УДК 004.4

Реализация симметричного алгоритма блочного шифрования «Rijndael» для больших данных информации

В.Ю. Соболева, Муниципальное бюджетное общеобразовательное учреждение «Лицей «Технический» имени С.П. Королева» городского округа Самара, г. Самара
Научный руководитель – к.ф.-м.н., М.А. Вержаковская, Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университете телекоммуникаций и информатики», г. Самара

В 1997 г. Национальный институт стандартов и технологий США (NIST) объявил о проведении конкурса по замене стандарта DES. Алгоритм — победитель этого конкурса должен был стать новым стандартом блочного симметричного шифрования США.

В конкурсе, которому было присвоено название AES (Advanced Encryption Standard), приняли участие 15 алгоритмов. Основными требованиями, предъявляемыми к шифрам-претендентам, были практическая стойкость и эффективность реализации.

Анализ алгоритмов-претендентов проводился как специалистами института NIST, так и различными независимыми экспертами. В результате победителем конкурса AES был выбран алгоритм Rijndael, который по большинству критериев оказался лучше остальных алгоритмов-финалистов.

Целью данной работы является реализация симметричного алгоритма блочного шифрования «Rijndael» на языках программирования C\C++ в среде разработки MicrosoftVisualStudio 2019. Алгоритм Rijndael позволяет шифровать данные блоками длиной 128, 192 и 256 бит, которые представляются в виде двумерных байтовых массивов размером 4x4, 4x6, 4x8. Все операции производятся над отдельными байтами массива, а также над независимыми столбцами и строками.

Для достижения поставленной цели были сформулированы задачи.

1. Провести теоретический обзор по вопросам темы проекта.
2. Провести проектирование программной системы реализации симметричного алгоритма блочного шифрования «Rijndael».
3. Обосновать выбор программных средств для разработки программной системы.
4. Описать разработку программной системы реализации симметричного алгоритма блочного шифрования «Rijndael».
5. Описать функциональные возможности программной системы реализации симметричного алгоритма блочного шифрования «Rijndael».

Основным функциональным назначением программного средства является шифрование и дешифрование данных (файлов) с использованием ключа длинной 16/24/32 байт. С возможностью передачи файла в программу тремя способами:

1) Drag-n-drop (перетаскивание файла) на интерфейс программы.
2) Через интерфейс программы (использование кнопок).
3) Вызов из командной строки (возможно просто перетащить файл на исполняемый файл программы).

Для создания интерфейса на C++ используем WinApi. Windows API спроектирован для использования в языке Си для написания прикладных программ, предназначенных для работы под управлением операционной системы MS Windows. Работа через Windows API – это наиболее близкий к операционной системе способ взаимодействия с ней из прикладных программ.

Входными данными является файл (т.е путь к файлу), который может быть передан несколькими путями. После определения зашифрованный этот файл или нет, вызываются соответственные функции шифрования или дешифрования. После чего на выходе мы получаем зашифрованный либо расшифрованный файл. К зашифрованным файлам добавляем «.crypto», а к дешифрованным «decrypto_».