**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский Авиационный Институт»**

**(Национальный Исследовательский Университет)**

**Институт: №8 «Информационные технологии   
и прикладная математика»   
Кафедра: 806 «Вычислительная математика   
и программирование»**

Лабораторная работа № 1   
по курсу «Криптография»

Группа: М8О-312Б-22

Студент: Куценко М.Д.

Преподаватель: А. В. Борисов

Оценка:

Дата: 07.03.2025

Москва, 2025

ОГЛАВЛЕНИЕ

[1 Тема 3](#__RefHeading___Toc272_1095258672)

[2 Задание 3](#__RefHeading___Toc274_1095258672)

[3 Теория 4](#__RefHeading___Toc276_1095258672)

[4 Ход лабораторной работы 5](#__RefHeading___Toc278_1095258672)

[5 Выводы 6](#__RefHeading___Toc280_1095258672)

[6 Список используемой литературы 7](#__RefHeading___Toc282_1095258672)

# **Тема**

Асимметричное шифрование, основанное на использовании пары ключей.

# **Задание**

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью почтового клиента thunderbird, или из командной строки терминала ОС семейства linux, или иным способом.

2. Установить связь с преподавателем, используя созданный ключ, следующим образом:

2.1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.

2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

2.3. Выслать сообщение, зашифрованное на открытом ключе собеседника.

2.4. Дождаться ответного письма.

2.5. Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа:

3.0. Получить сертификат открытого ключа одногруппника.

3.1. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

3.2. Подписать сертификат открытого ключа одногруппника.

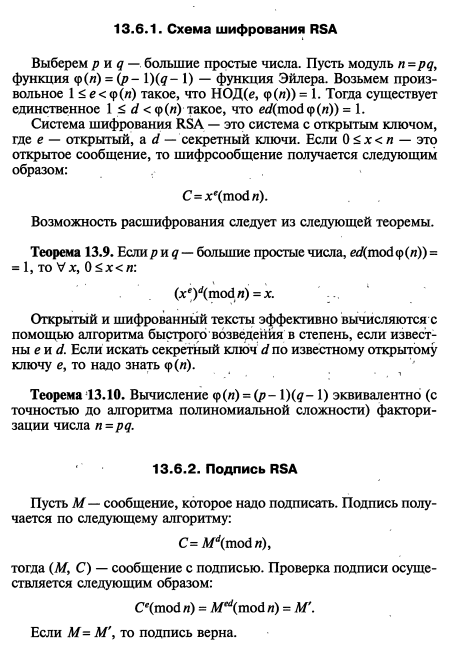
3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.

3.4. Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.

3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

# **Теория**



# **Ход лабораторной работы**

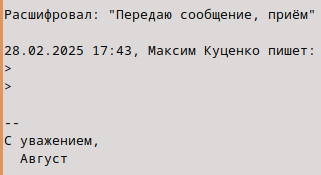
При помощи gpg —full-gen-key создал личные публичный и приватный ключи.

При помощи gpg -a —export экспортировал ключи для отправки другим пользователям.

При помощи gpg —import импортировал ключи других пользователей.

При помощи gpg —encrypt —recipient зашифровал сообщение для отправки другому пользователю.

При помощи gpg —decrypt расшифровал сообщение от другого пользователя.

При помощи gpg —fingerprint сверил отпечатки ключей других пользователей.

При помощи gpg —sign-key подписал ключи других пользователей.

# **Выводы**

Изучил, как пользоваться публичным и приватным ключами для обмена ключами и информацией с другими пользователями в защищённом виде. Публичный ключ используется для шифрования информации, а приватный — для её расшифровки, что позволяет защитить данные от несанкционированного доступа.

Применил данный навык на практике при выполнении данной лабораторной работы.

# **Список используемой литературы**

1. Применко Э.А. Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «ЛИБРОКОМ», 2013. — 288 с.
2. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. Заведений. — М.: Издательский центр «Академия», 2009. — 272 с.