**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №7**

**по дисциплине «Криптография и защита информации»**

Тема: **Изучение асимметричных протоколов и шифров**

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**Выводы**

* Изучен протокол Диффи-Хеллмана.

Данный протокол позволяет паре пользователей выработать секретный ключ, не обмениваясь секретными данными по небезопасному каналу связи. Математическая модель протокола: общедоступная пара чисел – первое — это большое простое число (более 300 десятичных цифр), второе — генератор (первообразный корень по модулю ), а также числа , известные только отправителям. Сгенерированный секретный ключ использовался для шифрования текста. Результат расшифровки совпал с исходным текстом.

* Изучен шифр RSA

Это ассиметричный блочный шифр. Параметрами шифра являются два больших простых числа , которые нужно уничтожить после вычисления пары закрытого и открытого ключей. Первый участник генерирует два ключа и передает открытый ключ () своему коллеге, ключ используется при зашифровке сообщений. Далее он же использует закрытый ключ для расшифровки.

* Исследовано время шифрования и расшифрования в зависимости от длины ключа.

Выполнение этих операций занимает мало времени. Время зашифровки во всех случаях составило 0 секунд, время расшифровки увеличивалось с ростом длины ключа. Для 512 битного ключа время составило 0.004 секунд, а для 2048 битного ключа – 0.049.

* Изучена атака грубой силы на шифр RSA.

При проведении атаки грубой силой был факторизован модуль, что привело к успешной атаке. Полученный результат был использован для расшифровки сообщения, полученного от коллеги. Результат расшифровки совпал с исходным текстом.

* Проведена атака на гибридную криптосистему.

Данная атака позволяет определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы. Нарушитель может перехватывать и модифицировать сообщения, адресованные серверу, сервер не определяет, от кого был получен конверт, нарушитель может классифицировать ответы сервера как случаи успешной и неуспешной расшифровки.