Аннотация

Данная дипломная работа посвящена защите алгоритмом шифрования протокола обмена данных в программно-аппаратном комплексе «Звезда» версии 1.2.

Назначение – обеспечение защищенного канала передачи данных посредством реализации алгоритма шифрования в качестве библиотеки, модуль которого подключается и используется в программно-аппаратном комплексе для предотвращения перехвата, чтения и изменения данных, которые определяют состояние и управляют системой «Звезда» версии 1.2.

В дипломной работе описаны существующие решения указанной проблемы и их сравнительный анализ. Приведено описание работы разработанной автоматизированной системы. Кроме того, дипломная работа включает в себя руководство оперативного пользователя , руководство программиста (для корректного сопровождения программного продукта), а так же главы, в которых произведена оценка качества и экономическое обоснование эффективности применения системы.

Annotation

This thesis is dedicated to protecting the encryption algorithm in the data exchange protocol software and hardware complex "Star" version 1.2.

Purpose - to ensure secure data transmission channel by implementing encryption algorithm as a library module which is included and used in the software and hardware complex to prevent eavesdropping, read and modify data that define the state of the system and run "Star" version 1.2.

In the research paper describes existing solutions to this problem and their comparative analysis. Describes the work developed an automated system. In addition, the thesis includes a manual operational user guide programmer (for correct tracking software), as well as chapters that evaluated the quality and efficiency of economic feasibility of the system.

Оглавление

[Введение 6](#_Toc390609683)

[1. Постановка задачи 7](#_Toc390609684)

[1.1. Описание предметной области 7](#_Toc390609685)

[1.2. Требования, предъявляемые к проекту 7](#_Toc390609686)

[1.3. Формулировка задачи 7](#_Toc390609687)

[Выводы по главе 8](#_Toc390609688)

[2. Аналитическая часть 9](#_Toc390609689)

[2.1. Система шифрования RSA 10](#_Toc390609690)

[2.2. Сложность теоретико-числовых алгоритмов 14](#_Toc390609691)

[2.2.1. Алгоритм вычисления ad(mod m) 15](#_Toc390609692)

[2.2.2. Алгоритм Евклида 15](#_Toc390609693)

[2.2.3. Алгоритм решения уравнения ax + by = 1 16](#_Toc390609694)

[2.2.4. Алгоритм нахождения делителей многочлена  в кольце Fp[x] 18](#_Toc390609695)

[2.3. Качественная теория алгоритма RSA 21](#_Toc390609696)

[2.3.1. Алгоритм доказывающий не простоту числа 22](#_Toc390609697)

[2.3.2. Нахождение больших простых чисел 24](#_Toc390609698)

[2.3.3. Проверка большого числа на простоту 28](#_Toc390609699)

[2.4. Выбор алгоритма шифрования 33](#_Toc390609700)

[Выводы по главе 36](#_Toc390609701)

[3. Проектирование 37](#_Toc390609702)

[3.1. Выбор платформы 37](#_Toc390609703)

[3.1.1. Описание существующих платформ 37](#_Toc390609704)

[3.2. Выбор языка программирования 44](#_Toc390609705)

[3.2.1. Java 44](#_Toc390609706)

[3.2.2. C++ 44](#_Toc390609707)

[3.2.3. PHP 45](#_Toc390609708)

[3.2.4. Python 45](#_Toc390609709)

[3.2.5. Perl 45](#_Toc390609710)

[3.2.6. Ruby 46](#_Toc390609711)

[3.2.7. Результат 46](#_Toc390609712)

[3.3. Проектирование функций 47](#_Toc390609713)

[3.4. Проектирование классов 49](#_Toc390609714)

[3.5. Проектирование классов исключений 51](#_Toc390609715)

[3.6. Модуль rsa.bigfile 52](#_Toc390609716)

[3.7. Формат VARBLOCK файла 52](#_Toc390609717)

[3.8. Модуль rsa.core 53](#_Toc390609718)

[Выводы по главе 53](#_Toc390609719)

[4. Тестирование и документирование 54](#_Toc390609720)

[4.1. Тестирование 54](#_Toc390609721)

[4.1.1. Монолитное тестирование 55](#_Toc390609722)

[4.1.2. Пошаговое тестирование 55](#_Toc390609723)

[4.2. Руководство программиста 56](#_Toc390609724)

[4.2.1. Назначение и область применения 56](#_Toc390609725)

[4.2.2. Характеристики программы 56](#_Toc390609726)

[4.2.3. Обращение к программе 57](#_Toc390609727)

[4.2.3.1. Генерация ключа 58](#_Toc390609728)

[4.2.3.2. Время генерации ключей 58](#_Toc390609729)

[4.2.3.3. Требования к размеру ключа 59](#_Toc390609730)

[4.2.3.4. Шифрование и дешифрование 60](#_Toc390609731)

[4.2.3.5. Низкоуровневые операции 61](#_Toc390609732)

[4.2.3.6. Подписывание и проверка 61](#_Toc390609733)

[4.2.3.7. Работа с большими файлами 63](#_Toc390609734)

[4.2.3.7.1. Применение 63](#_Toc390609735)

[4.2.3.7.2. Использование Python-RSA: VARBLOCK формат 63](#_Toc390609736)

[4.2.3.7.3. Формат VARBLOCK 65](#_Toc390609737)

[4.2.3.7.3.1. Простое сообщение 65](#_Toc390609738)

[4.2.3.7.3.2. Варианты формата base 128 65](#_Toc390609739)

[4.2.3.7.3.3. Структура сообщений 66](#_Toc390609740)

[4.3. Руководство пользователя 68](#_Toc390609741)

[4.3.1. Общие сведения о программе 68](#_Toc390609742)

[4.3.2. Установка 69](#_Toc390609743)

[4.3.2.1. Зависимости 70](#_Toc390609744)

[4.3.2.2. Разработка зависимостей 70](#_Toc390609745)

[Вывод по главе 70](#_Toc390609746)

[5. Экономическое обоснование разработки 71](#_Toc390609747)

[5.1. Описание работы 71](#_Toc390609748)

[5.2. Описание конкурентов 71](#_Toc390609749)

[5.3. Описание рынка сбыта 72](#_Toc390609750)

[5.4.1. Расчет трудоемкости 73](#_Toc390609751)

[5.4.2. Определение цены программной продукции 79](#_Toc390609752)

[5.4.3. Капитальные вложения 83](#_Toc390609753)

[5.4.4. Эксплуатационные расходы 84](#_Toc390609754)

[5.4.5. Показатель эффективности и годового экономического эффекта 85](#_Toc390609755)

[Вывод по главе 86](#_Toc390609756)

[Заключение 87](#_Toc390609757)

[Список литературы 88](#_Toc390609758)

[ПРИЛОЖЕНИЕ А: Исходный код шифрования и дешифрования 89](#_Toc390609759)

[ПРИЛОЖЕНИЕ Б: Исходный код работы с ключами 103](#_Toc390609760)

Введение

В программно-аппаратном комплексе «Звезда» версии 1.2(далее - «система»), позволяющей управлять механическими и электронными устройствами, а так же позволяющей следить за помещением, данные которых передаются на удаленные сервера и клиентские машины, защищены в связи с рисками последствий перехвата управления. В системе применено обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

В целом, шифрование состоит из двух составляющих — зашифрование и расшифрование.

С помощью шифрования обеспечиваются три состояния безопасности информации:

* Конфиденциальность. Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.
* Целостность. Шифрование используется для предотвращения изменения информации при передаче или хранении.
* Идентифицируемость. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор. Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию.

В настоящий момент существует огромное количество методов шифрования. Главным образом эти методы делятся, в зависимости от структуры используемых ключей, на симметричные и асимметричные методы.

1. Постановка задачи
   1. Описание предметной области

Безопасность передачи данных по каналам связи является актуальной. Современные компьютерные сети не исключение. К сожалению, в сетевых операционных системах (Windows NT/XP/Server, Novell и т.д.) иностранного производства, как следствие, из-за экспортных соображений уровень алгоритмов шифрования заметно снижен.

Исследовать современные методы шифрования и их применимость к шифрованию потоков данных. Разработать собственную библиотеку алгоритмов шифрования и программный продукт, демонстрирующий работу этих алгоритмов при передаче данных в сети.

* 1. Требования, предъявляемые к проекту

Поскольку техническое задание составлялось на основе готовой системы «Звезда», то и все действия были направленны на совместимость с ней. При составлении проекта были выделены основные требования:

* отказоустойчивость;
* легкое развертывание;
* разработка простого и удобного в использовании функционала;
* легкость и динамичность внесения изменения в программу;

В качестве модели реализации был выбран стандарт PKCS #1: RSA Encryption Version 1.5 RFC 2313.

* 1. Формулировка задачи

Основной задачей разработки является реализация удобного, гибкого механизма защиты протокола обмена данными.

Главными задачами системы являются:

Обеспечение надежного шифрования двунаправленной связи между сервером и клиентом;

* Легкое конфигурирование;
* Использование возможностей платформы.

Выводы по главе

В данной главе:

* было приведено общее описание требований для совместимости с системой «Звезда»;
* поставлена задача проектирования;
* принято решение создать программный продукт, удовлетворяющий выявленным требованиям.

1. Аналитическая часть

Труды Евклида и Диофанта, Ферма и Эйлера, Гаусса, Чебышева и Эрмита содер­жат остроумные и весьма эффективные алгоритмы решения диофантовых уравнений, выяснения разрешимости сравнений, построения больших по тем временам простых чисел, нахождения наилучших приближений и т.д. В последние два десятилетия, благодаря в первую очередь запросам криптографии и широкому распространению ЭВМ, исследова­ния по алгоритмическим вопросам теории чисел переживают период бур­ного и весьма плодотворного развития.

Вычислительные машины и электронные средства связи проникли практически во все сферы человеческой деятельности. Немыслима без них и современная криптография. Шифрование и дешифрование текстов можно представлять себе как процессы переработки целых чисел при помощи ЭВМ, а способы, которыми выполняются эти операции, как неко­торые функции, определённые на множестве целых чисел. Всё это делает естественным появление в криптографии методов теории чисел. Кроме того, стойкость ряда современных криптосистем обосновывается только сложностью некоторых теоретико-числовых задач.

Но возможности ЭВМ имеют определённые границы. Приходится раз­бивать длинную цифровую последовательность на блоки ограниченной длины и шифровать каждый такой блок отдельно. Мы будем считать в дальнейшем, что все шифруемые целые числа неотрицательны и по вели­чине меньше некоторого заданного (скажем, техническими ограничени­ями) числа m. Таким же условиям будут удовлетворять и числа, получае­мые в процессе шифрования. Это позволяет считать и те, и другие числа элементами кольца вычетов . Шифрующая функция при этом может рассматриваться как взаимно-однозначное отображение колец вычетов



а число  представляет собой сообщение  в зашифрованном виде.

Простейший шифр такого рода - шифр замены, соответству­ет отображению  при некотором фиксированном целом k. Подобный шифр использовал еще Юлий Цезарь. Конечно, не каждое отображение  подходит для целей надежного сокрытия инфор­мации.

В 1978 г. американцы Р. Ривест, А. Шамир и Л. Адлеман (R.L.Rivest. A.Shamir. L.Adleman) предложили пример функции , обла­дающей рядом замечательных достоинств. На её основе была построена реально используемая система шифрования, получившая название по пер­вым буквам имен авторов -система RSA. Эта функция такова, что

1) существует достаточно быстрый алгоритм вычисления значений ;

2) существует достаточно быстрый алгоритм вычисления значений об­ратной функции ;

3) функция  обладает некоторым «секретом», знание которого позво­ляет быстро вычислять значения ; в противном же случае вычисле­ние  становится трудно разрешимой в вычислительном отношении задачей, требующей для своего решения столь много времени, что по его  
прошествии зашифрованная информация перестает представлять инте­рес для лиц, использующих отображение  в качестве шифра.

Еще до выхода из печати статьи копия доклада в Массачусетском Технологическом институте, посвящённого системе RSA. была послана известному популяризатору математики М. Гарднеру, который в 1977 г. в журнале Scientific American опубликовал статью посвящённую этой системе шифрования. В русском переводе заглавие статьи Гарднера зву­чит так: Новый вид шифра, на расшифровку которого потребуются мил­лионы лет. Именно эта статья сыграла важнейшую роль в распростране­нии информации об RSA, привлекла к криптографии внимание широких кругов неспециалистов и фактически способствовала бурному прогрессу этой области, произошедшему в последовавшие 20 лет.

* 1. Система шифрования RSA

Пусть  и  натуральные числа. Функция  реализующая схему RSA, устроена следующим образом

. (1)

Для расшифровки сообщения  достаточно решить сравнение

. (2)

При некоторых условиях на  и  это сравнение имеет единственное решение .

Для того, чтобы описать эти условия и объяснить, как можно найти решение, нам потребуется одна теоретико-числовая функция, так назы­ваемая функция Эйлера. Эта функция натурального аргумента  обозна­чается  и равняется количеству целых чисел на отрезке от 1 до , взаимно простых с . Так  и  для любого простого числа  и натурального . Кроме того,  для лю­бых натуральных взаимно простых  и . Эти свойства позволяют легко вычислить значение , если известно разложение числа  на простые сомножители.

Если показатель степени  в сравнении (2) взаимно прост с , то сравнение (2) имеет единственное решение. Для того, чтобы найти его, определим целое число , удовлетворяющее условиям

. (3)

Такое число существует, поскольку , и притом единствен­но. Здесь и далее символом  будет обозначаться наибольший общий делитель чисел  и . Классическая теорема Эйлера, утверждает, что для каждого числа , взаимно простого с , выполняется сравнение  и, следовательно.

. (4)

Таким образом, в предположении , единственное решение срав­нения (2) может быть найдено в виде

. (5)

Если дополнительно предположить, что число  состоит из различных простых сомножителей, то сравнение (5) будет выполняться и без предпо­ложения . Действительно, обозначим  и . Тогда  делится на , а из (2) следует, что . Подобно (4), теперь легко находим . А кроме того, имеем . Получившиеся сравнения в силу  дают нам (5).

Функция (1), принятая в системе RSA, может быть вычислена доста­точно быстро. Обратная к  функция  вычисляется по тем же правилам, что и , лишь с заменой показателя степени  на . Таким образом, для функции (1) будут выполнены указанные выше свойства 1) и 2).

Для вычисления функции (1) достаточно знать лишь числа  и . Именно они составляют открытый ключ для шифрования. А вот для вы­числения обратной функции требуется знать число . оно и является «се­кретом», о котором речь идёт в пункте в). Казалось бы. ничего не стоит. зная число . разложить его на простые сомножители, вычислить затем с помощью известных правил значение  и, наконец, с помощью (3) определить нужное число . Все шаги этого вычисления могут быть реа­лизованы достаточно быстро, за исключением первого. Именно разложе­ние числа  на простые множители и составляет наиболее трудоемкую часть вычислений. В теории чисел несмотря на многолетнюю её историю и на очень интенсивные поиски в течение последних 20 лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден. Конечно, можно, перебирая все простые числа до , и. деля на них , найти требуемое разложение. Но, учитывая, что количество простых в этом промежутке, асимптотически равно , на­ходим, что при , записываемом 100 десятичными цифрами, найдётся не менее  простых чисел, на которые придётся делить  при разложе­нии его на множители. Очень грубые прикидки показывают, что компью­теру, выполняющему миллион делений в секунду, для разложения числа  таким способом на простые сомножители потребуется не менее, чем  лет. Известны и более эффективные способы разложения целых чисел на множители, чем простой перебор простых делителей, но и они работают очень медленно.

Авторы схемы RSA предложили выбирать число  в виде произведе­ния двух простых множителей  и , примерно одинаковых по величине. Так как

, (6)

то единственное условие на выбор показателя степени  в отображении (1) есть

. (7)

Итак, лицо, заинтересованное в организации шифрованной переписки с помощью схемы RSA, выбирает два достаточно больших простых числа  и . Перемножая их, оно находит число . Затем выбирается число , удовлетворяющее условиям (7), вычисляется с помощью (6) число  и с помощью (3) - число . Числа  и  публикуются, число  остается секретным. Теперь любой может отправлять зашифрованные с помощью (1) сообщения организатору этой системы, а организатор легко сможет расшифровывать их с помощью (5).

Для иллюстрации своего метода Ривест, Шамир и Адлеман зашифро­вали таким способом некоторую английскую фразу. Сначала она стан­дартным образом (а=01, b=02, .... z=26, пробел=00) была записана в виде целого числа , а затем зашифрована с помощью отображения (1) при

m=11438162575788886766932577997614661201021829672124236256256184293570 6935245733897830597123563958705058989075147599290026879543541

и . Эти два числа были опубликованы, причем дополнительно сообщалось, что . где  и  - простые числа, записываемые со­ответственно 64 и 65 десятичными знаками. Первому, кто расшифрует соответствующее сообщение

, была обещана награда в 100$.

Эта история завершилась спустя 17 лет в 1994 г., когда D. Atkins, M. Graff, А. К. Lenstra и Р. С. Leyland сообщили о расшифровке фразы. Числа  и  оказались равными

,

.

Этот замечательный результат (разложение на мно­жители 129-значного десятичного числа) был достигнут благодаря ис­пользованию алгоритма разложения чисел на множители, называемого методом квадратичного решета. Выполнение вычислений потребовало колоссальных ресурсов. В работе, возглавленной четырьмя авторами проекта, и продолжавшейся после предварительной теоретической под­готовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединённых сетью Inter­net. Наконец, отметим, что премия в 100$ была передана в Free Software Foundation.

* 1. Сложность теоретико-числовых алгоритмов

Сложность алгоритмов теории чисел обычно принято измерять коли­чеством арифметических операций (сложений, вычитаний, умножений и делений с остатком), необходимых для выполнения всех действий, пред­писанных алгоритмом. Впрочем, это определение не учитывает величины чисел, участвующих в вычислениях. Ясно, что перемножить два стозначных числа значительно сложнее, чем два однозначных, хотя при этом и в том, и в другом случае выполняется лишь одна арифметическая опе­рация. Поэтому иногда учитывают ещё и величину чисел, сводя дело к так называемым битовым операциям, т. е. оценивая количество необхо­димых операций с цифрами 0 и 1, в двоичной записи чисел.

Говоря о сложности алгоритмов, мы будем иметь в ви­ду количество арифметических операций. При построении эффективных алгоритмов и обсуждении верхних оценок сложности обычно хватает ин­туитивных понятий той области математики, которой принадлежит алго­ритм. Формализация же этих понятий требуется лишь тогда, когда речь идёт об отсутствии алгоритма или доказательстве нижних опенок слож­ности.

Приведем теперь примеры достаточно быстрых алгоритмов с опен­ками их сложности. Здесь и в дальнейшем мы не будем придерживаться формального описания алгоритмов, стараясь в первую очередь объяснить смысл выполняемых действий.

Следующий алгоритм вычисляет  за  арифмети­ческих операций. При этом, конечно, предполагается, что натуральные числа  и  не превосходят по величине .

* + 1. Алгоритм вычисления ad(mod m)

1. Представим  в двоичной системе счисления , где , цифры в двоичном представлении, равны 0 или 1, .
2. Положим  и затем для  вычислим

.

3)  есть искомый вычет .

Справедливость этого алгоритма вытекает из сравнения

,

легко доказываемого индукцией по .

Так как каждое вычисление на шаге 2 требует не более трёх умноже­ний по модулю  и этот шаг выполняется  раз, то сложность алгоритма может быть оценена величиной .

Второй алгоритм - это классический алгоритм Евклида вычисления наибольшего общего делителя целых чисел. Мы предполагаем заданными два натуральных числа  и  и вычисляем их наибольший общий дели­тель .

* + 1. Алгоритм Евклида

1. Вычислим  - остаток от деления числа  на , , .
2. Если , то  есть искомое число.
3. Если , то заменим пару чисел  парой  и перейдем к  
   шагу 1.

Теорема 1. При вычислении наибольшего общего делителя  с помощью алгоритма Евклида будет выполнено не более  операций де­ления с остатком, где  есть количество цифр в десятичной записи меньшего из чисел  и .

Доказательство. Положим  и определим  - последовательность делителей, появляющихся в процессе выполнения ша­га 1 алгоритма Евклида. Тогда

.

Пусть также , , , , - последователь­ность Фибоначчи. Индукцией по  от  до  легко доказывается неравенство . А так как , то имеем неравенства  и .

Немного подправив алгоритм Евклида, можно достаточно быстро ре­шать сравнения  при условии, что . Эта задача равносильна поиску целых решений уравнения .

* + 1. Алгоритм решения уравнения ax + by = 1

1) Определим матрицу .

2) Вычислим  - остаток от деления числа  на , , .

3) Если , то второй столбец матрицы  даёт вектор   
решений уравнения.

4) Если , то заменим матрицу  матрицей .

5) Заменим пару чисел  парой  и перейдем к шагу 1.

Если обозначить  через матрицу , возникающую в процессе работы алгоритма перед шагом 3 после  делений с остатком (шаг 2), то в обозначениях из доказательства теоремы 1 в этот момент выполняется векторное равенство . Поскольку числа  и  взаимно просты, имеем , и это доказы­вает, что алгоритм действительно даёт решение уравнения . Буквой  мы обозначили количество делений с остатком, которое в точ­ности такое же, как и в алгоритме Евклида.

Три приведённых выше алгоритма относятся к разряду так называе­мых полиномиальных алгоритмов. Это название носят алгоритмы, слож­ность которых оценивается сверху степенным образом в зависимости от длины записи входящих чисел. Если наибольшее из чисел, подаваемых на вход алгоритма, не превосходит , то сложность алгоритмов этого типа оценивается величиной , где  - некото­рая абсолютная постоянная. Во всех приведённых выше примерах .

Полиномиальные алгоритмы в теории чисел - большая редкость. Да и опенки сложности алгоритмов чаше всего опираются на какие-либо не доказанные, но правдоподобные гипотезы, обычно относящиеся к анали­тической теории чисел.

Для некоторых задач эффективные алгоритмы вообще не известны. Иногда в таких случаях все же можно предложить последовательность действий, которая, «если повезет», быстро приводит к требуемому ре­зультату. Существует класс так называемых вероятностных алгоритмов, которые дают правильный результат, но имеют вероятностную опен­ку времени работы. Обычно работа этих алгоритмов зависит от одного или нескольких параметров. В худшем случае они работают достаточно долго. Но удачный выбор параметра определяет быстрое завершение ра­боты. Такие алгоритмы, если множество «хороших» значений параметров велико, на практике работают достаточно эффективно, хотя и не имеют хороших опенок сложности.

Мы будем иногда использовать слова детерминированный алгоритм, чтобы отличать алгоритмы в обычном смысле от вероятностных алго­ритмов.

Как пример, рассмотрим вероятностный алгоритм, позволяющий эф­фективно находить решения полиномиальных сравнений по простому мо­дулю. Пусть  — простое число, которое предполагается большим, и  - многочлен, степень которого предполагается ограничен­ной. Задача состоит в отыскании решений сравнения

. (8)

Например, речь может идти о решении квадратичных сравнений, если степень многочлена  равна 2. Другими словами, мы должны отыскать в поле  все элементы, удовлетворяющие уравнению .

Согласно малой теореме Ферма, все элементы поля  являются од­нократными корнями многочлена . Поэтому, вычислив наибольший общий делитель , мы найдем многочлен , множест­во корней которого в поле  совпадает с множеством корней многочлена , причем все эти корни однократны. Если окажется, что многочлен  имеет нулевую степень, т. е. лежит в поле , это будет означать, что сравнение (8) не имеет решений.

Для вычисления многочлена  удобно сначала вычислить многочлен , пользуясь алгоритмом, подобным описанному выше алгоритму возведения в степень (напомним, что число  предполагается большим). А затем с помощью аналога алгоритма Евклида вычислить . Всё это выполняется за полиномиальное количество арифметических операций.

Таким образом, обсуждая далее задачу нахождения решений сравне­ния (8), мы можем предполагать, что в кольце многочленов  спра­ведливо равенство:



* + 1. Алгоритм нахождения делителей многочлена  в кольце Fp[x]

1) Выберем каким-либо способом элемент .

2) Вычислим наибольший общий делитель .

3) Если многочлен  окажется собственным делителем , то многочлен  распадётся на два множителя и с каждым из них незави­симо нужно будет проделать все операции, предписываемые настоящим алгоритмом для многочлена .

4) Если окажется, что  или , следует перейти к шагу 1 и. выбрав новое значение , продолжить выполнение алгоритма.

Количество операций на шаге 2 оценивается величиной , ес­ли вычисления проводить так, как это указывалось выше при нахожде­нии . Выясним теперь, сколь долго придётся выбирать числа , пока на шаге 2 не будет найден собственный делитель .

Количество решений уравнения  в поле  не превосходит . Это означает, что подмножество  элементов , удовлетворяющих условиям

,

состоит не менее, чем из  элементов. Учитывая теперь, что каждый ненулевой элемент  удовлетворяет одному из равенств , либо , заключаем, что для  одно из чисел  будет корнем многочлена , а другое - нет. Для таких элементов  многочлен , определённый на шаге 2 алгоритма, будет собственным делителем многочлена .

Итак, существует не менее  «удачных» выборов элемента , при которых на шаге 2 алгоритма многочлен  распадётся на два соб­ственных множителя. Следовательно, при «случайном» выборе элемента , вероятность того, что многочлен не разложится на множители после  повторений шагов алгоритма 1-4. не превосходит . Вероят­ность с ростом  убывает очень быстро. И действительно, на практике этот алгоритм работает достаточно эффективно.

Заметим, что при опенке вероятности мы использовали только два корня многочлена . При  эта вероятность, конечно, еще меньше. Более тонкий анализ с использованием опенок А. Вейля для сумм харак­теров показывает, что вероятность для многочлена  не распасться на множители при однократном проходе шагов алгоритма 1-4. не пре­восходит . Здесь постоянная в  зависит от .

Если в сравнении (8) заменить простой модуль  составным моду­лем , то задача нахождения решений соответствующего сравнения ста­новится намного более сложной. Известные алгоритмы её решения осно­ваны на сведении сравнения к совокупности сравнений (8) по простым модулям — делителям , и. следовательно, они требуют разложения чи­сла то на простые сомножители, что, как уже указывалось, является до­статочно трудоемкой задачей.

* 1. Качественная теория алгоритма RSA

Существует довольно эффективный способ убедиться, что заданное число является составным, не разлагая это число на множители. Согласно малой теореме Ферма, если число  простое, то для любого целого , не делящегося на , выполняется сравнение

. (9)

Если же при каком-то  это сравнение нарушается, можно утверждать, что  - составное. Проверка (9) не требует больших вычислений, это следует из алгоритма 1. Вопрос только в том, как найти для составного  целое число , не удовлетворяющее (9). Можно, например, пытаться найти необходимое число , испытывая все целые числа подряд, начиная с 2. Или попробовать выбирать эти числа случайным образом на отрезке .

К сожалению, такой подход не всегда даёт то, что хотелось бы. Име­ются составные числа , обладающие свойством (9) для любого целого  с условием . Такие числа называются числами Кармайкла. Рассмотрим, например, число . Так как 560 делится на каждое из чисел 2, 10, 16, то с помощью малой теоремы Ферма легко проверить, что 561 есть число Кармайкла. Можно доказать, что любое из чисел Кармайкла имеет вид , где все простые  различны, причем  делится на каждую разность . Лишь недавно, была решена проблема о бесконечности множества таких чисел.

В 1976 г. Миллер предложил заменить проверку (9) проверкой несколь­ко иного условия. Если  - простое число, , где  нечётно, то согласно ма­лой теореме Ферма для каждого  с условием  хотя бы одна из скобок в произведении



делится на . Обращение этого свойства можно использовать, чтобы от­личать составные числа от простых.

Пусть  - нечётное составное число, , где  нечётно. Назовем целое число , , «хорошим» для , если нарушается одно из двух условий:

1)  не делится на ;

2)  или существует целое , , такое, что

.

Из сказанного ранее следует, что для простого числа  не существует хороших чисел . Если же  составное число, то, как доказал Рабин, их существует не менее .

Теперь можно построить вероятностный алгоритм, отличающий со­ставные числа от простых.

* + 1. Алгоритм доказывающий не простоту числа

1. Выберем случайным образом число , , и проверим для  
   этого числа указанные выше свойства 1) и 2) п.2.
2. Если хотя бы одно из них нарушается, то число  составное.
3. Если выполнены оба условия 1) и 2) п.2, возвращаемся к шагу 1.

Из сказанного выше следует, что составное число не будет определено как составное после однократного выполнения шагов 1-3 с вероятностью не большей . А вероятность не определить его после  повторений не превосходит . т. е. убывает очень быстро.

Миллер предложил детерминированный алгоритм определения состав­ных чисел, имеющий сложность , однако справедливость его ре­зультата зависит от недоказанной в настоящее время так называемой расширенной гипотезы Римана. Согласно этому алгоритму достаточно проверить условия 1) и 2) п.2 для всех целых чисел , . Если при каком-нибудь  из указанного промежутка нарушается одно из условий а) или б), число  составное. В противном случае оно будет простым или степенью простого числа. Последняя возможность, конечно, легко проверяется.

Напомним некоторые понятия, необходимые для формулиров­ки расширенной гипотезы Римана. Они понадобятся нам и в дальнейшем. Пусть  - целое число. Функция  называется характе­ром Дирихле по модулю , или просто характером, если эта функция периодична с периодом , отлична от нуля только на числах, взаимно простых с , и мультипликативна, т. е. для любых целых  выполня­ется равенство . Для каждого  существует ровно  характеров Дирихле. Они образуют группу по умножению. Единичным элементом этой группы является так называемый главный характер , равный 1 на всех числах, взаимно простых с , и 0 на остальных це­лых числах. Порядком характера называется его порядок как элемента мультипликативной группы характеров.

С каждым характером может быть связана так называемая  - функция Дирихле - функция комплексного переменного , определённая рядом. Сумма этого ряда аналитична в области  и может быть аналитически продолжена на всю комплексную плос­кость. Следующее соотношение  связывает L - функцию, отвечающую главному характеру, с дзета-функцией Римана . Расширенная гипотеза Римана утверждает, что комплексные нули всех L -функций Дирихле, расположенные в полосе , лежат на прямой . В настоящее время не доказана даже простей­шая форма этой гипотезы - классическая гипотеза Римана, утвержда­ющая такой же факт о нулях дзета-функции.

В 1952 г. Анкени с помощью расширенной гипотезы Римана доказал, что для каждого простого числа  существует квадратичный невычет , удовлетворяющий неравенствам . Константа 70 была со­считана позднее. Именно это утверждение и лежит в основе алгоритма Миллера. В 1957 г. Берджесс доказал существование такого невычета без использования расширенной гипотезы Римана, но с худшей оценкой , справедливой при любом положительном  и , большем некоторой границы, зависящей от.

Алгоритм Миллера принципиально отличается от алгоритма 2.1., так как полученное с его помощью утверждение о том, что число  - со­ставное, опирается на недоказанную расширенную гипотезу Римана и по­тому может быть неверным. В то время как вероятностный алгоритм 2.1. даёт совершенно правильный ответ для составных чисел. Несмотря на отсутствие оценок сложности, на практике он работает вполне удовле­творительно.

* + 1. Нахождение больших простых чисел

Конечно же, большие простые числа можно строить сравнительно быстро. При этом можно обеспечить их случайное распределение в заданном диапазоне величин. В противном случае теряла бы всякий практический смысл система шифрования RSA. Наиболее эффективным средством построения простых чисел является несколько модифицированная малая теорема Ферма.

Теорема 2*.* Пусть  - нечётные натуральные числа, , причем для каждого простого делителя  числа  существует целое число  такое, что

. (10)

Тогда каждый простой делитель  числа  удовлетворяет сравнению

.

Доказательство. Пусть  - простой делитель числа , a  - не­который делитель . Из условий (10) следует, что в поле вычетов  спра­ведливы соотношения

. (11)

Обозначим буквой  порядок элемента  в мультипликативной группе поля . Первые два из соотношений (11) означают, что  входит в раз­ложение на простые множители числа  в степени такой же, как и в раз­ложение , а последнее - что  делится на . Таким образом, каждый простой делитель числа  входит в разложение  в степени не меньшей, чем в , так что  делится на . Кроме того,  четно. Теорема 2 доказана.

Следствие. Если выполнены условия теоремы 2 и , то  - простое число.

Действительно, пусть  равняется произведению не менее двух про­стых чисел. Каждое из них, согласно утверждению теоремы 2, не меньше, чем . Но тогда . Противоречие и доказывает следствие.

Покажем теперь, как с помощью последнего утверждения, имея боль­шое простое число , можно построить существенно большее простое число . Выберем для этого случайным образом чётное число  на про­межутке  и положим . Затем проверим число  на отсутствие малых простых делителей, разделив его на малые простые числа; испытаем  некоторое количество раз с помощью алгоритма 5. Если при этом выяснится, что  - составное число, следует выбрать новое значение  и опять повторить вычисления. Так следует делать до тех пор, пока не будет найдено число , выдержавшее испытания алго­ритмом 5 достаточно много раз. В этом случае появляется надежда на то, что  - простое число, и следует попытаться доказать простоту с помощью тестов теоремы 2.

Для этого можно случайным образом выбирать число , и проверять для него выполнимость соотношений

. (12)

Если при выбранном  эти соотношения выполняются, то, согласно след­ствию из теоремы 2, можно утверждать, что число  простое. Если же эти условия нарушаются, нужно выбрать другое значение  и повторять эти операции до тех пор, пока такое число не будет обнаружено.

Предположим, что построенное число  действительно является про­стым. Зададимся вопросом, сколь долго придётся перебирать числа , по­ка не будет найдено такое, для которого будут выполнены условия (12). Заметим, что для простого числа  первое условие (12), согласно малой теореме Ферма, будет выполняться всегда. Те же числа , для которых на­рушается второе условие (12), удовлетворяют сравнению . Как известно, уравнение  в поле вычетов  имеет не более  решений. Одно из них . Поэтому на промежутке  имеется не более  чисел, для которых не выполняются условия (12). Это означа­ет, что, выбирая случайным образом числа  на промежутке , при простом  можно с вероятностью большей, чем , найти чи­сло , для которого будут выполнены условия теоремы 2, и тем доказать, что  действительно является простым числом.

Заметим, что построенное таким способом простое число  будет удовлетворять неравенству , т. е. будет записываться вдвое боль­шим количеством цифр, чем исходное простое число . Заменив теперь число  на найденное простое число  и повторив с этим новым  все указанные выше действия, можно построить еще большее простое число. Начав с какого-нибудь простого числа, скажем, записанного 10 десятич­ными цифрами (простоту его можно проверить, например, делением на маленькие табличные простые числа), и повторив указанную процедуру достаточное число раз. можно построить простые числа нужной величи­ны.

Обсудим теперь некоторые теоретические вопросы, возникающие в связи с нахождением числа , удовлетворяющего неравенствам , и такого, что  - простое число. Прежде всего, со­гласно теореме Дирихле, доказанной еще в 1839 г., прогрессия ,  содержит бесконечное количество простых чисел. Нас интересуют простые числа, лежащие недалеко от начала прогрессии. Опенка наименьшего простого числа в арифметической прогрессии была полу­чена в 1944 г. Ю. В. Линником. Соответствующая теорема утверждает, что наименьшее простое число в арифметической прогрессии  не превосходит , где  - некоторая достаточно большая абсолютная постоянная.

Таким образом, в настоящее время никаких теоретических гарантий для существования простого числа  не сущес­твует. Тем не менее опыт вычислений на ЭВМ показывает, что простые числа в арифметической прогрессии встречаются достаточно близко к её началу. Упомянем в этой связи гипотезу о существовании бесконечного количества простых чисел  с условием, что число  также простое, т. е. простым является уже первый член прогрессии.

Очень важен в связи с описываемым методом построения простых чисел также вопрос о расстоянии между соседними простыми числами в арифметической прогрессии. Ведь убедившись, что при некотором  число  составное, можно следующее значение  взять равным  и действовать так далее, пока не будет найдено простое число . И если расстояние между соседними простыми числами в прогрессии ве­лико, нет надежды быстро построить нужное число . Перебор чисел  до того момента, как мы наткнемся на простое число  окажется слишком долгим. В более простом вопросе о расстоянии между соседни­ми простыми числами  и  в натуральном ряде доказано лишь, что , что, конечно, не очень хорошо для наших целей. Вместе с тем существует так называемая гипотеза Крамера (1936 г.), что , дающая вполне приемлемую опенку. Примерно такой же результат следует и из расширенной гипотезы Римана. Вычисления на ЭВМ показывают, что простые числа в арифметических прогрессиях расположены достаточно плотно.

В качестве итога обсуждения в этом пункте подчеркнём следующее: если принять на веру, что наименьшее простое число, а также расстояние между соседними простыми числами в прогрессии  при  оцениваются величиной , то описанная схема построения больших простых чисел имеет полиномиальную опенку сложности. Кро­ме того, несмотря на отсутствие теоретических опенок времени работы алгоритмов, отыскивающих простые числа в арифметических прогрес­сиях со сравнительно большой разностью, на практике эти алгоритмы работают вполне удовлетворительно. На обычном персональном компью­тере без особых затрат времени строятся таким способом простые числа порядка .

Конечно, способ конструирования простых чисел для использования в схеме RSA должен быть массовым, а сами простые числа должны быть в каком-то смысле хорошо распределёнными. Это вносит ряд дополнитель­ных осложнений в работу алгоритмов.

Наконец, отметим, что существуют методы построения больших про­стых чисел, использующие не только простые делители , но и делите­ли чисел . В основе их лежит использование после­довательностей целых чисел, удовлетворяющих линейным рекуррентным уравнениям различных порядков. Отметим, что последовательность , члены которой присутствуют в формулировке малой теоремы Ферма, со­ставляет решение рекуррентного уравнения первого порядка .

* + 1. Проверка большого числа на простоту

Есть некоторое отличие в постановках задач предыдущего и настоя­щего пунктов. Когда мы строим простое число , мы обладаем некото­рой дополнительной информацией о нем, возникающей в процессе постро­ения. Например, такой информацией является знание простых делителей числа . Эта информация иногда облегчает доказательство просто­ты .

В этом пункте мы предполагаем лишь, что нам задано некоторое чи­сло , например, выбранное случайным образом на каком-то промежут­ке, и требуется установить его простоту, или доказать, что оно является составным. Эту задачу за полиномиальное количество операций решает указанный в п. 3 алгоритм Миллера. Однако, справедливость полученного с его помощью утверждения зависит от недоказанной расширенной гипо­тезы Римана. Если число  выдержало испытания алгоритмом 5 для 100 различных значений параметра , то, по-видимому, можно утверждать, что оно является простым с вероятностью большей, чем . Эта вероятность очень близка к единице, однако всё же оставляет некоторую тень сомнения на простоте числа . В дальнейшем в этом пункте мы будем считать, что заданное число  является простым, а нам требуется лишь доказать это.

В настоящее время известны детерминированные алгоритмы различ­ной сложности для доказательства простоты чисел. Мы остановимся по­дробнее на одном из них, предложенном в 1983 г. в совместной работе Адлемана. Померанца и Рамели. Для доказательства простоты или непростоты числа  этот алгоритм требует  арифметиче­ских операций. Здесь  - некоторая положительная абсолютная посто­янная. Функция  хоть и медленно, но всё же возрастает с ростом , поэтому алгоритм не является полиномиальным. Но всё же его прак­тические реализации позволяют достаточно быстро тестировать числа на простоту. Существенные усовершенствования и упрощения в перво­начальный вариант алгоритма были внесены в работах X. Ленстры и А. Коена. Мы будем называть описываемый ниже алгоритм алго­ритмом Адлемана - Ленстры.

В основе алгоритма лежит использование сравнений типа малой те­оремы Ферма, но в кольцах целых чисел круговых полей, т. е. полей. порождённых над полем  числами  - корнями из 1. Пусть  - простое нечётное число и  — первообразный корень по модулю , т. е. образующий элемент мультипликативной группы поля , которая пиклична. Для каждого целого числа , не делящегося на , можно опре­делить его индекс, , называемый также *дискретным логарифмом*, с помощью сравнения . Рассмотрим далее два простых числа ,  с условием, что  делится на , но не делится на .

Следующая функция, определённая на множестве целых чисел.



является характером по модулю  и порядок этого характера равен .

Сумма:



называется суммой Гаусса. Формулируемая ниже теорема 3 представляет собой аналог малой теоремы Ферма, используемый в алгоритме Адлемана - Ленстры.

Теорема3. Пусть  - нечетное простое число, . Тогда в кольце  выполняется сравнение

.

Если при каких-либо числах  сравнение из теоремы 3 нарушается. можно утверждать, что  составное число. В противном случае, если сравнение выполняется, оно даёт некоторую информацию о возможных простых делителях числа . Собрав такую информацию для различных , в конце концов удаётся установить, что  имеет лишь один простой делитель и является простым.

В случае  легко проверить, что сравнение из теоремы 3 равно­сильно хорошо известному в элементарной теории чисел сравнению

, (13)

где  - так называемый символ Якоби. Хорошо известно также, что последнее сравнение выполняется не только для простых , но и для любых целых , взаимно простых с . Заметим также, что для вычисления символа Якоби существует быстрый алгоритм, основанный на законе вза­имности Гаусса и. в некотором смысле, подобный алгоритму Евклида вы­числения наибольшего общего делителя. Следующий пример показывает. каким образом выполнимость нескольких сравнений типа (13) даёт неко­торую информацию о возможных простых делителях числа .

Пример (X. Ленстра). Пусть  — натуральное число, . для которого выполнены сравнения

, (14)

а кроме того с некоторым целым числом  имеем

. (15)

Как уже указывалось, при простом  сравнения (14) выполняются для любого , взаимно простого с , а сравнение (15) означает, что  есть первообразный корень по модулю . Количество первообразных корней равно , т. е. достаточно велико. Таким образом, число  с усло­вием (15) при простом  может быть найдено достаточно быстро с помощью случайного выбора и последующей проверки (15).

Докажем, что из выполнимости (14-15) следует, что каждый делитель  числа  удовлетворяет одному из сравнений

 или . (16)

Не уменьшая общности, можно считать, что  - простое число. Введем теперь обозначения , где  и  - нечётные числа. Из (15) и сравнения  следует, что . Далее, согласно (14). выполняются следующие сравнения

,

означающие (в силу того, что символ Якоби может равняться лишь -1 или +1), что .

При  это равенство означает, что  при , и, следовательно, . Если же , то имеем  и . Этим (16) доказано.

Информация такого рода получается и в случае произвольных про­стых чисел  и  с указанными выше свойствами.

Опишем схему алгоритма Адлемана - Ленстры для про­верки простоты :

1. выбираются различные простые числа  и различные про­стые нечётные  такие, что
   1. для каждого  все простые делители числа  содержатся  
      среди  и  не делятся на квадрат простого числа;

1.2) .

1. для каждой пары выбранных чисел ,  проводятся тесты, подобные сравнению из теоремы 3. Если  не удовлетворяет какому-либо из  
   этих тестов - оно составное. В противном случае
2. определяется не очень большое множество чисел, с которыми толь­ко и могут быть сравнимы простые делители . А именно, каждый простой делитель  числа  должен удовлетворять сравнению вида

, .

1. проверяется, содержит ли найденное множество делители . Ес­ли при этом делители не обнаружены, утверждается, что  - простое  
   число.

Если число  составное, оно обязательно имеет простой делитель , меньший , который сам содержится среди возможных остатков. Именно на этом свойстве основано применение пункта 4) алгоритма.

Сумма Якоби:



определяется для двух характеров  модулю . Если характеры имеют порядок , то соответствующая сумма Якоби принадлежит кольцу . Поскольку числа , участвующие в алгоритме, сравнительно невели­ки, то вычисления с суммами Якоби производятся в полях существенно меньшей степени, чем вычисления с суммами Гаусса. Это главная при­чина, по которой суммы Якоби предпочтительнее для вычислений. При  выполняется классическое соотношение



связывающее суммы Гаусса с суммами Якоби и позволяющее переписать сравнение теоремы 3 в терминах сумм Якоби. Так. при  и  соответствующее сравнение, справедливое для простых , отлич­ных от 2,3,7, принимает вид

,

где  и  - некоторый корень кубический из 1.

В 1984 г. было внесено существенное усовершенствование в алгоритм, позволившее освободиться от требования неделимости чисел  на квадраты простых чисел. В результате, например, выбрав число  и взяв  равным произведению простых чисел  с условием, что  делится на , получим , что позволяет доказывать простоту чисел , записываемых сотней десятичных знаков. При этом вычисления будут проводиться в полях, порождённых корнями из 1 степеней 16, 9, 5 и 7.

Персональный компьютер с процессором Pentium-150. пользуясь реализацией этого алгоритма на языке UBASIC, доказал простоту записываемого 65 десятичными знаками, большего из простых чисел в при­мере Ривеста, Шамира и Адлемана за 8 секунд. Сравнение этих 8 секунд и 17 лет, потребовавшихся для разложения на множители предложенного в примере числа, конечно, впечатляет.

Отметим, что опенка сложности этого алгоритма представляет со­бой трудную задачу аналитической теории чисел. Как уже указывалось, количество операций оценивается величиной . Однако соот­ветствующие числа  и , возникающие в процессе доказательства, не могут быть явно указаны в зависимости от . Доказано лишь существо­вание чисел  и , для которых достигается оценка. Впрочем, есть веро­ятностный вариант алгоритма, доказывающий простоту простого числа  с вероятностью большей  за  арифметических операций. А в предположении расширенной гипотезы Римана эта опенка сложности может быть получена при эффективно указанных  и.

* 1. Выбор алгоритма шифрования

Выбор криптографического алгоритма и режима его использования зависит от особенностей передаваемой информации (ее ценности, объема, способа представления, необходимой скорости передачи и т.д.), а так же возможностей владельцев по защите своей информации. Все это существенным образом влияет на выбор криптографического алгоритма и организацию защиты данных. Анализ литературных источников показывает, что каждый из  наиболее распространенных типов симметричных и ассиметричных алгоритмов шифрования имеет свои преимущества и недостатки. Поэтому при выборе того или иного алгоритма шифрования или их сочетания, необходимо учитывать в какой ситуации, какой из алгоритмов работает лучше. При этом при выборе того или иного алгоритма шифрования могут учитываться такие показатели как:

* длина ключа;
* затраты на подбор;
* производительность;
* совместимость.

Результаты проведенной оценки  наиболее распространенных симметричных алгоритмов шифрования приведены в таблице 2.1.

В соответствии с таблицей 1 можно сделать вывод о том, что наиболее стойкими являются такие алгоритмы как: AES, IDEA, Triple DES. Так же данные алгоритмы позволяют использовать ключи различной длины, в частности наиболее распространенной длиной является 128 бит, наименьшей 56 обладает DES, а наибольшей Blowfish – до 448, 256 — AES и ГОСТ 28147-89. При этом, чем длиннее ключ, тем надежнее защита и тем медленнее будет работать алгоритм. А это означает, что в том случае если симметричный алгоритм будет использоваться совместно с ассиметричным, то на первое место выходит именно производительность, и длина ключа не будет столь критичной. Наибольшее распространение, а следовательно, и совместимость с другими криптосистемами и алгоритмами получили: DES, TripleDES или AES. Использование данных алгоритмов позволяет гарантировать то, что все стороны, имеющие криптографические средства, смогут использовать эти алгоритмы и расшифровать шифротекст.

Таблица 2.1. Сравнительная характеристика симметричных алгоритмов шифрования

|  |  |  |  |
| --- | --- | --- | --- |
| **Алгоритм** | **Длина ключа, бит** | **Размер блока, бит** | **Затраты на подбор ключа, MIPS** |
| DES | 56 | 64 | 5 102 |
| Triple DES | 128 (112) | 64 | 1018 |
| IDEA | 128 | 64 | 1021 |
| ГОСТ 28147-89 | 256 | 64 | нет данных |
| RC5 | 40 и выше | 32 и выше | 103 и выше |
| Blowfish | до 448 | 64 | нет данных |
| AES | Длина ключа может быть 128, 192 или 256 бит, в независимости от длины блока | | |

Наиболее распространенными среди ассиметричных алгоритмов шифрования являются: RSA, алгоритм Диффи-Хеллмана, Эль-Гамаля, на базе эллиптических кривых, сравнительная характеристика которых приведена в таблице 2.2.

Анализ представленных в таблице ассиметричных алгоритмов шифрования показывает, что данные алгоритмы позволяют использовать для шифрования ключи различной длины, что позволяет данным алгоритмам обеспечивать примерно одинаковую стойкость.

Таблица 2.2. Сравнительная характеристика ассиметричных алгоритмов шифрования

|  |  |  |  |
| --- | --- | --- | --- |
| **Алгоритм** | **Длина ключа** | **Метод взлома (мат. проблема)** | **Криптостойкость, MIPS** |
| RSA | 430 760 1024 1620 | факторизация больших простых чисел | 2,7•1028 для ключа 1300 бит |
| DH |  | Основан на предполагаемой сложности проблемы дискретного логарифмирования.  Сложность вычисления K=gab mod p по известным p, g, A=ga mod p и B=gb mod p | время, затрачиваемое на решение этой задачи, сравнимо со временем, затрачиваемым на разложение числа на множители. Для обеспечения безопасности надо брать число p длиной 1024 бита. |
| El-Gamal (Эль-Гамаль) |  | нахождение дискретного логарифма в конечном поле | при одинаковой длине ключа криптостойкость равная RSA |
| Эллиптические уравнения ECC | 112 160 192 256 | решение эллиптических уравнений | криптостойкость и скорость работы выше, чем у RSA |

Кроме того, большое значение имеет производительность алгоритма, сравнение алгоритмов с открытым ключом показывает, что RSA значительно быстрее, чем ECC который в свою очередь быстрее чем DH. Так же немаловажным значением при использовании алгоритма шифрования является его совместимость, т.е. наличие средств, которые позволяют расшифровывать данные, зашифрованные этим алгоритмом.

Алгоритм RSA является повсеместно распространенным, следовательно, при отправке зашифрованных данных или цифрового конверта RSA, получатель почти наверняка сможет вскрыть его, независимо от того использует ли данный корреспондент то же приложение что и отправитель. При использовании DH велика вероятность, что другая сторона будет иметь необходимый код для расшифровки, хотя этот алгоритм менее распространен и это необходимо учитывать. ECC еще менее распространен, чем DH. Большинство приложений использующих ECC, на сегодняшний день являются закрытыми, т.е. они могут общаться только друг с другом.

Таким образом в качестве защиты протокола в программно-аппаратном комплексе «Звезда» версии 1.2 будет использоваться алгоритм RSA.

Выводы по главе

В результате проведенного анализа требований пользователей:

* были проанализированы существующие алгоритмы шифрования и их математическое обоснование.
* был произведен обзор существующих разработок в данной области.

1. Проектирование

Разрабатываемую информационную систему можно отнести к клиент-серверной архитектуре. На стороне клиента используется приложение, написанное под операционную систему GNU/Linux Debian Wheezy на языке Python.

* 1. Выбор платформы

Платформа в качестве аппаратной части, используемая в программно-аппаратном комплексе «Звезда» версии 1.2. используется, как главное устройство, к которому подключены датчики для замера состояния и управления устройствами, позволяющее выполнять программу, написанную на высокоуровневом языке программирования и иметь возможность соединения с сервером по ЛВС.

Сегодня существует множество замечательных многофункциональных отладочных платформ, которые могут использоваться для разработки цифровых приложений на микроконтроллерах, и этот сегмент рынка постоянно развивается.

Для сравнения были отобраны следующие отладочные платформы:

* Arduino Uno
* BeagleBone
* RaspberryPi

Эти три модели были выбраны для сравнения не случайно: все они реально доступны, выполнены в компактном форм-факторе и могут использоваться для создания различных цифровых устройств. Прежде чем мы перейдем к сравнению,  представим краткое описание каждой из них.

* + 1. Описание существующих платформ

Плату Arduino Uno с некоторых пор можно считать основным компонентом в сообществе радиолюбителей (рисунок 3.1 и рисунок 3.2). Сейчас платы Arduino доступны в различных форм-факторах, с различным набором периферии. Большая их часть выполненыа на 8-разрядном микроконтроллере компании Atmel. А не так давно была анонсирована плата Arduino Due на мощном ARM микроконтроллере с ядром Cortex-M3. Для нашего обзора была выбрана Arduino Uno в качестве представителя платформы Arduino. Для нее доступны простая среда разработки и большая база знаний и наработок, что говорит о возможности создания достаточно функциональных приложений.

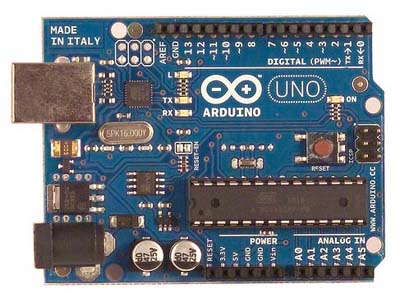


Рисунок 3.1. Arduino Uno



Рисунок 3.2. Arduino Uno обратная сторона

Плата Raspberry Pi является сравнительно новым продуктом – это одноплатный компьютер, позиционирующийся на рынке как дешевое решение для начинающих разработчиков встраиваемых систем (рисунок 3.3 и рисунок 3.4). Несмотря на скромный вид и низкую стоимость (около 35$), это реальный компьютер, который может стать основой для множества проектов.

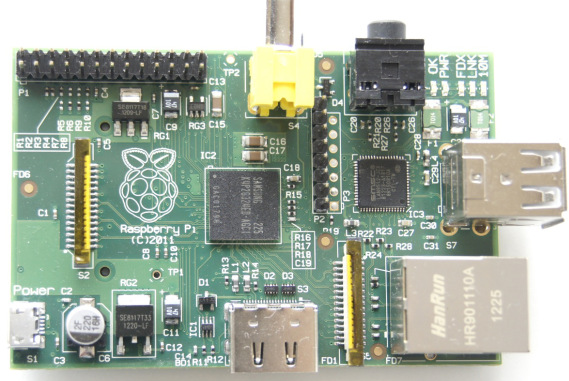


Рисунок 3.4. Raspberry Pi

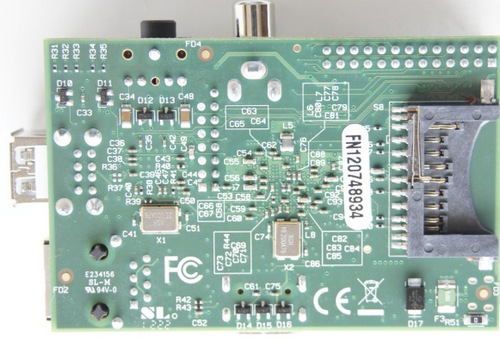


Рисунок 3.4. Raspberry Pi обратная сторона

BeagleBone является наименее известной из всех трех платформ, но ее возможности заслуживают внимания создателей встраиваемых приложений. Это мощный Linux-компьютер компактных размеров, который поддерживает работу с ОС Android и Ubuntu (рисунок 3.5 и рисунок 3.6).

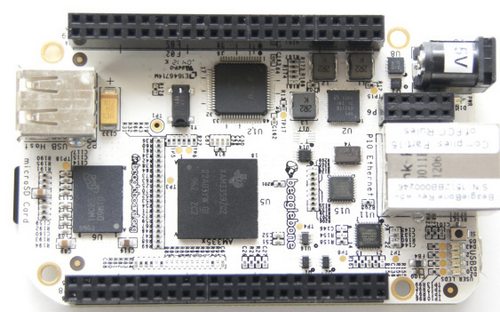


Рисунок 3.5. BeagleBone

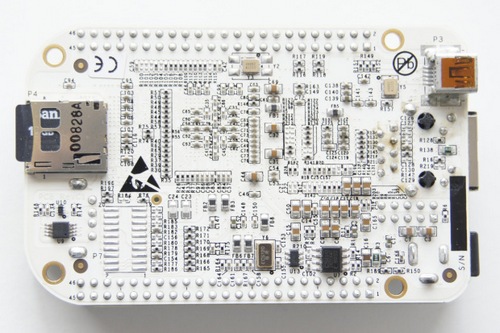


Рисунок 3.5. BeagleBone обратная сторона

Все три платы имеют определенный функционал и набор периферии, которые делают их ценными для разработчиков и проектировщиков микроконтроллерных систем. Ниже сравнение их по некоторым важным параметрам в таблице 3.1. Можно заметить, что именно отличия плат делают каждую из них идеальной для разработки определенного типа приложений.

**Таблица 3.1.** Сравнение характеристик плат Arduino Uno, BeagleBone, RaspberryPi.

|  |  |  |  |
| --- | --- | --- | --- |
| **Платформа** | **Arduino Uno** | **Raspberry Pi** | **BeagleBone** |
| **Модель** | **R3** | **Model B** | **Rev A5** |
| Ориентировочная цена | 29.95$ | 35$ | 89$ |
| Габаритные размеры | 7.5 × 5.3 см | 8.5 × 5.4 см | 8.6 × 5.3 см |
| Микроконтроллер | ATmega328 | ARM11 | ARM Cortex-A8 |
| Тактовая частота | 16 МГц | 700 МГц | 700 МГц |
| ОЗУ | 2 Кбайт | 256 Мбайт | 256 Мбайт |
| Flash-память | 32 Кбайт | SD карта | 4 Гбайт (SD карта) |
| EEPROM | 1 Кбайт | - | - |
| Напряжение питания | 7 – 12 В | 5 В | 5 В |
| Минимальное энергопотребление | 42 мА (0.3 Вт) | 700 мА (3.5 Вт) | 170 мА (0.85 Вт) |
| Цифровые линии ввода/вывода | 14 | 8 | 66 |
| Аналоговые входы | 6 (10-битный АЦП) | - | 7 (12-битный АЦП) |
| Каналы ШИМ | 6 | - | 8 |
| Интерфейс TWI/I2C | 2 | 1 | 2 |
| Интерфейс SPI | 1 | 1 | 1 |
| Интерфейс UART | 1 | 1 | 5 |
| Инструменты разработки | Arduino IDE | Python, IDLE, Scratch, Squeak/Linux | Python, Scratch, Squeak, Cloud9/Linux |
| Порт Ethernet | - | 10/100 | 10/100 |
| Интерфейс USB Master | - | 2 USB 2.0 | USB 2.0 |
| Видео выход | - | HDMI, композитный | - |
| Аудио выход | - | HDMI, аналоговый | Аналоговый |

Arduino и Raspberry Pi – недорогие платы стоимостью до 40$. BeagleBone предлагается по цене почти трех Arduino Uno. Однако Arduino в 40 раз медленнее и имеет в 128,000 раз меньше оперативной памяти, чем два оставшихся участника. Уже на данном этапе видны важные отличия. Arduino и Raspberry Pi – дешевые платы, а Raspberry Pi и BeagleBone – гораздо более мощные.

На Raspberry Pi и BeagleBone возможно запускать программные приложения с карты памяти (SD-карта для Raspberry Pi, microSD – для BeagleBone). Это означает, что можно иметь различные конфигурации ОС, приложения, сборки и образы ОС на разных картах памяти, и выбор того или иного проекта осуществляется просто заменой карты памяти. Таким же образом можно сменить операционную систему.

**Самая компактная платформа - Arduino.** Все три тестируемые модели плат для разработки являются малогабаритными. Единственный отрицательный момент присущ Raspberry Pi – установленная в слот карта памяти SD делает плату больше остальных участников теста.

Существует очень много вариаций плат Arduino, но у всех есть две общие черты: используется определенный микроконтроллер компании Atmel и программный загрузчик (bootloader) Arduino, который реализует базовые функции платы. Для компактных устройств (возможно, не требующих применения печатной платы) можно приобрести этот дешевый микроконтроллер и запрограммировать в него загрузчик с помощью любого программатора AVR микроконтроллеров.

На платформе Arduino тоже можно реализовать приложения с поддержкой обмена данными по Ethernet с помощью плат расширения, именуемых Shield, однако сетевая функциональность таких приложений будет очень ограничена. Приобретение отдельных плат расширения также потребует дополнительных финансовых затрат.

**Для приложений и систем взаимодействующих с внешними датчиками и исполнительными механизмами лучше всего подойдут Arduino или BeagleBoard.** Любой вариант аппаратной платформы Arduino подразумевает простое подключения внешних сенсоров и взаимодействие с ними. Для радиолюбителей доступно нескольких вариантов плат с напряжением питания 3.3 В и 5 В, что упрощает подключение внешней периферии. Напряжение питания платы BeagleBone составляет 3.3 В, поэтому в случае подключения некоторых типов внешних устройств необходимо использовать дополнительные резисторы или схемы согласования логических уровней.  И Arduino, и BeagleBone имеют интерфейс аналого-цифрового преобразователя (разрешение АЦП, встроенного в микроконтроллер на плате BeagleBoard, несколько выше), что говорит о возможности подключения различных аналоговых датчиков.

С учетом сказанного, важно отметить, что многие современные датчики снабжены цифровыми интерфейсами I2C или SPI. Все три платы поддерживают этот тип последовательного интерфейса и реализовать взаимодействие с ним можно довольно легко.

**Для устройств с батарейным питанием подойдет Arduino.** Такое решение связано с тем, что Arduino имеет наименьшее энергопотребление, однако с точки зрения соотношения вычислительной мощности на Ватт BeagleBoard является явным лидером. Тем не менее, преимущество Arduino в том, что ее работоспособность сохраняется в широком диапазоне питающего напряжения. Таким образом, в качестве источника питания платы можно использовать различные типы элементов питания, работоспособность микроконтроллера сохраняется даже в случае, когда элементы питания израсходовали свой ресурс.

**Для приложений с графическим пользовательским интерфейсом рекомендуется использовать Raspberry Pi.** Одноплатный компьютер Raspberry Pi действительно можно выделить в отдельную категорию, поскольку плата снабжена выходом HDMI. Это означает, что можно подключить к плате мышь и клавиатуру, а саму плату подключить непосредственно к телевизору. Таким образом, получается полнофункциональный компьютер, который идеально подходит для применения в торговых терминалах и киосках.

Arduino достаточно функциональная и гибкая платформа разработки встраиваемых приложений с огромными возможностями для взаимодействия с внешним миром. Она прекрасно подойдет для изучения микроконтроллеров и может служить основой для небольших проектов. Raspberry Pi будет оптимальным выбором для приложений, требующих наличия дисплея, графического пользовательского интерфейса и подключения к интернету, в том числе и для системы «Звезда»

* 1. Выбор языка программирования

Алгоритм синтетический, долгий цикл (двухуровневый) и в нём вычисление математического выражения. Таким образом оценивается вычислительная производительность самого языка (интерпретатора или скомпилированного кода), никаких привязок к качеству реализации тех или иных библиотек, никаких внешних сервисов, никаких системозависимых операций (диск, сеть, графика). Результат сравнения в таблице 3.2.

Далее будут представлены примеры программ, которые использовались для тестирования производительности и для демонстрирования простоты написания программы на том или ином языке программирования.

* + 1. Java

package ru.dchekmarev.test.performance;  
public class Test01 {  
    public static void main(String[] args) {  
//        long start = System.currentTimeMillis();  
        int r = 0;  
        for (int i = 0; i < 10000; i++) {  
            for (int j = 0; j < 10000; j++) {  
                r = (r + (i \* j) % 100) % 47;  
            }  
        }  
        System.out.println("answer: " + r);  
//        закомментировано, т.к. замеры делаются из командной строки  
//        System.out.println("run time (millis): " + (System.currentTimeMillis() - start));  
    }  
}

* + 1. C++

#include <iostream>  
using namespace std;  
int main(void) {  
    long r = 0;  
    for (int i = 0; i < 10000; i++) {  
        for (int j = 0; j < 10000; j++) {  
            r = (r + (i \* j) % 100) % 47;  
        }  
    }  
    cout << "answer: " << r << endl;  
}

* + 1. PHP

<?php  
$r = 0;  
for ($i = 0; $i < 10000; $i++) {  
    for ($j = 0; $j < 10000; $j++) {  
        $r = ($r + ($i \* $j) % 100) % 47;  
    }  
}  
echo 'answer: ' . $r . "\n";  
?>

* + 1. Python

def test():  
  r = 0  
  for i in range(0, 10000):  
      for j in range(0, 10000):  
          r = (r + (i \* j) % 100) % 47  
test()  
print("answer: ", r)

* + 1. Perl

$r = 0;  
# старый вариант, C-подобный синтаксис  
# for ($i = 0; $i < 10000; $i++) {  
#   for ($j = 0; $j < 10000; $j++) {  
for my $i (0..9999) {  
  for my $j (0..9999) {  
    $r = ($r + ($i \* $j) % 100) % 47;  
  }  
}  
print "answer: $r\n";

* + 1. Ruby

r = 0  
for i in 0..10\_000 do  
  for j in 0..10\_000 do  
    r = ( r + ( i \* j ) % 100) % 47  
  end  
end  
puts "answer: #{r}"

* + 1. Результат

Таблица 3.2. Сравнение производительности

|  |  |  |
| --- | --- | --- |
| **Язык** | **Время исполнения, сек** | **Производительность, %** |
| Java | 5,3 | 160 |
| Java -server | 2,8 | 303 |
| C++ | 8,5 | 100 |
| C++, -O2 | 2,6 | 327 |
| PHP | 62 | 14 |
| Python 2.6 | 91 | 9 |
| Python 3.1 | 145 | 6 |
| Perl 5.8 |  | 9 |
| Ruby 1.8 | 91 | 4.11 |
| Ruby 1.9(?) | 207 | 28 |
|  | ~30 |  |

Из таблицы сравнения видно, что самым производительным языком оказался C++ с флагом оптимизации O2 (максимизировать скорость). Но самым простым языком в написании кода, оказался python 3.1.

* 1. Проектирование функций
* rsa.**encrypt**(message, pub\_key)

Шифрует данное сообщение используя PKCS#1 v1.5

**Parameters:**

1. **message** – сообщение для шифрования. Должен быть строкой не более k-11, где k – число байтов, для кодирования n компонент открытого ключа.
2. **pub\_key** –открытый ключ rsa.PublicKey для шифрования.

**Выдает OverflowError:**

Сообщение слишком велико, чтобы уместить блок кодирования.

* rsa.**decrypt**(*crypto*, *priv\_key*)

Расшифровывает данное сообщение с помощью PKCS # 1 v1.5

Расшифровка считается "не удалась", когда в результате открытый текст не начинается с байтов 00 02, или когда 00 байт между внутренним отступом и сообщением, не могут быть найдено.

**Parameters:**

1. **crypto** – крипто текст как результат выполнения rsa.PublicKey()
2. **priv\_key** – закрытый ключ rsa.PrivateKey для дешифрования.

**Выдает DecryptionError:**

Когда не поддается расшифровке. Никаких подробностей не приводится, почему не получилось расшифровать, т.к. это будет наводящей информацией о закрытом ключе.

* rsa.**sign**(message, priv\_key, hash)

Подписывает сообщение с секретным ключом.

Хэширует сообщение, затем подписывает хэш с данным ключом. Это известно как «Отдельная сигнатура», потому что само сообщение не изменяется.

**Parameters:**

1. **message** – подписываемое сообщение
2. **priv\_key** – закрытый ключ rsa.PrivateKey для подписывания сообщения.
3. **hash** – способ хеширования сообщения. Возможно использовать ‘MD5’, ‘SHA-1’, ‘SHA-256’, ‘SHA-384’ или ‘SHA-512’.

**Возвращает:**

Блок подписанного сообщения.

**Выдает OverflowError:**

Если закрытый ключ слишком мал, чтобы содержать выбранный хэш.

* rsa.**verify**(message, signature, pub\_key)

Проверяет подпись сообщения на совпадение.

Хэш метод определяется автоматически с момента подписания.

**Parameters:**

1. **message** – подписанное сообщение. Может быть 8-битной строкой или файл-подобный объект.
2. **signature**  – блок подписи, созданный с rsa.sign()
3. **pub\_key** – публичный ключ rsa.PublicKey подписавшего сообщение.

**Выдает VerificationError:**

Когда подпись не совпадает с сообщением.

* rsa.**newkeys**(keysize)

Создает открытый и закрытый ключи и возвращает их в виде (открытый, закрытый).

Открытый ключ нужен как «ключ шифрования» и является объектом rsa.PublicKey. Закрытый ключ нужен как «ключ дешифрования» и является объектом rsa.PrivateKey.

**Parameters:**

1. **nbits** – количество бит необходимых для хранения n = p \* q
2. **accurate**  – когда истина, n будет иметь запрошенное количество битов.
3. **poolsize** – количество используемых процессов для генерации простых чисел. Если установлено число большее 1, параллельный алгоритм будет использоваться. Это требует Python 2.6 и новее.

**Возвращает:**

Запись (rsa.PublicKey, rsa.PrivateKey)

* 1. Проектирование классов
* class rsa.**PublicKey**(n, e)

Представляет открытый ключ RSA

Этот ключ используется как «ключ шифрования». Он содержит ‘N’ и ‘E’ значения.

Поддерживает атрибуты, а также словарь доступа. Атрибуты доступа все же быстрее.

**load\_pkcs1**(keyfile, format='PEM')

Загружает ключ PKCS#1 в DER или PEM форматах.

**Parameters:**

1. **keyfile** – содержимое DER или PEM закодированного файла, содержащего открытый ключ.
2. **format**  – загружаемый формат файла DER или PEM.

**Возвращает:**

Объект публичного ключа PublicKey.

classmethod **load\_pkcs1\_openssl\_pem**(keyfile)

Загружает файл открытого ключа PKCS#1 в DER – кодировке из OpenSSL

**Parameters:**

Параметр **keyfile** – содержимое файла в DER кодировке, что содержит открытый ключ OpenSSL

**Возвращает:**

Объект публичного ключа PublicKey.

classmethod **load\_pkcs1\_openssl\_der**(n, e, d, p, q, exp1=None, exp2=None, coef=None)

Загружает файл открытого ключа PKCS#1 в PEM – кодировке из OpenSSL

Этот файл признается в том случае, если начинается с BEGIN PUBLIC KEY, а не с BEGIN RSA PUBLIC KEY.

Содержимое файла перед “—–BEGIN PUBLIC KEY—–” и после “—–END PUBLIC KEY—–” линий, игнорируются.

**Parameters:**

Параметр **keyfile** – содержимое файла в PEM кодировке, что содержит открытый ключ OpenSSL

**Возвращает:**

Объект публичного ключа PublicKey.

**save\_pkcs1**(format='PEM')

Сохраняет публичный ключ PKCS#1 в DER или PEM формате

**Parameters:**

**format** – формат сохранения (DER или PEM формат).

**Возвращает:**

Публичный ключ шифрования в DER или PEM формате.

* class rsa.PrivateKey(n, e, d, p, q, exp1=None, exp2=None, coef=None)

Представляет секретный ключ RSA.

Этот ключ используется как «ключ дешифрования». Он содержит ‘n’, ‘e’, ‘d’, ‘p’, ‘q’ и другие значения.

Поддерживает атрибуты, а также словарь доступа. Атрибут доступа все же быстрее.

**load\_pkcs1**(keyfile, format='PEM')

Загружает ключ PKCS#1 в DER или PEM формате

**Parameters:**

1. **keyfile** – содержимое в DER или PEM формате закодированного файла, содержащего открытый ключ.
2. **format -** формат файла для загрузки (DER или PEM формат).

**Возвращает:**

Объект публичного ключа.

**save\_pkcs1**(format='PEM')

Сохраняет публичный ключ PKCS#1 в DER или PEM формате

**Parameters:**

1. **format -** формат файла для сохранения (DER или PEM формат).

**Возвращает:**

Публичный ключ в DER или PEM формате.

* 1. Проектирование классов исключений
* *class* rsa.pkcs1.**CryptoError**(Exception)

Базовый класс для всех исключений в этом модуле.

* *class* rsa.pkcs1.**DecryptionError**(CryptoError)

Возникает, когда расшифровать не удается.

* *class* rsa.pkcs1.**VerificationError**(CryptoError)

Возникает, когда верифицировать не удается.

* 1. Модуль rsa.bigfile

Модуль rsa.bigfile содержит функции для шифрования и дешифрования файлов, размер которых превышает размер ключа RSA.

rsa.bigfile.**encrypt\_bigfile**(infile, outfile, pub\_key)

Шифрует файл, записывая его в выходной файл «outfile» в формате VARBLOCK

**Parameters:**

1. **infile –** файл-подобный объект, чтобы читать открытым ткстом.
2. **outfile** – файл-подобный объект, чтобы зашифровать в формате VARBLOCK.
3. **pub\_key** – публичный ключ шифрования rsa.PublicKey

rsa.bigfile.**decrypt\_bigfile**(infile, outfile, priv\_key)

Дешифрует зашифрованный VARBLOCK файл, записывая в входной файл «outfile».

**Parameters:**

1. **infile –** файл-подобный объект, чтобы прочитать шифрованный VARBLOCK файл.
2. **outfile** – файл-подобный объект, чтобы читать открытым ткстом.
3. **priv\_key** – закрытый ключ дешифрования rsa.PrivateKey
   1. Формат VARBLOCK файла

Формат файла VARBLOCK позволяет шифровать файлы, размер которых превышает размер ключа RSA. Формат должен быть следующим; || обозначает конкатенацию байт строк:

VARBLOCK := VERSION || BLOCK || BLOCK || ...

VERSION := 1

BLOCK := LENGTH || DATA

LENGTH := varint-кодировка длины в байтах

DATA := данные для хранения в блоке

Varint-формат был взят из Protobuf Google, и позволяет эффективно кодировать сколь угодно длинное целое.

* 1. Модуль rsa.core

В основе метода шифрования RSA лежат эти две функции. Они обе работают только на (сколько угодно длинных) целых числах. Эти функции являются ядром всей библиотеки.

rsa.core.**encrypt\_int**(message, ekey, n)

Шифрует сообщения с использованием ключа шифрования «Ekey» по модулю n.

rsa.core.**decrypt\_int**(cyphertext, dkey, n)

Дешифрует зашифрованный текст с помощью дешифрующего ключа «dkey» по модулю n.

Выводы по главе

В данной главе:

* были подобраны необходимые аппаратные средства;
* разработана схема взаимодействия аппаратных средств необходимых для её функционирования;
* выяснены требования к программному обеспечению, необходимые для разработки и, частично, функционирования программы.
* разработан алгоритм работы системы.

Исходные код основных классов приложены в приложения А и Б.

1. Тестирование и документирование
   1. Тестирование

Проверка качества проекта и информационной системы. Поиск и исправление ошибок после распространения продукта обходится значительно дороже, чем до распространения, поэтому тестирование должно быть максимально полным.

Тестирование позволяет:

* объективно оценить состояние системы;
* выявить противоречия в требованиях;
* проверить устойчивость к риску;
* выявить дефекты в проектировании на ранних этапах;
* применять автоматизированные средства тестирования;

Контроль изменения предполагает:

* непрерывное наблюдение за ходом разработки системы;
* координацию изменений на этапах завершения очередной версии и устранение несогласованности путем возврата на предыдущие этапы разработки.
* непрерывное накопление возможных изменений и поэтапное их внедрение или отклонение.

В тестирование программ можно выделить четыре этапа:

* тестирование отдельных модулей;
* совместное тестирование модулей;
* тестирование спецификации программы;
* тестирование всего комплекса в целом (т.е. поиск несоответствия созданного программного продукта сформулированным ранее целям проектирования, отраженным в техническом задании).

На первых двух этапах используются, прежде всего, методы структурного тестирования, т.к. на последующих этапах тестирования эти методы использовать сложнее из-за больших размеров проверяемого программного обеспечения; последующие этапы тестирования ориентированы на обнаружение ошибок различного типа, которые не обязательно связаны с логикой программы.

Известны два подхода к тестированию модулей: монолитное и пошаговое тестирование.

* + 1. Монолитное тестирование

При монолитном тестировании сначала по отдельности тестируются все части программного комплекса, а затем все они объединяются в рабочую программу для комплексного тестирования.

* + 1. Пошаговое тестирование

При пошаговом тестировании каждый модуль для своего тестирования подключается к набору уже проверенных модулей. При пошаговом тестировании модули проверяются не изолированно друг от друга, поэтому требуются либо только драйверы, либо только заглушки.

При пошаговом тестировании возможны две стратегии подключения модулей: нисходящая и восходящая.

Нисходящее тестирование начинается с главного (или верхнего) модуля программы, а выбор следующего подключаемого модуля происходит из числа модулей, вызываемых из уже протестированных. Одна из основных проблем, возникающих при нисходящем тестировании, - создание заглушек.

Основные достоинства нисходящего тестирования: уже на ранней стадии тестирования есть возможность получить работающий вариант разрабатываемой программы; быстро могут быть выявлены ошибки, связанные с организацией взаимодействие с пользователем.

При восходящем тестировании проверка программы начинается с терминальных модулей (т.е. тех, которые не вызывают не каких других модулей программы). Эта стратегия во многом противоположна нисходящему тестированию (в частности, преимущества становятся недостатками и наоборот).

Преимущества восходящего тестирования:

* поскольку нет промежуточных модулей, нет проблем, связанных с возможностью или трудностью задания тестов;
* нет трудностей, вызывающих желание перейти к тестированию следующего модуля, не завершив проверки предыдущего.

Недостатком восходящего тестирования является то, что проверка всей структуры разрабатываемого программного комплекса возможна только на завершающей стадии тестирования.

Хотя однозначного вывода о преимуществах той или иной стратегии пошагового тестирования сделать нельзя (нужно учитывать конкретные характеристики тестируемой программы), в большинстве случаев более предпочтительным является восходящее тестирование.

* 1. Руководство программиста
     1. Назначение и область применения

Библиотека алгоритма шифрования решает основные проблемы в области защищенной передачи данных:

* Генерация псевдо-случайных чисел;
* Подписывание данных сертификатом;
* Проверка сертификатов;
* Установка защищенного соединения;
* Шифрование или дешифрование неограниченно больших файлов;

В библиотеке алгоритма шифрования версии 1.1 предусмотрены возможности автоматической настройки с рекомендуемыми параметрами. Данная возможность позволяет использовать алгоритм шифрования с минимальными настройками, что в свою очередь повышает надежность и предостерегает от неопытного использования.

* + 1. Характеристики программы

Размер программы 109 Кб, размер всех файлов, включая код тестирования программы, а также файлов установки составляет 132 Кб.

В каталоге запуска программы должны быть файлы:

* key\_priv.rsa – файл с приватным ключом. Используется для личного использования. Этот файл нельзя передавать или открывать доступ к этому файлу в целях безопасности.
* key\_pub.rsa – файл с публичным ключом. Открытый ключ нужен для шифрования передаваемых данных, его можно передавать другим.

Для выполнения программы необходима следующая минимальная конфигурация оборудования:

* процессор с частотой не менее 700 МГц;
* жесткий диск с размером не менее 2Гб;
* оперативная память не менее 128Мб;
* клавиатура
* сетевой адаптер

Для функционирования библиотеки алгоритмов необходима предварительная установка следующих компонентов:

* Python не ниже версии 2.6
* VirtualEnv
* PIP
* GNU/Linux Debian Wheezy

В случае отсутствия необходимых пакетов на компьютере пользователя, в директории с инсталляционным файлом программы имеется все необходимое для установки. Инсталляционный пакет автоматически выполнит проверку, и установит все необходимое.

* + 1. Обращение к программе

Открытый ключ используется для шифрования сообщения так, чтобы он мог быть прочитан только владельцем закрытого ключа. Расшифровка сообщения может быть выполнена только с помощью закрытого ключа, поэтому он называется ключ дешифрования.

Закрытый ключ используется для подписи сообщения. С помощью открытого ключа и подписи, приемник может проверки того, что сообщение было подписано владельцем закрытого ключа, и что сообщение не было изменено после подписания.

* + - 1. Генерация ключа

Для генерации ключа можно использовать два способа:

* генерация с помощью функции rsa.newkeys(), пример на рисунке 4.1.
* альтернативная генерация с помощью rsa.PrivateKey.load\_pkcs1() и rsa.PublicKey.load\_pkcs1(), пример на рисунке 4.2.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\Screenshot-3215.jpg

Рисунок 4.1. Генерация ключа с помощью функции rsa.newkeys()

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\Screenshot-3214.jpg

Рисунок 4.2. Альтернативная генерация ключа.

* + - 1. Время генерации ключей

Генерирование ключей может занять длительное время, в зависимости от необходимого числа битов,. Число битов определяет криптостойкость ключа, а также размером сообщения, которое нужно зашифровать. Есть возможность, немного уменьшить размер ключа, указав параметр accurate= False, чтобы ускорить процесс генерации ключа.

Еще один способ ускорить процесс генерации ключа - параллельное использование нескольких процессов для ускорения генерации ключей. Стоит указывать число не больше, чем есть на самом деле в процессоре используемого оборудования; двухъядерная машина должна использовать PoolSize = 2; на четырехъядерном процессоре с двумя потоками, на каждом ядре, можно использовать PoolSize = 8.

В таблице 4.1 «Скорость генерации ключей» на разных процессорах с использованием 64-разрядного CPython 2.7. Поскольку генерация ключа является случайным процессом, результаты могут отличаться даже на аналогичном оборудовании. На всех тестах использован параметр accurate= True.

Таблица 4.1. Скорость генерации ключей.

|  |  |  |
| --- | --- | --- |
| **Keysize (бит)** | **Один поток** | **8 потоков** |
| 128 | 0.01 sec. | 0.01 sec. |
| 256 | 0.03 sec. | 0.02 sec. |
| 384 | 0.09 sec. | 0.04 sec. |
| 512 | 0.11 sec. | 0.07 sec. |
| 1024 | 0.79 sec. | 0.30 sec. |
| 2048 | 6.55 sec. | 1.60 sec. |
| 3072 | 23.4 sec. | 7.14 sec. |
| 4096 | 72.0 sec. | 24.4 sec. |

Если генерация ключей занимает слишком много времени, тогда можно в качестве альтернативы использовать OpenSSL а затем загрузить их в коде Python. OpenSSL генерирует 4096-битный ключ за 3,5 секунды на той же машине, используемой выше.

* + - 1. Требования к размеру ключа

Python-RSA версии 3.0 описывает PKCS # 1 в стиле случайного заполнения. Это означает, что 11 байтный (88 битный) сгенерированный ключ не пригоден для шифрования. Чем больше размер ключа, тем выше стойкость к атакам. Таблица 4.2.

Для создания подписи также требуется ключ определенного размера, в зависимости от используемого метода хеширования:

Таблица 4.2. Минимальные требования к длине генерируемого ключа.

|  |  |
| --- | --- |
| **Метод хеширования** | **Допустимый минимальный**  **размер ключа (бит)** |
| MD5 | 360 |
| SHA-1 | 368 |
| SHA-256 | 496 |
| SHA-384 | 624 |
| SHA-512 | 752 |

* + - 1. Шифрование и дешифрование

Чтобы зашифровать или расшифровать сообщение, используйтся rsa.encrypt() и rsa.decrypt() соответственно.

К примеру предположим, что Алиса хочет послать сообщение, так чтобы только Боб смог его прочитать.

1. Боб создает пару ключей, и дает открытый ключ Алисе. Это делается таким образом, чтобы Алиса точно знала, что ключ действительно принадлежит Бобу. Рисунок 4.3.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.4\Screenshot-3216.jpg

Рисунок 4.3. Создание новой пары ключей.

1. Алиса пишет сообщение. Рисунок 4.4.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.4\Screenshot-3217.jpg

Рисунок 4.4. Создание сообщения.

1. Алиса шифрует сообщение используя открытый ключ Боба и посылает зашифрованное сообщение. Рисунок 4.5.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.4\Screenshot-3218.jpg

Рисунок 4.5. Шифрование сообщения.

1. Боб получает сообщение и расшифровывает его с помощью своего закрытого ключа. Рисунок 4.6.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.4\Screenshot-3219.jpg

Рисунок 4.6. Дешифрование сообщения.

Поскольку Боб держал закрытый приватный ключ, Алиса может быть уверена, что он единственный, кто может прочитать её сообщение. Боб не знает наверняка, что это была Алиса, которая отправила сообщение, так как она не подписала его.

RSA может только шифровать сообщения, которые меньше, чем ключ. Пару байт теряются на случайные заполнения, а остальное уже доступны для самого сообщения. Например, 512-битный ключ может кодировать сообщение 53-байт (512 бит = 64 байт, 11 байт используются для случайного заполнения и другие вещи).

Альтернативное шифрование информации, скорее всего, может привести к возникновению исключения rsa.pkcs1.DecryptionError. Желательно использовать rsa.sign (). Рисунок 4.7.



Рисунок 4.7. Исключительная ситуация.

Никогда не стоит отображать трассировку стека исключения rsa.pkcs1.DecryptionError. Это покажет, где в коде произошла ошибка, и, таким образом, может произойти утечка информации о ключе. Это всего лишь крошечная часть информации, но каждый бит повышает вероятность взлома ключа.

* + - 1. Низкоуровневые операции

Основной алгоритм RSA поддерживает большие целые числа. Эти операции считаются низкоуровневыми и поддерживаются функциями rsa.core.encrypt\_int() и rsa.core.decrypt\_int().

* + - 1. Подписывание и проверка

Можно создать отдельную подпись для сообщения, используя функцию rsa.sign(). Рисунок 4.8.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.5\Screenshot-3221.jpg

Рисунок 4.8. Подписывание сообщения.

Этот хэш сообщения, использует алгоритм SHA-1. Затем результат вычисления хэш-функции был подписан закрытым ключом. Также возможно использовать другие хэш методы.

Для проверки подписи, существует функция rsa.verify(). Эта функция возвращает истину, если проверка проходит успешно. Рисунок 4.9.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.6\Screenshot-3222.jpg

Рисунок 4.9. Проверка подписанного сообщения и открытого ключа.

Изменение сообщения или подписи приведет к ошибке верификации и вызовет исключение rsa.pkcs1.VerificationError. Рисунок 4.10.

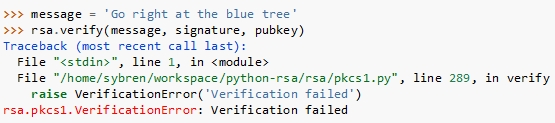


Рисунок 4.10. Ошибка верификации.

Вместо сообщения, можно также вызывать функции rsa.sign() и rsa.verify() с файл-подобным объектом. Если объект сообщения имеет метод read(int), тогда предполагается, что этот объект был построен из файла. В этом случае файл хешируется в 1024-байтные блоки. Рисунок 4.11 и рисунок 4.12.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.6\Screenshot-3224.jpg

Рисунок 4.11.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.6\Screenshot-3225.jpg

Рисунок 4.12.

* + - 1. Работа с большими файлами

RSA может шифровать только сообщения, длина которых меньше, чем длина ключа. Пару байт теряются на случайные заполнения, а остальное используется для самого сообщения. Например, 512-битный ключ может кодировать сообщение 53-байт (512 бит = 64 байт, 11 байт используются для случайного заполнения).

* + - * 1. Применение

Самый распространенный способ использования RSA с большими файлами - это использование блочного шифра, таких как AES или DES3 для шифрования файлов со случайным ключом, предварительно передав этот ключ по защищенному каналу, установленного с помощью RSA. Пример:

1. Генерация случайного ключа. Рисунок 4.13.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.1\Screenshot-3226.jpg

Рисунок 4.13. Генерация случайного ключа.

1. Использование этого ключа для шифрования файла с помощью AES.
2. Шифрование ключа AES с помощью RSA. Рисунок 4.14.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.1\Screenshot-3227.jpg

Рисунок 4.14. Шифрование ключа AES.

1. Отправка шифрованного файла вместе с encrypted\_aes\_key.
2. Получатель обращает этот процесс, чтобы получить зашифрованный файл.

Модуль Python-RSA не содержит функцию шифрования AES.

* + - * 1. Использование Python-RSA: VARBLOCK формат

Предыдущие версии Python-RSA содержали функции для шифрования больших файлов с помощью RSA. Текущая версия была улучшена, однако нет функции Python AES.

Шифрование работает следующим образом: входной файл разбивается на блоки, которые достаточно большие, но позволяют шифровать с ключом RSA. Затем каждый блок шифруется с помощью RSA. После все зашифрованные блоки собираются в выходной файл. Этот формат называется форматом VARBLOCK.

Расшифровка работает в обратном направлении. Зашифрованный файл разделяется на зашифрованные блоки. Потом каждый блок расшифровывается и обратно собираются в большой файл.

Зашифрованный файл получится больше исходного по размеру, так как каждый зашифрованный блок имеет 8 байт случайно заполненного места и еще 3 байта для дополнительной информации.

Так как функции шифрования/дешифрования предназначены для очень больших файлов, они используют другой подход. Там, где регулярные функции хранят сообщение в памяти на протяжении всего времени, эти функции работают над одним блоком в определенный момент времени. В результате, необходимо вызывать их с файл-подобными объектами в виде параметра.

Перед использованием, конечно, нужно сгенерировать пару ключей keypair. Рисунок 4.15.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.2\Screenshot-3228.jpg

Рисунок 4.15. Генерация новой пары ключей.

Шифрование работает с дескрипторами файлов с помощью функции rsa.bigfile.encrypt\_bigfile(). Рисунок 4.16.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.2\Screenshot-3229.jpg

Рисунок 4.16. Шифрование большого файла.

Дешифрование с помощью функции rsa.bigfile.decrypt\_bigfile(). Рисунок 4.17.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.2\Screenshot-3230.jpg

Рисунок 4.17. Дешифрование большого файла.

Функции rsa.sign() и rsa.verify() работают на произвольно длинных файлах, поэтому они не имеют «bigfile» реализации.

* + - * 1. Формат VARBLOCK

Этот раздел описывает двоичный формат связи для протокола буферных сообщений. Нет большой необходимости знать как использовать буфер протокол в своих приложениях, но очень полезно знать, как различные форматы буфера протокола влияют на размер закодированных сообщений.

Простое сообщение

При необходимости зашифровать простое сообщение (рисунок 4.18), в созданном приложении, создается сообщение Test1 и устанавливается до 150. Затем серийно посылаются сообщение в выходной поток. В результате получится три байта. Рисунок 4.19.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.1\Screenshot-3231.jpg

Рисунок 4.18.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.1\Screenshot-3232.jpg

Рисунок 4.19. Результат выполнения.

Варианты формата base 128

При кодировании буфера протокола, в первую очередь необходимо понять, varints. Varints - это метод сериализации целых чисел, используя один или несколько байт. Меньшее число принимает меньшее количество байт.

Каждый байт в varint, за исключением последнего байта, имеет самый старший бит (MSB) - это означает, что есть еще байт. Младшие 7 бит каждого байта используются для хранения в дополнение до двух представленных чисел в группах по 7 бит, наименее значительна первая группа.

Так, например, номером 1 - это один байт, поэтому старший бит не установлен. Рисунок 4.20.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.2\Screenshot-3233.jpg

Рисунок 4.20.

Для 300 необходимо немного больше. Рисунок 4.21.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.2\Screenshot-3234.jpg

Рисунок 4.21.

Чтобы определить, что это 300, нужно сначала опустить MSB от каждого байта, так как только это поможет определить достигли ли конца числа. Рисунок 4.22.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.2\Screenshot-3235.jpg

Рисунок 4.22.

Далее нужно инвертировать две группы по 7 бит, потому что varints хранит номера в первую очередь с наименьшим значением группы. После нужно объединить их, чтобы получить окончательное значение. Рисунок 4.23.

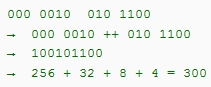


Рисунок 4.23.

Структура сообщений

Протокол буферных сообщений представляет собой серию пар ключ-значение. В бинарных сообщениях просто используется номер поля в качестве ключа - название и объявленный тип для каждого поля можно определить только в конце декодирования ссылаясь на определение типа сообщения (то есть файл .proto).

Когда сообщение кодируется, ключи и значения объединяются в поток байтов. Когда сообщение декодируется, анализатор должен пропустить поля, которые не может распознать. Таким образом, новые поля могут быть добавлены в сообщение, не нарушая целостность структуры для старых программ, которые не умеют с этим работать. С этой целью, «ключ» для каждой пары в сообщении связь-формат на самом деле два значения - значение поля сиз файла .proto, а также тип связи, что обеспечивает достаточно информации, чтобы найти длину следующего значения.

Возможные типы связей указаны в таблице 4.3.

Таблица 4.3.

|  |  |  |
| --- | --- | --- |
| **Тип** | **Значение** | **Используется для** |
| 0 | Varint | int32, int64, uint32, uint64, sint32, sint64, bool, enum |
| 1 | 64-bit | fixed64, sfixed64, double |
| 2 | Length-delimited | string, bytes, embedded messages, packed repeated fields |
| 3 | Start group | groups (устаревший) |
| 4 | End group | groups (устаревший) |
| 5 | 32-bit | fixed32, sfixed32, float |

Каждый ключ в потоковом сообщения является varint со значением (field\_number << 3) | wire\_type - иными словами, последние три бита числа хранят типа связи.

Первое число в потоке всегда является ключевым varint, и здесь эти 08 или MSB. Рисунок 4.24.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.2.3.7.3.3\Screenshot-3240.jpg

Рисунок 4.24.

Последние три бита нужны, чтобы получить тип связи(0) и тогда сдвиг вправо на три даст номер поля(1). Таким образом, тег является 1 и следующее значение является varint. Используя varint-декодирования можно увидеть, что в ближайших двух байтах хранится значение 150. Рисунок 4.25.

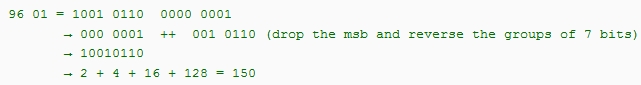


Рисунок 4.25.

* 1. Руководство пользователя
     1. Общие сведения о программе

*Обозначение и наименование программы*

Обозначение программы: «rsa.py»

Наименование программы: «Библиотека алгоритма шифрования»

*Язык программирования, на котором написана программа*

Программа написана на языке Python

*Назначение и возможности программы*

* Программа предназначена для защиты протокола обмена данных.
* Программа «Обозреватель контрактов» версии 1.0 выполняет следующие основные функции:
* Генерация псевдо-случайных чисел;
* Подписывание данных сертификатом;
* Проверка сертификатов;
* Установка защищенного соединения;
* Шифрование или дешифрование неограниченно больших файлов;
* Применять сторонние алгоритмы шифрования для большей защиты

*Ограничения области применения программы*

Программа «Библиотека алгоритма шифрования» версии 1.1 может быть применима только для защиты протокола обмена данными в качестве модуля для системы «Звезда» версии 1.2. Для использования программы в других системах не предусмотрены функции взаимодействия, что приводит к необходимости создания дополнительных функций, с учетом специфичных особенностей других систем.

*Сведения о функциональных ограничениях на применение*

Для функционирования программы «Библиотека алгоритма шифрования» версии 1.0 необходима предварительная установка следующих компонентов:

* Python не ниже версии 2.6
* VirtualEnv
* PIP
* GNU/Linux Debian Wheezy.

В случае отсутствия необходимых пакетов на компьютере пользователя, в директории с инсталляционным файлом программы имеется все необходимое для установки. Инсталляционный пакет автоматически выполнит проверку, и установит все необходимое.

* + 1. Установка

Установить можно по разному. Простой способ использует PIP или easy\_install. Либо один из способов, указанных на рисунках 4.26, 4.27 и 4.28:

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.3.2\Screenshot-3244.jpg

Рисунок 4.26

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.3.2\Screenshot-3245.jpg

Рисунок 4.27

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.3.2\Screenshot-3246.jpg

Рисунок 4.28

* + - 1. Зависимости

Python-RSA имеет очень мало зависимостей. На самом деле, для его использования нужен только Python. Загрузка и сохранение ключей может потребовать дополнительный модуль: pyasn1. Если вы используется pip или easy\_install как описано выше, все должно быть готовы к работе.

* + - 1. Разработка зависимостей

Для того, чтобы приступить к разработке на Python-RSA необходимо немного больше. Использование pip установки разработки зависимостей в виртуальной среде для Python 2.x представлено на рисунке 4.29. Для Python 3.x на рисунке 4.30.

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.3.2\Screenshot-3247.jpg

Рисунок 4.29

F:\Diplom\Защита протокола обмена данных. Олег\Diplom\Картинки\4.3.2\Screenshot-3248.jpg

Рисунок 4.30

Вывод по главе

В данной главе:

* приведены результаты тестирования программы. В ходе тестирования была проведена работа по проверке корректности работы программы с различными наборами входных данных. В результате была подтверждена правильность алгоритмов и отсутствие ошибок в их реализации;
* разработаны «руководство пользователя» и «руководство программиста»;

1. Экономическое обоснование разработки
   1. Описание работы

Разработанный программный продукт предназначен для программно-аппаратного комплекса «Звезда». Система шифрования закрывает основную уязвимость в протоколе передачи данных, а именно:

* Шифрует передаваемые данные
* Проверяет подлинность подписанных данных

Дополнительными возможностями является:

* Передача больших шифрованных файлов
* Легкое подключение к системе «Звезда»
* Совместимость с выбранной платформой

В рамках данной дипломной работы реализован модуль проверки подлинности данных управления. Использование этого модуля не накладывает какие-либо ограничения на продажу конечного продукта.

* 1. Описание конкурентов

На сегодняшний день существует достаточно много систем охраны и примененных в них алгоритмов шифрования. По своим функциональным возможностям они все схожи между собой. Однако существует ряд отличий. Рассмотрим некоторые из конкурирующих продуктов.

1. Pure-Python RSA - реализация чистого Python RSA. Он поддерживает шифрование и дешифрование, подписания и проверки подписей и генерацию ключей в соответствии с PKCS # 1 версии 1.5. Он может быть использован в качестве библиотеки Python, а также в командной строке. Код был в основном написан Sybren А. Stüvel.

Достоинства:

* Поддержка кода большим сообществом
* Хорошая документация

Недостатки:

* Ограничения на использование и изменение названия продукта лицензией ASL 2 (Apache License 2.0)
* Несовместимость с лицензией GPL

1. OpenSSL - криптографический пакет с открытым исходным кодом для работы с SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать CSR и CRT. Также имеется возможность шифрования данных и тестирования SSL/TLS соединений.

Достоинства:

* Поддержка алгоритмов ГОСТ
* Мощный инструмент защиты протоколов передачи данных

Недостатки:

* Уязвимость реализации дистрибутива Linux Debian, что не совместимо с безопасностью выбранного оборудования.

В связи с ограниченным бюджетом проекта и техническим требованиям, выявилась необходимость разработки собственного продукта.

* 1. Описание рынка сбыта

Основными потребителями программно-аппаратного комплекса «Звезда» являются обычные люди и компании, которым необходима система охраны помещения, но без модуля шифрования протокола обмена данных эта система не может выступать сильным звеном в защите помещения, поэтому столько внимания уделено защите протокола обмена данных. В результате выше описанного этот продукт пригоден для продажи как на территории Российской Федерации и стран СНГ, так и за ее пределами.

5.4. Расчет стоимости программной продукции

* + 1. Расчет трудоемкости

Трудоемкость разработки программной продукции зависит от ряда факторов, основными из которых являются: степень новизны разрабатываемого программного комплекса, сложность алгоритма его функционирования, объем используемой информации, вид ее представления и способ обработки, а также уровень используемого алгоритмического языка программирования.

Функциональным назначением разработанной в дипломном проекте программной продукции является управление документопотоком.

По степени новизны программная продукция относится к группе B (разработка программной продукции, имеющей аналоги).

По степени сложности алгоритма функционирования программная продукция относится к группе 3 (программная продукция, реализующая алгоритмы стандартных методов решения задач).

Используемая информация представлена в виде базы данных. Учитывая вид представления, способ контроля и структуру выходных документов, исходную информацию можно отнести к группе 1.1 – исходная информация представлена в форме документов, имеющих различный формат и структуру, требуется учитывать взаимовлияние показателей в различных документах. Структура выходных документов требует вывод на печать документов многоуровневой структуры - группа 2.1.

Количество разновидностей форм входной информации равно одному виду (информация об абитуриентах), количество разновидностей форм выходной информации также равно одному (отчеты) [11].

Трудоемкость разработки программной продукции  может быть определена как сумма величин трудоемкости выполнения отдельных стадий разработки ПП из выражения (5.1):

, (5.1)

где - трудоемкость разработки технического задания на создание ПП;  - трудоемкость разработки эскизного проекта ПП;  - трудоемкость разработки технического проекта ПП;  - трудоемкость разработки рабочего проекта ПП;  - трудоемкость внедрения разрабатываемого ПП.

Трудоемкость разработки технического задания рассчитывается по формуле(5.2):

, (5.2)

где  - затраты времени разработчика постановки задач на разработку ТЗ, чел.дн.;  - затраты времени разработчика ПО на разработку ТЗ, чел.дн.

Значения величин  и  рассчитывают по формулам (5.3) и (5.4)

, (5.3)

, (5.4)

где  - норма времени на разработку ТЗ на программный продукт в зависимости от функционального назначения и степени новизны разрабатываемого ПП, чел.дн.;  - коэффициент, учитывающий удельный вес трудоемкости работ, выполняе­мых разработчиком постановки задач на стадии ТЗ (в случае сов­местной с разработчиком ПО разработки =0,65);  - коэффи­циент, учитывающий удельный вес трудоемкости работ, выполняемых разработчиком ПО на стадии ТЗ (в случае совместной с разработчиком постановки задач =0,35).

Для разработанного ПП норма времени =24 [2] (в данном случае 12), следовательно, после подстановки значений в (5.2), (5.3) и (5.4), получается:







Трудоемкость разработки эскизного проекта ПП  рассчитывают по формуле (5.5):

, (5.5)

где  - затраты времени разработчика постановки задач на разработку ЭП, чел.дн.;  - затраты времени разработчика ПО на разработку ЭП, чел.дн.

Значения величин и  рассчитывают по формулам (5.6) и (5.7):

, (5.6)

, (5.7)

где  - норма времени на разработку ЭП программного продукта в зависимости от его функционального назначения и степени новизны, чел.дн.;  – коэффициент, учитывающий удельный вес трудоемкости работ, выполняемых разработчиком постановки задач на стадии ЭП (в случае сов­местной с разработчиком ПО разработки  = 0,7);  - коэффициент, учитывающий удельный вес трудоемкости работ, выполняемых разработчиком ПО на стадии ЭП (в случае совместной с разработчиком постановки задач =0,3).

Для разработанного ПП норма времени  = 70 [2] (в данном случае 20), следовательно, после подстановки значений в (5.5), (5.6) и (5.7), получается:







Трудоемкость разработки технического проекта  зависит от функционального назначения ПП, количества разновидностей форм входной и выходной информации и определяется как сумма времени, затраченного разработчиком постановки задач и разработчиком программного обеспечения (5.8):

*,* (5.8)

где ,  – норма времени, затрачиваемого на разработку ТП разработчиком постановки задач и разработчиком ПО соответственно, чел.дн.;  – коэффициент учета вида используемой информации;  – коэффициент учета режима обработки информации.

Значение коэффициента  определяют из выражения (5.9):

, (5.9)

где , ,  - значения коэффициентов учета вида используемой информации для переменной, нормативно-справочной инфор­мации и баз данных соответственно; , ,  – количество наборов данных переменной, нормативно-справочной информации и баз данных соответственно.

Для разработанного ПП = 23, = 6, =1,32, =1,00,  =0,72,  = 2,08, =0, =0, =1 [2], следовательно, после подстановки значений в (5.8) и (5.9), получается:





Трудоемкость разработки рабочего проекта  зависит от функционального назначения ПП, количества разновидностей форм входной и выходной информации, сложности алгоритма функционирования, сложности контроля информации, степени использования готовых программных модулей, уровня алгоритмического языка про­граммирования и определяется по формуле (5.10):

, (5.10)

где *КК*– коэффициент учета сложности контроля информации; *КЯ* – коэффициент учета уровня используемого алгоритмического языка программирования; *КЗ* – коэффициент учета степени использования готовых программных модулей; *КИА* – коэффициент учета вида исполь­зуемой информации и сложности алгоритма ПП.

Значение коэффициента *КИА* определяется из выражения (5.11):

, (5.11)

где , ,  - коэффициенты учета сложности алгоритма ПП и вида используемой информации для переменной. нормативно-справочной информации и баз данных соответственно; ,  - норма времени, затраченного на разработку РП на алгоритмическом языке высокого уровня разработчиком постановки задач и программного обеспечения соответственно, чел.дн.

Для разработанного ПП *КК*=1,16, *КЯ*=1,00, *КЗ*=0,8, =1,00, =0,48, =0,40, =6, =38 [2] ,следовательно, после подстановки значений в (5.10) и (5.11), получается:





При разработке программной продукции стадии «Технический проект» и «Рабочий проект» объединены в стадию «Технорабочий проект», поэтому трудоемкость ее выполнения  опреде­ляется по формуле (5.12):

*,* (5.12)

Таким образом: **

Трудоемкость выполнения стадии «Внедрение» tВ рассчитывается по формуле (5.13):

*,* (5.13)

где ,  - норма времени, затрачиваемого разработчиком постановки задач и разработчиком ПО соответственно на выполнение процедур внедрения ПП, чел.дн.

Для разработанного ПП =8, =8 [2], следовательно, после подстановки значений в (5.12), получается:

**

В итоге, после подстановки полученных значений в (5.1), трудоемкость разработки ПП составляет:



Таким образом, трудоемкость составляет 143 дней.

* + 1. Определение цены программной продукции

Процесс разработки сложной программной продукции сопровождается, кроме решения чисто программных аспектов, необходимостью решения многих социальных и экономических проблем. Одна из серьезных экономических проблем - определение стоимости ПП.

Если ПП рассматривается и создается как продукция производственно-технического назначения, допускающая многократное тиражирование и отчуждение от непосредственных разработчиков, то ее цена определяется по формуле (5.14)

, (5.14)

где *С* - затраты на разработку программной продукции (сметная себестоимость); *К* - коэффициент учета затрат на изготовление опытного образца ПП как продукции производственно-технического назначения (*К* = 1,1...1,2); *Пр* - нормативная прибыль, рассчитываемая по формуле (5.15)

, (5.15)

где *рн* - норматив рентабельности, %; *См* - материальные затраты, руб./изд.

Затраты на разработку программной продукции могут быть представлены в виде сметы затрат, включающей в себя следующие статьи: материалы, специальное оборудование, основная заработная плата, дополнительная заработная плата, отчисления на социальное нужды, производственные командировки, накладные расходы, контрагентские расходы.

1) Материалы.

В статье указываются суммарные затраты на материалы, приобретаемые для разработки данной ПП.

Для разработки ПП приобретение материалов не требуется, то есть *См* = 0 руб.

2) Специальное оборудование.

Затраты, связанные с использованием вычислительной техники, определяют по формуле (5.16):

, (5.16)

где  - время использования ЭВМ для разработки данного ПП, ч; *КИ*- поправочный коэффициент учета времени использования ЭВМ;  - цена 1-го часа работ ЭВМ, руб.; *КЭ* - коэффициент учета быстродействия ЭВМ (*КЭ*=1,0 - быстродействие ЭВМ более 20\*1030 опер./с, *КЭ* =1,2 - быстродействие ЭВМ менее 20\*1030 опер./с).

Для разработанного ПП =44, *КИ* =1,19, =15 руб., *КЭ* =1,0 [2], следовательно, после подстановки значений в (5.16), получается:



3) Основная заработная плата.

В статью включается основная заработная плата всех исполнителей, непосредственно занятых разработкой данного ПП, с учетом их должностного оклада и времени участия в разработке. Расчет ведется по формуле (5.17):

, (5.17)

где *Зi*- среднемесячный оклад i-го исполнителя, руб.;  - среднее количество рабочих дней в месяце; *ti* - трудоемкость работ, чел.дн. (определяется из календарного плана-графика).

Для разработанного ПП должностной оклад программиста составляет Зi=10 тыс.руб., среднее количество рабочих дней в месяце =22, трудоемкость работ *t*=146,23, следовательно, после подстановки значений в (5.17), получается:



4) Дополнительная заработная плата.

В статье учитываются все выплаты непосредственным исполнителя за время (установленное законодательством), непроработанное на производстве, в том числе: оплата очередных отпусков, компенсации за недоиспользованный отпуск, оплата льготных часов подросткам и др. Расчет ведется по формуле (5.18):

, (5.18)

где  - коэффициент отчислений на дополнительную зарплату.

Для разработанного ПП =0,2 [2], следовательно, после подстановки значений в (5.18), получается:



5) Отчисления на социальное страхование.

В статье учитываются отчисления в единый социальный налог по установленному законодательством тарифу от суммы основной и дополнительной заработной платы (5.19):

, (5.19)

где - коэффициент отчислений на социальное страхование.

Для разработанного ПП [2], следовательно, после подстановки значений в (5.19), получается:



6) Накладные расходы.

В статье учитываются затраты на общехозяйственные расходы, непроизводительные расходы и расходы на управление. Накладные расходы определяют в процентном отношении к основной заработной плате (5.20):

, (5.20)

где  - коэффициент накладных расходов.

Для разработанного ПП [2], следовательно, после подстановки значений в (5.20), получается:



7) Производственные командировки.

В статье учитываются все расходы на командировки, связанные с разработкой данной Ш. В ходе разработки программной продукции командировок не было.

8) Контрагентские расходы.

В статье учитываются затраты на выполнение сторонними организациями работ, непосредственно связанных с разработкой данного ПП. Сторонние организации к разработке программной продукции не привлекались. Результаты расчета сметной стоимости ПП приведены в таблице 5.1.

Таблица 5.1 Сметная стоимость программного продукта

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование статьи | Сметная  себе­стоимость, руб. | Удельный вес, % |
| 1. | Материалы | 0 |  |
| 2. | Специальное оборудование | 785,4 |  |
| 3. | Основная заработная плата | 66468,18 |  |
| 4. | Дополнительная заработная плата | 13293,64 |  |
| 5. | Отчисления на социальное страхование | 27119 |  |
| 6. | Накладные расходы | 33234,09 |  |
| 7. | Производственные командировки | 0 |  |
| 8. | Контрагентские расходы | 0 |  |
|  | Итого | 140900,31 |  |

Нормативная прибыль, рассчитываемая по формуле (5.15) составляет:



По формуле (5.14) определяется цена ПП:



* + 1. Капитальные вложения

Если еще не было программы (алгоритма) для решения данных задач, то разработанная программа сопоставляется с решением этих задач вручную, т.е. с тем, как они решались раньше. В этом случае дополнительные капитальные вложения Кд (р./одного потребителя программы), связанные с внедрением разработанной программы (алгоритма), определяются так:

*КД = (Тм.в КЭВМ* / *Тпол) + Цп* ,

где *КЭВМ* – капитальные вложения в ПЭВМ, для которой предназначена данная программа (алгоритм);

*Тпол* – полезный годовой фонд работы этой ПЭВМ (за вычетом простоев в ремонте), ч/год;

*Тм.в* – машинное время ПЭВМ, нужное данному потребителю для тех задач, которые он решает с помощью разработанной программы, машино-ч/год;

*Цп* – цена новой программы (алгоритма), которую должен приобрести потребитель, р./программу.

*КД* = (500 \* 20000 / 2112) + 198669,43 = 203404,28

* + 1. Эксплуатационные расходы

Расходы, связанные с эксплуатацией программы (алгоритма) *Е* (р./год на потребителя программы), определяются как

*Е* = (*Тм.в Цэвм*) + *Цп* / *Тс*,

где *Тм.в* – продолжительность машинного времени ПЭВМ, используемой в течение года для решения задач с помощью данной программы (алгоритма), машино-ч/год/потребителя алгоритма (программы);

*Цэвм* – эксплуатационные расходы, приходящиеся на 1 ч машинного времени этой ПЭВМ, р./машино-ч (по табл. 66 Цэвм = 5 [2]);

*Цп* – цена разработанной программы (алгоритма), р./программу;

*Тс* – срок службы данной программы (алгоритма).

Е = (500 \* 5) + 198669,43 / 10 = 42233,88

Если в прежнем варианте задача решалась вручную, то экономия эксплуатационных расходов *Еэ*, получаемая у одного потребителя данной новой программы (алгоритма), составит

*Еэ*= (1 + *αд*) (1 + *αcc*) *Зi* – *Е*,

где *Зi*  – основная заработная плата *i*-го работника, решавшего эту задачу вручную, р./год;

*Е* – эксплуатационные расходы.

*Еэ* = (1 + 0,2) \* (1 + 0,34) \* 6 \*15000– 42233,88= 102486,12

* + 1. Показатель эффективности и годового экономического эффекта

Срок окупаемости дополнительных капитальных вложений Ток в новом варианте по сравнению с прежним составит

Ток =  = 203404,28 / 102486,12≈ 1,98.

При Ток = 3 года < Тн = 6,6 года применение разработанной программы (алгоритма) является экономически эффективным.

В тех случаях, когда использование новой программы позволяет экономить как капитальные вложения (*К2* < *К1*), так и эксплуатационные расходы (*Е2* < *Е1*), годовой экономический эффект *Эг*, получаемый от внедрения новой программы (алгоритма), определяется как

*Эг* = *Еэ* + *ен Кэ* = 102486,12 + 0,15\*203404,28 = 132996,76.

Вывод по главе

В данной главе рассчитаны основные экономические показатели, свидетельствующие об экономической оправданности разработки. Кроме того, были подробно описаны достоинства и недостатки программ-конкурентов. Сводные экономические показатели по разработке и эксплуатации программы приведены в таблице 5.2.

Таблица 5.2. Сводные экономические показатели

|  |  |  |
| --- | --- | --- |
| Показатель | Размерность | Значение |
| Затраты на разработку программы | р. | 140900,31 |
| Цена программного продукта | р. | 198669,43 |
| Капитальные вложения | р./год | 203404,28 |
| Экономия эксплуатационных расходов | р./год | 102486,12 |
| Годовой экономический эффект | р./год | 132996,76 |
| Срок окупаемости, Ток | годы | 1,98 |

Заключение

В дипломной работе представлены результаты разработки алгоритма шифрования в программно-аппаратном комплексе «Звезда» версии 1.2. Приводится обоснование необходимости разработки, а также разработка функциональной и алгоритмической модели программы с применением объектно-ориентированного подхода.

* было приведено общее описание требований для совместимости с системой «Звезда»;
* поставлена задача проектирования;
* принято решение создать программный продукт, удовлетворяющий выявленным требованиям;
* были подобраны необходимые аппаратные средства;
* разработана схема взаимодействия аппаратных средств необходимых для её функционирования;
* выяснены требования к программному обеспечению, необходимые для разработки и, частично, функционирования программы;
* разработан алгоритм работы системы;
* приведены результаты тестирования программы. В ходе тестирования была проведена работа по проверке корректности работы программы с различными наборами входных данных. В результате была подтверждена правильность алгоритмов и отсутствие ошибок в их реализации;
* разработаны «руководство пользователя» и «руководство программиста»;

Результаты тестирования подтвердили соответствие разработки предъявленным требованиям.

Необходима доработка программного комплекса, так как проект является незаконченным и находится на этапе доработки и внесения изменений.

Результаты организационно-экономической части показали экономическую целесообразность создания данного программного продукта.

Список литературы

Книги

1. С. Бернет, С. Пэйн - Криптография. Официальное руководство RSA Security: БИНОМ, 2002 – 384 c.
2. Марк Лутц - Программирование на Python. Том 2, 4-е издание: Символ-Плюс, 2011 – 992 с.
3. Стенг Д., Мун С. Секреты безопасности сетей. – Киев: Диалектика, 1995.
4. Б. Шнайер, Прикладная криптография - М.: Издательство ТРИУМФ, 2002.
5. Василенко О. Н. Современные способы проверки простоты чисел. Кибернетический сборник, вып. 25. 1988. С. 162-188.

Электронные документы

1. Документация на официальном сайте Python. <http://docs.python.org/>
2. Сайт EMC. <http://russia.emc.com/domains/rsa/index.htm>
3. Сайт производителя Raspberry Pi. <http://www.raspberrypi.org/>
4. Стандарт RFC 2313. <http://tools.ietf.org/html/rfc2313/>

Учебные пособия и методические указания

1. Программное обеспечение вычислительной техники и автоматизированных систем; Методические указания к дипломному проектированию / Сост. Стоменский С.Н.; Чуваш. ун-т, Чебоксары, 2003. – 60 с.
2. Экономическое обоснование разработки программ и алгоритмов: Методические указания к выполнению организационно-экономической части дипломных проектов / Сост. Е.Ф. Перфилова; Чуваш. ун-т. Чебоксары, 2001. 50 с.
3. Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю. Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998
4. Алферов А.П., Зубов А.Ю., Кузьмин А.С. Черемушкин А.В. Основы криптографии: Учебное пособие - М.: Гелиос, 2001

ПРИЛОЖЕНИЕ А: Исходный код шифрования и дешифрования

'''Commandline scripts.

These scripts are called by the executables defined in setup.py.

'''

from \_\_future\_\_ import with\_statement, print\_function

import abc

import sys

from optparse import OptionParser

import rsa

import rsa.bigfile

import rsa.pkcs1

HASH\_METHODS = sorted(rsa.pkcs1.HASH\_METHODS.keys())

def keygen():

'''Key generator.'''

# Parse the CLI options

parser = OptionParser(usage='usage: %prog [options] keysize',

description='Generates a new RSA keypair of "keysize" bits.')

parser.add\_option('--pubout', type='string',

help='Output filename for the public key. The public key is '

'not saved if this option is not present. You can use '

'pyrsa-priv2pub to create the public key file later.')

parser.add\_option('-o', '--out', type='string',

help='Output filename for the private key. The key is '

'written to stdout if this option is not present.')

parser.add\_option('--form',

help='key format of the private and public keys - default PEM',

choices=('PEM', 'DER'), default='PEM')

(cli, cli\_args) = parser.parse\_args(sys.argv[1:])

if len(cli\_args) != 1:

parser.print\_help()

raise SystemExit(1)

try:

keysize = int(cli\_args[0])

except ValueError:

parser.print\_help()

print('Not a valid number: %s' % cli\_args[0], file=sys.stderr)

raise SystemExit(1)

print('Generating %i-bit key' % keysize, file=sys.stderr)

(pub\_key, priv\_key) = rsa.newkeys(keysize)

# Save public key

if cli.pubout:

print('Writing public key to %s' % cli.pubout, file=sys.stderr)

data = pub\_key.save\_pkcs1(format=cli.form)

with open(cli.pubout, 'wb') as outfile:

outfile.write(data)

# Save private key

data = priv\_key.save\_pkcs1(format=cli.form)

if cli.out:

print('Writing private key to %s' % cli.out, file=sys.stderr)

with open(cli.out, 'wb') as outfile:

outfile.write(data)

else:

print('Writing private key to stdout', file=sys.stderr)

sys.stdout.write(data)

class CryptoOperation(object):

'''CLI callable that operates with input, output, and a key.'''

\_\_metaclass\_\_ = abc.ABCMeta

keyname = 'public' # or 'private'

usage = 'usage: %%prog [options] %(keyname)s\_key'

description = None

operation = 'decrypt'

operation\_past = 'decrypted'

operation\_progressive = 'decrypting'

input\_help = 'Name of the file to %(operation)s. Reads from stdin if ' \

'not specified.'

output\_help = 'Name of the file to write the %(operation\_past)s file ' \

'to. Written to stdout if this option is not present.'

expected\_cli\_args = 1

has\_output = True

key\_class = rsa.PublicKey

def \_\_init\_\_(self):

self.usage = self.usage % self.\_\_class\_\_.\_\_dict\_\_

self.input\_help = self.input\_help % self.\_\_class\_\_.\_\_dict\_\_

self.output\_help = self.output\_help % self.\_\_class\_\_.\_\_dict\_\_

@abc.abstractmethod

def perform\_operation(self, indata, key, cli\_args=None):

'''Performs the program's operation.

Implement in a subclass.

:returns: the data to write to the output.

'''

def \_\_call\_\_(self):

'''Runs the program.'''

(cli, cli\_args) = self.parse\_cli()

key = self.read\_key(cli\_args[0], cli.keyform)

indata = self.read\_infile(cli.input)

print(self.operation\_progressive.title(), file=sys.stderr)

outdata = self.perform\_operation(indata, key, cli\_args)

if self.has\_output:

self.write\_outfile(outdata, cli.output)

def parse\_cli(self):

'''Parse the CLI options

:returns: (cli\_opts, cli\_args)

'''

parser = OptionParser(usage=self.usage, description=self.description)

parser.add\_option('-i', '--input', type='string', help=self.input\_help)

if self.has\_output:

parser.add\_option('-o', '--output', type='string', help=self.output\_help)

parser.add\_option('--keyform',

help='Key format of the %s key - default PEM' % self.keyname,

choices=('PEM', 'DER'), default='PEM')

(cli, cli\_args) = parser.parse\_args(sys.argv[1:])

if len(cli\_args) != self.expected\_cli\_args:

parser.print\_help()

raise SystemExit(1)

return (cli, cli\_args)

def read\_key(self, filename, keyform):

'''Reads a public or private key.'''

print('Reading %s key from %s' % (self.keyname, filename), file=sys.stderr)

with open(filename, 'rb') as keyfile:

keydata = keyfile.read()

return self.key\_class.load\_pkcs1(keydata, keyform)

def read\_infile(self, inname):

'''Read the input file'''

if inname:

print('Reading input from %s' % inname, file=sys.stderr)

with open(inname, 'rb') as infile:

return infile.read()

print('Reading input from stdin', file=sys.stderr)

return sys.stdin.read()

def write\_outfile(self, outdata, outname):

'''Write the output file'''

if outname:

print('Writing output to %s' % outname, file=sys.stderr)

with open(outname, 'wb') as outfile:

outfile.write(outdata)

else:

print('Writing output to stdout', file=sys.stderr)

sys.stdout.write(outdata)

class EncryptOperation(CryptoOperation):

'''Encrypts a file.'''

keyname = 'public'

description = ('Encrypts a file. The file must be shorter than the key '

'length in order to be encrypted. For larger files, use the '

'pyrsa-encrypt-bigfile command.')

operation = 'encrypt'

operation\_past = 'encrypted'

operation\_progressive = 'encrypting'

def perform\_operation(self, indata, pub\_key, cli\_args=None):

'''Encrypts files.'''

return rsa.encrypt(indata, pub\_key)

class DecryptOperation(CryptoOperation):

'''Decrypts a file.'''

keyname = 'private'

description = ('Decrypts a file. The original file must be shorter than '

'the key length in order to have been encrypted. For larger '

'files, use the pyrsa-decrypt-bigfile command.')

operation = 'decrypt'

operation\_past = 'decrypted'

operation\_progressive = 'decrypting'

key\_class = rsa.PrivateKey

def perform\_operation(self, indata, priv\_key, cli\_args=None):

'''Decrypts files.'''

return rsa.decrypt(indata, priv\_key)

class SignOperation(CryptoOperation):

'''Signs a file.'''

keyname = 'private'

usage = 'usage: %%prog [options] private\_key hash\_method'

description = ('Signs a file, outputs the signature. Choose the hash '

'method from %s' % ', '.join(HASH\_METHODS))

operation = 'sign'

operation\_past = 'signature'

operation\_progressive = 'Signing'

key\_class = rsa.PrivateKey

expected\_cli\_args = 2

output\_help = ('Name of the file to write the signature to. Written '

'to stdout if this option is not present.')

def perform\_operation(self, indata, priv\_key, cli\_args):

'''Decrypts files.'''

hash\_method = cli\_args[1]

if hash\_method not in HASH\_METHODS:

raise SystemExit('Invalid hash method, choose one of %s' %

', '.join(HASH\_METHODS))

return rsa.sign(indata, priv\_key, hash\_method)

class VerifyOperation(CryptoOperation):

'''Verify a signature.'''

keyname = 'public'

usage = 'usage: %%prog [options] public\_key signature\_file'

description = ('Verifies a signature, exits with status 0 upon success, '

'prints an error message and exits with status 1 upon error.')

operation = 'verify'

operation\_past = 'verified'

operation\_progressive = 'Verifying'

key\_class = rsa.PublicKey

expected\_cli\_args = 2

has\_output = False

def perform\_operation(self, indata, pub\_key, cli\_args):

'''Decrypts files.'''

signature\_file = cli\_args[1]

with open(signature\_file, 'rb') as sigfile:

signature = sigfile.read()

try:

rsa.verify(indata, signature, pub\_key)

except rsa.VerificationError:

raise SystemExit('Verification failed.')

print('Verification OK', file=sys.stderr)

class BigfileOperation(CryptoOperation):

'''CryptoOperation that doesn't read the entire file into memory.'''

def \_\_init\_\_(self):

CryptoOperation.\_\_init\_\_(self)

self.file\_objects = []

def \_\_del\_\_(self):

'''Closes any open file handles.'''

for fobj in self.file\_objects:

fobj.close()

def \_\_call\_\_(self):

'''Runs the program.'''

(cli, cli\_args) = self.parse\_cli()

key = self.read\_key(cli\_args[0], cli.keyform)

# Get the file handles

infile = self.get\_infile(cli.input)

outfile = self.get\_outfile(cli.output)

# Call the operation

print(self.operation\_progressive.title(), file=sys.stderr)

self.perform\_operation(infile, outfile, key, cli\_args)

def get\_infile(self, inname):

'''Returns the input file object'''

if inname:

print('Reading input from %s' % inname, file=sys.stderr)

fobj = open(inname, 'rb')

self.file\_objects.append(fobj)

else:

print('Reading input from stdin', file=sys.stderr)

fobj = sys.stdin

return fobj

def get\_outfile(self, outname):

'''Returns the output file object'''

if outname:

print('Will write output to %s' % outname, file=sys.stderr)

fobj = open(outname, 'wb')

self.file\_objects.append(fobj)

else:

print('Will write output to stdout', file=sys.stderr)

fobj = sys.stdout

return fobj

class EncryptBigfileOperation(BigfileOperation):

'''Encrypts a file to VARBLOCK format.'''

keyname = 'public'

description = ('Encrypts a file to an encrypted VARBLOCK file. The file '

'can be larger than the key length, but the output file is only '

'compatible with Python-RSA.')

operation = 'encrypt'

operation\_past = 'encrypted'

operation\_progressive = 'encrypting'

def perform\_operation(self, infile, outfile, pub\_key, cli\_args=None):

'''Encrypts files to VARBLOCK.'''

return rsa.bigfile.encrypt\_bigfile(infile, outfile, pub\_key)

class DecryptBigfileOperation(BigfileOperation):

'''Decrypts a file in VARBLOCK format.'''

keyname = 'private'

description = ('Decrypts an encrypted VARBLOCK file that was encrypted '

'with pyrsa-encrypt-bigfile')

operation = 'decrypt'

operation\_past = 'decrypted'

operation\_progressive = 'decrypting'

key\_class = rsa.PrivateKey

def perform\_operation(self, infile, outfile, priv\_key, cli\_args=None):

'''Decrypts a VARBLOCK file.'''

return rsa.bigfile.decrypt\_bigfile(infile, outfile, priv\_key)

encrypt = EncryptOperation()

decrypt = DecryptOperation()

sign = SignOperation()

verify = VerifyOperation()

encrypt\_bigfile = EncryptBigfileOperation()

decrypt\_bigfile = DecryptBigfileOperation()

ПРИЛОЖЕНИЕ Б: Исходный код работы с ключами

'''RSA key generation code.

Create new keys with the newkeys() function. It will give you a PublicKey and a

PrivateKey object.

Loading and saving keys requires the pyasn1 module. This module is imported as

late as possible, such that other functionality will remain working in absence

of pyasn1.

'''

import logging

from rsa.\_compat import b, bytes\_type

import rsa.prime

import rsa.pem

import rsa.common

log = logging.getLogger(\_\_name\_\_)

class AbstractKey(object):

'''Abstract superclass for private and public keys.'''

@classmethod

def load\_pkcs1(cls, keyfile, format='PEM'):

r'''Loads a key in PKCS#1 DER or PEM format.

:param keyfile: contents of a DER- or PEM-encoded file that contains

the public key.

:param format: the format of the file to load; 'PEM' or 'DER'

:return: a PublicKey object

'''

methods = {

'PEM': cls.\_load\_pkcs1\_pem,

'DER': cls.\_load\_pkcs1\_der,

}

if format not in methods:

formats = ', '.join(sorted(methods.keys()))

raise ValueError('Unsupported format: %r, try one of %s' % (format,

formats))

method = methods[format]

return method(keyfile)

def save\_pkcs1(self, format='PEM'):

'''Saves the public key in PKCS#1 DER or PEM format.

:param format: the format to save; 'PEM' or 'DER'

:returns: the DER- or PEM-encoded public key.

'''

methods = {

'PEM': self.\_save\_pkcs1\_pem,

'DER': self.\_save\_pkcs1\_der,

}

if format not in methods:

formats = ', '.join(sorted(methods.keys()))

raise ValueError('Unsupported format: %r, try one of %s' % (format,

formats))

method = methods[format]

return method()

class PublicKey(AbstractKey):

'''Represents a public RSA key.

This key is also known as the 'encryption key'. It contains the 'n' and 'e'

values.

Supports attributes as well as dictionary-like access. Attribute accesss is

faster, though.

>>> PublicKey(5, 3)

PublicKey(5, 3)

>>> key = PublicKey(5, 3)

>>> key.n

5

>>> key['n']

5

>>> key.e

3

>>> key['e']

3

'''

\_\_slots\_\_ = ('n', 'e')

def \_\_init\_\_(self, n, e):

self.n = n

self.e = e

def \_\_getitem\_\_(self, key):

return getattr(self, key)

def \_\_repr\_\_(self):

return 'PublicKey(%i, %i)' % (self.n, self.e)

def \_\_eq\_\_(self, other):

if other is None:

return False

if not isinstance(other, PublicKey):

return False

return self.n == other.n and self.e == other.e

def \_\_ne\_\_(self, other):

return not (self == other)

@classmethod

def \_load\_pkcs1\_der(cls, keyfile):

r'''Loads a key in PKCS#1 DER format.

@param keyfile: contents of a DER-encoded file that contains the public

key.

@return: a PublicKey object

First let's construct a DER encoded key:

>>> import base64

>>> b64der = 'MAwCBQCNGmYtAgMBAAE='

>>> der = base64.decodestring(b64der)

This loads the file:

>>> PublicKey.\_load\_pkcs1\_der(der)

PublicKey(2367317549, 65537)

'''

from pyasn1.codec.der import decoder

from rsa.asn1 import AsnPubKey

(priv, \_) = decoder.decode(keyfile, asn1Spec=AsnPubKey())

return cls(n=int(priv['modulus']), e=int(priv['publicExponent']))

def \_save\_pkcs1\_der(self):

'''Saves the public key in PKCS#1 DER format.

@returns: the DER-encoded public key.

'''

from pyasn1.codec.der import encoder

from rsa.asn1 import AsnPubKey

# Create the ASN object

asn\_key = AsnPubKey()

asn\_key.setComponentByName('modulus', self.n)

asn\_key.setComponentByName('publicExponent', self.e)

return encoder.encode(asn\_key)

@classmethod

def \_load\_pkcs1\_pem(cls, keyfile):

'''Loads a PKCS#1 PEM-encoded public key file.

The contents of the file before the "-----BEGIN RSA PUBLIC KEY-----" and

after the "-----END RSA PUBLIC KEY-----" lines is ignored.

@param keyfile: contents of a PEM-encoded file that contains the public

key.

@return: a PublicKey object

'''

der = rsa.pem.load\_pem(keyfile, 'RSA PUBLIC KEY')

return cls.\_load\_pkcs1\_der(der)

def \_save\_pkcs1\_pem(self):

'''Saves a PKCS#1 PEM-encoded public key file.

@return: contents of a PEM-encoded file that contains the public key.

'''

der = self.\_save\_pkcs1\_der()

return rsa.pem.save\_pem(der, 'RSA PUBLIC KEY')

@classmethod

def load\_pkcs1\_openssl\_pem(cls, keyfile):

'''Loads a PKCS#1.5 PEM-encoded public key file from OpenSSL.

These files can be recognised in that they start with BEGIN PUBLIC KEY

rather than BEGIN RSA PUBLIC KEY.

The contents of the file before the "-----BEGIN PUBLIC KEY-----" and

after the "-----END PUBLIC KEY-----" lines is ignored.

@param keyfile: contents of a PEM-encoded file that contains the public

key, from OpenSSL.

@return: a PublicKey object

'''

der = rsa.pem.load\_pem(keyfile, 'PUBLIC KEY')

return cls.load\_pkcs1\_openssl\_der(der)

@classmethod

def load\_pkcs1\_openssl\_der(cls, keyfile):

'''Loads a PKCS#1 DER-encoded public key file from OpenSSL.

@param keyfile: contents of a DER-encoded file that contains the public

key, from OpenSSL.

@return: a PublicKey object

'''

from rsa.asn1 import OpenSSLPubKey

from pyasn1.codec.der import decoder

from pyasn1.type import univ

(keyinfo, \_) = decoder.decode(keyfile, asn1Spec=OpenSSLPubKey())

if keyinfo['header']['oid'] != univ.ObjectIdentifier('1.2.840.113549.1.1.1'):

raise TypeError("This is not a DER-encoded OpenSSL-compatible public key")

return cls.\_load\_pkcs1\_der(keyinfo['key'][1:])

class PrivateKey(AbstractKey):

'''Represents a private RSA key.

This key is also known as the 'decryption key'. It contains the 'n', 'e',

'd', 'p', 'q' and other values.

Supports attributes as well as dictionary-like access. Attribute accesss is

faster, though.

>>> PrivateKey(3247, 65537, 833, 191, 17)

PrivateKey(3247, 65537, 833, 191, 17)

exp1, exp2 and coef don't have to be given, they will be calculated:

>>> pk = PrivateKey(3727264081, 65537, 3349121513, 65063, 57287)

>>> pk.exp1

55063

>>> pk.exp2

10095

>>> pk.coef

50797

If you give exp1, exp2 or coef, they will be used as-is:

>>> pk = PrivateKey(1, 2, 3, 4, 5, 6, 7, 8)

>>> pk.exp1

6

>>> pk.exp2

7

>>> pk.coef

8

'''

\_\_slots\_\_ = ('n', 'e', 'd', 'p', 'q', 'exp1', 'exp2', 'coef')

def \_\_init\_\_(self, n, e, d, p, q, exp1=None, exp2=None, coef=None):

self.n = n

self.e = e

self.d = d

self.p = p

self.q = q

# Calculate the other values if they aren't supplied

if exp1 is None:

self.exp1 = int(d % (p - 1))

else:

self.exp1 = exp1

if exp1 is None:

self.exp2 = int(d % (q - 1))

else:

self.exp2 = exp2

if coef is None:

self.coef = rsa.common.inverse(q, p)

else:

self.coef = coef

def \_\_getitem\_\_(self, key):

return getattr(self, key)

def \_\_repr\_\_(self):

return 'PrivateKey(%(n)i, %(e)i, %(d)i, %(p)i, %(q)i)' % self

def \_\_eq\_\_(self, other):

if other is None:

return False

if not isinstance(other, PrivateKey):

return False

return (self.n == other.n and

self.e == other.e and

self.d == other.d and

self.p == other.p and

self.q == other.q and

self.exp1 == other.exp1 and

self.exp2 == other.exp2 and

self.coef == other.coef)

def \_\_ne\_\_(self, other):

return not (self == other)

@classmethod

def \_load\_pkcs1\_der(cls, keyfile):

r'''Loads a key in PKCS#1 DER format.

@param keyfile: contents of a DER-encoded file that contains the private

key.

@return: a PrivateKey object

First let's construct a DER encoded key:

>>> import base64

>>> b64der = 'MC4CAQACBQDeKYlRAgMBAAECBQDHn4npAgMA/icCAwDfxwIDANcXAgInbwIDAMZt'

>>> der = base64.decodestring(b64der)

This loads the file:

>>> PrivateKey.\_load\_pkcs1\_der(der)

PrivateKey(3727264081, 65537, 3349121513, 65063, 57287)

'''

from pyasn1.codec.der import decoder

(priv, \_) = decoder.decode(keyfile)

# ASN.1 contents of DER encoded private key:

#

# RSAPrivateKey ::= SEQUENCE {

# version Version,

# modulus INTEGER, -- n

# publicExponent INTEGER, -- e

# privateExponent INTEGER, -- d

# prime1 INTEGER, -- p

# prime2 INTEGER, -- q

# exponent1 INTEGER, -- d mod (p-1)

# exponent2 INTEGER, -- d mod (q-1)

# coefficient INTEGER, -- (inverse of q) mod p

# otherPrimeInfos OtherPrimeInfos OPTIONAL

# }

if priv[0] != 0:

raise ValueError('Unable to read this file, version %s != 0' % priv[0])

as\_ints = tuple(int(x) for x in priv[1:9])

return cls(\*as\_ints)

def \_save\_pkcs1\_der(self):

'''Saves the private key in PKCS#1 DER format.

@returns: the DER-encoded private key.

'''

from pyasn1.type import univ, namedtype

from pyasn1.codec.der import encoder

class AsnPrivKey(univ.Sequence):

componentType = namedtype.NamedTypes(

namedtype.NamedType('version', univ.Integer()),

namedtype.NamedType('modulus', univ.Integer()),

namedtype.NamedType('publicExponent', univ.Integer()),

namedtype.NamedType('privateExponent', univ.Integer()),

namedtype.NamedType('prime1', univ.Integer()),

namedtype.NamedType('prime2', univ.Integer()),

namedtype.NamedType('exponent1', univ.Integer()),

namedtype.NamedType('exponent2', univ.Integer()),

namedtype.NamedType('coefficient', univ.Integer()),

)

# Create the ASN object

asn\_key = AsnPrivKey()

asn\_key.setComponentByName('version', 0)

asn\_key.setComponentByName('modulus', self.n)

asn\_key.setComponentByName('publicExponent', self.e)

asn\_key.setComponentByName('privateExponent', self.d)

asn\_key.setComponentByName('prime1', self.p)

asn\_key.setComponentByName('prime2', self.q)

asn\_key.setComponentByName('exponent1', self.exp1)

asn\_key.setComponentByName('exponent2', self.exp2)

asn\_key.setComponentByName('coefficient', self.coef)

return encoder.encode(asn\_key)

@classmethod

def \_load\_pkcs1\_pem(cls, keyfile):

'''Loads a PKCS#1 PEM-encoded private key file.

The contents of the file before the "-----BEGIN RSA PRIVATE KEY-----" and

after the "-----END RSA PRIVATE KEY-----" lines is ignored.

@param keyfile: contents of a PEM-encoded file that contains the private

key.

@return: a PrivateKey object

'''

der = rsa.pem.load\_pem(keyfile, b('RSA PRIVATE KEY'))

return cls.\_load\_pkcs1\_der(der)

def \_save\_pkcs1\_pem(self):

'''Saves a PKCS#1 PEM-encoded private key file.

@return: contents of a PEM-encoded file that contains the private key.

'''

der = self.\_save\_pkcs1\_der()

return rsa.pem.save\_pem(der, b('RSA PRIVATE KEY'))

def find\_p\_q(nbits, getprime\_func=rsa.prime.getprime, accurate=True):

''''Returns a tuple of two different primes of nbits bits each.

The resulting p \* q has exacty 2 \* nbits bits, and the returned p and q

will not be equal.

:param nbits: the number of bits in each of p and q.

:param getprime\_func: the getprime function, defaults to

:py:func:`rsa.prime.getprime`.

\*Introduced in Python-RSA 3.1\*

:param accurate: whether to enable accurate mode or not.

:returns: (p, q), where p > q

>>> (p, q) = find\_p\_q(128)

>>> from rsa import common

>>> common.bit\_size(p \* q)

256

When not in accurate mode, the number of bits can be slightly less

>>> (p, q) = find\_p\_q(128, accurate=False)

>>> from rsa import common

>>> common.bit\_size(p \* q) <= 256

True

>>> common.bit\_size(p \* q) > 240

True

'''

total\_bits = nbits \* 2

# Make sure that p and q aren't too close or the factoring programs can

# factor n.

shift = nbits // 16

pbits = nbits + shift

qbits = nbits - shift

# Choose the two initial primes

log.debug('find\_p\_q(%i): Finding p', nbits)

p = getprime\_func(pbits)

log.debug('find\_p\_q(%i): Finding q', nbits)

q = getprime\_func(qbits)

def is\_acceptable(p, q):

'''Returns True iff p and q are acceptable:

- p and q differ

- (p \* q) has the right nr of bits (when accurate=True)

'''

if p == q:

return False

if not accurate:

return True

# Make sure we have just the right amount of bits

found\_size = rsa.common.bit\_size(p \* q)

return total\_bits == found\_size

# Keep choosing other primes until they match our requirements.

change\_p = False

while not is\_acceptable(p, q):

# Change p on one iteration and q on the other

if change\_p:

p = getprime\_func(pbits)

else:

q = getprime\_func(qbits)

change\_p = not change\_p

# We want p > q as described on

# http://www.di-mgt.com.au/rsa\_alg.html#crt

return (max(p, q), min(p, q))

def calculate\_keys(p, q, nbits):

'''Calculates an encryption and a decryption key given p and q, and

returns them as a tuple (e, d)

'''

phi\_n = (p - 1) \* (q - 1)

# A very common choice for e is 65537

e = 65537

try:

d = rsa.common.inverse(e, phi\_n)

except ValueError:

raise ValueError("e (%d) and phi\_n (%d) are not relatively prime" %

(e, phi\_n))

if (e \* d) % phi\_n != 1:

raise ValueError("e (%d) and d (%d) are not mult. inv. modulo "

"phi\_n (%d)" % (e, d, phi\_n))

return (e, d)

def gen\_keys(nbits, getprime\_func, accurate=True):

'''Generate RSA keys of nbits bits. Returns (p, q, e, d).

Note: this can take a long time, depending on the key size.

:param nbits: the total number of bits in ``p`` and ``q``. Both ``p`` and

``q`` will use ``nbits/2`` bits.

:param getprime\_func: either :py:func:`rsa.prime.getprime` or a function

with similar signature.

'''

(p, q) = find\_p\_q(nbits // 2, getprime\_func, accurate)

(e, d) = calculate\_keys(p, q, nbits // 2)

return (p, q, e, d)

def newkeys(nbits, accurate=True, poolsize=1):

'''Generates public and private keys, and returns them as (pub, priv).

The public key is also known as the 'encryption key', and is a

:py:class:`rsa.PublicKey` object. The private key is also known as the

'decryption key' and is a :py:class:`rsa.PrivateKey` object.

:param nbits: the number of bits required to store ``n = p\*q``.

:param accurate: when True, ``n`` will have exactly the number of bits you

asked for. However, this makes key generation much slower. When False,

`n`` may have slightly less bits.

:param poolsize: the number of processes to use to generate the prime

numbers. If set to a number > 1, a parallel algorithm will be used.

This requires Python 2.6 or newer.

:returns: a tuple (:py:class:`rsa.PublicKey`, :py:class:`rsa.PrivateKey`)

The ``poolsize`` parameter was added in \*Python-RSA 3.1\* and requires

Python 2.6 or newer.

'''

if nbits < 16:

raise ValueError('Key too small')

if poolsize < 1:

raise ValueError('Pool size (%i) should be >= 1' % poolsize)

# Determine which getprime function to use

if poolsize > 1:

from rsa import parallel

import functools

getprime\_func = functools.partial(parallel.getprime, poolsize=poolsize)

else: getprime\_func = rsa.prime.getprime

# Generate the key components

(p, q, e, d) = gen\_keys(nbits, getprime\_func)

# Create the key objects

n = p \* q

return (

PublicKey(n, e),

PrivateKey(n, e, d, p, q)

)

\_\_all\_\_ = ['PublicKey', 'PrivateKey', 'newkeys']

if \_\_name\_\_ == '\_\_main\_\_':

import doctest

try:

for count in range(100):

(failures, tests) = doctest.testmod()

if failures:

break

if (count and count % 10 == 0) or count == 1:

print('%i times' % count)

except KeyboardInterrupt:

print('Aborted')

else:

print('Doctests done')