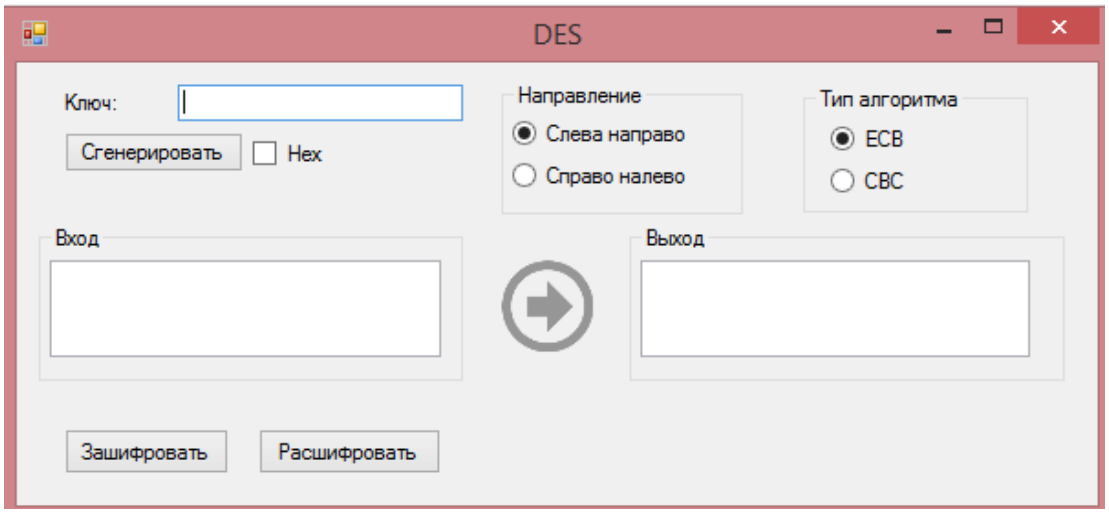
Лабораторная работа 1

Программная реализация шифра DES

Цель работы – создать криптографическую систему шифрования данных, которая базируется на алгоритме шифровании DES. Алгоритм DES является первым симметричным алгоритмом блочного шифрования данных.

Отчёт:

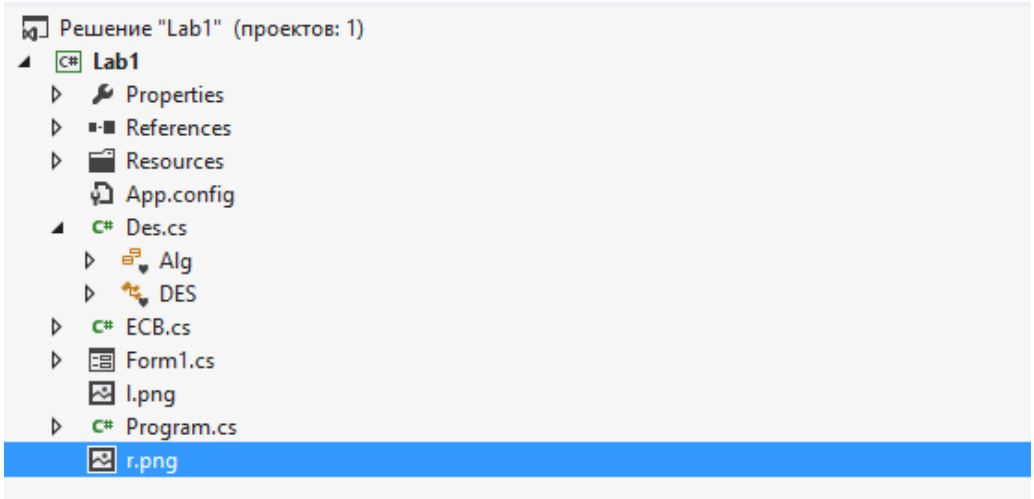
Программная реализация криптографической системы, основанной на алгоритме шифрования DES, оформлена быть оформлена как программная оболочка:



Разработан интерфейс, в котором предусмотрено:

- Два режима формирования ключа
- Режимы шифрования ECB и CBC
- Режим шифрования и режим дешифрования
- Вывод результата на экран

Структура данных:



Алгоритм генерации ключа:

```
BitArray L = new BitArray(28);
BitArray R = new BitArray(28);
bool Ls, Rs;

for (byte i = 0; i < 28; i++)
{
    L[i] = data[i];
    R[i] = data[28 + i];
}

for (byte i = 0; i < n; i++)
{
    for (byte m = 0; m < LSTable[i]; m++)
    {
        Ls = L[0];
        Rs = R[0];
        for (byte j = 0; j < 27; j++)
        {
            L[j] = L[j + 1];
            R[j] = R[j + 1];
        }
        L[27] = Ls;
        R[27] = Rs;
    }
}

for (byte i = 0; i < 28; i++)
{
    data[i] = L[i];
    data[28 + i] = R[i];
}
```