УДК 004.42.056.53

ШИФРОВЩИК ДАННЫХ

Ли Д.
Костанайский государственный университет им.А.Байтурсынова, Костанай

Научный руководитель: Махамбетова Г. И. ст. преподаватель кафедры программного обеспечения

Данная программа наглядно демонстрирует сущность работы алгоритмов шифрования данных DES (Data Encryption System) и RSA (Rivest, Shamir ,Adleman).

Дан анализ математических методов преобразования информации и их применения к шифрованию данных; разработке и реализации программного продукта , демонстрирующего работу этих алгоритмов при передаче данных. Актуальность данной разработки обусловлена постоянно повышающимся интересом к вопросам защиты информации, и в частности, анализу работы и применения криптосистем DES и RSA; сложностью теоретико-числовых алгоритмов и отсутствием достаточно эффективных методов их решения, лежащих в основе рассматриваемых криптосистем.

Рассматриваемая тема затронула два аспекта:

- разработку средств, реализующих криптографические алгоритмы;
- методику использования этих средств.

Каждый из криптографических методов могут быть реализованы либо программным, либо аппаратным способом.

Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы.

Описание работы шифровщика

DES представляет собой блочный шифр, он шифрует данные 64-битовыми блоками. С одного конца алгоритма вводится 64-битовый блок открытого текста, а с другого конца выходит 64-битовый блок шифротекста. DES является симметричным алгоритмом: для шифрования и дешифрования используются одинаковые алгоритм и ключ (за исключением небольших отличий в использовании ключа).

Длинна ключа равна 56 битам. (Ключ обычно представляется 64-битовым числом, но каждый восьмой бит используется для проверки четности и игнорируется.) Безопасность полностью определяется ключом.

Алгоритм представляет собой комбинацию 2-х основных методов шифрования: смещение и диффузия. Фундаментальным строительным блоком DES является применение к тексту единичной комбинации этих методов (подстановка, а за ней – перестановка), зависящей от ключа. Такой блок называется этапом. DES состоит из 16 этапов, одинаковая комбинация методов применяется к открытому тексту 16 раз.

RSA (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом.

RSA стал первым алгоритмом такого типа, пригодным и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

Интерфейс программы состоит из одного, главного окна, разделенного на 2 половины. Рассмотрим левую часть окна с шифровщиком DES (Рис. 1).

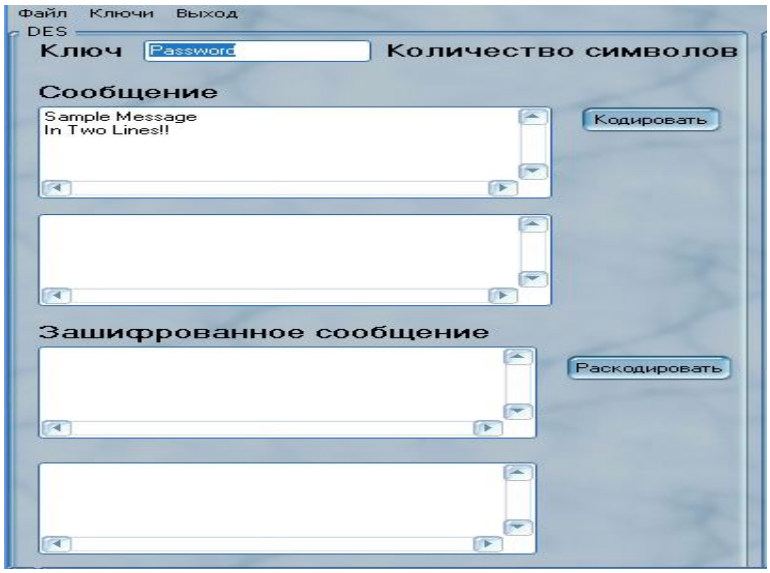

Рис. 1 (Шифровщик DES)

В верхней части находится поле в которое необходимо ввести пароль. Пароль обязательно должен состоять из 8 символов (особенность алгоритма DES).

В нижеследующем поле необходимо ввести текст сообщения которое необходимо зашифровать. Количество символов должно быть кратно 8, причем переход на новую строку считается как 2 символа. Для облегчения над полем ввода будет отображаться количество введенных символов. При вводе сообщения символы будут автоматически переводится в бинарный код. Это сделано для наглядности работы алгоритма. После ввода сообщения необходимо нажать кнопку с надписью «Кодировать», чтобы начать шифрование. При несоблюдении условия о кратности 8 будет выдано сообщение об ошибке. По окончании шифрования в нижнем поле появится зашифрованное сообщение и его бинарная интерпретация. Для расшифровки сообщения необходимо ввести зашифрованный текст в поле, ввести правильный пароль и нажать кнопку «Раскодировать».

Рассмотрим правую часть окна с шифровщиком RSA (Рис. 2).

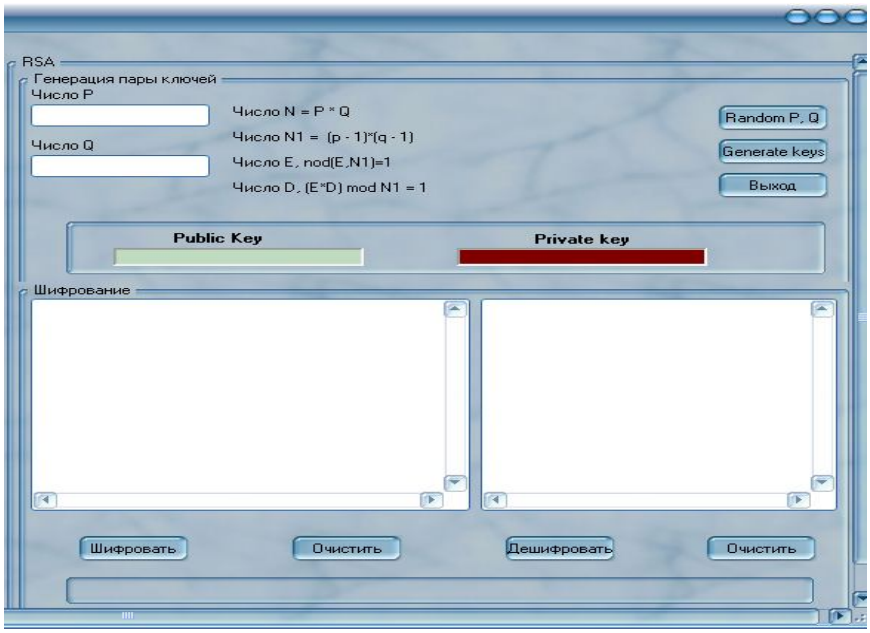

Рис 2. Шифровщик RSA

При нажатии на кнопку «Random P,Q», на экран выводятся числа P и Q. Далее при нажатии на кнопку «Generate keys», генерируется пара ключей: публичный и частный. После того, как в соответствии с заданными формулами сгенерированы ключи, сохраняем их (Рис. 3).

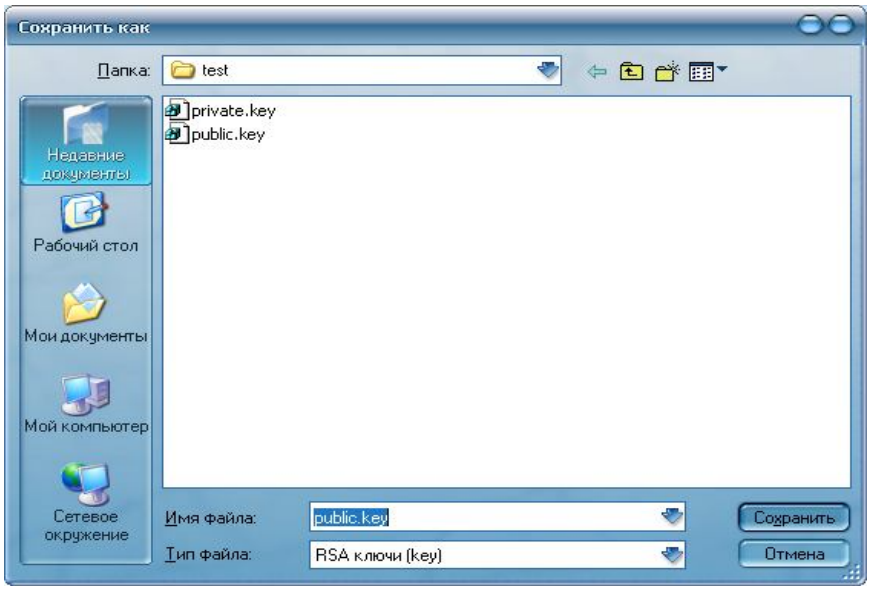

Рис. 3 Сохранение сгенерированных ключей

После сохранения сгенерированных ключей, загружаем текстовый файл (Рис. 4).

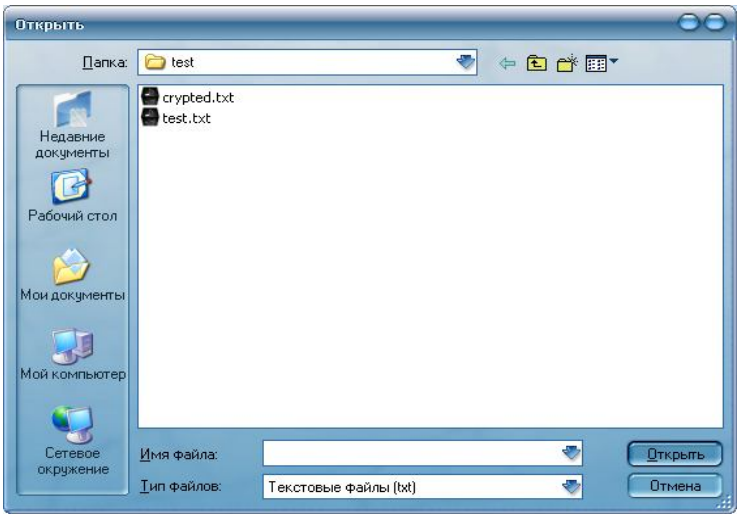

Рис. 4 Загрузка текстового файла

После загрузки текстового файла, нажимаем кнопку «Шифровать», далее сохраняем зашифрованный текст.

Для дешифровки, загружаем полученные ключи, загружаем зашифрованный файл и нажимаем кнопку «Дешифровать».

Литература

1. С. Панасенко, "Алгоритмы шифрования", 2009
2. Ростовцев А.Г., Маховенко Е.Б. «Теоретическая криптография», 2005
3. Нечаев В.И. Элементы криптографии. «Основы теории защиты информации», 1999
4. Сергей Бобровский «Технологии Delphi 2006. Новые возможности», 2006