show encoding & decoding of the message – 'ATTACK FROM EAST SIDE TOMORROW' with depth=2 using Rail Fence Cipher. (15M)
- Q. 3 Attempt the following (Any THREE)**
- (a) Illustrate Diffie-Hellman Key Exchange Algorithm.
  - (b) How Message Digest Generation is done Using SHA-512?
  - (c) Explain HMAC structure.
  - (d) Write down the steps of Digital Signature Algorithm (DSA).
  - (e) Give Overview of Kerberos.
  - (f) Describe the format of X.509 Certificate. (15)
- Q. 4 Attempt the following (Any THREE)**
- (a) Explain PGP Cryptographic Functions in context of Confidentiality and authentication.
  - (b) What is MIME? What are the five header fields defined in MIME?
  - (c) Give Benefits of IPSec.
  - (d) Explain SSL protocol stack.
  - (e) Write a short note on Intruders.
  - (f) Explain Backdoors. (15)
- Q. 5 Attempt the following (Any FIVE)**
- (a) Explain Steganography.
  - (b) Briefly explain AES Encryption Process.
  - (c) Discuss PKIX Architectural Model.
  - (d) What is Realm?
  - (e) Discuss the scope and limitations of Firewall.
  - (f) Write a short note on Worms.
  - (g) Explain Playfair Cipher.
  - (h) Give general Format PGP Message (from A to B). (15)
- .....