Московский Авиационный Институт

(Национальный Исследовательский Университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

**Лабораторная работа №1 по курсу**

**«Криптография»**

Студент: Почечура Артемий Андреевич

Группа: М80-306Б-20

Преподаватель: Борисов Август Валерьевич

Дата: 14.02.2023

Оценка:

Подпись: \_\_\_\_\_\_\_\_\_\_\_

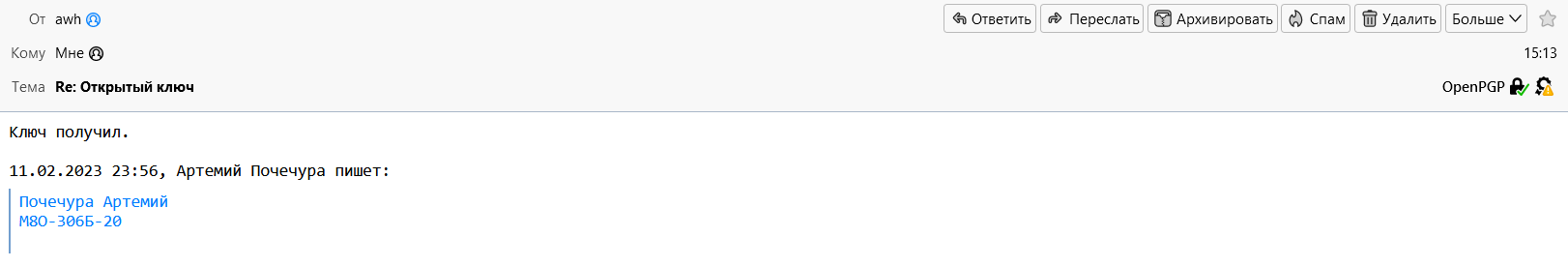
Москва, 2023

**1. Создание пары Open-PGP-ключей**

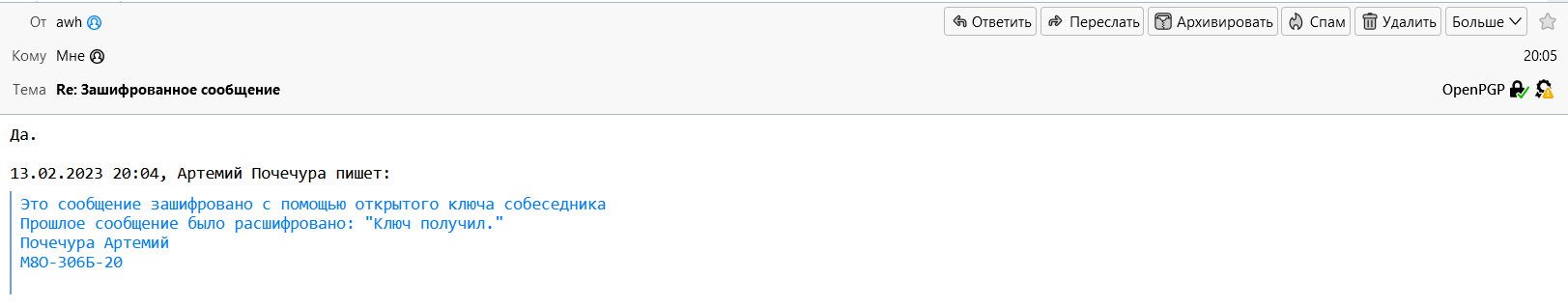
Создание открытого и секретного ключа для почтового ящика производилось с помощью программы Thunderbird.

**2. Установление связи с преподавателем, используя созданный ключ**

В начале преподавателю был отправлен открытый ключ, в ответ на который было отправлено сообщение, зашифрованное с помощь этого ключа:



Затем, используя открытый ключ преподавателя, я отправил зашифрованное письмо, на которое также получил зашифрованный ответ (на скриншоте он уже расшифрован с помощью моего секретного ключа):



**3. Сбор подписей однокурсников под своим сертификатом открытого ключа**

Вся суть заключалась в обмене с однокурсниками открытыми ключами и подписании их цифровой подписью. Я осуществлял это с помощью инструмента gpg в операционной системе Unix. Сначала я добавлял новый ключ с помощью команды gpg --import. Затем, благодаря команде gpg --list-sigs, узнавал нужный номер ключа, чтобы с помощью gpg --sign-key поставить печать на этот ключ. Потом, используя команду gpg -a -o --export, создавал файл ключа, на котором уже теперь имеется моя подпись, после чего отправлял подписанный ключ однокурснику. Подписанный мой ключ однокурсником я также добавлял с помощью команды gpg –import, чтобы его подпись перенеслась на ключ в системе.

**4. Вывод**

В процессе работы над данной лабораторной работой, я ознакомился с такой технологией шифрования сообщений, как Open-PGP ключи. Мною впервые была создана пара таких ключей для своей электронной почты, опробованы функции зашифровки и расшифровки сообщений, подписаны открытые ключи других пользователей цифровой подписью. Изучать принцип работы Open-PGP ключей, а также учиться взаимодействовать при помощи них с другими пользователями было очень интересно и полезно. Также в ходе работы с Thunderbird очень понравилось то, как просто и удобно реализованы функции зашифровки и расшифровки сообщений в данной программе.