Разработка программного комплекса для поточного шифрования , дешифрования информации .

Выполнил:
студент группы ФРМ 202
Гергерт Р.В.

Руководитель:
начальник лаборатории 31
ОАО «ЦКБА» Володин М.В.

Цель работы:

Разработать программный комплекс для поточного шифрования , дешифрования информации на основе регистра сдвига с перестраиваемой структурой обратных связей.

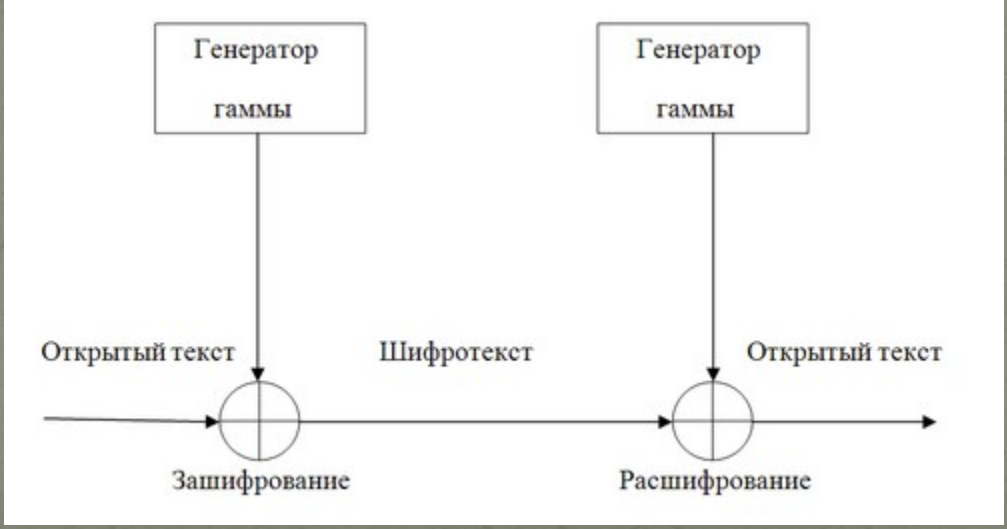
Поточный шифр

Поточный шифр — это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры. При блочном шифровании открытый текст разбивается на блоки равной длины, при этом совпадающие блоки при данном ключе всегда шифруется одинаково, при поточном шифровании это не так.

Режим гаммирования для поточных шифров.

Простейшая реализация поточного шифра изображена на рисунке. Генератор гаммы выдаёт ключевой поток (гамму): $k_1, k_2, k_3 \dots k_i$. Обозначим поток битов открытого текста $m_1, m_2, m_3 \dots m_i$. Тогда поток битов шифротекста получается с помощью применения опе $c_1, c_2, c_3 \dots c_i$ R $c_i = m_i \oplus k_i$ е . . Расшифрование производится операцией XOR между той же самой гаммой и зашифрованным текстом: $m_i = c_i \oplus k_i$ . .

Очевидно, что если последовательность битов гаммы не имеет периода и выбирается случайно, то взломать шифр невозможно. Но у данного режима шифрования есть и отрицательные особенности. Так ключи, сравнимые по длине с передаваемыми сообщениями, трудно использовать на практике. Поэтому обычно применяют ключ меньшей длины (например, 128 бит). С помощью него генерируется псевдослучайная гаммирующая последовательность. Естественно, псевдослучайность гаммы может быть использована при атаке на поточный шифр.

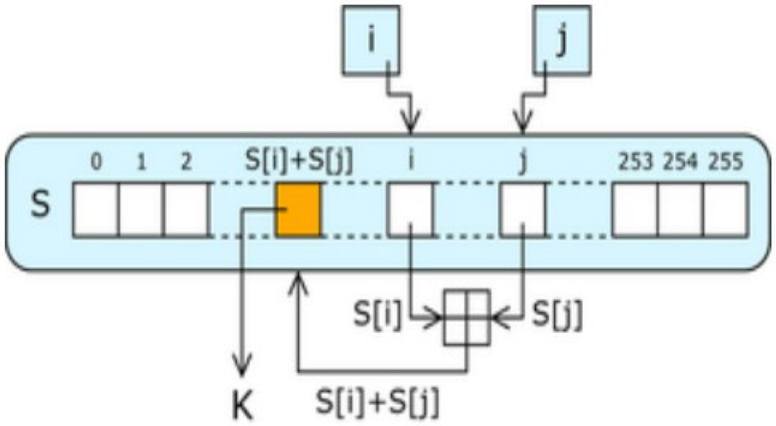


Поточные шифры на регистрах сдвига с линейной обратной связью (РСЛОС)

Несколько причин использования линейных регистров сдвига в криптографии:

- высокое быстродействие криптографических алгоритмов ;
- применение только простейших операций сложения и умножения, аппаратно реализованных практически во всех вычислительных устройствах ;
- хорошие криптографические свойства (генерируемые последовательности имеют большой период и хорошие статистические свойства) ;
- легкость анализа с использованием алгебраических методов за счет линейной структуры .

Схема шифра RC4



Схемы шифратора и дешифратора

Схема шифрования с обычной обратной связью.

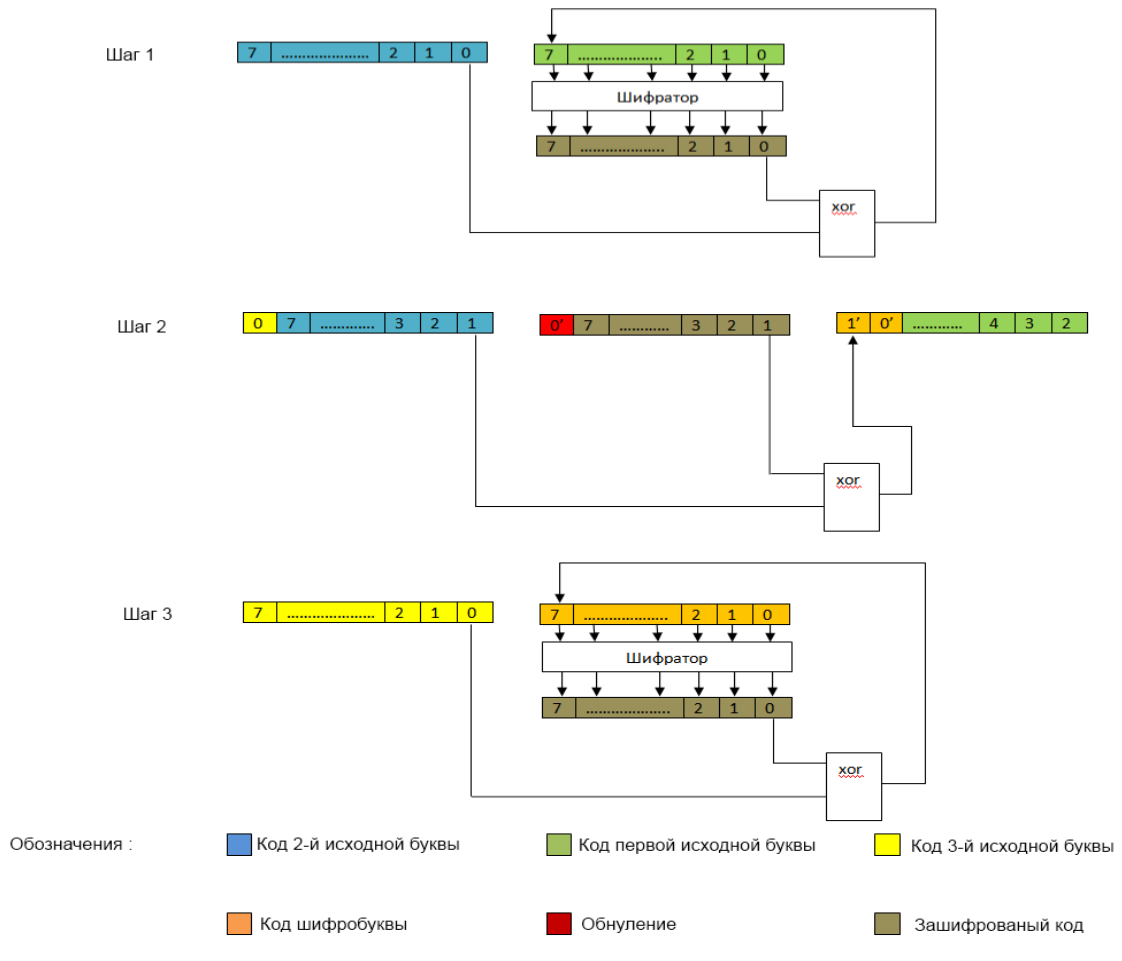


Схема дешифрования с обычной обратной связью.

Схема шифрования с ключом

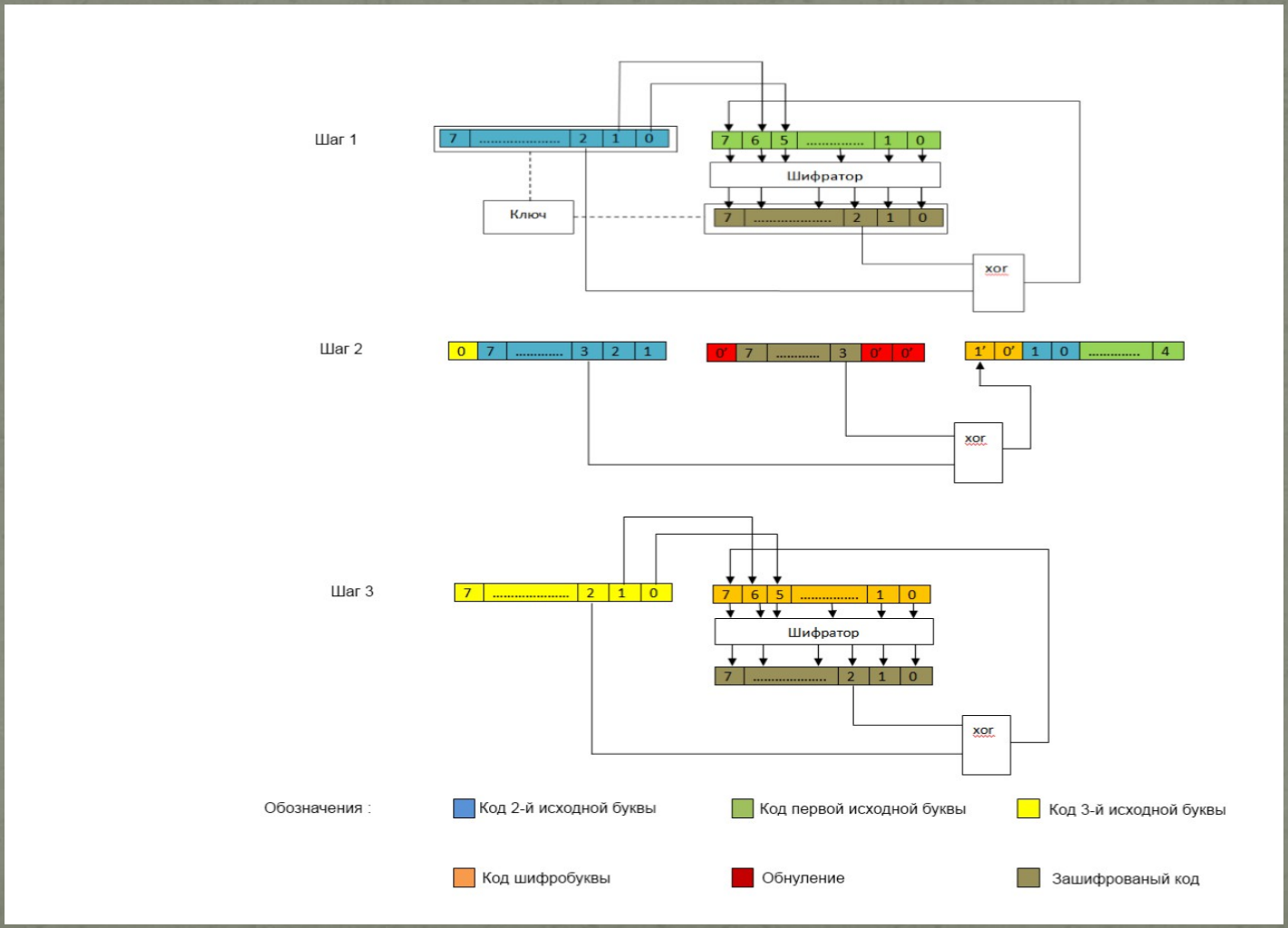
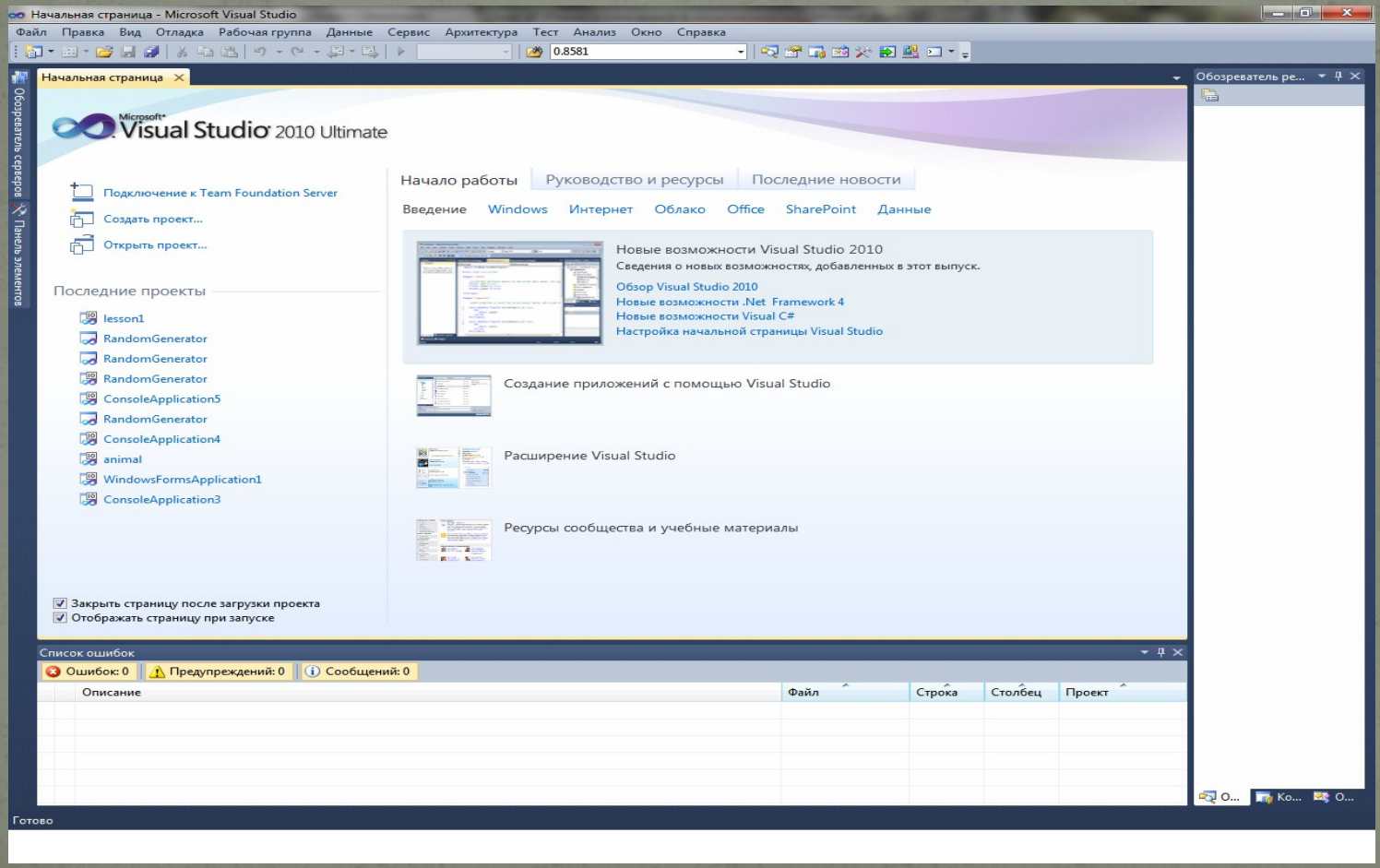


Схема дешифрования с ключом

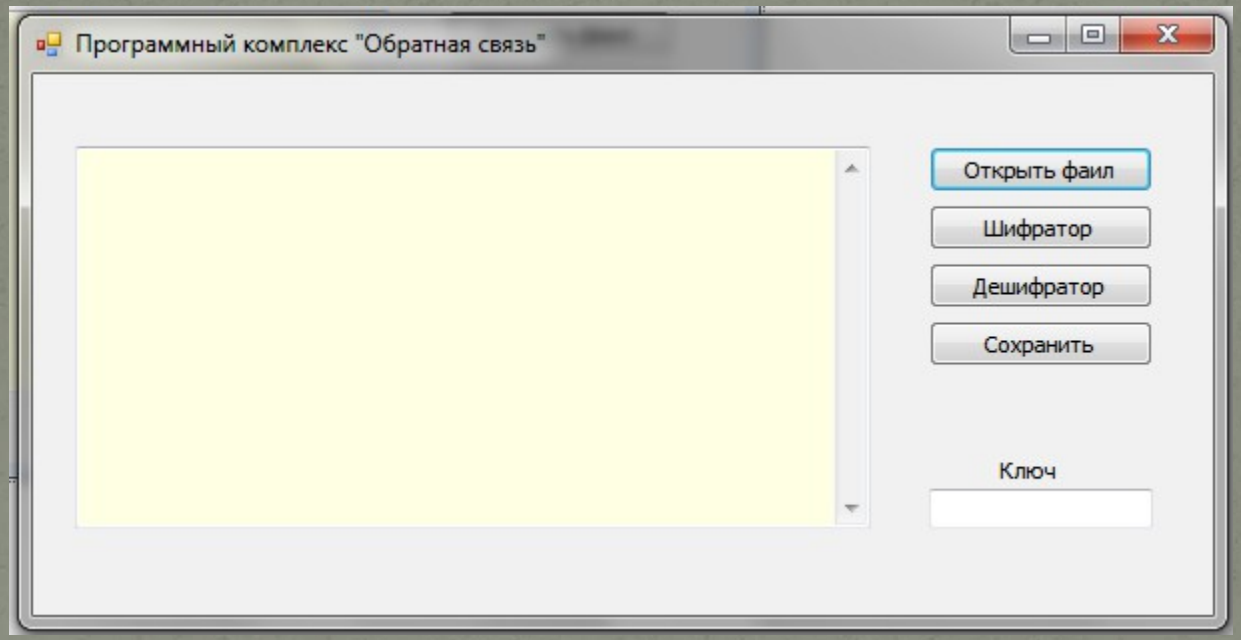
Главные особенности и преимущества шифра:

- Для большей криптостойкости в систему введено динамическое переключение обратной связи на разные разряды и с разным периодом, используя ключ;
- псевдослучайная последовательность формируется из исходного текста;
- псевдослучайная последовательность примерно равна длине исходного текста;
- весь алгоритм шифрования реализован на трех сдвиговых регистрах.

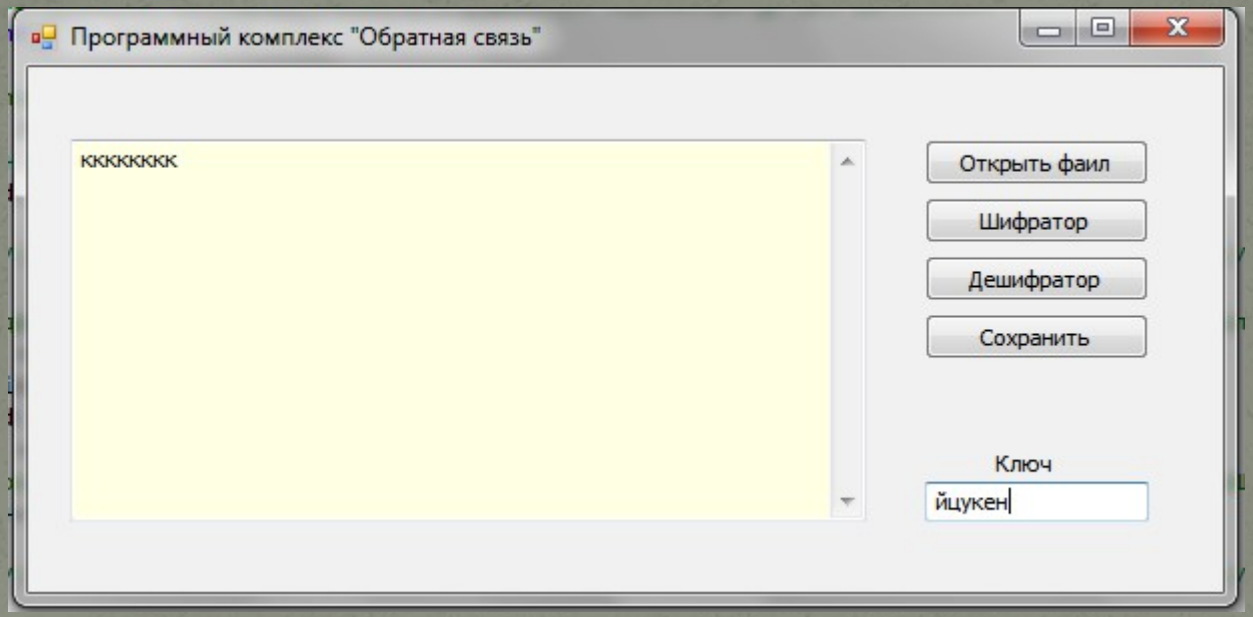
Среда реализации

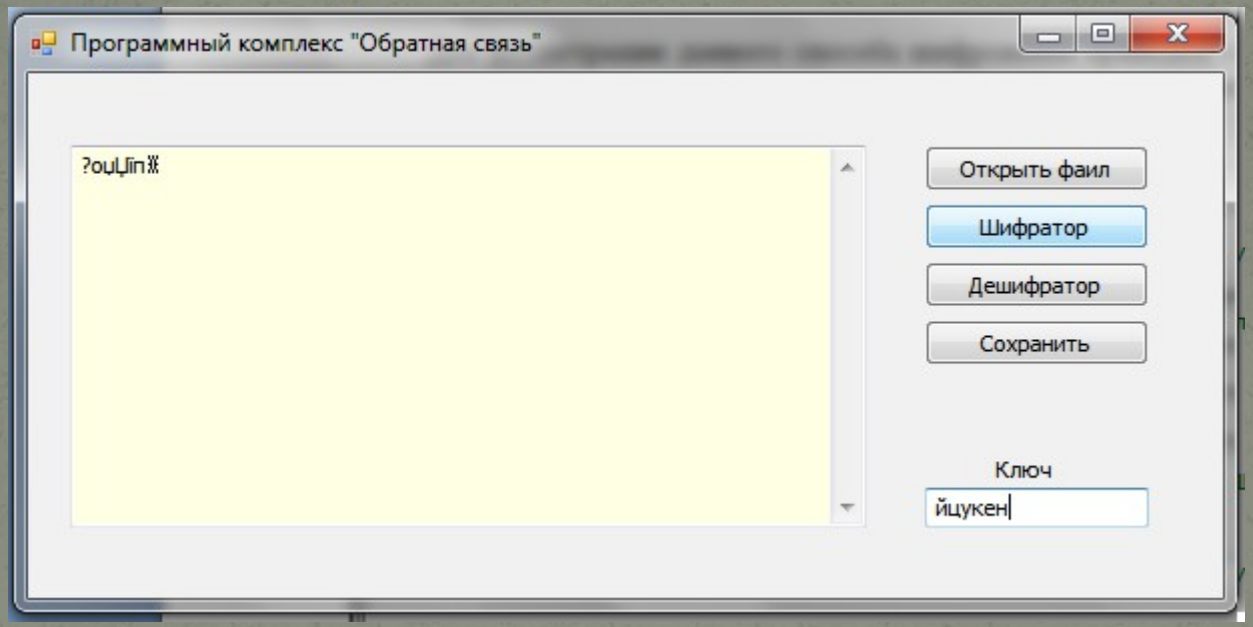


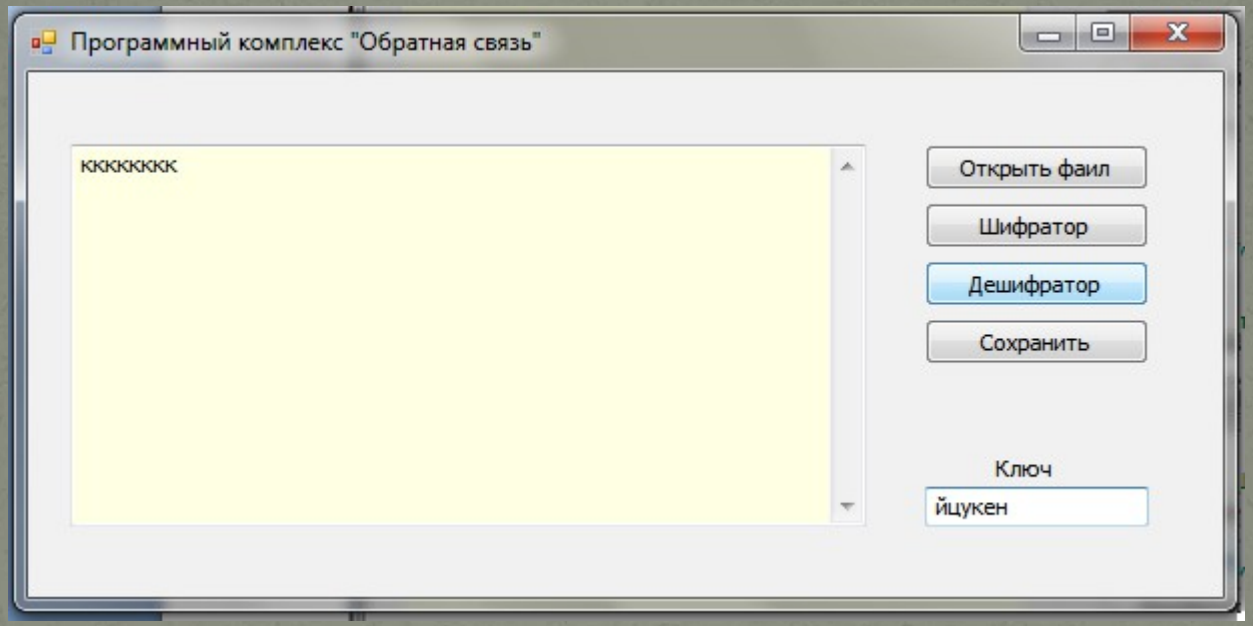
Интерфейс программы



Демонстрация особенностей шифра.




Программный комплекс "Обратная связь"
?ou_Ji
Открыть фаил
Шифратор
Дешифратор
Сохранить
Ключ
йцукен


Программный комплекс "Обратная связь"
кккккккк
Открыть фаил
Шифратор
Дешифратор
Сохранить
Ключ
йцукен

Перспективы развития программного комплекса

Разработанный программный комплекс можно использовать в качестве базы на основе которой можно реализовать алгоритм без ввода ключа , ключ сам будет генерироваться из самого текста (Самоключ Вижинера).

Такое развитие алгоритма резко увеличит криптостойкость системы, но и сложность алгоритма.

Заключение:

- В рамках программного комплекса реализована перестраиваемая структура обратных связей ;
- реализованная перестраиваемая структура обратных связей демонстрирует высокую криптостойкость;
- данный программный комплекс позволяет повысить , защиту информации , тем самым понижая вероятность ее утечки и попадания в руки злоумышленников ;
- весь алгоритм шифрования подробно разобран и детально показан на схемах.