УДК 003.26+004.56

КРИПТОГРАФИЧЕКОЕ ШИФРОВАНИЕ ОСАЖДАЕМОГО СООБЩЕНИЯ В МНОГОКЛЮЧЕВОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЕ

Берников В.О., Урбанович П.П.
БГТУ, г.Минск, Республика Беларусь; vladbernikovronaldo@gmail.com

Реферат. В докладе анализируется подход и кратко описывается программное средство для криптографического зашифрования/расшифрования осаждаемого/извлекаемого тайного сообщения в стеганографической системе на основе многоключевой модели такой информационной системы. Тайные ключи в системе соотносятся с выбранными методами стеганографии, криптографии, помехоустойчивого кодирования и иными преобразованиями для повышения стегано- (крипто-)стойкости системы. Представлен пример использования алгоритма RSA с хешированием зашифрованного сообщения на основе SHA256. Программное средство может использоваться в научных исследованиях и в учебном процессе.

Как известно, стеганография – это наука о скрытой передаче (или хранении) информации путём сохранения в тайне самого факта передачи [1]. Это направление науки и техники приобретает все большую актуальность. Как и в любой системе с повышенным уровнем защищенности информации, в стеганографической системе важнейшим элементом ее анализа и синтеза является информационная модель. Наши исследования базируются на так называемой многоключевой модели [2]. Охарактеризуем некоторые элементы этой модели.

Определение 1. Функцию $\mathbf{F}$, определенную на $\mathbf{M} \times \mathbf{C} \times \mathbf{K}$ со значениями в $\mathbf{S}$, будем отождествлять с осаждением или встраиванием сообщения M_i из множества $\mathbf{M}$ в контейнер C_j из множества $\mathbf{C}$ на основе ключа из множества $\mathbf{K}$**,** предусматривающего использование соответствующего алгоритма осаждения и пространственных (геометрических или иных) параметров элементов контейнера C_j множества $\mathbf{C}$:

$$\mathbf{F}: \mathbf{M} \times \mathbf{C} \times \mathbf{K} \rightarrow \mathbf{S}. \quad (1)$$

Соотношение (1) формально описывает процедуру осаждения сообщения в контейнере на основе выбранного метода.

Определение 2.Функцию $\mathbf{F}^{-1}$, определенную на $\mathbf{S} \times \mathbf{K}^*$($\mathbf{K}^* = \{K^*_1, K^*_2, \ldots, K^*_z\}$ (соотношение 2), в общем случае $K_m \neq K^*_m$; $K_m \in \mathbf{K}$, $K^*_m \in \mathbf{K}^*$; $m = 1,2,\ldots,z$) со значениями в $\mathbf{M}$, будем отождествлять с извлечением тайного сообщения $M_i \in \mathbf{M}$ из стегосообщения $S_q \in \mathbf{S}$*:*

$$\mathbf{F}^{-1}: \mathbf{S} \times \mathbf{K}^* \rightarrow \mathbf{M}, \mathbf{C}. \quad (2)$$

Множеств $\mathbf{F}^{-1}$состоит из l элементов (соотношение 3):

$$\mathbf{F}^{-1} = \{(F^{-1})_1, (F^{-1})_2, \ldots, (F^{-1})_l\}, \quad (3)$$

где каждому конкретному отображению $F_w (w = 1, 2,\ldots,l)$ соответствует фиксированный ключ $K^*_w \in \mathbf{K}^*$.

Важнейшим компонентом (ключом) многоключевой модели информационной системы является использование криптографических методов защиты информации. Прежде, чем секретная информации будет осаждена в электронный документ, она может быть предварительно зашифрована.

Для анализа эффективности некоторых решений нами разработано специализированное программное средство. Для шифрования/расшифрования стегосообщения (по алгоритму RSA) использовалась стандартная библиотека, написанная на языке C# [3,4].

В качестве входной используется 1024-битная последовательность. Далее происходит генерация необходимых параметров для вычисления значений публичного и тайного ключей (простые большие числа, функция Эйлера и др.). Все эти параметры будут записываться в

текстовые файлы. Продемонстрируем процесс шифрования секретного сообщения на основе созданного программного средства, одно из основных диалоговых окон показано на рис. 1.

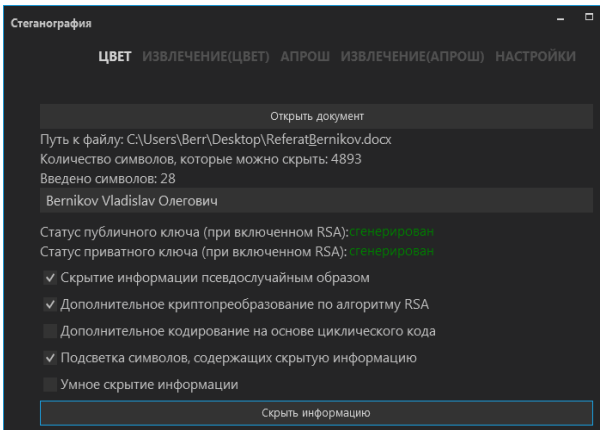

Рис. 1 – Диалоговое окно для шифрования стегосообщения

Выбирается электронный документ-контейнер (C_j) для осаждения секретной информации (M_i). Заполняется поле для секретного сообщения. В данном случае используется псевдорандомизация битов стегосообщения, подсветка осажденных символов, а также дополнительное криптопреобразование по алгоритму RSA. Как видно из рисунка, публичный и тайный ключи были успешно сгенерированы. Как известно, для зашифрования данных необходим публичный ключ, для обратного процесса – тайный. Содержимое текстового файла *private.txt* представляет собой *xml*-файл, узлы которого содержат всю информацию о параметрах RSA, которая необходима для шифрования и расшифрования секретного сообщения (рис. 2).

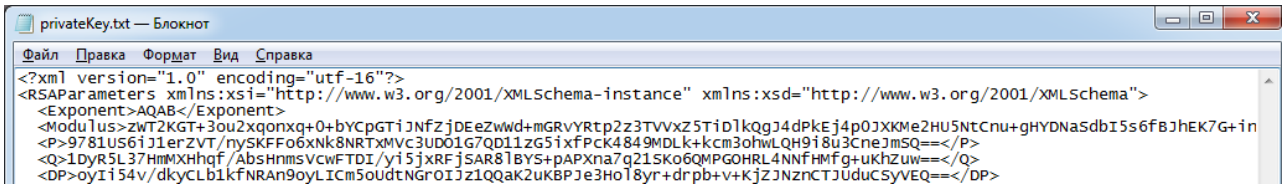

Рис. 2 – Содержимое тайного ключа криптопреобразования

Отметим, что зашифрованное сообщение дополнительно хешируется согласно алгоритму SHA256. Данное преобразование используется в стандартной библиотеке при реализации алгоритма RSA для повышения криптостойкости системы. Рассмотрим, как изменился стеганоконтейнер после осаждения нашего секретного сообщения (рисунок 3).

Отметим, что в этом примере показано осаждение зашифрованного сообщения на основе стеганографического метода по цвету [3] с включенной псевдорандомизацией секретных бит. Здесь внедряется больше бит, чем при использовании отдельного стеганографического метода. Объясняется это тем, что зашифрованное сообщение дополнительно хешируется, и выходная последовательность всегда составляет 172 байта, что в сумме дает 1376 бит. Отметим, что все параметры RSA в текстовых файлах хранятся в хешированном виде.

Для того, чтобы извлечь внедренное сообщение в стеганоконтейнер, необходимо для начала выбрать наш документ с осажденной информацией, а далее выбрать текстовый файл с закрытым ключом. Как видно из рисунка, наше секретное сообщение было успешно извлечено (рис. 4). Перед осаждением секретное сообщение (M_i) «Bernikov Vladislav Олегович» сначала было зашифровано согласно алгоритму RSA, а далее выходная последовательность была хеширована по алгоритму SHA256. Данная хешированная последовательность «TLWMCRqdqqRiCC2VH0GIryA4ZFKSiiveopDneRqyiFwq6ELIXACXKZUcWAGgydhmr22R3 KPQbezhC9ewqNM2WbP7b02Zi/+7zdC3LBdG/M0XpEsim4Av4tNiqQoJbXuMzBiPmcfJ65sz9a QLx3ttswRssIYx1KSyxsNlYaDFsNo=» и была внедрена непосредственно в электронный документ-контейнер в виде бинарной последовательности согласно кодировке Unicode [4-5].

день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения [1].

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование.

Рис. 3 – Часть документа-контейнера после осаждения зашифрованного сообщения

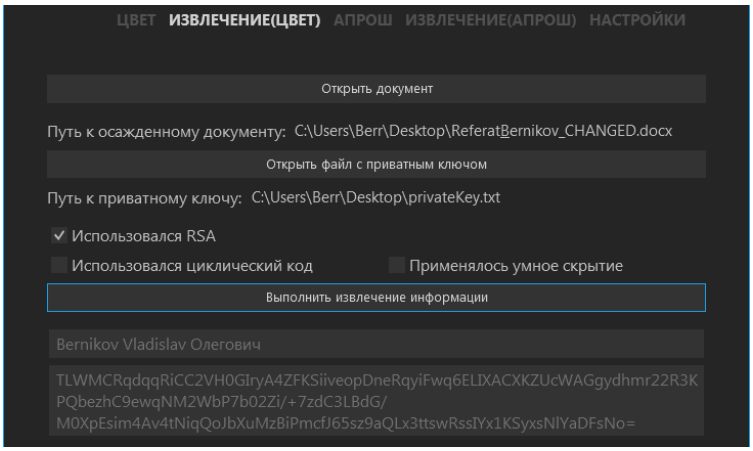

Рис. 4 – Диалоговое окно для извлечения зашифрованного стегосообщения

Дальнейшим шагом исследований является моделирование и анализ стойкости стеганографической системы.

Подводя краткий итог, отметим, что описанное программное средство реализовано на основе модели информационной системы, которая подразумевает применение практически неограниченного числа ключей. Мы представили процесс внедрения и извлечения стегосообщения при использовании контейнера текстового типа формата DOCX. Разработанное средство используется также в учебном процессе при изучении студентами дисциплин «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации».

Список литературы:

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Pavel Urbanovich, Nadzeya Shutko. Theoretical Model of a Multi-Key Steganography System, in: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Computer Science Vol. 2, Ed. A. Zapała. – Wydawnictwo KUL, Lublin, 2016, Part II, Chapter 11. – P. 181-202.

3. Шутько, Н.П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста/ Н.П. Шутько, Д.М. Романенко, П.П. Урбанович// Труды БГТУ. Серия 6: Физ.- мат. науки и информатика. – Минск: БГТУ. – 2015. – №6. – С. 152-156.

4. Берников, В.О. Разработка стеганографических методов на основе многоключевой модели информационной системы/ В.О. Берников // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях. – Гомель: ГГУ им. Ф. Скорины. – 2018. – С. 192-193.

5. Берников, В.О. Анализ стеганографической стойкости текстового документа-контейнера в многоключевой стеганосистеме // 69-я НТК студентов и магистрантов: сб. науч. работ: в 4-х ч. 17-22 апреля 2018 г. – Минск: БГТУ, 2018. – Ч. 4.. – С.14-17.