СИСТЕМА ШИФРОВАНИЯ ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Янкелевич А. М.

Егоров В. В. – старший преподаватель

Целью работы является разработка системы шифрования данных. В информационную систему входят: аппаратная часть, которой является ПК под управлением ОС Windows 8, 7, Vista, XP и криптографическое приложение. Целью разработки информационной системы шифрования данных является предоставление пользователю зашифровку и дешифровку конфиденциальных документов различный типов: .doc, .txt, .jpg.

Рис. 1 – Структура информационной системы

Для работы система использует автоматически генерируемый ключ с использованием смешивающих хэш-функций и специальный алгоритм шифрования. В работе используются хэш-функции трех видов: SHA1, RIPEMD160 и WHIRELPOOL. SHA1 разбивает исходное сообщение на блоки по 512 бит в каждом. Последний блок дополняется до длины, кратной 512 бит. Сначала добавляется 1, а потом нули, чтобы длина блока стала равной 512 - 64 = 448 бит. В оставшиеся 64 бита записывается длина исходного сообщения в битах. Если последний блок имеет длину более 448, но менее 512 бит, то дополнение выполняется следующим образом: сначала добавляется 1, затем нули вплоть до конца 512-битного блока; после этого создается ещё один 512-битный блок, который заполняется вплоть до 448 бит нулями, после чего в оставшиеся 64 бита записывается длина исходного сообщения в битах. Дополнение последнего блока осуществляется всегда, даже если сообщение уже имеет нужную длину. Оставшиеся виды хэш-функций работают аналогично с минимальными отличиями.

В работе используются два алгоритма шифрования: Blowfish и DESX. Blowfish – криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа. Алгоритм DESX использует метод отбеливания ключа с целью усиления устойчивости к атакам на основе полного перебора. Данные алгоритмы были выбраны за свою быстроту выполнения операций и криптостойкость.

Система разработана с удобный для пользователя графическим интерфейсом и обладает дополнительными возможностями, например, отправка зашифрованного файла по email, очистка следов пользователя, открытие командной строки, сжатие документов в zip-архив.

Таким образом, в ходе работы создана криптографическая система для шифрования данных, разработанная в среде программирования Microsoft Visual Studio на языке C#.

Список использованных источников:

1. Петцольд. Программирование Для Microsoft Windows На C#. В 2-х Томах. Том 1: Пер. с англ. – Москва: Русская редакция, 2002. — 624 с.
2. Б. Шнайдер. Прикладная криптография: Пер. с англ. - Москва: Русская редакция, 2007- - 460 стр.
3. С. Панасенко. Алгоритмы шифрования 2010. — 176 с.