# Review Questions

1. Define the following terms:

1. Confidentiality
2. Integrity
3. Availability

2. For each of the five attack examples mentioned below, indicate which security aspect (confidentiality, integrity, availability) this attack targets. **Explain your answer**:

1. User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.
2. A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to computer E, which accepts the message as coming from manager D and updates its authorization file accordingly.
3. Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to computer E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.
4. An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee’s account. When the invalidation is accomplished, the server is to post a notice to the employee’s file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee’s action may go unnoticed for some considerable time.
5. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

3. Explain how the lack of network security can facilitate electronic crimes. Provide real life examples.

4. What is the difference between a block cipher and a stream cipher? What type of application for which each of them is more suitable?

5. How can cryptanalyst obtain pairs of plaintext-cipher text pairs (known plaintext)? Give an example.

# Problems

1. What is the minimum key size (in bits) that will make brute force attack infeasible for a computer that can perform 180 decryptions per microsecond? Assume feasible time is 10 days.

2. Using the Vigenère cipher, encrypt the word "*departmental*" using the key *computer*.

3. The following ciphertext was generated using Transposition Matrix applied **twice**.

RJVCEIBOOAMRMNORSSHELEYOESKU

The key used is 3751624. Find the original message, which is an English statement.