УДК 004

РАЗРАБОТКА МОДУЛЯ ЗАЩИЩЁННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ГИБРИДНОЙ КРИПТОСИСТЕМЫ

Смалёха М.В.
Научный руководитель: Рейзлин В.И. к.ф-м.н., доцент

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: mvs17@tpu.ru

*This article describes the process of creation hybrid cryptosystem. A*lso considered the creation of extensions for the browser.

Ключевые слова: *веб-приложение, криптография, гибридная криптосистема, расширения для браузера.*

Key words: *web-application, cryptography, hybrid cryptosystem, browser extension.*

Для обеспечения безопасности электронного документооборота в рамках предприятия необходимо обеспечить криптографическую защиту секретных документов от несанкционированного доступа. Существует несколько типов криптосистем: симметричные, асимметричные и гибридные.

Симметричные системы используют симметричное шифрование, и обладают следующими параметрами: высокая скорость шифрования\дешифрования данных, малое требование к вычислительным мощностям, но уязвимое место – ключ, т. к. для шифрования и дешифрования используется один и тот же ключ, и при передаче данных от клиента серверу он может быть перехвачен третьими лицами.

Ассиметричные системы, которые ещё называют криптосистемы с открытым ключом, используют ассиметричное шифрование. Они обладают большей надёжностью, за счёт использования публичных и приватных ключей, но они требуют большее количество вычислительных мощностей, и, следовательно, времени для шифрования\дешифрования.

Гибридные системы объединяют положительные стороны обоих систем: производительность симметричной и защищённость ассиметричной. Симметричный ключ используется для шифрования данных, а асимметричный – для шифрования самого симметричного ключа [1]. Схема гибридной криптосистемы представлена на рис. 1.

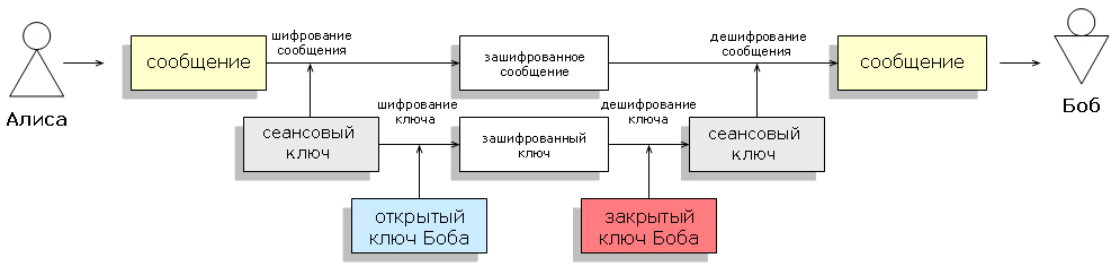

Рис. 1. Схема гибридной криптосистемы

В качестве симметричного алгоритма используется AES с длиной ключа 256 бит, в качестве ассиметричного – RSA [2].

Каждый пользователь системы имеет пару ключей (публичный и приватный), причём публичный ключ пользователь должен загрузить в систему, а приватный ключ – хранить на личном съёмном носителе. Работа для пользователя с системой очень проста и интуитивно понятна. При добавлении файла пользователь выбирает других пользователей, кому будет доступен этот файл. Дальнейшие действия происходят внутри системы: создаётся сеансовый ключ AES, которым шифруется файл, и этот ключ шифруется алгоритмом RSA публичным ключом каждого выбранного пользователя. Шифрованные ключи каждого пользователя добавляются в БД, где в таблице связываются документ, пользователь, и полученный зашифрованный ключ. Благодаря этому, пользователи, у кого нет доступа к документу, его не видят.

Для автоматизации работы с системой при получении доступа к зашифрованным файлам были написаны плагины для двух популярных браузеров: Firefox и Chrome. Для того чтобы получишь зашифрованный файл, необходимо вставить съёмный носитель с ключом и нажать на иконку расширения на панели браузера. Расширение находит нужный файл, считывает его, и отсылает на сервер. Схема работы расширения представлена на рис. 2. Для индикации наличия расширения в браузере используется content-script [3], который добавляет невидимый DOM-элемент, сообщающий о наличии расширения [4]. Только для браузера Chrome есть ещё прослойка в виде Chrome app, который получает команду от расширения, считывает файл, и возвращает данные расширению.

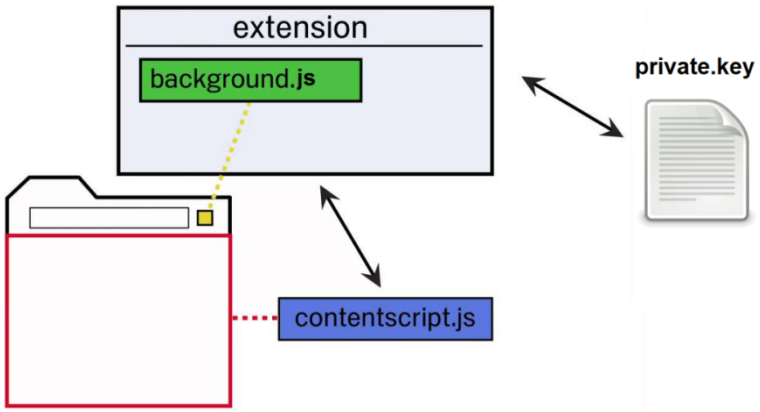

Рис. 2. Общая схема работы расширения для браузера

В результате работы был реализован прототип модуля работы с зашифрованными файлами, который поддерживает шифрование файлов, и распределение доступа к ним. Также реализованы дополнения для браузеров Firefox и Chrome, для удобной работы с системой.

Список литературы

1. Гибридная криптосистема [Электронный ресурс]: Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Гибридная_криптосистема (дата обращения: 08.03.16).
2. System.Security.Cryptography – пространство имён [Электронный ресурс]: MSDN – Microsoft Developer Network. URL: https://msdn.microsoft.com/ru-ru/library/system.security.cryptography (дата обращения: 04.03.16).
3. What are extensions? [Электронный ресурс]: Официальная документация Google по разработке расширений. URL: https://developer.chrome.com/extensions (дата обращения: 05.03.16).
4. Extensions [Электронный ресурс]: Официальная документация Mozilla по разработке расширений. URL: https://developer.mozilla.org/en-US/Add-ons (дата обращения: 04.03.16).