



Information Security (CS3002)

Assignment # 1

Assignment deadline Tuesday, 10th September 2024, 11:00 PM

Read Guidelines carefully

Make a plaintext consists of following information, clearly show it on top of the assignment, and should be unique for each student.

Your Roll No-Your FatherName-Your CNICno

e.g. 18f6776-FirstName SecondName-88739-3797973-9

Encrypt/Decrypt above text using following ciphers:

- **Ceaser Cipher**, Key should be your third number of CNIC
- **Monoalphabetic**, Think of a suitable key yourself.
- **Vigenere Cipher**, Key should be your father name.
- **One Time Pad**, Think of a suitable key yourself.

Write also the problems you find in each cipher while doing its encryption/decryption and what is the possible solution for it?

Guidelines:

- A single violation of guideline will lead to **Zero mark** in your assignment.
- Deadlines should be kept in mind. **No extension** in assignment dates would be given.
- Proper name the file and submit the *assignment* in **Word** file on **Google classroom**.
- You are encouraged to take help from Internet and books.
- You will have maximum marks if you have done the entire task.
- This is an individual assignment. **PLAGARISM IS NOT ACCEPTABLE!**
- Follow the instructions as it is, otherwise, your assignment would not be accepted at all.