**SN627   PRINCIPLES OF CRYPTOGRAPHY**

**Lab assignment 1: Substitution ciphers**

**Note: You are required to write computer programs in a language of your choice to solve each question**

1. Caesar cipher encrypts text by shifting a character 3 places forward in the alphabet. For example, the character ‘a’ becomes ‘d’, ‘b’ becomes ‘e’, ‘z’ becomes ‘c’ and so on. So in order to decrypt, one has to simply shift backwards by an equal amount. For example, the character‘d’ becomes ‘a’, ‘e’ becomes ‘b’, ‘c’ becomes ‘z’ and so on. Implement a variant of Caesar cipher (Additive Cipher) where the user can specify the key of his/her choice.
2. Also implement the decryption procedure and could you help me decrypt the given text (1\_cipher.txt)? (Can use brute force method)
3. Frequency analysis is a technique of using English language alphabet frequencies to decrypt a file. If you have noticed that in almost every text, some alphabets occur more frequently than others and this information could be used to decrypt mono-alphabetic ciphers (a cipher which maps one alphabet to another). Using the frequency analysis method try to decrypt the file (2\_cipher.txt).