

Answer any FIVE Questions
All Questions carry equal marks

- - -

1. What makes a secure encryption algorithm? Explain.

2. (a) Write notes on timing channels.
(b) Define buffer overflows attacks. Give an example. What are its security implications?

3. (a) With a neat sketch explain how public-key cryptosystem offers secrecy and authentication.
(b) "Message encryption by itself can provide a measure of authentication". Justify.

4. (a) What are the requirements of digital signatures?
(b) Mention the problems associated with direct digital signatures. How are they handled using arbitrated digital signatures?

5. (a) What are MIME transfer encodings?
(b) Write the different cryptographic algorithms used in S/MIME.

6. (a) Mention the three functional areas of IP-level security.
(b) Discuss in detail the basic combinations of security associations.

7. (a) List the sequence of events that are required for a secure electronic transaction.
(b) Explain the concept of dual signature.

8. (a) Explain in detail intrusion detection.
(b) Explain in detail trusted systems.