Note:

I. In both of the programs, students should implement encryption function as well as Decryption function.
II. In Encryption, plaintext and key are given as inputs. This returns cipher text.
III. In Decryption, cipher text. and key are given as inputs. This returns the text. If the returned text is equals to plaintext, the implementation is correct.
IV. Always assume that Algorithm/Cipher is known to attacker. Only the thing that should be kept secret is the Key for encryption-decryption. Key must be available to sender and receiver.
V. These are symmetric ciphers. So, same key is used for both encryption and Decryption.

Practical 1:

(I) To implement Caesar/Additive Cipher
-->Encrypt
-->Decrypt
-->Do cryptanalysis by applying Brute-Force attack. Here only cipher text is given as input. All keys are tried for Decryption and all possible messages should be printed as output. Here key space is 25, so total 25 messages should be printed.

(II) To implement Playfair Cipher
--> Use MONARCHY and Construct 5*5 Matrix as Key.
--> Encrypt plaintext using the rules given in Text Book.
--> Decrypt in reverse way.

M	**O**	**N**	**A**	**R**
C	**H**	**Y**	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Example: Here "BALLOON" is plaintext.

1. To remove repeating characters in a group, add Filler. "X" is not in the plain text , so it can be used.
BA LL OO N ---> BA LX LO ON

2. For doing Encryption, following steps are followed:
If characters in a pair are in same row, encrypt by taking next character.
E.g. ON will be NA
If characters in a pair are in same column, encrypt by taking next character.
E.g. BA will be IB or JB as decided.
If characters in a pair are not in same row and column, then see their joining points in the row and column.
E.g. LX. Here L is in 4^{th} row and 1^{st} column, while X is in 5^{th} row and 4^{th} column.
(4,1) and (5,4) then make it (4,4) and (5,1) i.e. "SU".
(See the **color combination** and **order of pairs**)
In general if (a,b) , (c,d) then (a,d) ,(c,b) will be the output.

3. For doing Decryption, reverse steps are followed:

If characters in a pair are in same row, decrypt by taking previous character.

E.g. NA will be ON

If characters in a pair are in same column, encrypt by taking previous character.

E.g. IB/JB will be BA.

If characters in a pair are not in same row and column, then see their joining points in the row and column.

E.g. SU. Here S is in 4th row and 4st column, while U is in 5th row and 1st column.

(4,4) and (5,1) then make it (4,1) and (5,4) i.e. “LX”.

(See the **color combination and order of pairs**)

In general if (a,b) , (c,d) then (a,d) ,(c,b) will be the output.