электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

Симметричное и асимметричное шифрование

 # 01, январь 2013
УДК: 004.056.55
Гончаров Н. О.

Введение

Целью работы является изучение симметричного и асимметричного шифрования, которые являются актуальными и криптографически гарантированными методами защиты информации, а также изучение методов и принципов работы шифрования. Разработка программного обеспечения по реализации алгоритмов симметричного и асимметричного шифрования с целью их сравнения.

В процессе выполнения работы выполнен анализ известных данных о методах симметричного шифрования. Рассмотрен метод классического шифрования Шеннона [1], блочные шифры - американский шифр *DES* [2] и отечественный шифр, определённый стандартом ГОСТ 28147-89, *IDEA (International Data Encryption Algorithm)*, *CAST*, Шифр *Skipjack*, *RC2* и *RC4* и др. [3].

Кроме того, выполнена опытно-экспериментальная работа по разработке программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании и схемы *RSA*, используя при этом язык объектно-ориентированного программирования *Visual Basic* [4].

1.Шифрование открытого текста

Шифрование бывает двух типов: симметричное и асимметричное (шифрованием с открытым ключом).

При симметричном шифровании генерируется ключ, который используется программой для шифрования данных. После результат пересылается адресату, а сам ключ (пароль или некоторый файл данных) передаётся отдельно и чаще всего по защищённому каналу связи. Запустив ту же самую шифровальную программу с полученным ключом, адресат сможет прочитать сообщение. Симметричное шифрование надежно, как и асимметричное, и из-за высокой скорости оно широко используется в операциях

электронной торговли. Виды и методы симметричного шифрования были более подробно рассмотренные мною в предыдущей статье [5].

Асимметричное шифрование является более сложным в реализации. Для работы алгоритмов асимметричного шифрования необходимо сгенерировать два взаимосвязанных ключа: открытый и закрытый. Владелец такой пары ключей, сообщает открытый ключ всем желающим, что позволяет им зашифровывать данные. Закрытый ключ знает только владелец, что и позволяет только ему расшифровать данные. Данный вид шифрования основан на сложных математических преобразованиях. Производимые вычисления в этом случае намного сложнее, чем в симметричном шифровании и процедура занимает больше времени.

Ключи, применяемые для шифрования, различаются по длине и по силе: ведь чем длиннее ключ, тем больше число возможных комбинаций. Если программа шифрования использует 128-битовые ключи, то ваш конкретный ключ будет одной из 3,4 триллиона миллиардов, или 2128 возможных комбинаций нулей и единиц.

2.Асимметричное шифрование

Асимметричное шифрование, или шифрование с открытым ключом, основано на использовании пары ключей: закрытого (частного) и открытого (публичного). Послание можно зашифровать и частным, и публичным ключом, а расшифровать только вторым ключом из пары. Частный ключ известен только владельцу, в то время как публичный ключ распространяется открыто и известен всем. Пару ключей можно использовать для решения задач аутентификации, для обеспечения конфиденциальности.

Аутентификацией (*Authentication*) называется процедура проверки подлинности предъявляемого пользователем идентификатора[6].

На рисунке 1 представлена схема шифрования для решения задач аутентификации. Пользователь А отсылает публичный ключ пользователям В и С, затем А отправляет им сообщение, зашифрованное его частным ключом.

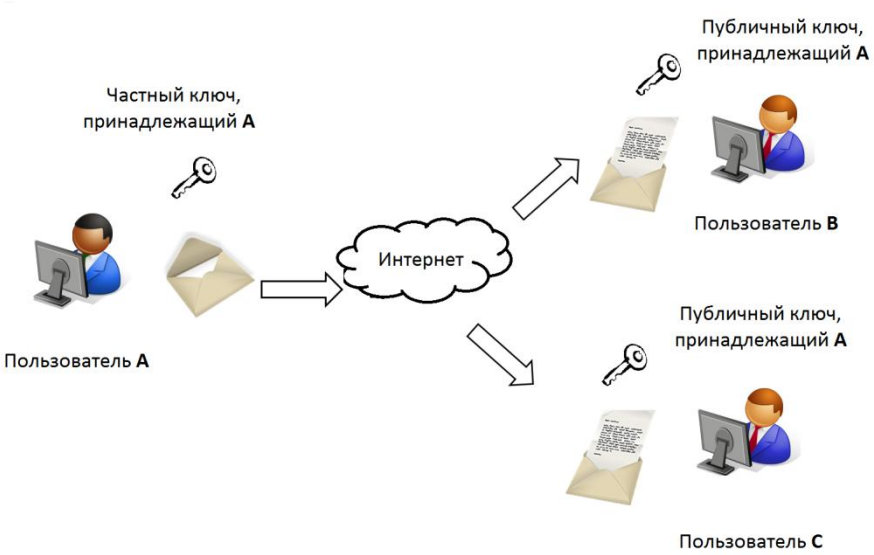

Рисунок 1. Схема шифрования для решения задач аутентификации

Сообщение мог послать только А (лишь он обладает частным ключом), проблема аутентификации решена. Но В не уверен, что письмо не прочитал также С. Таким образом, конфиденциальность не обеспечена.

На рисунке 2 представлена схема, обеспечивающая конфиденциальность. Пользователи В и С зашифровывают сообщения полученным от пользователя А публичным ключом, и передают его А.

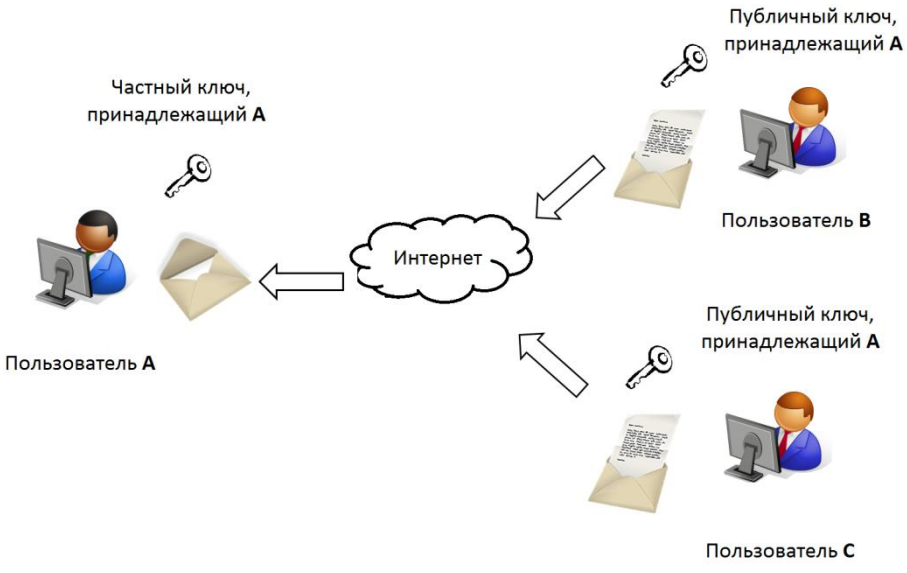

Рисунок 2. Схема шифрования обеспечивающая конфиденциальность

Сообщение может прочесть только пользователь А, так как лишь он обладает частным ключом, проблема конфиденциальности решена. Но А не может быть уверен, что сообщение не прислал С, выдающий себя за В. Таким образом, аутентификация не

обеспечивается. Для обеспечения конфиденциального обмена сообщениями в переписке двух лиц необходимо иметь две пары ключей. Удобно выложить публичный ключ в Сети на сервере с открытым доступом. Каждый может скачать данный ключ и послать А секретное сообщение, которое, кроме него, никто не прочтет.

3. Шифрование с симметричным и асимметричным ключом

Алгоритмы асимметричного шифрования сильно проигрывают симметричным алгоритмам с точки зрения времени шифрования и расшифрования данных, поэтому многие современные системы шифрования используют комбинацию асимметричного и традиционного симметричного шифрования. Шифрование с открытым ключом используется для передачи симметричного ключа, который служит непосредственно для шифрования передаваемой информации. Схема работы данной системы приведена на рисунке 3.

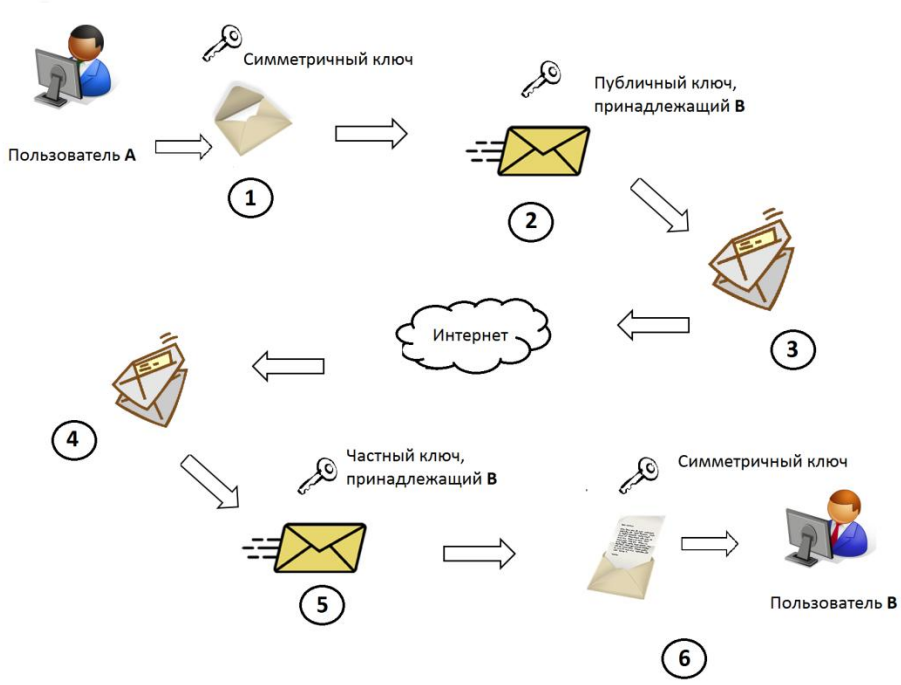

Рисунок 3. Схема шифрования с симметричным и ассиметричным алгоритмом

На первом этапе пользователь А шифрует исходный файл с помощью симметричного алгоритма. Затем на втором этапе пользователь А получает из открытых источников публичный(открытый) ключ принадлежащий пользователю В, и с помощью этого ключа зашифровывает симметричный ключ, который использовался на первом этапе. На третьем этапе зашифрованный файл и зашифрованный симметричный ключ

передаются пользователю B посредством интернета. После того как пользователь B на четвёртом этапе получил передаваемые ему данные, он на пятом этапе расшифровывает симетричный ключ с помощью своего частного(закрытого) ключа. На последнем, шестом этапе пользователь B, применяя расшифрованный на предыдущем этапе симметричный ключ, расшифровывает посланный ему файл.

Когда кто-то получает от вас сообщение, зашифрованное вашим частным ключом, он уверен в аутентичности послания, шифрование эквивалентно поставленной подписи (электронная цифровая подписи).

Электронная цифровая подпись (ЭЦП) - это метод аутентификации отправителя, подтверждающий, что содержание документа не было изменено. ЭЦП может быть поставлена в зашифрованном, и в открытом послании.

4.Схемы и принципы асимметричного шифрования.

Схемой открытого шифрования (или асимметричной схемой шифрования) AE=(K,E,D) называется совокупность трёх алгоритмов:

1) алгоритма генерации ключей K;

2) алгоритма зашифрования E;

3) алгоритма расшифрования D.

Существует два главных фактора, определяющих качество любых криптосистем – стойкость и производительность. Ещё существует два главных фактора, влияющих на стойкость асимметричных криптосистем – выбор вычислительно сложной задачи и выбор алгебраической структуры, на базе которой реализуется криптосистема. Сложность решения одной и той же теоретико-числовой задачи в разных алгебраических структурах может быть различна: от полиномиальной сложности до экспоненциальной.

В современной криптографии широко применяются три класса вычислительно сложных задач. Первый класс – это задача факторизации целых чисел и различные её варианты. Второй класс – это задача дискретного логарифмирования и производные от неё задачи. Третьим классом являются задачи, основанные на отображениях между алгебраическими структурами.

Криптосистемы с открытым ключом используют необратимые, однонаправленные функции. При заданном x просто вычислить $f(x)$, однако вычисление x из $f(x)$ проблематично за разумное время.

Алгоритм Диффи-Хелмана (1976) использует функцию дискретного возведения в степень и используется для открытого распределения ключей по открытому каналу связи. Первая публикация появилась в статье Диффи и Хеллмана, в которой вводились понятия криптографии с открытым ключом и в общих чертах упоминался алгоритм обмена ключа Диффи-Хеллмана [7].

Целью алгоритма является безопасный обмен ключами между участниками. Алгоритм основан на трудности вычислений дискретных логарифмов. Безопасность обмена ключа в алгоритме Диффи-Хеллмана вытекает из факта, что, хотя относительно легко вычислить экспоненты по модулю простого числа, трудно вычислить дискретные логарифмы. Для больших простых чисел задача считается неразрешимой.

5.Алгоритм шифрования с несимметричным ключом (*RSA*)

Алгоритм *RSA* стоит у истоков асимметричной криптографии. Он предложен исследователями-математиками Рональдом Ривестом, Ади Шамиром, Леонардом Адлеманом.

Первым этапом любого асимметричного алгоритма шифрования является создание пары ключей: открытого и закрытого (с последующим свободным распространением открытого ключа).

Для алгоритма RSA этап создания ключей состоит из следующих операций:

- Выбираются два простых числа $\boldsymbol{p}$ и $\boldsymbol{q}$;
- Вычисляется их произведение $\boldsymbol{n = p*q}$;
- Вычисляется значение функции Эйлера от числа $\boldsymbol{n}$, $\boldsymbol{\varphi(n) = (p-1)(q-1)}$;
- Выбирается произвольное $\boldsymbol{e}$ ($\boldsymbol{e<n}$), такое, что наименьший общий делитель (НОД) $\boldsymbol{\left(e,(p-1)(q-1)\right)=1}$, т.е. должно быть взаимно простым с числом $\boldsymbol{\varphi(n) = (p-1)(q-1)}$;
- Методом Евклида решается в целых числах уравнение $\boldsymbol{e*d+(p-1)(q-1)*y=1}$. Неизвестными являются переменные $\boldsymbol{d}$ и $\boldsymbol{y}$ – метод Евклида находит множество пар ($\boldsymbol{d}$, $\boldsymbol{y}$), каждая из которых является решением уравнения в целых числах;
- два числа ($\boldsymbol{e}$, $\boldsymbol{n}$) – публикуются как открытый ключ;
- число $\boldsymbol{d}$ хранится в строжайшем секрете – это закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел ($\boldsymbol{e}$, $\boldsymbol{n}$).

Шифрование с помощью этих чисел производится так:

- отправитель разбивает свое сообщение на блоки, равные $\boldsymbol{k = [log_2(n)]}$ бит, где квадратные скобки обозначают взятие целой части от дробного числа;
- для каждого такого числа (назовем его $\boldsymbol{m_i}$) вычисляется выражение $\boldsymbol{c_i = (m_i)^e mod\ n}$.

Демонстрация работы данного алгоритма приведена на рисунке 6. Блок-схема представлена на рисунке 5.

Блоки $\boldsymbol{c_i}$ являются зашифрованным сообщением, их можно передавать по открытому каналу. Операция возведения в степень по модулю простого числа является необратимой математической задачей. Обратная задача носит название «логарифмирование в конечном поле» и является более сложной. Если злоумышленник знает числа $\boldsymbol{e}$ и $\boldsymbol{n}$, то по значению $\boldsymbol{c_i}$ прочесть исходные сообщения $\boldsymbol{m_i}$ он может, только выполнив полный перебор $\boldsymbol{m_i}$.

Эксперементальная часть

Для сравнительного анализа и демонстрации симметричного и асимметричного метода мною были написаны две программы на языке объектно-ориентированного программирования *Visual Basic*.

Первая программа демонстрирует симметричный метод (гаммирование), алгоритм работы программы приведён на рисунке 4.

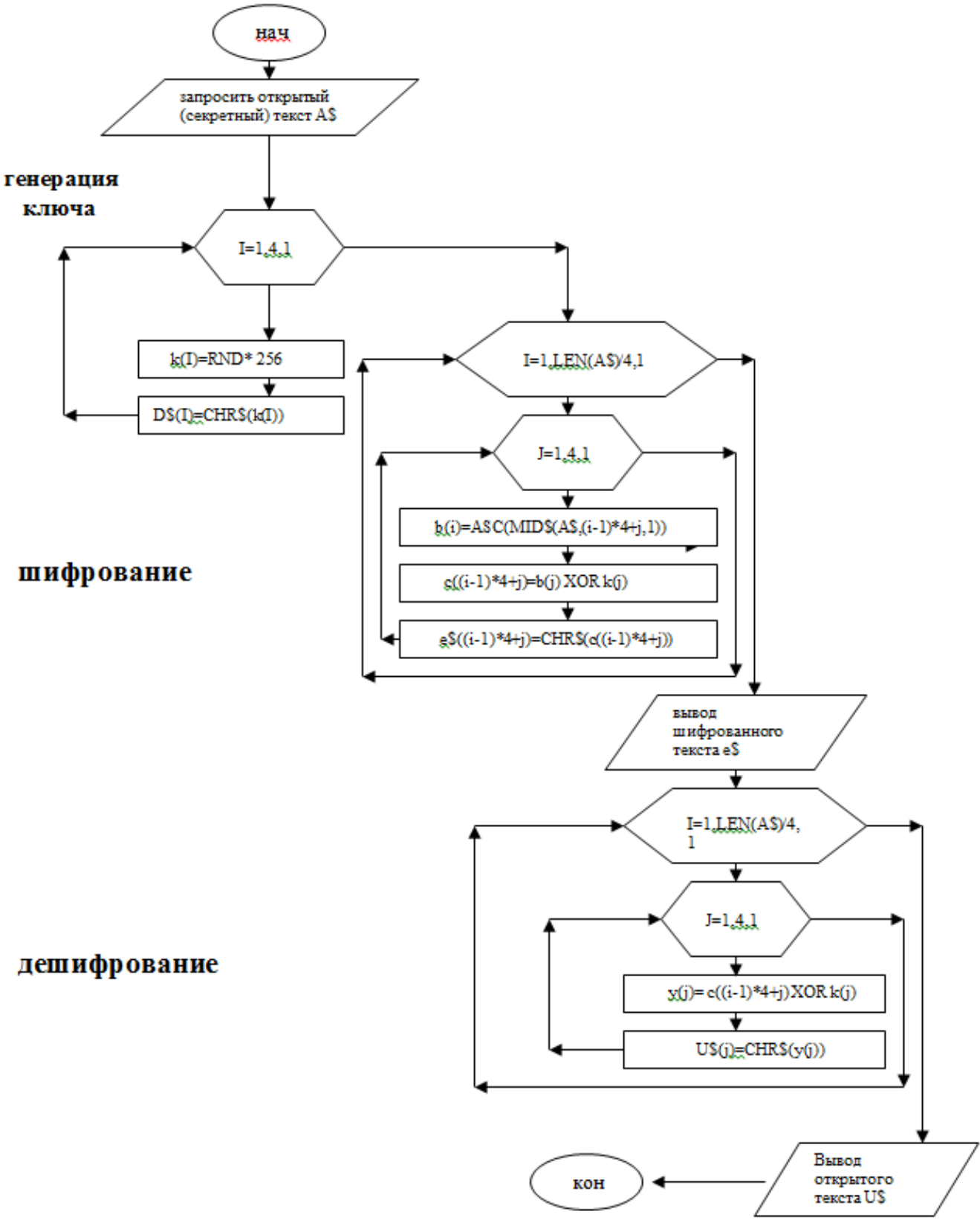

Рисунок 4. Блок-схема работы программы основанной на гаммировании

Во второй программе реализован алгоритм симметричного шифрования *RSA*. Алгоритм работы программы с примером представлен на рисунке 5.

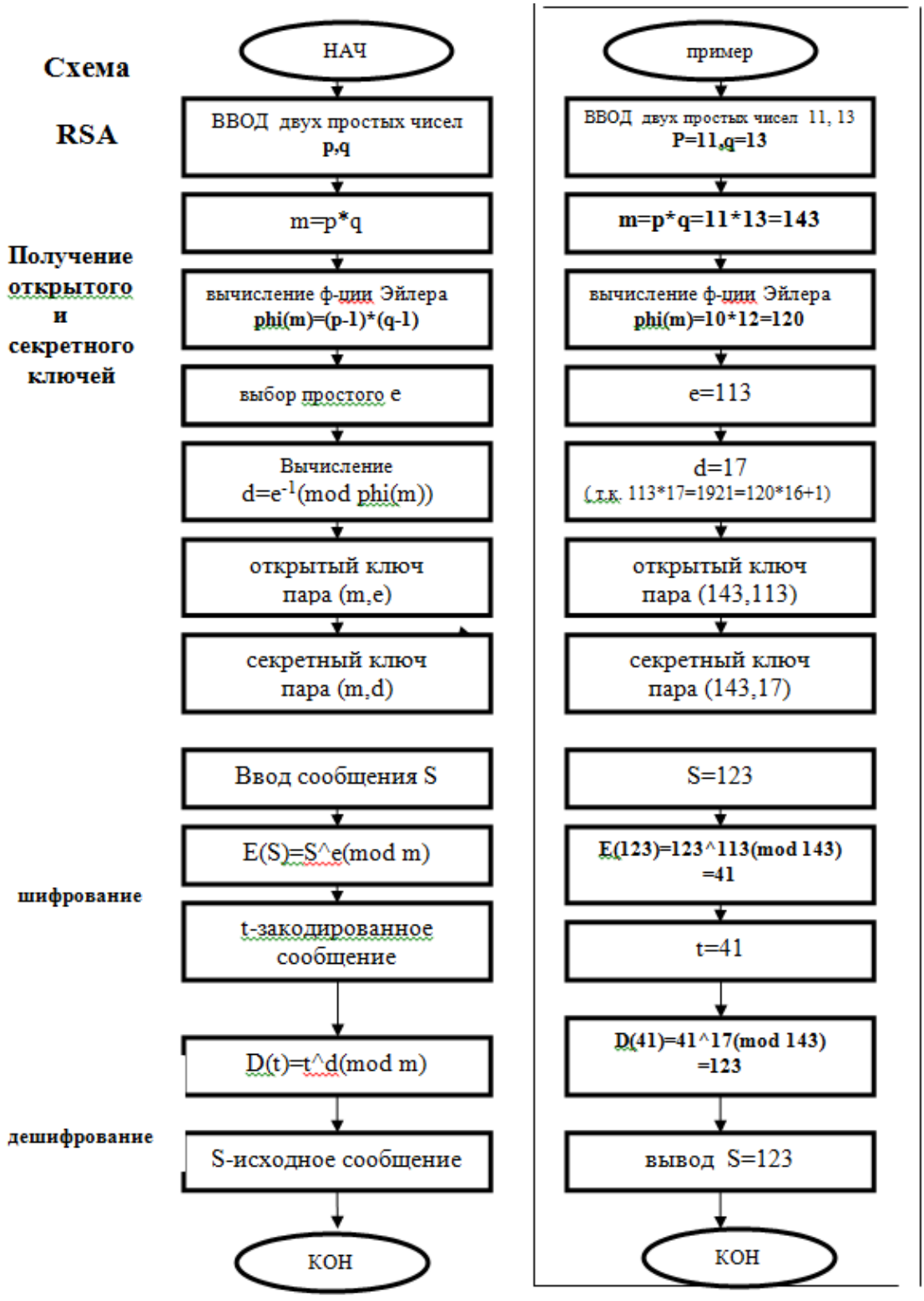

Рисунок 5. Блок-схема работы программы основанной на криптосистеме *RSA*

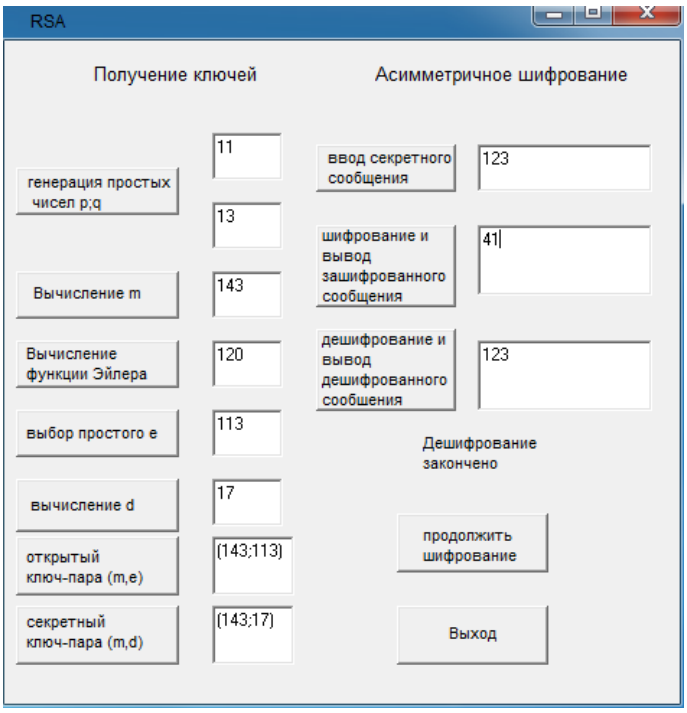

Рисунок 6. Программа демонстрирующая пример работы криптосистемы *RSA*

Для сравнения работы этих двух методов произвёдем шифрование сообщения «security». Сначала зашифруем данное сообщение симметричным методом.

На первом этапе программа генерирует псевдослучайную последовательность длинной 32 бита, она будет являтся ключом шифрования. В нашем случае это «8©уЄ».

Вторым этапом является ввод сообщения «security».

Далее прозводится шифрование сообщения и на выходе мы получаем зашифрованное сообщение «KMђЯJA‡У».

На последнем этапе происходит процесс дешифрования и выводится дешифрованное сообщение, которое совпадает с исходным. Работа программы приведена на рисунке 7.

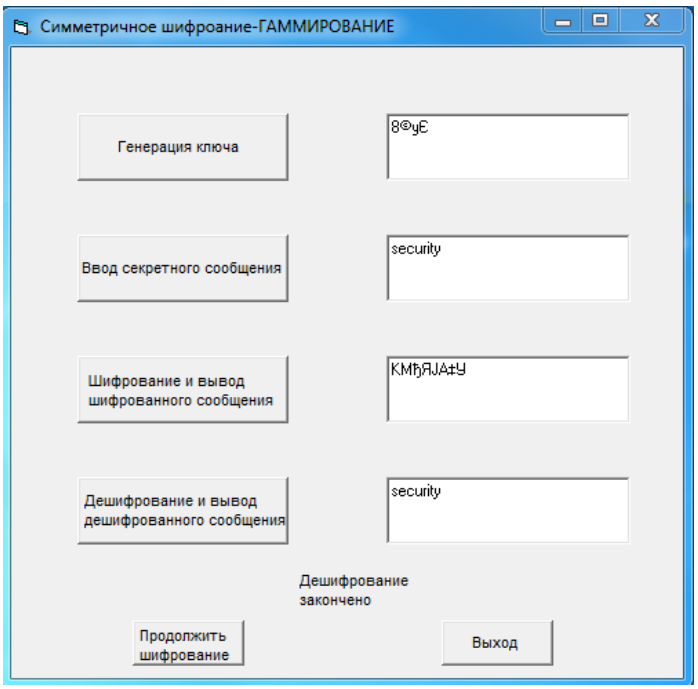

Рисунок7. Работы программы реализующей симметричное шифрование

Теперь зашифруем тоже самое сообщение асимметричным методом.

Сначала программа вычисляет открытую и закрытую пару ключей. Затем мы вводим сообщение «security» и производим шифрование, используя открытую пару ключей, получаем зашифрованное сообщение «7CQ9>G0#».

На заключительном этапе, используя закрытую пару ключей, производим дешифрование и получаем сообщение совпадающее с исходным. Работы программы приведена на рисунке 8.

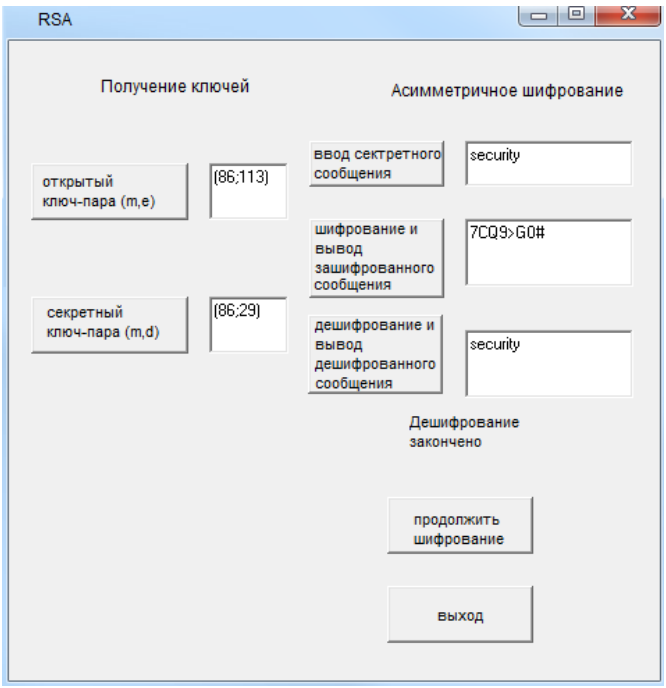

Рисунок 8. Работы программы реализующей асимметричное шифрование

Заключение

Симметричное и асимметричное шифрование остаются актуальными и криптографически гарантированными методами защиты информации. При передаче и хранении ценной или секретной информации её защищают с помощью криптосистем смешанного типа. С помощью двухключевых асимметричных алгоритмов решается задача распределения ключей для симметричных шифров.

Алгоритмы с симметричными ключами имеют очень высокую производительность. Криптография с симметричными ключами очень стойкая, что делает практически невозможным процесс дешифрования без знания ключа. При прочих равных условиях стойкость определяется длиной ключа. Так как для шифрования и дешифрования используется один и тот же ключ, при использовании таких алгоритмов требуются очень надежные механизмы для распределения ключей.

Асимметричное шифрование сложнее. В схеме кодирования с открытым ключом невозможно вычислить процедуру дешифрования, зная процедуру шифрования. Более точно, время работы алгоритма, вычисляющего процедуру расшифровки, настолько велико, что его нельзя выполнить на любых современных компьютерах, равно как и на любых компьютерах будущего.

Следует отметить, что алгоритм асимметричного шифрования сильно проигрывает симметричным с точки зрения времени шифрования и расшифровки данных, поэтому многие современные системы шифрования используют комбинацию асимметричной и

традиционной симметричной систем шифрования. Шифрование с открытым ключом используется для передачи симметричного ключа, который служит непосредственно для шифрования информации.

Всем системам открытого шифрования присущи следующие основные недостатки: ключ должен передаваться по секретному каналу; к службе генерации ключей предъявляются повышенные требования, обусловленные тем, что для ***n*** абонентов при схеме взаимодействия "каждый с каждым" требуется ***n*(n-1)/2*** ключей, то есть зависимость числа ключей от числа абонентов является квадратичной. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

Шифрование с несимметричным ключом является более криптостойким, но более медленным и дорогим по сравнению с шифрованием с симметричным ключом. Двухключевые шифры редко применяются для непосредственного шифрования. Они в основном используются при работе с электронными документами.

В перспективах возможно разработать методы и их программно-аппаратную реализацию по увеличению длины псевдослучайной последовательности, а также осуществить передачу ключей на основе квантовой криптографии. Идея вычислительной системы основана на вероятностной логике и работает с квантовыми битами – кубитами, которые могут находится в трёх состояниях - двух фиксированных и в состояние суперпозиции. Квантовые компьютеры должны обладать высокой вычислительной мощностью, но ограничение квантовой механики не позволяли создать рабочий модели. В конце 2012 года учёным удалось создать из двух кубитов первый прототип квантового логического инвертора – элемент осуществляющий операцию «контролируемое НЕ». Конечно, одного логического элемента не достаточно для создания полноценной вычислительной системы, но последние исследования в области квантовой физики открывают пути к дальнейшим развитиям в данной области.

Литература:

1. Шеннон К. Э. Работы по теории информации и кибернетике, М.: ИЛ, 1963. 832 с.

2. А.В. Аграновский, Р.А. Хади. Практическая криптография (серия «Аспекты защиты»), М.: Солон-Пресс, 2002. 254 с.

3. Т.Л. Партыка, И.И. Попов. Информационная безопасность. М.: Форум-Инфра, 2007. 368 с.

4. С.В. Глушаков А.С.Сурядный. Программирование на Visual Basic 6. Х.: Фалио, 2004. 497с.

5. Н.О. Гончаров. Симметричное шифрование (гаммирование). // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 3. Режим доступа: http://technomag.edu.ru/doc/187185.html (дата обращения 05.01.2013).

6. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

7. У.Диффи и М.Э.Хеллман. Новые направления в криптографии,1976 . 654 с.