МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №5**

**″Исследование блочных шифров″**

Выполнила:

Студентка 3 курса 2 группы

Бобрик В.С.

Проверила: Копыток Д.В.

Минск 2021

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости блочных шифров.
* Разработать приложение для реализации указанных преподавателем методов блочного зашифрования/расшифрования.
* Выполнить анализ криптостойкости блочных шифров.
* Оценить скорость зашифрования/расшифрования реализованных шифров.
* Оценить скорость зашифрования/расшифрования реализованных способов шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** Блочное зашифрование (расшифрование) предполагает разбиение исходного открытого (зашифрованного) текста на равные блоки, к которым применяется однотипная процедура зашифрования (расшифрования). Указанная однотипность характеризуется, прежде всего, тем, что процедура зашифрования (расшифрования) состоит из совокупности повторяющихся наборов преобразований, называемых раундами.

Основные требования к шифрам рассматриваемого класса можно сформулировать следующим образом:

* даже незначительное изменение исходного сообщения должно приводить к существенному изменению зашифрованного сообщения;
* устойчивость к атакам по выбранному тексту;
* алгоритмы зашифрования/расшифрования должны быть реализуемыми на различных платформах;
* алгоритмы должны базироваться на простых операциях;
* алгоритмы должны быть простыми для написания кода, вероятность появления программных ошибок должна быть низкой;
* алгоритмы должны допускать их модификацию при переходе на иные требования по уровню криптостойкости.

В данной лабораторной работе необходимо было разработать авторское приложение в соответствии с целью лабораторной работы.

Для **варианта №1** в качестве рассматриваемого метода был взят алгоритм DES c ключом, состоящим из первых восьми символов собственных фамилии и имени.

Итак, для того, чтобы зашифровать сообщение алгоритмом DES, необходимо выполнить следующую последовательность шагов:

* довести исходное сообщение до такого размера (в битах), чтобы оно нацело делилось на размер блока;
* разделить исходное сообщение на блоки;
* довести длину ключа до длины половины блока;
* перевести ключ в бинарный формат (в нули и единицы);
* провести над каждым блоком прямое преобразование сетью Фейстеля в течении 16-ти раундов. После каждого раунда необходимо выполнять циклический сдвиг ключа на заданное количество символов;
* соединить все блоки вместе; таким образом получим сообщение, зашифрованное алгоритмом DES.

Расшифровка DES производится по аналогии. Используется обратное преобразование сетью Фейстеля.

Программный код разработанного в данной лабораторной работе программного средства представлен на рисунках. Алгоритм DES реализован без использования каких-либо стандартных библиотек. Рассмотрим его более детально.

На рисунке 1 представлен код функции, выполняющей преобразование исходного текста в его бинарное представление.

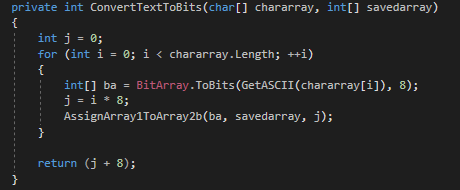


Рис. 1 – Функция преобразования исходного текста в его бинарный вид

На рисунке 2 представлен код функции, выполняющей доведение бинарного представления исходного текста до размера, который делится на размер блока, а именно 64 бит. Это происходит путем добавления в конец текста нулей.

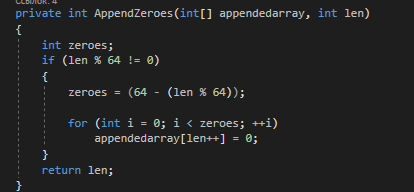


Рис. 2 – Функция доведения размера блока

Функции преобразования в бинарный вид и доведения размера выполняются и для ключа. Далее над ключом выполняется функция, отбрасывающая каждый восьмой бит ключа, чтобы привести ключ к размеру в 56 бит. Код этой функции представлен на рисунке 3.

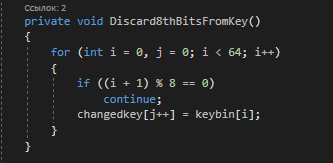


Рис. 3 – Функция, отбрасывающая каждый восьмой бит ключа

Далее в цикле разбиваем текст на блоки длиной в 64 бита и выполняем следующий алгоритм над каждый таким блоком. Функция, выполняющая начальную перестановку представлена на рисунке 4.

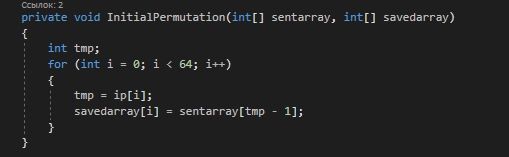


Рис. 4 – Функция начальной перестановки

После начальной перестановки над блоком выполняется функция, которая делит его на левую и правую части, где каждая размером в 32 бита. Код этой функции представлен на рисунке 5.

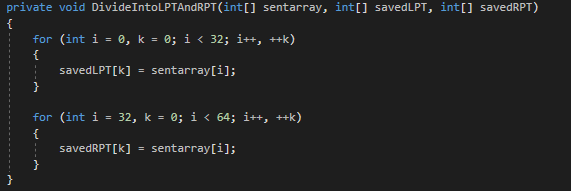


Рис. 5 – Функция, разбивающая блок на левую и правую часть

Далее над ключом выполняется циклический сдвиг.Следующий этап в алгоритме DES подразумевает выполнение одних и тех же действий в 16 раундов. Результат работы алгоритма и замеры времени выполнения операция шифрования и расшифрования слова veronika представлены на рисунке 6.

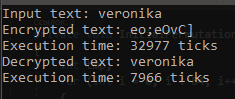


Рис. 6 – Результат работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для выполнения зашифрования и дешифрования текстов с помощью блочного шифра под названием DES. Также был проведен анализ его криптостойкости.