



Subject: Information Security Lab (ICT 3141)

Date: 01-09-2025

Semester & Branch: 5th Sem, CCE A1 – Program Check

Name:

Reg. No:

Roll No:

Question:

Implement the following scenario in python showcasing various cryptographic techniques:

- Use the Vigenère cipher with the keyword "POTATO" to encipher the message "The key is hidden under the mattress", and then decrypt it back to verify correctness. Display both the ciphertext and the recovered plaintext along with the key used for the process.
- Generate RSA key pairs for an encoder and a decoder. Create a random AES-128 session key, and share this AES key securely from the encoder to decoder. Show the key pairs generated along with encrypted and decrypted values..
- Encrypt the message "Information Security Lab Evaluation One" using AES-128 with the key "0123456789ABCDEFGHIJKLMN012345", and decrypt it to verify correctness. Read the message from the user.
- Compare the encryption times of these techniques and plot the graph.

Show the output for all steps above.