

Assignment – 7

Implement the following Modern Block Ciphers techniques.

- 1) Electronic Codebook (ECB) Mode**
- 2) Cipher Block Chaining (CBC) Mode**
- 3) Cipher Feedback (CFB) Mode**
- 4) Output Feedback (OFB) Mode**
- 5) Counter (CTR) Mode**

1. Electronic Codebook (ECB) Mode:

Code:

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

string generateKey(string key, int x)
{
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == x)
            break;
        key.push_back(key[i]);
    }
    return key;
}

string cipherText(string str, string key)
{
    string cipher_text;

    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) % 26;

        x += 'a';

        cipher_text.push_back(x);
    }
    return cipher_text;
}
```

```

int main()
{
    int n;
    cout<<"Enter the value of n(size of each block) : ";
    cin>>n;
    string plain, cipher="";
    cout<<"Enter the plain text : ";
    cin>>plain;
    string key;
    cout<<"Enter the key for vigenere cipher :";
    cin>>key;
    key = generateKey(key,n);
    cout<<"key "<<key<<"\n";
    int blocks;
    if(plain.length()%n!=0)
    {
        int k= (plain.length()/n) * n;
        int g= plain.length()-k;
        g=n-g;

        for(int i=0; i<g; ++i)
            plain.append("z");
    }

    blocks= plain.length()/n;
    for(int i=0;i<blocks; ++i)
    {   string tp= plain.substr(i*n, i*n+n);

        string ci= cipherText(tp,key);
        cipher.append(ci);
    }

    cout<<"The Cipher text is: "<<cipher<<"\n";
}

```

Output:

```

"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\electronicCodebookMode.exe"
Enter the value of n(size of each block) : 3
Enter the plain text : ankit
Enter the key for vigenere cipher :abc
key abc
The Cipher text is: mayugn

Process returned 0 (0x0)   execution time : 23.366 s
Press any key to continue.

```

2. Cipher Block Chaining (CBC) Mode

Code:

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

string xor_operation(string a, string b)
{
    string ans="";
    int n=a.length();
    for(int i=0; i<n; ++i)
    {
        char k= ((a[i]^b[i])%26 )+'a';
        ans+=k;
    }

    return ans;
}

string generateKey(string key, int x)
{
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == x)
            break;
        key.push_back(key[i]);
    }
    return key;
}

string cipherText(string str, string key)
{
    string cipher_text;

    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) % 26;

        x += 'a';

        cipher_text.push_back(x);
    }
}
```

```

    }
    return cipher_text;
}

```

```

int main()
{
    int n;
    cout<<"Enter the value of n(size of each block) : ";
    cin>>n;
    string plain, cipher="";
    cout<<"Enter the plain text : ";
    cin>>plain;
    string key;
    cout<<"Enter the key for vigenere cipher : ";
    cin>>key;
    key = generateKey(key,n);

    int blocks;
    if(plain.length()%n!=0)
    {
        int k= (plain.length()/n) * n;
        int g= plain.length()-k;
        g=n-g;

        for(int i=0; i<g; ++i)
            plain.append("z");
    }

    blocks= plain.length()/n;
    string x;
    for(int i=0;i<blocks; ++i)
    {
        string tp= plain.substr(i*n, i*n+n);
        if(i!=0)
        {
            tp= xor_operation(tp,x);
        }

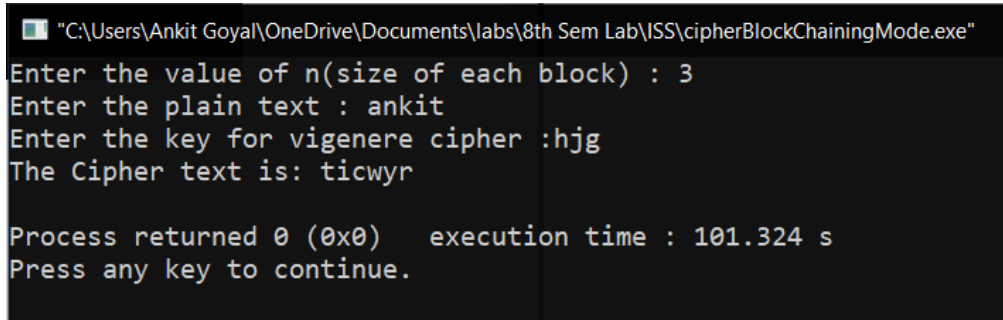
        string ci= cipherText(tp,key);
        x=ci;
        cipher.append(ci);
    }

    cout<<"The Cipher text is: "<<cipher<<"\n";
}

```

```
}
```

Output:



```
"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\cipherBlockChainingMode.exe"
Enter the value of n(size of each block) : 3
Enter the plain text : ankit
Enter the key for vigenere cipher :hjg
The Cipher text is: ticwyr

Process returned 0 (0x0)   execution time : 101.324 s
Press any key to continue.
```

3. Cipher Feedback (CFB) Mode

Code:

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

string xor_operation(string a, string b)
{
    string ans="";
    int n=a.length();
    for(int i=0; i<n; ++i)
    {
        char k= ((a[i]^b[i])%26 )+'a';
        ans+=k;
    }

    return ans;
}

string generateKey(string key, int x)
{
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == x)
            break;
        key.push_back(key[i]);
    }
}
```

```

    }
    return key;
}

string cipherText(string str, string key)
{
    string cipher_text;

    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) % 26;

        x += 'a';

        cipher_text.push_back(x);
    }
    return cipher_text;
}

int main()
{
    int r;
    cout<<"Enter the value of r(size of each block) : ";
    cin>>r;
    string plain, cipher="", S;
    cout<<"Enter the plain text : ";
    cin>>plain;
    string key;
    cout<<"Enter the key for vigenere cipher : ";
    cin>>key;
    cout<<"Enter the initial value of shift register : ";
    cin>>S;
    int n=S.length();
    key = generateKey(key,n);
    cout<<"\nKey : "<<key;

    int blocks;
    if(plain.length()%r!=0)
    {
        int k= (plain.length()/r) * r;
        int g= plain.length()-k;
        g=r-g;

        for(int i=0; i<g; ++i)
            plain.append("z");
    }
}

```

```

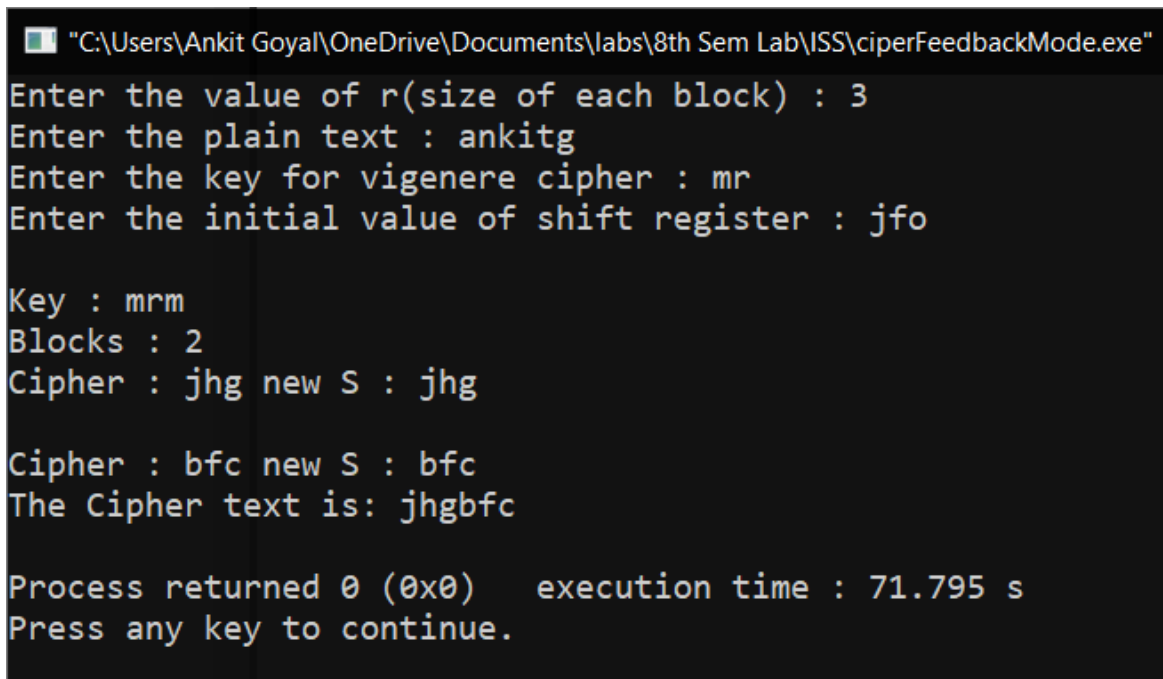
    }

    blocks= plain.length()/r;
    cout<<"\nBlocks : "<<blocks;

    for(int i=0;i<blocks; ++i)
    {
        string cip=cipherText(S,key);
        cip= cip.substr(0,r);
        string tp= plain.substr(i*r, i*r+r);
        tp= xor_operation(tp,cip);
        S=S.substr(r, n);
        S.append(tp);
        cout<<"\nCipher : "<<tp<<" new S : "<<S<<"\n";
        cipher.append(tp);
    }

    cout<<"The Cipher text is: "<<cipher<<"\n";
}

```

Output:


```

"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\cipherFeedbackMode.exe"
Enter the value of r(size of each block) : 3
Enter the plain text : ankitg
Enter the key for vigenere cipher : mr
Enter the initial value of shift register : jfo

Key : mrm
Blocks : 2
Cipher : jhg new S : jhg

Cipher : bfc new S : bfc
The Cipher text is: jhgbfc

Process returned 0 (0x0)   execution time : 71.795 s
Press any key to continue.

```

4. Output Feedback (OFB) Mode

Code:

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

string xor_operation(string a, string b)
{
    string ans="";
    int n=a.length();
    for(int i=0; i<n; ++i)
    {
        char k= ((a[i]^b[i])%26 )+'a';
        ans+=k;
    }

    return ans;
}

string generateKey(string key, int x)
{
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == x)
            break;
        key.push_back(key[i]);
    }
    return key;
}

string cipherText(string str, string key)
{
    string cipher_text;

    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) %26;

        x += 'a';

        cipher_text.push_back(x);
    }
}
```



```

    return cipher_text;
}

int main()
{
    int r;
    cout<<"Enter the value of r(size of each block) : ";
    cin>>r;
    string plain, cipher="", S;
    cout<<"Enter the plain text : ";
    cin>>plain;
    string key;
    cout<<"Enter the key for vigenere cipher : ";
    cin>>key;
    cout<<"Enter the initial value of shift register : ";
    cin>>S;
    int n=S.length();
    key = generateKey(key,n);
    cout<<"\nKey : "<<key;

    int blocks;
    if(plain.length()%r!=0)
    {
        int k= (plain.length()/r) * r;
        int g= plain.length()-k;
        g=r-g;

        for(int i=0; i<g; ++i)
            plain.append("z");
    }

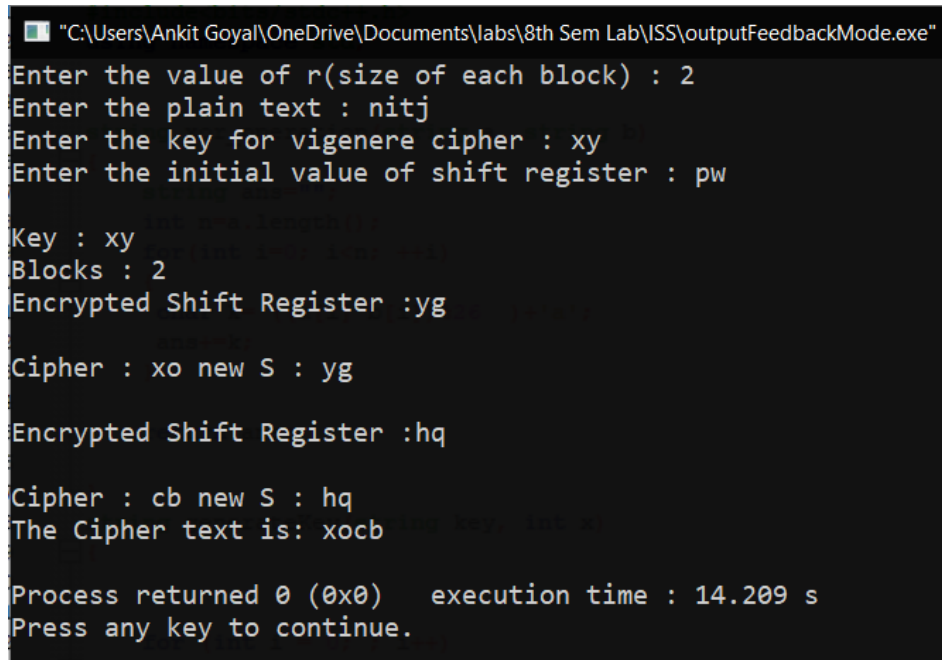
    blocks= plain.length()/r;
    cout<<"\nBlocks : "<<blocks;

    for(int i=0;i<blocks; ++i)
    {
        string cip=cipherText(S,key);
        cout<<"\nEncrypted Shift Register : "<<cip<<"\n";
        cip= cip.substr(0,r);
        string tp= plain.substr(i*r, i*r+r);
        tp= xor_operation(tp,cip);
        S=S.substr(r, n);
        S.append(cip);
        cout<<"\nCipher : "<<tp<<" new S : "<<S<<"\n";
        cipher.append(tp);
    }
}

```

```
    cout<<"The Cipher text is: "<<cipher<<"\n";
}
```

Output:



```
"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\outputFeedbackMode.exe"
Enter the value of r(size of each block) : 2
Enter the plain text : nitj
Enter the key for vigenere cipher : xy
Enter the initial value of shift register : pw

Key : xy
Blocks : 2
Encrypted Shift Register :yg

Cipher : xo new S : yg

Encrypted Shift Register :hq

Cipher : cb new S : hq
The Cipher text is: xocb

Process returned 0 (0x0)   execution time : 14.209 s
Press any key to continue.
```

5. Counter (CTR) Mode

Code:

```
#include<bits/stdc++.h>
using namespace std;
string xor_operation(string a, string b)
{
    string ans="";
    int n=a.length();
    for(int i=0; i<n; ++i)
    {
        char k= ((a[i]^b[i])%26 )+'a';
        ans+=k;
    }
    return ans;
}
string generateKey(string key, int x)
{
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == x)
            break;
    }
}
```

```

        key.push_back(key[i]);
    }
    return key;
}
string cipherText(string str, string key)
{
    string cipher_text;

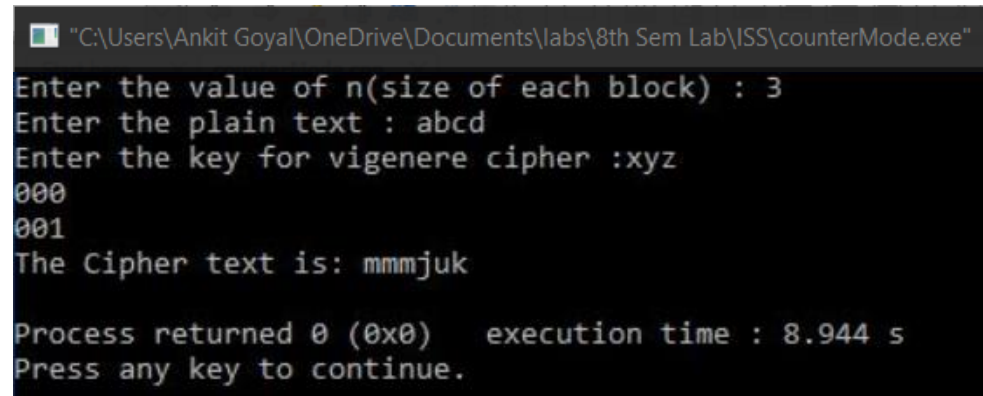
    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) % 26;
        x += 'a';
        cipher_text.push_back(x);
    }
    return cipher_text;
}
int main()
{
    int n;
    cout<<"Enter the value of n(size of each block) : ";
    cin>>n;
    string plain, cipher="";
    cout<<"Enter the plain text : ";
    cin>>plain;
    string key;
    cout<<"Enter the key for vigenere cipher : ";
    cin>>key;
    key = generateKey(key,n);

    int blocks;
    if(plain.length()%n!=0)
    {
        int k= (plain.length()/n) * n;
        int g= plain.length()-k;
        g=n-g;

        for(int i=0; i<g; ++i)
            plain.append("z");
    }
    blocks= plain.length()/n;
    string counter(n,'0');
    int count=0;
    for(int i=0;i<blocks; ++i)
    {
        string x = to_string(count);
        counter = counter.substr(0,n-x.length())+x;
        cout<<counter<<"\n";
        string tp= plain.substr(i*n, i*n+n);
        string ci= cipherText(counter,key);
        tp= xor_operation(tp,ci);
    }
}

```

```
        cipher.append(tp);  
        count++;  
    }  
    cout<<"The Cipher text is: "<<cipher<<"\n";  
}
```

Output:

```
"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\counterMode.exe"  
Enter the value of n(size of each block) : 3  
Enter the plain text : abcd  
Enter the key for vigenere cipher :xyz  
000  
001  
The Cipher text is: mmmjuk  
  
Process returned 0 (0x0)   execution time : 8.944 s  
Press any key to continue.
```