CS-304: Introduction to Cryptography and Network Security Laboratory

LAB Assignment I

Course Instructor: Dr. Dibyendu Roy Due: Feb 11, 2024, 11:59 pm

Instructions: Code must be written in C language and it must be well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. The file name of your code will be YOUR ROLL-NO.c. Write your roll number and name on the top of your code.

Implement the encryption as well as the decryption of the following cipher. Here you need to consider the followings:

1. Plaintext space $\mathcal{P} = \{$all alphabets A to Z along with , . ? ; $\}$. Note that $|\mathcal{P}| = 30$.
2. Key space $\mathcal{K} = \{$all alphabets A to Z along with , . ? ; $\}$. Note that $|\mathcal{K}| = 30$.
3. Ciphertext space $\mathcal{C} = \mathcal{P}$.

The encryption works as follows:

1. Consider a word (without any space) as a plaintext, where every element of the plaintext is from $\mathcal{P}$. (Input)
2. Adjust the length of the plaintext and handle the repetition of letter (if present) according to the rule of the Playfair cipher. Here I, J are not considered as same. Let the final word be Δ.
3. Print the word Δ. (Output)
4. Consider a word (without any space) as input and that word is the first key K_1, where every element of K_1 is from $\mathcal{K}$. (Input)
5. Generate the 6×5 key matrix similar to the Playfair cipher from K_1 and print it. (Output)
6. Encrypt Δ using the rule of 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 Affine cipher where the key is $K_2 = (11, 15) \in \mathbb{Z}_{30} \times \mathbb{Z}_{30}$. Let the ciphertext be C_2. Print the ciphertext C_2. (Output)
8. Encrypt C_2 using the Shift cipher where the key is K_3 $(0 \leq K_3 \leq 29)$. Let the ciphertext be C_3. Print the ciphertext C_3. (Output)
9. Now you have to think on the decryption to write the code for the decryption print the decrypted text (say Δ_1). If the code is correct then the decrypted text Δ_1 after doing the Playfair cipher decryption should match with Δ. You have to print all the middle layered decrypted texts in the code.