Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №3

По дисциплине «Методы защиты информации»
По теме «Асимметричная криптография. RSA»

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

Минск 2019

Введение

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Опубликованная в ноябре 1976 года статья Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» перевернула представление о криптографических системах, заложив основы криптографии с открытым ключом. Разработанный впоследствии алгоритм Диффи — Хеллмана позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Однако этот алгоритм не решал проблему аутентификации. Без дополнительных средств пользователи не могли быть уверены, с кем именно они сгенерировали общий секретный ключ.

Алгоритм

Алгоритм создания открытого и секретного ключей

1. Выбираются два различных случайных числа p и q
2. Вычисляется их произведение n = p * q
3. Вычисляется значение функции Эйлера от n

$$\varphi(n) = (p-1)\cdot(q-1).$$

4. Выбирается целое число *e,* взаимно простое со значение функции
5. Вычисляется число *d* мультипликативно обратное к числу *e*
6. Пара (*e, n*) публикуется как открытый ключ RSA
7. Пара *(d, n)* играет роль закрытого ключа RSA

Алгоритм шифрования

1. Взять открытый ключ
2. Взять открытый текст
3. Зашифровать сообщение с использованием открытого ключа

$$c = E(m) = m^e \mod n$$

Алгоритм расшифровки

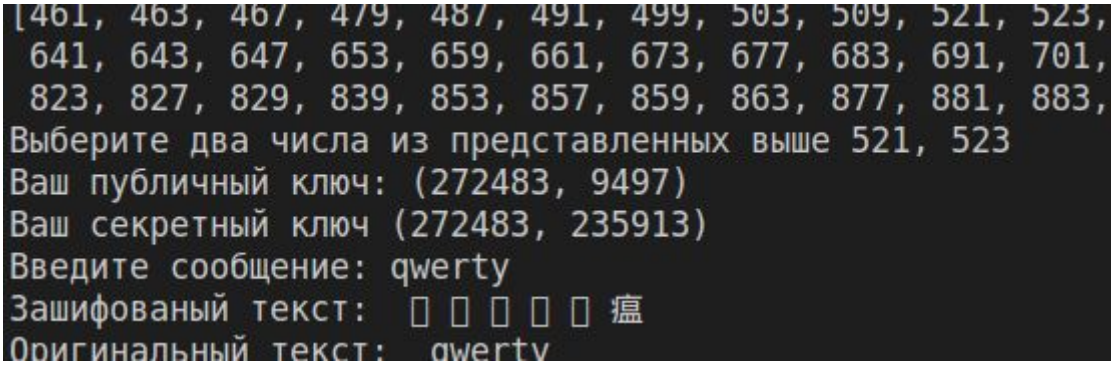
1. Принять зашифрованное сообщение
2. Взять закрытый ключ
3. Применить закрытый ключ для расшифрования сообщения

$$m = D(c) = c^d \mod n$$

Выполнение программы

Простый числа: 521, 523
Текст для кодировки: qwerty

Ход выполнения программы



Вывод

Алгоритм RSA отлично вписывается в рамки текущих лабораторных работ, т.к представляет собой простое, а главное малозатратное решение для кодирования сообщений, которое позволяет скрытно общаться с собеседником.