УДК 512.624.95

МАТЕМАТИКА КРИПТОГРАФИИ. КРИПТОГРАФИЧЕСКИЙ ИНСТРУМЕНТ STEGACRYPT

Жуковский Д.М.
Научный руководитель – Федосик Е.А., к.ф.-м.н., доцент

Одной из важнейших областей применений математики является криптография – наука о шифрах, т. е. способах преобразования информации, позволяющих скрывать её содержание от посторонних. Государство, не имеющее возможности защищать дипломатическую, военную и иную секретную переписку, неизбежно проиграет в борьбе с конкурентами.

С развитием электронных коммуникаций криптография стала предметом интереса более широкого круга потребителей: возникла необходимость защиты технических, коммерческих, персональных и других данных, передаваемых негосударственными организациями по общедоступным каналам связи.

В рамках данной работы было принято решение о создании программного инструмента StegaCrypt (рисунок 1), предназначенного для шифрации и сокрытия информации в файлах.

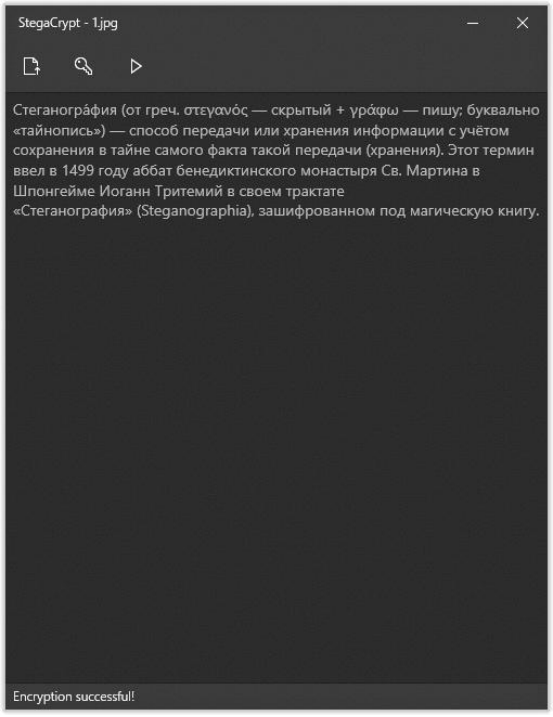

Рисунок 1 – интерфейс программного инструмента StegaCrypt

В последние десятилетия в криптографии стали появляться шифры, стойкость которых обосновывается сложностью решения чисто математических задач: разложения больших чисел на множители, решения

показательных сравнений в целых числах и других. Стойкость шифров зависит также и от качества генераторов случайных чисел, порождающих ключи. Одним из таких шифров является DES.

Программный инструмент StegaCrypt использует алгоритм шифрования Triple-DES. Его отличие заключается в том, что шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

Стандарт шифрования данных (алгоритм) DES – один из старых и наиболее известных алгоритмов шифрования, который был изобретен корпорацией IBM и был американским правительственным стандартом с 1976 до 2001 года. В значительной степени DES основан на алгоритме Люцифер (Lucifer) Хорста Фейстеля (Horst Feistel), который не получил широкого распространения. Существенно то, что в алгоритме DES используется единственный 64-битовый ключ: 56 бит значащие и 8 бит – проверочные биты для контроля на четность. Алгоритм обрабатывает блоки данных порциями по 64 бита. Ключ разбивается на 16 отдельных 48-битовых подключей по одному на каждый раунд, который называется циклом Фейстеля (Feistel cycles). На рисунке 2 показана схема работы алгоритма DES.

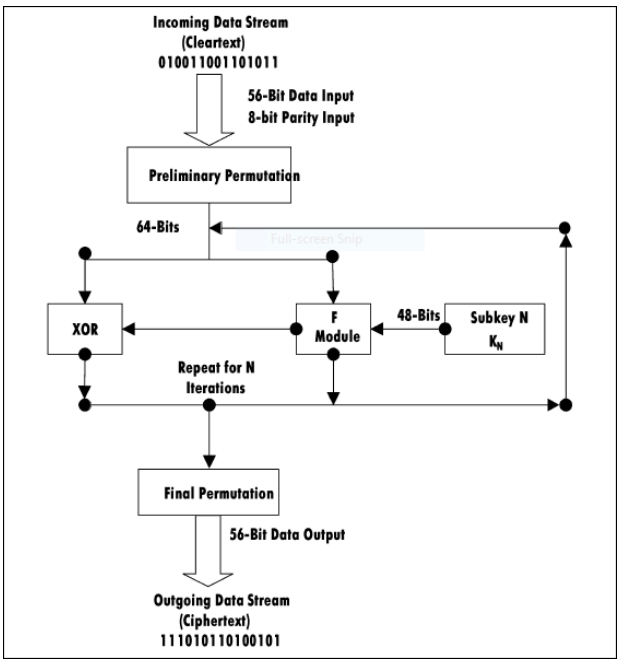

Рисунок 2 – интерфейс программного инструмента StegaCrypt

В каждом раунде выполняются подстановка, во время которой биты данных заменяются битами ключа, и перестановка, во время которой замененные данные переставляются (перемешиваются). Операции перестановки, которые иногда называют перемешиванием, выполняются в S-блоках, а операции перестановки, иногда называемые операциями рассеивания, – в P-блоках. Два названных класса операций реализованы в

«F-модуле» диаграммы. Безопасность DES чаще основывается на том, что операции перестановки нелинейные, поэтому зашифрованный текст ничем не напоминает исходное сообщение. Поэтому методы языкового анализа зашифрованного текста, которые обсуждаются далее в этой главе, не приводят к положительному результату. Операции перестановки повышают безопасность, дополнительно шифруя уже частично зашифрованное сообщение.

Для получения более высокой степени безопасности, зашифрованное сообщение сохраняется в выбираемом в программном инструменте файле. При необходимости можно задать тройной пароль, по которому будет осуществляться шифрование.

Программный инструмент написан на языке программирования C# и языке разметки XAML, с использованием инструментальной среды разработки MicrosoftVisualStudio на программной платформе .NET Framework 4.5.

StegaCrypt имеет простой и дружелюбный интерфейс. В случаях, когда необходимо скрыть или передать сообщение, без его утечки, программный инструмент StegaCrypt отлично подойдет для реализации этого.

Литература

1. Мэтью Макдональд. Windows Presentation Foundation в .NET 4.5 с примерами на C# 5.0 для профессионалов, 2013. – 1015 с.
2. Джон Шарп. Microsoft Visual C#. Подробное руководство. 8-е издание, 2017. – 845 с.
3. Руководство по языку C#. [Электронный ресурс]. – 2018. – Режим доступа: – https://docs.microsoft.com/ru-ru/dotnet/csharp/ – Дата доступа: 30.01.2018.
4. Проектирование XAML в Visual Studio. [Электронный ресурс]. – 2017. – Режим доступа: – https://docs.microsoft.com/ru-ru/visualstudio/designers/designing-xaml-in-visual-studio – Дата доступа: 17.07.2017
5. Документация по MahApps.Metro. [Электронный ресурс]. – 2018. – Режим доступа: – http://mahapps.com/ – Дата доступа: 13.04.2017