УДК 004.056.55

Криптографию — на службу ЕГЭ!

М. М. Грунтович
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Предложен метод обеспечения конфиденциальности, целостности и неотказуемости при рассылке информации из центра с использованием типовых ключевых USB-токенов, при котором получить доступ к ее содержанию могут не менее двух из трех получателей.

Ключевые слова: шифрование, целостность, неотказуемость, разделение секрета.

Поставленная заказчиком задача разработать безопасную систему рассылки контрольно-измерительных материалов (КИМ) ЕГЭ на первый взгляд типовая, однако у заказчика имелась еще одна вводная: для вскрытия КИМ необходимо присутствие не менее двух человек из трех представителей регионального центра тестирования.

В инвариантной форме это звучит так. Необходимо обеспечить безопасную доставку файла из центра к получателям с обеспечением следующих свойств информационной безопасности:

- конфиденциальность,
- целостность,
- неотказуемость (центр не может отрицать, что именно он разослал этот файл),
- невозможность получения монопольного доступа к содержанию только одним лицом из трех получателей.

При этом предпочтительно максимально использовать существующие средства криптографической защиты информации (СКЗИ), например персональные USB-токены.

Это, очевидно, СКЗИ с пороговой схемой разделения секрета. Естественно было бы использовать линейную схему разделения секрета Шамира (см. п.12.71 в [1]), однако штатное СКЗИ, каковым является USB-токен, не способно делать необходимые вычисления, а изменять прошивку устройства нежелательно. Удалось придумать, как можно реализовать разделение секрета с использованием типовых персональных USB-токенов [2].

Грунтович Михаил Михайлович, руководитель обособленного подразделения.
E-mail: gmm@okbsapr.ru.

Статья поступила в редакцию 26 июня 2016 г.

Архитектура системы

Система защиты состоит из следующих элементов:

- центр управления ключами (ЦУК), организующий криптографическую защиту сети,
- центр рассылки, обладающий ключевой информацией для связи со всеми остальными участниками и использующий HSM с неизвлекаемой персональной ключевой информацией на борту,
- региональные пункты получения информации, организующие работу на местах,
- получатели информации в количестве трех человек в каждом региональном пункте, каждый из которых обладает ключевым носителем (USB-токеном) с неизвлекаемой персональной ключевой информацией.

Принцип работы

Идея:

- ключевая система с архитектурой "звезда" (центр рассылки имеет ключи парной связи со всеми получателями),
- центр рассылки подписывает содержимое файла для каждого регионального пункта,
- центр рассылки выполняет шифрование файла на случайно сгенерированном разовом ключе,
- этот ключ шифруется в адрес каждой из трех пар получателей (три получателя – три пары),
- три экземпляра зашифрованного разового ключа вместе с зашифрованным файлом и подписью образуют защищенный контейнер,
- контейнер отсылается в региональный пункт,
- любые двое получателей в региональном пункте предоставляют свои ключевые носители,
- разовый ключ извлекается из файла контейнера и расшифровывается,
- извлекается и расшифровывается целевой файл,

- проверяется электронная подпись центра рассылки.

Ключевая система

Центр управления ключами (ЦУК) представляет собой удостоверяющий центр с соответствующей ключевой информацией:

- ключ подписи сертификатов,
- сертификат ключа проверки электронной подписи центра рассылки,
- сертификаты открытых ключей Диффи—Хеллмана (Д—Х) центра рассылки и получателей.

У центра рассылки имеется следующая ключевая информация:

- ключ электронной подписи (ЭП) центра рассылки,
- закрытый ключ Д—Х центра рассылки,
- сертификат ключа проверки ЭП ЦУК,
- сертификаты открытых ключей Д—Х получателей,
- собственные сертификаты ключа ЭП и открытого ключа Д—Х.

Каждый получатель владеет минимальной ключевой информацией:

- свой закрытый ключ Д—Х,
- сертификат ключа проверки ЭП ЦУК.

Помимо этого, в вычислениях система использует:

- ключи парной связи центра рассылки и получателя,
- разовый ключ шифрования контейнера, которые вычисляются/генерируются непосредственно перед использованием и уничтожаются сразу же после него.

Подготовительный этап

Центр управления ключами:

- генерирует ключевую информацию всех участников системы и готовит соответствующие ключевые носители,
- безопасным образом доставляет в центр рассылки ключевой носитель, сертификат ключа проверки ЭП ЦУК и базу сертификатов открытых ключей получателей,
- безопасным образом доставляет в региональные пункты по три ключевых носителя (токена) с ключевой информацией получателей.

Формирование контейнера

Для защиты файла, высылаемого в адрес регионального пункта, представленного тройкой получателей, центр рассылки выполняет следующую последовательность действий:

1. проверяет сертификаты трех получателей;
2. вычисляет ЭП содержимого файла;
3. генерирует случайный разовый ключ;
4. шифрует содержимое файла на разовом ключе;
5. шифрует разовый ключ на каждой из трех пар ключей получателей;
6. вкладывает в контейнер зашифрованное содержимое файла, значение ЭП, три экземпляра зашифрованного разового ключа, сертификаты открытых ключей центра рассылки;
7. вычисляет контрольную сумму контейнера как код аутентификации на разовом ключе и добавляет ее в контейнер.

Шифрование данных выполняется в режиме гаммирования с обратной связью, ключей — в режиме простой замены.

Шифрование разового ключа K в адрес пары получателей i и j ($i < j$) на шаге 5 в HSM центра рассылки предлагается выполнить следующим образом:

- экспортировать разовый ключ K на открытом ключе получателя i (результат: K_i^* — зашифрованный K на ключе парной связи центра рассылки и получателя i),
- вычислить ключ парной связи с получателем j,
- зашифровать на нем *данные* K_i^* (результат: ключ K^*, последовательно зашифрованный на ключах связи центра рассылки с получателями i и j).

Расшифрование контейнера

Получив контейнер с файлом, любая пара представителей регионального пункта выполняет следующую последовательность действий:

1. извлекает и проверяет сертификаты открытых ключей центра рассылки,
2. считывает экземпляр разового ключа, зашифрованный для данной пары получателей,
3. расшифровывает разовый ключ,
4. проверяет контрольную сумму контейнера,
5. расшифровывает содержимое файла на разовом ключе,
6. проверяет ЭП центра рассылки.

Расшифрование разового ключа K^* на шаге 3 с использованием персональных USB-токенов пользователей i и j ($i < j$) предлагается выполнить следующим образом:

- в токене j расшифровать *данные* K^* на ключе парной связи с центром рассылки (результат — K_i^*),

- импортировать ключ K_i^* в токен *i* на открытом ключе центра рассылки.

Далее токен *j* должен выполнить операции проверки кода аутентификации и расшифрования содержимого файла. При этом разовый ключ не появляется в открытом виде в ОЗУ компьютера.

В описании алгоритмов формирования/разбора контейнера мы опустили служебную часть (идентификация, отметка времени). Ее описание тоже необходимо, но не является целью данной заметки.

Таким образом, с помощью типовых персональных USB-токенов может быть построена пороговая схема разделения секрета. При этом изменения штатной прошивки токенов не требуется, во время работы долговременная персональная ключевая информация не появляется в ОЗУ компьютеров, а также обеспечиваются необходимые свойства безопасности информации при передаче по открытому каналу связи.

Литература

1. *Menezes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. – CRC Press, 1996.

2. Персональное средство криптографической защиты информации (ПСКЗИ) ШИПКА. [Электронный ресурс]. URL: http://www.shipka.ru (дата обращения 06.07.2016).

Cryptography to the service of the exams!

M. M. Gruntovich
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The paper proposes a method of provision confidentiality, integrity and non-repudiation when sending information from the center using the typical USB-tokens, at which only at least two of the three recipients can access its content.

Keywords: encryption, integrity, non-repudiation, secret sharing.

Bibliography — 2 references. *Received June 26, 2016*