ЛАБОРАТОРНА РОБОТА №6

ТЕМА: СИСТЕМА ШИФРУВАННЯ DES.

МЕТА: РЕАЛІЗУВАТИ ШИФРУВАННЯ DES В ПРИКЛАДНІЙ ПРОГРАМІ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Одним з найбільш розповсюджених алгоритмів блокового шифрування є DES (Data Encryption Standard), розроблений у 1977 році. Цей алгоритм затвердився як перший доступний всім бажаючим офіційний алгоритм. Тому його слід відмітити як найважливішу віху на шляху криптографії від чисто військового використання до широкомасштабного застосування. Незважаючи на присутні йому недоліки, DES і на сьогоднішній день залишається одним з найбільш популярних в комерційній сфері і в системах електронних розрахунків.

На платформі .NET передбачена можливість використання ряду симетричних криптографічних алгоритмів: DES, TripleDES, Rijndael. Реалізуються вони за допомогою об'єктів двох класів з простору імен System.Security.Cryptography:

- *CryptographicServiceProvider class* – клас, що надає криптопровайдери для кожного з вказаних алгоритмів.
- *CryptoStream class* – клас для роботи з криптографічним потоком.

Порядок шифрування за їх допомогою такий:

1. Створюється потрібний крипто провайдер і задаються його ключ і вектор ініціалізації[1] :

```
DESCryptoServiceProvider cryptic = new DESCryptoServiceProvider();

cryptic.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");

cryptic.IV = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");
```

2. Відкривається звичайний файловий потік для запису зашифрованих даних:

```
FileStream stream = new FileStream(@"d:\test.txt", FileMode.OpenOrCreate,FileAccess.Write)
```

3. Відкритий файловий потік трансформується в крипто потік для запису:

```
CryptoStream crStream = new CryptoStream(fs, cryptic.CreateEncryptor(),CryptoStreamMode.Write);
```

4. Дані для шифрування перетворюються у бітову послідовність і всі біти (від 0 до data.Length) записуються в крипто потік за допомогою методу Write ():

```
byte[] data = ASCIIEncoding.ASCII.GetBytes("Hello World!");

crStream.Write(data,0,data.Length);
```

[1] Тут для бітового представлення ключа і вектора ініціалізації використаний клас ASCIIEncoding з простору імен System.Text. Довжина ключа і вектора ініціалізації має точно відповідати вимогам алгоритму. Зокрема для DES вони мають бути 64-бітними, тобто складатися з 8 символів ASCII-кодів.

5. Використані файловий і крипто – потоки закриваються:

crStream.Close();

fs.Close();

Порядок розшифрування полягає у такому:

1. Створюється потрібний крипто провайдер і задаються його ключ і вектор ініціалізації :

DESCryptoServiceProvider cryptic = new DESCryptoServiceProvider();

cryptic.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");

cryptic.IV = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");

2. Відкривається звичайний файловий потік для читання зашифрованих даних:

FileStream stream = new FileStream(@"d:\test.txt", FileMode.Open,FileAccess.Read)

3. Відкритий файловий потік трансформується в крипто потік для читання:

CryptoStream crStream = new CryptoStream(stream,
cryptic.CreateDecryptor(),CryptoStreamMode.Read).

4. Дані з крипто потоку зчитуються за допомогою об'єкта StreamReader і присвоюються текстовій змінній:

StreamReader reader = new StreamReader(crStream);

string data = reader.ReadToEnd();

5. Значення текстової змінної виводиться виводиться на екран і зчитувач та потік закриваються:

Console.WriteLine(data);

reader.Close();

stream.Close();

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Ознайомитись з алгоритмом шифрування DES.

2. Написати програму для шифрування та розшифрування за допомогою алгоритму шифрування DES.

3. Підготувати звіт про виконання роботи. Звіт оформлюється у вигляді документу Word з такою структурою:

   a. титульний лист,

   b. тема і мета роботи,

c. опис алгоритму роботи програми у вигляді блок-схеми або UML- діаграм (класів, діяльності тощо),

d. функціональні можливості програми (основні і додаткові),

e. фрагмент програмного коду, що реалізує базову функціональність,

f. особливості програмної реалізації окремих функцій.

4. Електронну копію звіту відправити за адресою: George@aprodos.kpi.ua.