Q1.

Encrypt the following plaintext into ciphertext using the Vigenère Cipher where the key is the keyword ***strawberry***. While encoding, you need to show the working of Vigenère cipher for the first 3 letters.

Plaintext: heart holds boundless wisdom

NOTE: Do not encrypt the spaces and keep them in the ciphertext as they are in the given plaintext.

Q2.

Compare and contrast between active attacks and passive attacks on networked systems with respect to their effectiveness and impact on cyber security. Provide three examples for each attack category.

Q3.

Decipher the following encrypted text which is known to have been encoded using the Caesar cipher with a key value of +7. While deciphering, you need to show the working of Caesar cipher for the first 3 letters.

Ciphertext: SPML PZ YLHSSF ZPTWSL

NOTE: Keep the spaces in the plaintext as they are in the given ciphertext.

Q4.

Discuss the difference in the working principles of computer viruses, worms, and trojans.

Q5.

Consider the following scenario: David works in an organization where he needs to communicate frequently with Mathew, one of his colleagues working from a different site of the organization through the Internet, which is considered an inherently insecure communication channel.

Demonstrate a secure scheme that David and Mathew can use so that David can be assured that messages indeed come from Mathew without any modification.

NOTE: Demonstrate the scheme with the help of figure(s)/diagram(s).