|  |
| --- |
|  |

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Институт электроники и светотехники

Кафедра информационной безопасности и сервиса

ЛАБОРАТОРНАЯ РАБОТА №4

по теме:

«Электронная цифровая подпись»

Автор отчёта о лабораторной работе  А. Е. Конышев

подпись, дата

Обозначение лабораторной работы ЛР–02069964–02.03.02–08–23

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Проверил работу

канд. техн. наук, доц.  И. П. Карьгин

подпись, дата

Саранск 2023

**Протокол на базе алгоритма RSA**

Этап 1. Отправитель генерирует открытый и закрытый ключи на базе алгоритма RSA.

Этап 2. Отправка сообщения и электронной подписи. Производится отправителем в 3 действия:

1. Вычисление хэш-образа текста сообщения (можно воспользоваться функцией квадратичной свертки);
2. Выработка электронной подписи , полученной по формуле , где - закрытый ключ отправителя, - часть открытого ключа;
3. Отправка получателю текста сообщения и цифровой подписи.

Этап 3. Получение сообщения и проверка электронной подписи. Производится получателем в три действия:

1. Вычисление хэш образа полученного текста (требуется воспользоваться тем же методом, что и отправитель);
2. Вычисление хэш образа из электронной подписи , полученного по формуле , где – открытый ключ отправителя.
3. Сравнение и . Если они равны, то получатель делает вывод, что сообщение действительно отправлено отправителем.

Протоколы ЭЦП позволяют убедиться, что сообщение отправлено от достоверного отправителя, а также гарантируют, что сообщение пришло в неизменном виде. Но она не позволяет идентифицировать отправителя. От нее этого и не требуется.

Генерация ключей алгоритмом RSA:

1. Выбираются два различных простых числа и .
2. Вычисляется их произведение , называемое модулем.
3. Вычисляется значение функции Эйлера для . Из свойства этого числа, как произведения 2х простых следует, что .
4. Выбирается число , называемое открытой экспонентой, взаимно простое с .
5. Вычисляется число , называемое секретной экспонентой, мультипликативно обратное к числу по модулю .
6. Пара публикуется в качестве открытого ключа.
7. Пара или только играет роль секретного ключа.

