Subject: Information Security Lab (ICT 3141) **Date: 02-09-2025**

Semester & Branch: 5th Sem, CCE B2 – Program Check

Name: **Reg. No:** **Roll No:**

Question:

Implement the following scenario as a menu driven python program showcasing various cryptographic techniques:

- Use the **Hill cipher** with the key matrix `[[3, 3], [2, 5]]` to encipher the message *"The key is hidden under the mattress"*, and then decrypt it to verify correctness. Display the key matrix, the ciphertext, and the recovered plaintext. Ensure that padding is handled for messages not fitting the block size.
- Generate RSA key pairs for an encoder and a decoder. Share the AES key: "0123456789ABCDEFGHIJKLMNOP012345", securely from the encoder to decoder. Show the key pairs generated along with encrypted and decrypted values.
- Encrypt the message using AES-128 with the key, and decrypt it to verify correctness. Read the message from the user and the message to be read is "Information Security Lab Evaluation One".
- Compare the encryption times of these techniques and plot the graph.

Show the output for all steps above.