Experiment No. 6

Write A Program To Implements Vernam Cipher

I. Minimum Theoretical Background

Vernam Cipher is a method of encrypting alphabetic text. It is simply a type of substitution cipher. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).

Method to take key:

In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

Encryption Algorithm:

1. Assign a number to each character of the plain-text and the key according to alphabetical order.
2. Add both the number (Corresponding plain-text character number and Key character number).
3. Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

II. Procedure

1.C Program:

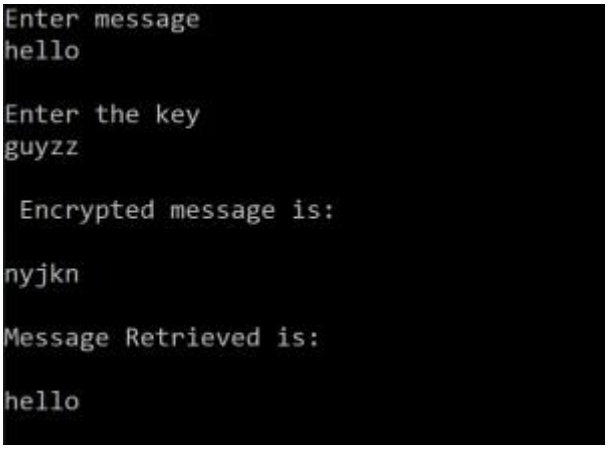
```
#include<stdio.h>
char arr[26][26];
char message[22],key[22],emessage[22],retMessage[22];
int findRow(char);
int findColumn(char);
int findDecRow(char,int);
int main() {
    int i=0,j,k,r,c;
    clrscr();
```

```
k=96;
for (i=0;i<26;i++) {
        k++;
        for (j=0;j<26;j++) {
                arr[i][j]=k++;
                if(k==123)
                   k=97;
        }
}
printf("\nEnter message\n");
gets(message);
printf("\nEnter the key\n");
gets(key);
// Encryption
for (i=0;key[i]!=NULL;i++) {
        c=findRow(key[i]);
        r=findColumn(message[i]);
        emessage[i]=arr[r][c];
}
emessage[i]='\0';
printf("\n Encrypted message is:\n\n");
for (i=0;emessage[i]!=NULL;i++)
printf("%c",emessage[i]);
//decryption
for (i=0;key[i]!=NULL;i++) {
```

```
            c=findColumn(key[i]);
            r=findDecRow(emessage[i],c);
            retMessage[i]=arr[r][0];
    }
    retMessage[i]='\0';
    printf("\n\nMessage Retrieved is:\n\n");
    for (i=0;retMessage[i]!=NULL;i++)
    printf("%c",retMessage[i]);
    getch();
    return(0);
}
int findRow(char c) {
    int i;
    for (i=0;i<26;i++) {
            if(arr[0][i]==c)
              return(i);
    }
}
int findColumn(char c) {
    int i;
    for (i=0;i<26;i++) {
            if(arr[i][0]==c)
              return(i);
    }
}
```

```
int findDecRow(char c,int j) {
    int i;
    for (i=0;i<26;i++) {
            if(arr[i][j]==c)
              return(i);
    }
}
```

2.Output:



III. Conclusion

Hence we have successfully installed and configured antivirus on system.

IV. Exercise

Q.1 What Is Meant By vernam cipher?

Q2. How Can You Use key in Vernam cipher?

Q3. What Are The main use of vernam ciper?

Q4. Write algorithm step of encryption meassage in vernam ciper?

Answers

……..…
……..
……..…
……..…
……..…
……..…
……..…
……..…
……..…
……..…
……..…
……..

Marks obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total(25)**	