Practical no.1

Aim :- To apply the knowledge of symmetric cryptography to implement classical ciphers.

Theory:- Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present. In cryptography there are two processes i.e. encryption and decryption performed at sender and receiver end respectively. Encryption is the processes where a simple multimedia data is combined with some additional data (known as key) and converted into unreadable encoded format known as Cipher. Decryption is the reverse method as that of encryption where the same or different additional data (key) is used to decode the cipher and it is converted in to the real multimedia data.

Caesar Cipher in Cryptography

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text been moved down.
The encryption can be represented using modular arithmetic by first

transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

The formula of encryption is:

$$E_n(x) = (x + k) \bmod 26$$

The formula of decryption is:

$$D_n(x) = (xi - k) \bmod 26$$

Example :- encryption

Key : 3

Plaintext : vartak

Plaintext	**v**	**a**	**r**	**t**	**a**	**k**
Plaintext value	**21**	**0**	**17**	**19**	**0**	**10**
(x + k) mod 26	**24**	**3**	**20**	**22**	**3**	**13**
ciphertext	**Y**	**D**	**U**	**W**	**D**	**N**

Plaintext : vartak

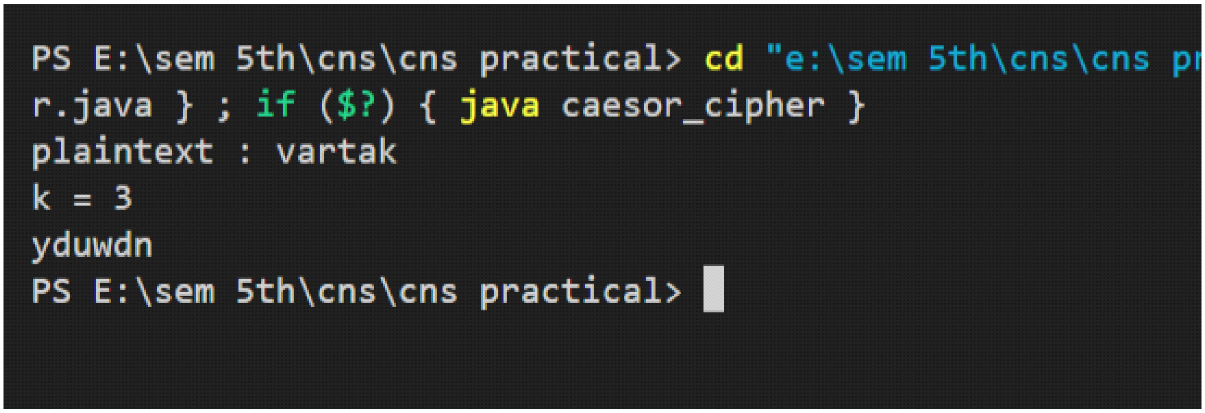
Ciphertext : YDUWDN

Code:-

Java code

```
public class caesor_cipher
{
public static void main(String args[]){
Scanner scn = new Scanner(System.in);
System.out.print("plaintext : ");
String p = scn.nextLine();
System.out.print("k = ");
int k = scn.nextInt();
for(int i =0 ; i < p.length(); i++)
{
char ch = p.charAt(i);
int num = ch + k;
ch = (char)num;
System.out.print(ch);
}
}
}
```

Output:

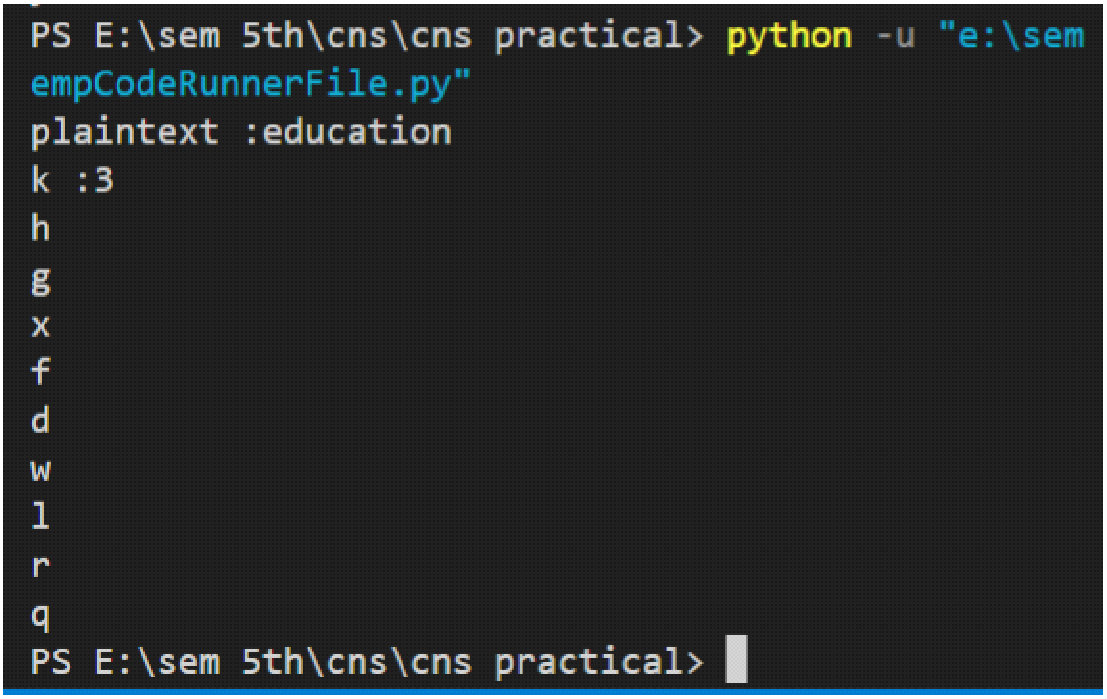


```
PS E:\sem 5th\cns\cns practical> cd "e:\sem 5th\cns\cns pr
r.java } ; if ($?) { java caesor_cipher }
plaintext : vartak
k = 3
yduwdn
PS E:\sem 5th\cns\cns practical>
```

Python code

```
a = str(input("plaintext :"))
k = int(input("k :"))
for i in range(0,len(a)):
    ch = a[i]
    num = ord(ch)
    num += k
    ch =chr(num)
    print(ch)
```

Output:

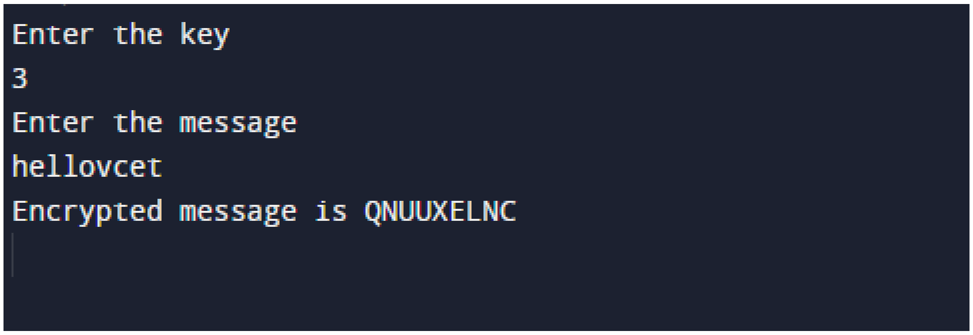


```
PS E:\sem 5th\cns\cns practical> python -u "e:\sem
empCodeRunnerFile.py"
plaintext :education
k :3
h
g
x
f
d
w
l
r
q
PS E:\sem 5th\cns\cns practical> 
```

C++ code :-

```
#include<iostream>
#include<string>
using namespace std;
int main(){
    int i,j,k;
    string s,t;
    int key;
    cout<<"Enter the key\n";
    cin>>key;
    cout<<"Enter the message\n";
    cin>>s;
    for(i=0;i<s.size();i++){
        t+=(s[i]-'A'+key)%26+'A';
    }
    cout<<"\n\nEncrypted message is "<<t<<'\n';
    return 0;
}
```

Output:



```
Enter the key
3
Enter the message
hellovcet
Encrypted message is QNUUXELNC
```

concusion :

The information security can be easily achieved by using Cryptography technic. Caesar cipher algorithm can be implemented in many encryption projects to make data secure and better. Security is one of the important aspects in computing. In data transfer,security must be considered as one of the method implemented to ensure secure data transfer.