МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №7

Изучение асимметричных протоколов и шифров

Студент гр. 8382 Мирончик П.Д.

Преподаватель Племянников А.К.

Санкт-Петербург
2021

ВЫВОДЫ

В ходе выполнения работы были рассмотрены принципы работы ассиметричных шифров.

Рассмотрен протокол Диффи-Хеллмана, позволяющий осуществлять генерацию секретного ключа на двух сторонах без передачи непосредственно ключа между сторонами, проведена пробная генерация ключей и их использование для зашифрования и расшифрования сообщения.

Далее был рассмотрен шифр RSA. Сгенерированы ключи небольшой длины, с помощью которых было зашифровано и расшифровано сообщение, что позволило проверить корректность работы алгоритма. Исследована также скорость работы алгоритма при зашифровании и расшифровании текста длиной примерно 1000 символов на ключах разной длины. Выяснено, что зашифрование выполняется немного быстрее, чем расшифрование, что связано, скорее всего, исключительно с подобранными значениями ключей. Также определено, что длительность зашифрования и расшифрования напрямую зависит от длины ключа.

Проведена атака грубой силы на шифр RSA при помощи коллеги. Для этого были сгенерированы ключи небольшой длины так, что модуль $n = pq > 256$. Коллеге были переданы открытые данные $e = 12333$ и значение модуля. По этим данным была выполнена факторизация модуля и найден закрытый ключ d, с использованием которого удалось расшифровать сообщение.

В конце была изучена гибридная криптосистема. Рассмотрен принцип ее работы, а также проведения атак на такую систему с использованием CrypTool 1.