Cryptography & Network Security- Lab2

Implement the following cryptosystems to provide data confidentiality

a) **Affine Cipher**: The Affine Cipher is a Monoalphabetic Substitution cipher wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

- Encryption process for each letter is given by: **$c=ap+b \pmod m$**
- Decryption process for each letter is given by: **$p=a^{-1}(c-b) \pmod m$**

Expected Output:
Enter the values of a & b (Key):
Enter the plaintext:
Encrypted Message is:

b) **Playfair Cipher**: The Playfair cipher encrypts pairs of letters (digraphs), instead of single letters as is the case with simpler substitution ciphers such as the Caesar Cipher. The playfair cipher starts with creating a key table. The key table is a 5×5 grid of letters that will act as the key for encrypting your plaintext.
The Playfair cipher uses a few simple rules relating to where the letters of each digraph are in relation to each other. The rules are:

- If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle

Expected Output:
Key text: Monarchy
Plain text: instruments
Cipher text: gatlmzclrqtx