

LAB ASSIGNMENT I

Course Instructor: Dr. Dibyendu Roy

Due: Feb 11, 2022, 11:59 pm

Instructions: Code must be written in C and well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. The file name of the code will be YOUR ROLL NO.c

---

Implement the encryption as well as the decryption of the following cipher. The encryption works as follows:

1. Consider a word (without any space) as a plaintext. (Input)
2. Adjust the length of the plaintext and handle the repetition of letter (if present) according to the rule of the Playfair cipher. If there is any  $J$  in the word convert it to  $I$ . Let the final word be  $\Delta$ .
3. Print the word  $\Delta$ . (Output)
4. Consider a word as input and convert  $J$  (if any) to  $I$  and consider that converted word as the key  $K_1$ . (Input)
5. Generate the  $5 \times 5$  key matrix of the Playfair cipher from  $K_1$  and print it. (Output)
6. Encrypt  $\Delta$  using the Playfair cipher where the key is  $K_1$ . Let the ciphertext be  $C_1$ . Print the ciphertext  $C_1$ . (Output)
7. Encrypt  $C_1$  using the CAESAR cipher where the key is  $K_2 = 3$ . Let the ciphertext be  $C_2$ . Print the ciphertext  $C_2$ . (Output)
8. Encrypt  $C_2$  using the Affine cipher where the key is  $K_3 = (7, 5) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ . Let the ciphertext be  $C_3$ . Print the ciphertext  $C_3$ . (Output)

Now you have to think on the decryption to write the code for the decryption. If the code is correct then the decrypted text after doing the Playfair cipher decryption should match with  $\Delta$ . You have to print all the middle layered decrypted texts in the code.