```
                    KEY FOUND! [ qwerty123 ]

Master Key     : ED FF 23 E4 68 76 CE C7 BA A3 49 9F 8E 3C 32 CD
                 44 96 43 9E DC 30 C7 5E 46 73 F0 40 CE 2B BE C8

Transcient Key : 7F 5E AD AE 34 94 39 AD AC 4E C5 64 B2 7B FE CF
                 28 CF F5 1D 64 AC 5B BA B5 CB F6 25 11 0B 3C F4
                 C1 A6 8B 85 E3 68 C1 97 27 4C 03 65 D1 67 E3 1E
                 67 22 1E 51 9A 6D 49 67 F6 5F BE 47 4A 7A D6 51

EAPOL HMAC     : 36 33 8C 56 61 C7 9C 93 9D 47 A4 B5 A4 1F 05 F4
```

Рисунок 8 – Результат успешного взлома

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

3. Нефёдова, М. Анонсирован стандарт WPA3, Wi-Fi обещают сделать безопаснее / М. Нефёдова. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2018/01/09/wap3/. – Дата доступа: 10.04.2019.

УДК004.056

Магистрант А. А. Сущеня
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ВНЕДРЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ В КОНТЕЙНЕР ФОРМАТА EPUB

Актуальность исследования стеганографии обострена проблемами защиты цифрового контента от несанкционированного использования. Ввиду этого существует необходимость расширения и углубления теоретической базы стеганографии как платформы для тайной передачи и хранения информации [1].

С развитием информационных технологий стали появляться цифровые объекты, имеющие в своей структуре избыточность, которую можно использовать для реализации стеганографических методов передачи данных. Одними из таких объектов являются электронные книги. На сегодняшний день, наиболее популярным форматом электронных книг являются EPUB. Рассмотрим структуру данного формата. EPUB — это ZIP-файл, сжатый особым образом. В этом можно

убедиться, изменив расширение файла .epub на .zip и разархивировав его любым архиватором.

Минимальный набор файлов, который входит в EPUB должен быть следующим:

— файл mimetype, сострочкой «application/epub+zip»;

— папка META-INF с файлом container.xml, который указывает, где хранится содержимое книги;

— папка OPS, в которой должны быть: файл с метаданными книги, списком всех файлов, которые нужны для ее содержимого, описанием последовательности чтения файлов и путеводителем по ключевым файлам; файл toc.ncx, содержащий оглавление книги в том виде, в котором оно будет прочитано программой для чтения; файл stylesheet.css с описанием стилей оформления текста; файлы содержимого в формате XHTML; папки с иллюстрациями и шрифтами.

XHTML — это основанный на XML язык разметки гипертекста, максимально приближенный к стандартам HTML. XHTML отличается от HTML строгостью написания кода. Если HTML позволяет писать практически любые конструкции и браузер их корректно распознавал, то, с появлением XHTML это стало невозможным. Последний требует строгого соблюдения всех правил, предъявляемых W3C. Строгие требования к оформлению XHTML-кода позволяют избежать многих ошибок ещё на стадии написания и отладки.

Для защиты авторского права на электронную книгу формата EPUB предлагается внедрять метку, содержащую уникальный идентификатор пользователя в системе распространения, а также международный стандартный книжный номер. Значение метки предварительно шифруется и кодируется в бинарную последовательность.

Исходя из того, что книга состоит из определенного количества глав, закодированная последовательность последовательно внедряется в эти главы (рис. 1). Для внедрения информации в XHTML файлы выбран метод кавычек [2-6]. Данный метод позволяет размещать двоичную информацию в файлах языков разметки. Метод основан на замене одинарных кавычек на двойные или наоборот в файлах с разметкой, т. е. на нечувствительности языка разметки к типу кавычек. Предварительно осаждаемая бинарная последовательность шифруется. Для увеличения стеганографической стойкости системы вводится дополнительный ключ, которым является название файла главы.

При наличии дополнительного числа после знака «-» в наименовании главы, осаждение информации производится, начиная с конца файла.

Рисунок 1 — Структура файлов электронной книги формата EPUB

Для контроля достоверности внедренной метки вводится дополнительный метод осаждения информации в электронные книги на основе использования каскадных таблиц стилей. Стиль — это совокупность правил, применяемых к элементу гипертекста и определяющих способ его отображения. Стиль включает все типы элементов дизайна: шрифт, фон, текст, цвета ссылок, поля и расположение объектов. Таблица стилей — это совокупность стилей, применимых к гипертекстовому документу. Каскадирование — это порядок применения различных стилей.

При создании CSS файлов существует возможность хранения изображений в формате base64. Base64 — способ кодирования произвольных двоичных данных в ASCII текст. Кодирование Base64 занимает три байта, каждый из которых состоит из восьми битов, и представляет их в виде четырех печатных символов в стандарте ASCII. Хранение картинки небольшого размера, в data:image base64 в CSS — существенно экономит количество запросов к серверу.

Для проверки осажденной метки необходимо закодировать изображение в формат base64. Далее разместить получившуюся строку в CSS файл, заменяя «ТИП» на MIME-тип изображения — JPEG/PNG/GIF или BMP и «КОД» на нужную строку в base64.

Предварительно во внедряемое изображение встраивается контрольная сумма метки, используя стеганографический метод LSB [1, 7,8]. Суть метода LSB заключается в следующем: заменяются младшие биты в байтах, отвечающих за кодирование цвета изображения. Допустим, если очередной байт секретного сообщения – 11001011, а байты в изображении –…11101100 01001110 01111100 0101100111…, то кодирование будет выглядеть так: байт секретного сообщения разбивается на 4 двухбитовые части: 11, 00, 10, 11. После чего заменяем полученными фрагментами младшие биты изображения: …11101**11** 01001**00** 01111**10** 0101100**11**…. Такая замена в общем случае не заметна человеческому глазу. Можно менять не только два младших

бита, но и любое их количество. Однако есть следующая закономерность: при замене большего количества бит, теряется больший объем информации, следовательно, факт наличия закодированного сообщения обнаружить проще.

ЛИТЕРАТУРА

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

2. Сущеня, А. А. Стеганографическое преобразование текстов-контейнеров на основе языков разметки / А. А. Сущеня // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск: сборник научных работ: в 4 ч., Ч. 4 / Белорусский государственный технологический университет. – Минск: БГТУ, 2017.– С. 145-149.

3. Сущеня, А. А. Способ стеганографического осаждения информации в документ с расширением .DOCX / А. А. Сущеня // XXI Республиканская научная конференция студентов и аспирантов, 19–21 марта, Гомель: сборник научных работ / Гомельский государственный университет имени Ф. Скорины. – С. 303-304.

4. Сущеня, А.А. Идея и архитектура веб-приложения, использующего в качестве стеганографического контейнера документы формата DOCX / А. А. Сущеня // Международная научно-практическая конференция, 14–18 мая, Минск: сборник научных работ / Белорусский государственный университет. – С. 170.

5. Сущеня, А.А. Модификация стеганографического метода изменения междустрочного расстояния электронного документа/ А.А. Сущеня, Е.А. Блинова, П.П. Урбанович// Технические средства защиты информации: Тезисы докладов XVI Белорусско-российской научно-технической конференции, 5 июня 2018 г., Минск. – Минск: БГУИР, 2018. – С 90-91.

6. Сущеня, А. А. Программное средство стеганографического преобразования текстов-контейнеров на основе языка разметки XML / А. А. Сущеня // 69-я научно-техническая конференция учащихся, студентов и магистрантов, 2-13 апреля, Минск: сборник научных работ: в 4 ч., Ч. 4 / Белорусский государственный технологический университет. – Минск: БГТУ, 2018. –С. 81-84.

7. Урбанович, П. П. Стеганография в графических объектах / П. П. Урбанович, Т. В. Коваленок, Н. П. Урбанович // Международная научно-техническая конференция "Автоматический контроль и авто-

матизация производственных процессов": материалы конференции, Минск, 28-29 октября 2009 г. – Минск, 2009. – С. 69-70.

8. Шутько, Н. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста / Н. П. Шутько, П. П. Урбанович // Информационные технологии: материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 г. / отв. за изд. И. В. Войтов; УО БГТУ. – Минск: БГТУ, 2019. – С. 41-43.

УДК 004.056+003.26

Студ. М. А. Тихонович
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий,БГТУ)

КРИПТОСТОЙКОСТЬ ГОМОМОРФНЫХ ШИФРОВ

Гомоморфное шифрование – форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом.

Задачи гомоморфной криптографии:

– необходимо производить вычисления над зашифрованными данными так, чтобы результат после расшифрования соответствовал результату тех же вычислений над открытыми данными (m_1 иm_1). Сформулирована в 1978 году Ривестом, Адлеманом и Дертузосом. Является основной для систем полностью гомоморфного шифрования (FHE);

– имеется 2 или более стороны. Необходимо вычислить произвольную функцию, аргументы которой являются секретными данными этих сторон, таким образом, чтобы ни одна из сторон не узнала вход другой стороны, а результат вычисления функции был корректен. Сформулирована Яо в 1982 году. Является основной задачей протоколов секретных распределенных вычислений (SMC).

Риверст и Адлеман впервые обосновали, что методом, позволяющим успешно проводить операции над зашифрованными данными, не искажая и не расшифровывая их, является так называемое гомоморфное шифрование [1].

Полностью гомоморфные схемы шифрования позволяют выполнять арифметические операции над зашифрованными данными без их предварительного расшифровывания. Частично гомоморфные