УДК 004.056.55

АНАЛИЗ И РЕАЛИЗАЦИЯ СИСТЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Кутепова О.А., Ковальская О.Н.
к.т.н., доцент кафедры ИС Болтенков В.А.
Одесский национальный политехнический университет, Украина

АННОТАЦИЯ. Исследованы современные алгоритмы разделения секрета и принципы построения криптографических с временным замком. Система разделения секрета реализована практически в виде Web-приложения с клиентской частью на Android-устройстве.

Введение. В настоящее время актуальным является вопрос защиты секретных ключей в различных программно-аппаратных комплексах (ПАК) с распределенной структурой доступа, таких как удостоверяющие центры (УЦ) и аппаратные модули защиты конфиденциальной информации (*англ.* HSM - Hardware Secure Module). Известны различные методы повышения секретности ключей, среди которых можно выделить метод, основанный на применении криптографических схем разделения секрета (СРС). По таким схемам секретный ключ (секрет, который разделяется) путем математических преобразований «распределяется» на N частей (долей) секрета и раздается N участникам структуры доступа ПАК. Далее, для восстановления исходного секретного ключа необходимо «собрать вместе» как минимум K ($K<N$)долей секрета. Такие схемы называются *(N, K)* - пороговыми схемами разделения секрета.

Цель работы. Цель работы – исследование алгоритмов разделения секрета, разработка СРС с временным замком и программная реализация такой СРС.

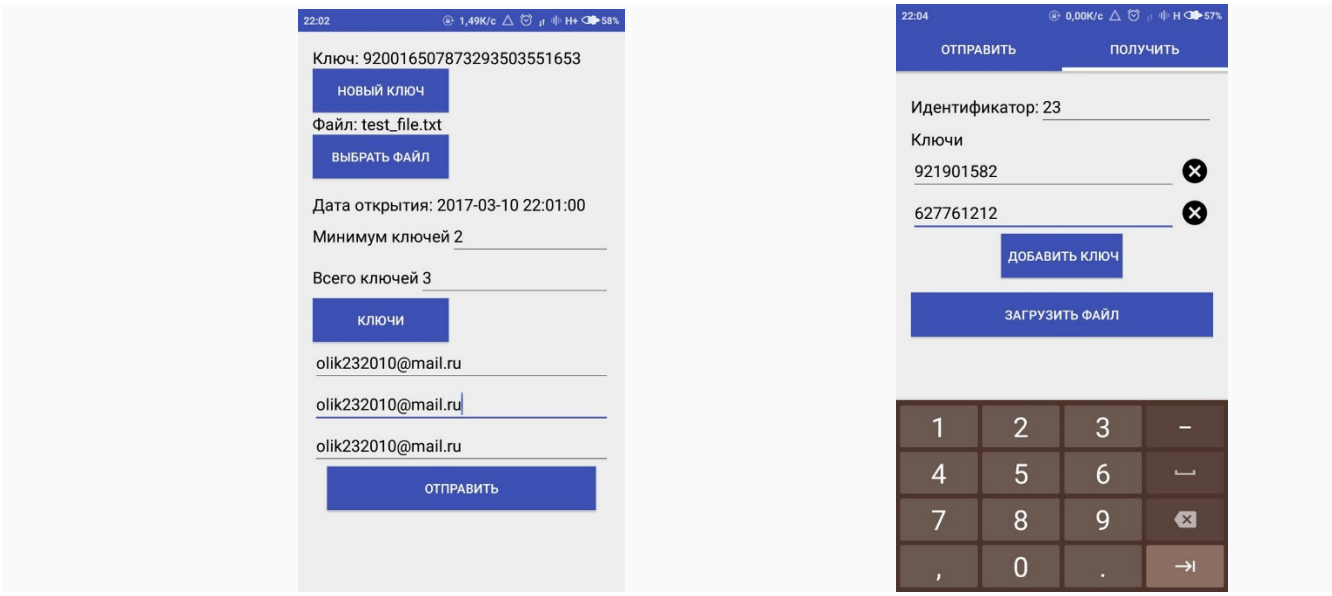
Основная часть работы. Анализ СРС. Известен ряд алгоритмов разделения секрета: схема Шамира, схема Блэкли, схема Карнина–Грина–Хеллмана[1,2]. В процессе исследования проанализированы все перечисленные алгоритмы с точки зрения теоретической криптостойкости и требуемого объема оперативной памяти на фазах разделения и восстановления секрета. Установлено, что схема Шамира, в отличие от схем Блэкли и Карнина-Грина-Хеллмана, является доказательно совершенной, т.е. запрещенное подмножество участников не может получить никакой дополнительной информации о секрете. Схемы Блэкли и Карнина-Грина-Хеллмана требуют высоких вычислительных ресурсов на этапе разделения секрета. Доказано, что схема Шамира в силу своей совершенности имеет более высокую криптографическую стойкость и требует наименьших затрат памяти.

СРС с временным замком. Далее исследованы СРС с временным замком. Криптографические системы с возможностью раскрытия секретной информации только по истечении определённого времени, называется криптоситемами с временным раскрытием (*англ.* timed-release crypto).

Криптосистема разделения секрета с временным раскрытием, предложенная Р.Л.Райвестом, А.Шамиром и Д.А.Вагнером [3], получила название «шарады» с временным замком (*англ.* time – lock puzzles). Данный подход к защите информации иногда называют «отправкой секретного сообщения в будущее». Его специфика заключается в том, что в отличие от традиционных криптографических методов, предполагающих наличие у получателя сообщения секретного ключа отправителя (в симметричных криптосистемах) или у отправителя сообщения аутентичного (подлинного) открытого ключа получателя (в асимметричных криптосистемах), секретный ключ уничтожается сразу после шифрования и неизвестен как отправителю, так и получателю сообщения. Идея данного метода основана на использовании доверенных агентов для хранения сообщения M в течение заданного интервала времени t. Для большей надёжности схемы шифрования, ключ K, на котором мы собираемся зашифровать сообщение M, поделим на N долей («теней») с использование схемы Шамира. Далее распределим “тени“ секретного ключа среди нескольких агентов, заручившись с их стороны обязательством, что соответствующие фрагменты будут предъявлены по истечении времени t . Отметим, что используемая техника разделения секрета обладает избыточностью и позволяет

восстанавливать секретный ключ в случае, когда некоторые агенты не в состоянии выполнять свои функции. Тогда криптограмма $C = E(K,M)$ может быть помещена в общедоступное место (например, в облачный сервер) с тем, чтобы можно было получить сообщение M (восстановив ключ K и расшифровав сообщение C) по истечении времени t .

Реализация системы. Разработана программа для Android-устройств, которая воспроизводит работу алгоритма Шамира с добавлением временного замка. Входными данными является секрет (ключ в виде текстового файла), а выходными данными – части ключа, которые распределены между участниками. На скриншоте (рис. 1а) показаны входные данные для фазы разделения секрета. Ключ, который распределяется, генерируется случайным образом, затем разбивается на соответвующее участникам количество подключей и отправляется на почту каждому участнику. Также устанавливается дата, по наступлению которой файл станет доступным для открытия. Указывается количество подключей, кворум, и почтовые адреса участников. Зашифрованный файл отправляется на сервер.



а б

Рис. 1 – Экранные формы программы (а – фаза разделения секрета, б – фаза восстановления)

Для получения файла с сервера (рис.2) нам необходимо знать его идентификатор (сообщается пользователю, как только файл был отправлен на сервер), под которым он помещен на сервер, и соответствующие ключи. Если все параметры совпадают, программа восстанавливает и загружает всем пользователям исходный файл.

Выводы. Проведен сравнительный анализ трех схем разделения секрета: алгоритмов Шамира, Блэкли, Карнина–Грина–Хеллмана. Установлено, что схема Шамира является наиболее защищенной и экономичной. Исследованы принципы построения СРС с временным замком. Впервые реализована практически пороговая схема разделения секрета с временным замком в виде Web-приложения для N участников процесса разделения/восстановления.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шнайер Б. Прикладная криптография // М. : Изд-во ТРИУМФ, 2003. – 653 с.
2. L. Harn, C. Lin. Detection and identification of cheaters in (t, n) secret sharing scheme. – Des. Codes Cryptography – v. 52(1). – 2009. – P. 15-243.
3. Запечников С. В.. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия – Телеком, 2007. - 320 с.