УДК 004.021

РАЗРАБОТКА ГИБРИДНОЙ КРИПТОСИСТЕМЫ ДЛЯ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ

А.В. СУББОТИН
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

Рассматривается проектирование гибридной криптосистемы для защиты данных. Проведён анализ технологий, наиболее подходящих, для разработки данной схемы.

Введение. Важнейшим требованием к системе шифрования является стойкость данной системы. К сожалению, повышение стойкости при помощи любого метода приводит, как правило, к трудностям и при шифровании открытого текста и при его расшифровке. Одним из наиболее эффективных методов повышения стойкости шифротекста является метод комбинированного шифрования. Этот метод заключается в использовании и комбинировании нескольких простых способов шифрования.

Основная часть. Степень изученности методов шифрования достаточно высокая. Каждый год создается множество программ, литературы, посвящённые криптографическим системам. Криптографическая система – семейство преобразований шифра и совокупность ключей. Существуют симметричные и асимметричные криптосистемы.

Симметричные криптосистемы (с секретным ключом) – данные криптосистемы построены на основе сохранения в тайне ключа шифрования. Процессы шифрования и расшифровки используют один и тот же ключ. Секретность ключа является постулатом.

Асимметричные криптосистемы (системы открытого шифрования – с открытым ключом) – смысл данных криптосистем состоит в том, что для шифрования и расшифровки используются разные преобразования. Одно из них – шифрование – является абсолютно открытым для всех. Другое же – расшифровка – остается секретным [1].

На данный момент чаще используются достаточно стойкие системы, системы с достаточно сложным алгоритмом шифрования. Из-за необходимости различных объектов зашифровывать секретные данные и криптографические системы не стоят на месте и постоянно совершенствуются.

Выбор алгоритмов шифрования. На основании анализа наиболее криптоустойчивых алгоритмов были сделаны следующие выводы:

– шифрование информации с помощью симметричного алгоритма AES, так как, несмотря на недостатки, взломать защищенную с помощью этого алгоритма информацию практически нереально. Суть AES в том, что любая «лобовая атака» на защищенные данные – то есть подбор всех возможных паролей – в перспективе очень сильно растягивается. Если представить, что взломщик располагает огромными ресурсами, то есть целой коллекцией суперкомпьютеров, то при усердном старании доступ к зашифрованным данным он мог бы получить через десятки лет.

–шифрование сеансового ключа с помощью асимметричным алгоритмом RSA-OAEP, так как это не только возведение в степень по модулю большого числа. Это еще и добавление избыточных данных позволяющих реализовать дополнительную защиту вашей информации [2].

Структурная схема протокола обмена данными. Пусть два абонента договорились обмениваться данными. Схема, показанная на рисунке, предполагает наличие у каждого участника информационного обмена двух ключей: открытого PK и закрытого SK. Рассмотрим процесс пересылки некоего документа M. Отправитель (абонент A) вырабатывает секретный ключ – случайное число, используемое только один раз и поэтому называемое одноразовым или сеансовым ключом. Этот ключ используется для шифрования документа M при помощи симметричного криптоалгоритма. Сеансовый ключ зашифровывается на открытом ключе получателя (абонент B) и присоединяется к ранее зашифрованному документу. Сформированное сообщение отсылается получателю. Последний, получив сообщение, повторяет те же процедуры, но в обратном порядке. С помощью своего секретного ключа получатель восстанавливает сеансовый ключ, а затем с его помощью расшифровывает и сам документ.

Выбор длины сеансового ключа. Вторым шагом является выбор длины сеансового ключа. От размера ключа зависит число раундов шифрования:

– длина 128 бит – 10 раундов;
– длина 192 бита – 12 раундов;
– длина 256 бит – 14 раундов.

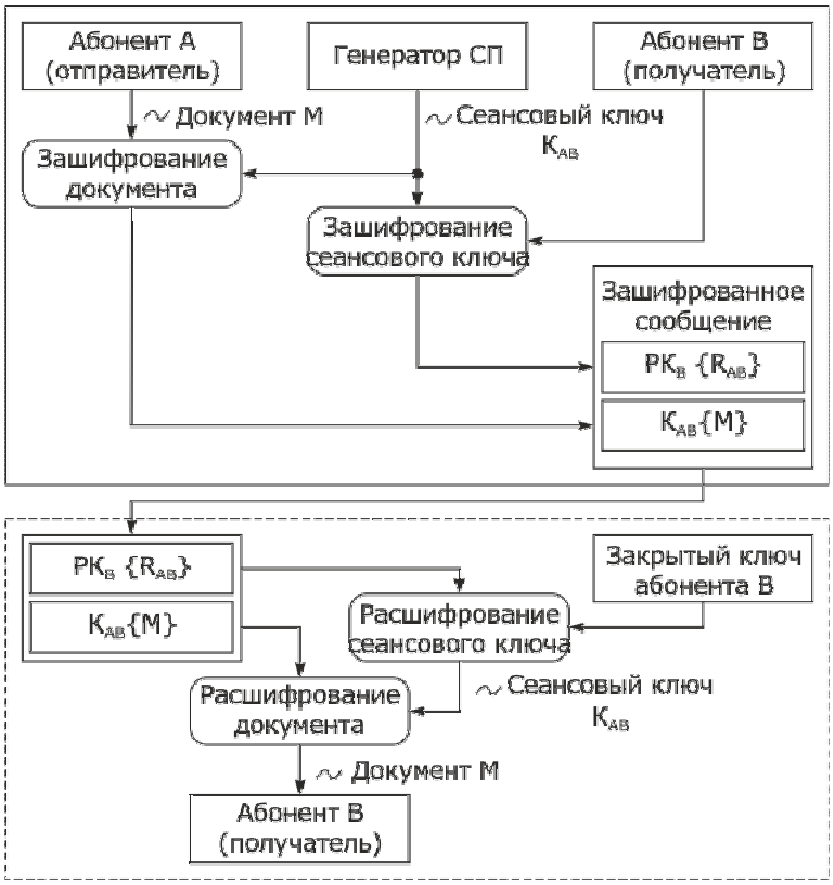

Рисунок. – Схема обмена двух ключей

В качестве примера примем длину ключа, равную 128 бит. Входными данными для операций шифрования есть массив из 16 байт. Перед началом шифрования байты этого массива размещаются последовательно в столбцы матрицы. Внутри алгоритма операции выполняются над матрицей байт, называемой матрицей состояний. Конечное значение матрицы состояния является выходом алгоритма и преобразуется в последовательность байтов шифротекста. Аналогично в столбцы исходной матрицы попадают и 16 байтов ключа шифра. Размерность всех матриц – 4 × 4. Четыре байта в каждом столбце матрицы состояний или ключа можно рассматривать как одно 32-х битовое слово. Поэтому матрица состояний – это массив из 4 слов. Матрица, поступающая на вход каждого раунда, называется матрицей входящего состояния, а на выходе раунда образуется матрица выходящего состояния [3].

Заключение. В ходе данного исследования был спроектирована гибридная криптосистема для защиты пользовательских данных с использованием алгоритмов AES, RSA-OAEP. При этом разработанная схема оставляет возможность для доработки и введения дополнительных средств защиты.

ЛИТЕРАТУРА

1. Мао Венбо, Современная криптография: теория и практика : пер. с англ. / Мао Венбо. – М. : Издат. дом «Вильямс», 2005.
2. Pointcheval, D. HD-RSA: hybrid dependent RSA, a new public-key encryption scheme. Submission to IEEE P1363: A symmetric Encription / D. Pointcheval. – 1999.
3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты ДМК / А.А. Петров. – 2000.