SEM - VII - 2022-23
CNS Lab
B3 - 2019BTECS00094 - Sweety Shrawan Gupta
Assignment 4
Vigenere Cipher

Vigenere Cipher

- The vigenere cipher is an algorithm of encrypting an alphabetic text that uses a series of interwoven caesar ciphers.
- It is based on a keyword's letters.
- It is an example of a polyalphabetic substitution cipher.
- In vigenere cipher,the encryption and decryption are done by Vigenere algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).

Formula of encryption is,

$$E_i = (P_i + K_i) \bmod 26$$

Formula of decryption is,

$$D_i = (E_i - K_i) \bmod 26$$

If any case (D_i) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Code:

```
#include <bits/stdc++.h>
using namespace std;

int main()
{
    string s, x, k;
    cout << "Enter plain text" << endl;
```

```
getline(cin, s);
for (int i = 0; i < s.length(); i++)
    if (s[i] != ' ')
        x += s[i];
s = x;

cout << "Enter key" << endl;
cin >> k;

cout << "\nPlain text is: " << s << endl;
cout << "key is: " << k << endl;

int j = 0;
for (int i = 0; i < s.length(); i++)
{
    if (s[i] >= 'a' and s[i] <= 'z')
        s[i] = (s[i] - 'a' + k[j] - 'a'  + 26) % 26 + 'a';
    if (s[i] >= 'A' and s[i] <= 'Z')
        s[i] = (s[i] - 'A' + k[j] - 'a'  + 26) % 26 + 'A';

    j++;
    if (j >= k.size())j = 0;
}

cout << "\nCipher text is: " << s;
j = 0 ;
for (int i = 0; i < s.length(); i++)
{
    if (s[i] >= 'a' and s[i] <= 'z')
        s[i] = (s[i] - 'a' - (k[j] - 'a') + 26) % 26 + 'a';
    if (s[i] >= 'A' and s[i] <= 'Z')
        s[i] = (s[i] - 'A' - (k[j] - 'a') + 26) % 26 + 'A';


    j++;
    if (j >= k.size())j = 0;
}

cout << "\n\nPlain text after decryption is: " << s;
```

```
    return 0;
}
```

Output:

inputf.in

```
sweety shrawan gupta
priya
```

outputf.in

```
Enter plain text
Enter key

Plain text is: sweetyshrawangupta
key is: priya

Cipher text is: hnmctnjppalrveueki

Plain text after decription is: sweetyshrawangupta
```