Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина «Методы защиты информации»

**ОТЧЕТ**

к лабораторной работе

на тему:

**«Асимметричная криптография. Криптосистема Рабина»**

|  |  |
| --- | --- |
|  | Выполнил:  Слуцкий Никита Сергеевич,  студент группы 053505 |
|  | Проверил: Лещенко Евгений Александрович, ассистент каф. Информатики |

Минск 2023

СОДЕРЖАНИЕ

[Введение 3](#_Toc147588793)

[1 Краткие теоретические сведения 4](#_Toc147588794)

[2 Ход выполнения работы 5](#_Toc147588795)

[Заключение 6](#_Toc147588796)

[Приложение А 7](#_Toc147588797)

# Введение

Целью данной лабораторной работы является реализовать программное средство шифрования и дешифрования текстовых файлов при помощи алгоритма криптосистемы Рабина на выбранном языке программирования.

# 1 Краткие теоретические сведения

Генерируются два простых числа p и q. В реальных условиях это должны быть большие простые числа, которые при этом оба должны при делении на 4 давать в остатке 3. В условиях лабораторной работы ввиду отсутствия достаточно большого встроенного типа данных в стандарте языка программирования C++ условие больших чисел сужается до допустимого диапазона предоставляемых встроенных типов данных. Пара этих чисел – это закрытый ключ. Открытый ключ – их перемножение. Ключи генерируются на стороне получателя, открытый ключ передаётся отправителю. Отправитель с помощью него шифрует сообщение и передаёт зашифрованное сообщение получателю.

Шифрование сводится к простой операции возведения исходного числа в квадрат и взятие остатка от деления на открытый ключ.

Декодирование сводится к вычислению «квадратных корней» от зашифрованного числа и выбору какого-нибудь из них. Для расшифрования требуется расширенный алгоритм Евклида и китайская теорема об остатках. По расширенному алгоритму Евклида вычисляются два коэффициента yp и yq­ таких, что yp \* p + yq­ \* q = 1, где p, q – части закрытого ключа. Это происходит на стороне получателя, когда он получает зашифрованное сообщение. После этого необходимо просчитать значения mp и mq. Это делается по формуле (1). В этой формуле вместо x необходимо подставить p и q для mp и mq соответственно.

После этого по формулам на рисунке 1 можно вычислить четыре предполагаемых значения.

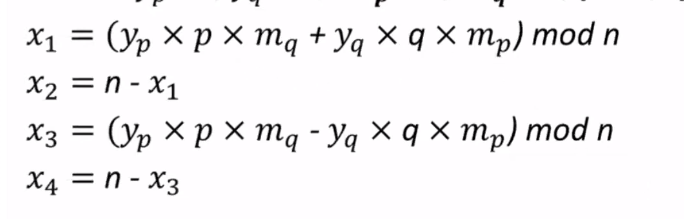


Рисунок 1 – Вычисление четырёх возможных значений

Криптосистема Рабина не позволяет однозначно расшифровать сообщение. Она позволяет предположить 4 возможных варианта. По какому-то признаку надо выбирать верный вариант. Поэтому система не прижалась – и используется RSA. Схематично жизненный цикл данной криптосистемы отображён на рисунке 2.

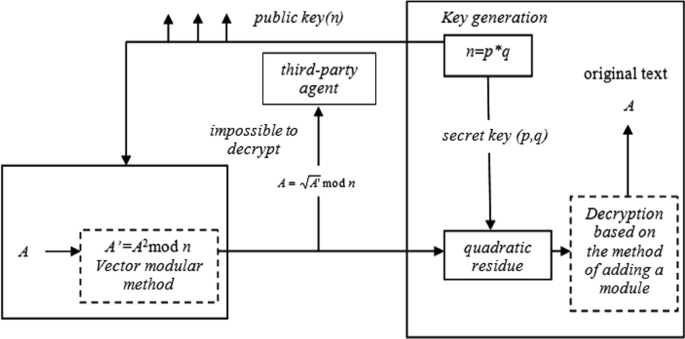


Рисунок 2 – Схематичное изображение криптосистемы Рабина

# 2 Ход выполнения работы

Программное средство написано на языке программирования C++. В файле rabin/rabin.cpp находятся, соответственно, тела функций, отвечающих за шифрование числа, файла и вспомогательные действия. В группе файлов utils находятся вспомогательные функции для ввода, вывода, работы со строками и массивами. Программа написана на современном стандарте языка C++ 17 с использованием контейнеров STL, итераторов и современного «синтаксического сахара», а также некоторых практик по именованию из Google Style Guide для написания читаемого кода.

В приложении с листингом кода предоставлена вырезка кода с функцией шифрования и дешифрования.

Реализованное программное средство имеет возможность считать файл, зашифровать или расшифровать его содержимое в режиме простой замены или гаммирования с обратной связью и сохранить преобразованный результат.

# Заключение

В ходе выполнения данной работы было произведено ознакомление с теорией об алгоритме шифрования криптосистемы Рабина, реализовано программное средство для шифрования и расшифрования текстовых файлов.

Итог заключается в том, что криптосистема Рабина не позволяет однозначно расшифровать сообщение. Она позволяет предположить 4 возможных варианта. По какому-то признаку надо выбирать верный вариант. Поэтому используется алгоритм RSA. Криптографическая система Рабина безопасна, пока p и q – большие числа. Сложность криптографической системы Рабина такая же, как и у процедуры разложения на множители больших чисел n на два простых сомножителя p и q

Цель лабораторной работы, поставленная во введении настоящего отчёта, можно считать достигнутой.

# Приложение А

(Листинг кода)

Number modulo(Number a, Number b) {

// just correct implementation for a % b --> because in algebra it differs :)

return a >= 0 ? a % b : (b - (Number) llabs(a % b)) % b;

}

Number decrypt(const Number c, const Number p, const Number q) {

const Number n{p \* q};

Number mp{mod((p + 1) / 4, c, p)}; // c^((p+1)/4)

Number mq{mod((q + 1) / 4, c, q)}; // c^((q+1)/4)

// y[p] \* p + y[q] \* q = 1

std::vector<Number> arr{extended\_euclid(p, q)};

Number rootp{arr[0] \* p \* mq};

Number rootq{arr[1] \* q \* mp};

long double r = modulo((rootp + rootq), n); // x1

if (r < 128) {

return (Number) r;

}

if (Number negative\_r = n - r; negative\_r < 128) // x2

return negative\_r;

Number s{modulo((rootp - rootq), n)}; // x3

if (s < 128)

return s;

Number negative\_s{n - s}; // x4

return negative\_s;

}