РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ НА ЯЗЫКЕ C++

Куделя А. А., Макарич Д. А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е. Д. – ст. преп. кафедры информатики

В работе исследованы некоторые симметричные и асимметричные криптографические алгоритмы, осуществлена их реализация на языке программирования C++, проведён анализ результатов программ, выявлены оптимальные случаи использования тех или иных криптографических методов.

В настоящее время, с развитием информационных технологий, обеспечение секретности и приватности при коммуникациях между людьми является одной из основных задач. Криптология – наука, исследующая криптографические преобразования, т. е. преобразования, которые обеспечивают защиту информации от несанкционированного доступа. В криптологии различают следующие направления: криптографию и криптоанализ. Криптография – это часть криптологии, связанная с проектированием секретных систем. Криптоанализ – это часть криптологии, посвящённая изучению уязвимости секретных

систем.

В работе были изучены симметричные (с закрытым ключом) и асимметричные (с открытым ключом) криптосистемы. В симметричных криптосистемах для шифрования и дешифрования используется общий секретный ключ. В асимметричных же криптосистемах для шифрования используется открытый ключ, а для дешифрования – закрытый ключ. Симметричное шифрование благодаря своей скорости широко используется для защиты информации во многих современных компьютерных системах. Асимметричное шифрование может применяться в системах зашифровывания и расшифровывания пакетов данных, когда скорость и вычислительная мощность не являются приоритетными.

На примере криптографических алгоритмов XOR, Triple DES (3DES) и RSA в работе проведены анализ и сравнение симметричного, симметричного блочного и асимметричного криптографических алгоритмов. Также выявлены случаи наиболее удобного использования того или иного метода шифрования. В практической части реализованы данные и гибридные криптографические методы на языке программирования C++.

XOR – самый простой пример симметричного алгоритма шифрования. XOR – логическая операция, которая принимает значение «истина», если хотя бы один из аргументов имеет значение «истина». Минусом такого шифрования является то, что, зная часть зашифрованного текста, можно с лёгкостью восстановить ключ и, соответственно, расшифровать весь текст. Поэтому в чистом виде данный метод редко используется на практике, хотя его применяют как часть более сложных алгоритмов шифрования.

На рисунке 1 представлен скриншот работы программы, реализующей зашифровывание и расшифровывание сообщения «Hello world!» с помощью алгоритма XOR. В данной программе ключом является строка (string). В цикле, используя операцию XOR, шифруется каждый символ строки, который соответствует коду ASCII, с помощью ключа. Аналогичным методом дешифруется строка в цикле с помощью XOR.

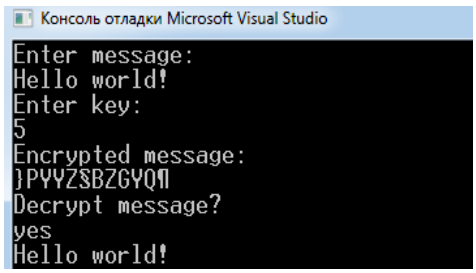

Рисунок 1 – Пример работы программы, реализующей криптографический метод XOR

3DES – симметричный блочный шифр, созданный на основе алгоритма DES. В работе программно реализованы этапы шифрования и дешифрования с использованием сети Фейстеля, изучены криптостойкость и области применения 3DES. Шифр 3DES с тремя различными ключами имеет длину ключа, равную 168 бит, но из-за атак «встреча посередине» эффективная криптостойкость составляет только 112 бит. Для успешной атаки на 3DES потребуется около 2^32 бит известного открытого текста, 2^113 шагов, 2^90 циклов DES-шифрования и 2^88 бит памяти. На данный момент это непрактично, и, по оценкам НИСТ, алгоритм с выбором трёх различных ключей должен остаться надёжным до 2030-х. В настоящее время известных криптографических атак, применимых на практике, на 3DES не существует. 3DES с тремя ключами реализован во многих приложениях, ориентированных на работу с Интернетом, в том числе в PGP и S/mime. Индустрия электронных платежей использует 3DES и продолжает активно разрабатывать и публиковать стандарты, основанные на нём (например EMV).

Криптографический алгоритм RSA основан на вычислительной сложности факторизации больших чисел. В работе программно реализованы этапы генерации ключей, шифрования и дешифрования алгоритма RSA. Проанализирована скорость работы алгоритма. Поскольку генерация ключей происходит значительно реже операций, реализующих шифрование и дешифрование, задача возведения в степень по модулю представляет основную вычислительную сложность. В программе эта проблема решается с помощью алгоритма быстрого возведения в степень. Атака Винера позволяет узнать расшифровывающую экспоненту d, поочерёдно подставляя в выражение $(m^e)^d \equiv m \pmod n$ для некоторого случайного m знаменатели подходящих дробей k/d из разложения e/n в непрерывную дробь. RSA используется для защиты программного обеспечения и в схемах цифровой подписи. Из-за низкой скорости шифрования сообщения обычно шифруют с помощью более производительных симметричных алгоритмов со случайным сеансовым ключом, а с помощью RSA шифруют лишь этот ключ, таким образом, реализуется гибридная система.

На рисунке 2 представлен скриншот работы программы, реализующей генерацию открытого

ключа (3, 9173503) с помощью алгоритма RSA. На рисунке 3 представлен скриншот работы программы, реализующей зашифровывание и расшифровывание сообщения «111111» с помощью алгоритма RSA.

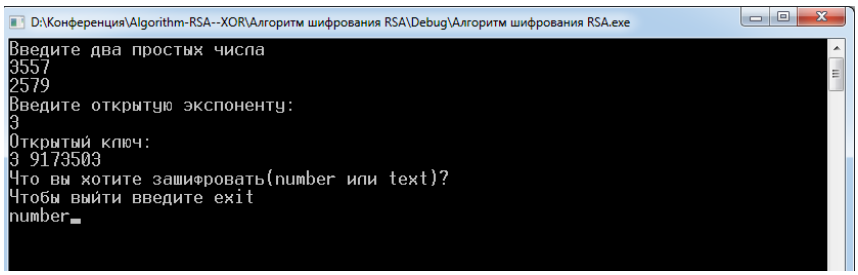

Рисунок 2 – Пример работы программы, реализующей генерацию открытого ключа алгоритмом RSA

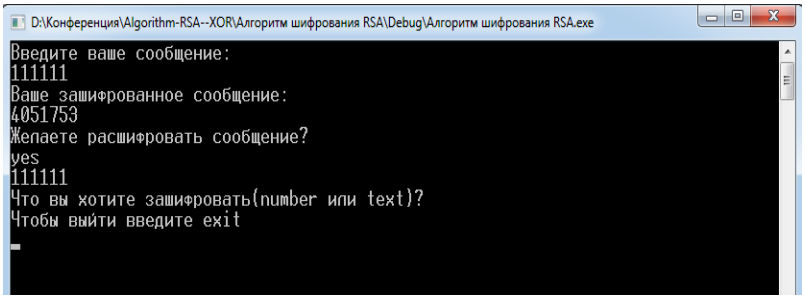

Рисунок 3 – Пример работы программы, реализующей зашифровывание и расшифровывание сообщения алгоритмом RSA

На примерах XOR, Triple DES и RSA рассмотрены особенности программной реализации методов шифрования на языке C++, изучены недостатки и предложены способы их устранения с использованием гибридных алгоритмов. Коды программ доступны по ссылкам:

1) https://github.com/DmitryMakarich/Algorithm-RSA--XOR – программы RSA, XOR;
2) https://github.com/alexku31/Repp/blob/master/3des.c – программа 3DES.

Список использованных источников:

1. Криптографические методы защиты информации [Электронный ресурс]. – Режим доступа : https://urok.1sept.ru/%D1%81%D1%82%D0%B0%D1%82%D1%8C%D0%B8/636966/.

2. Алгоритм RSA [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/RSA#%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_RSA.

3. Алгоритм шифрования XOR [Электронный ресурс]. – Режим доступа : https://evileg.com/ru/post/271/.

4. Triple DES [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/Triple_DES#%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D1%82%D0%BE%D0%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C.

5. DES [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/DES#%D0%9F%D1%80%D0%B5%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D1%81%D0%B5%D1%82%D1%8C%D1%8E_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F.

6. Асимметричное шифрование на практике [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/449552/.

7. Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания [Электронный ресурс]. – Режим доступа : https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/system-cryptography-use-fips-compliant-algorithms-for-encryption-hashing-and-signing.

8. Представлен Sweet32, новый вид атаки на HTTPS и OpenVPN [Электронный ресурс]. – Режим доступа : https://www.opennet.ru/opennews/art.shtml?num=45023.