

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники

Лабораторная работа №3
по дисциплине: «Методы и средства защиты информации»

«Изучение стандартных средств криптографической аутентификации –
электронной цифровой подписи»

Факультет: АВТ

Группа: АВТ-922

Студенты: Николаев Е.
Рожков А.

Преподаватель: Вихман В.В.

Новосибирск, 2013

Цель работы

Изучить возможности и уяснить порядок работы с программой электронной цифровой подписи PGP.

Ход работы

Для работы с ЭЦП используем программу *gpg4win* с менеджером сертификатов *Kleopatra*.

Создание сертификатов

Перед началом переписки каждый из участников создаёт свой сертификат. На рисунках показан процесс создания подписи отправителем.

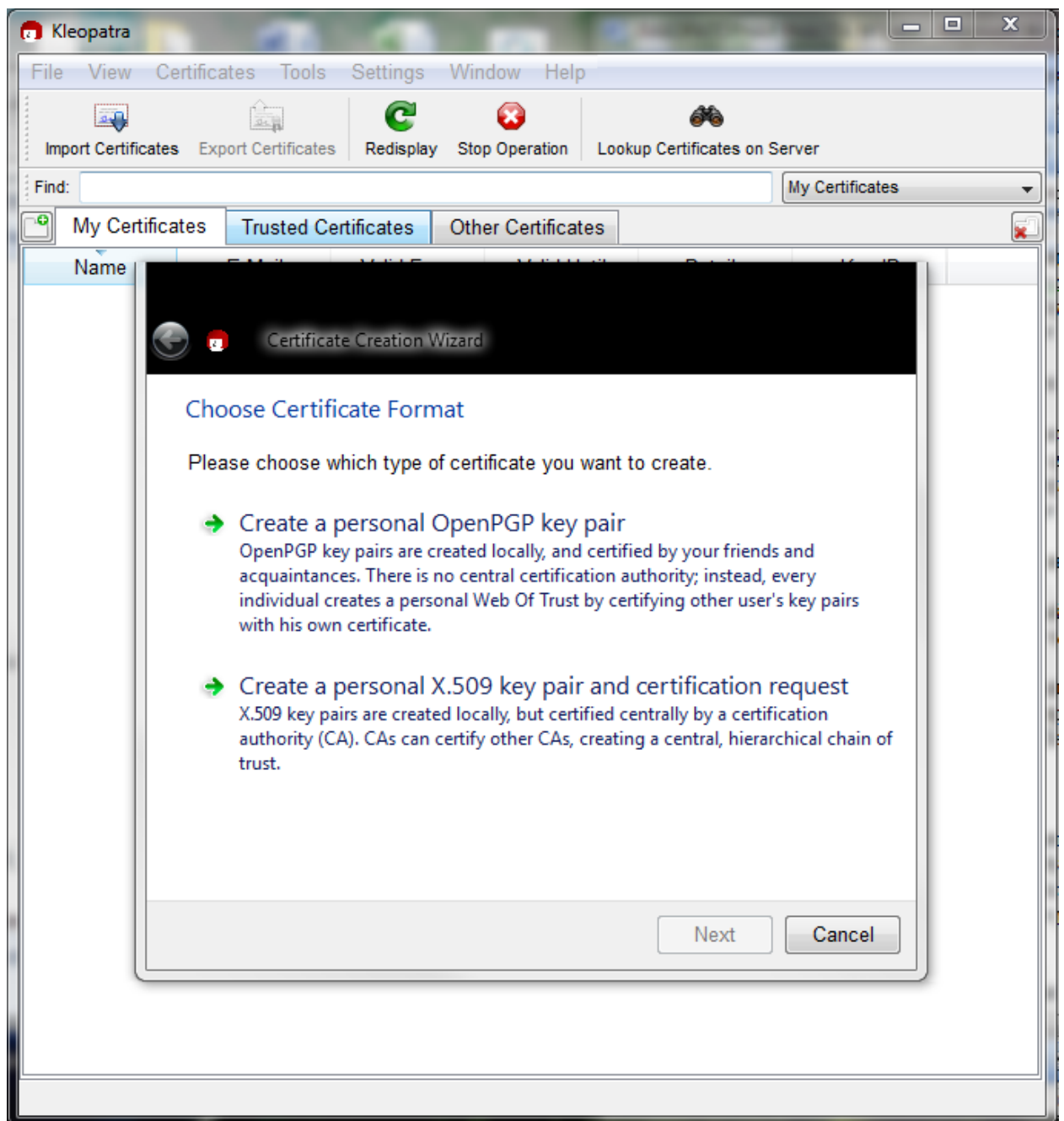
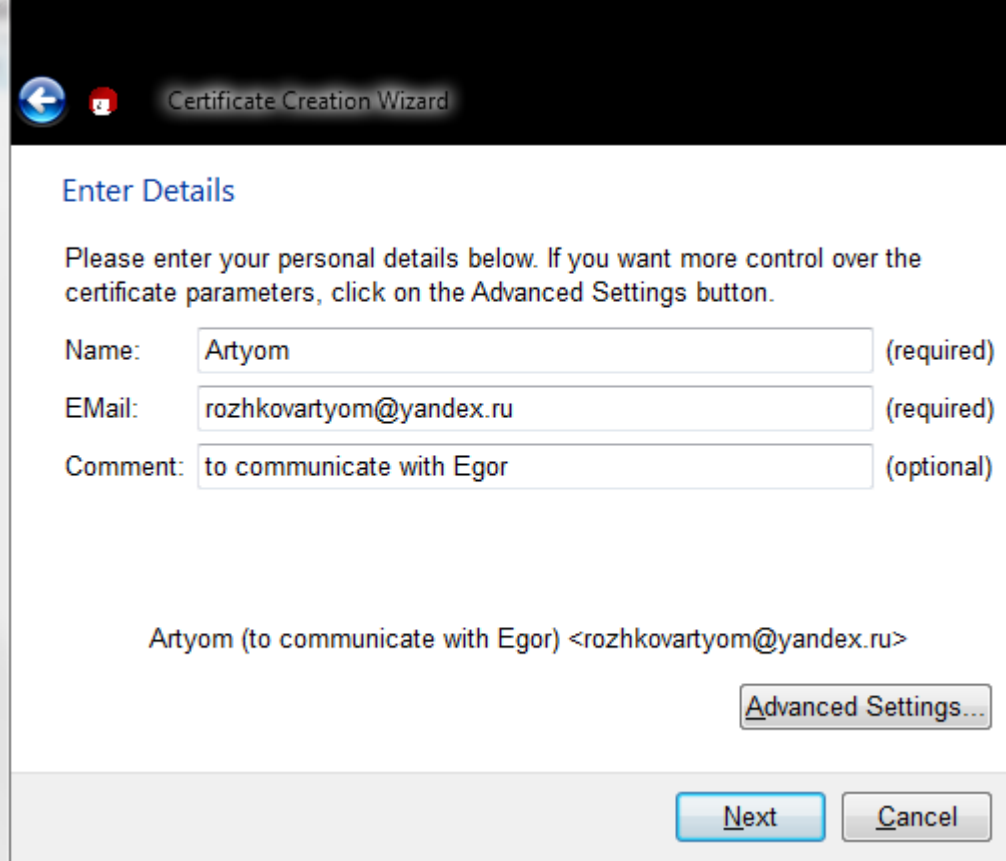


Рисунок 1. Создание сертификата (OpenPGP)



The screenshot shows the 'Enter Details' step of the Certificate Creation Wizard. The window has a dark header with a back arrow icon, a red icon, and the title 'Certificate Creation Wizard'. The main area is white with the heading 'Enter Details' in blue. Below the heading is a paragraph: 'Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.' There are three input fields: 'Name' with the value 'Artyom' (marked '(required)'), 'EMail' with the value 'rozhkovartyom@yandex.ru' (marked '(required)'), and 'Comment' with the value 'to communicate with Egor' (marked '(optional)'). Below these fields, the text 'Artyom (to communicate with Egor) <rozhkovartyom@yandex.ru>' is displayed. To the right of this text is a button labeled 'Advanced Settings...'. At the bottom right are two buttons: 'Next' and 'Cancel'.

← Certificate Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

Name: Artyom (required)

EMail: rozhkovartyom@yandex.ru (required)

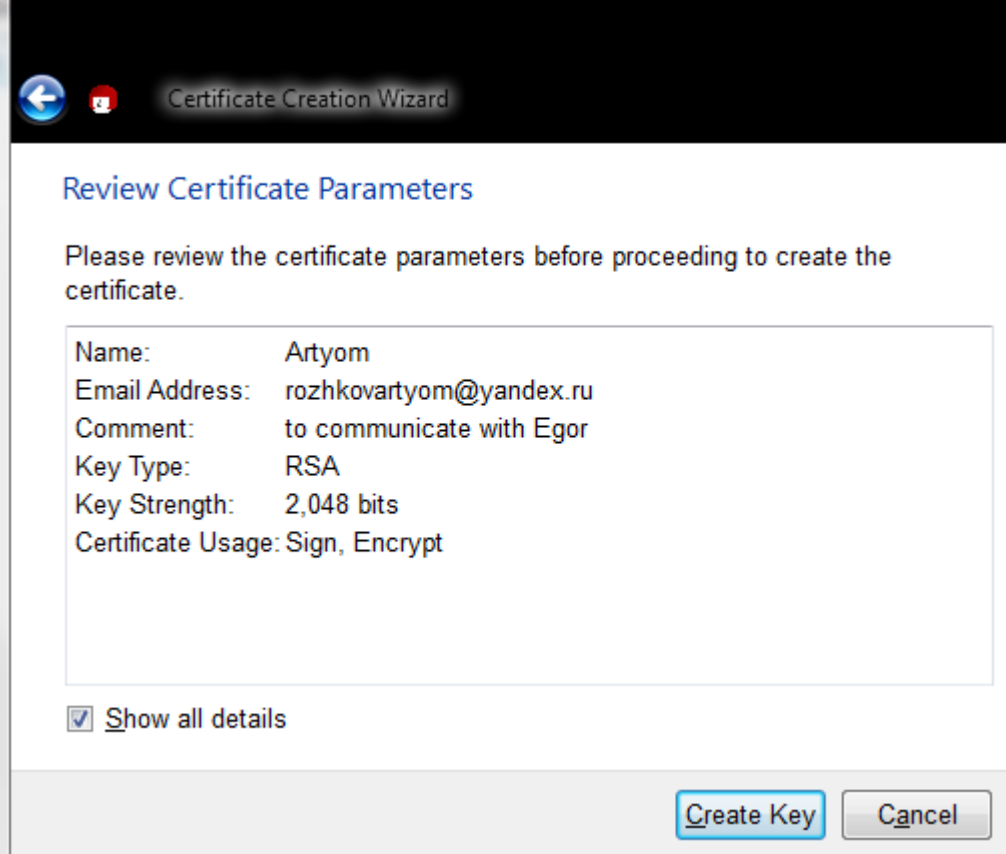
Comment: to communicate with Egor (optional)

Artyom (to communicate with Egor) <rozhkovartyom@yandex.ru>

Advanced Settings...

Next Cancel

Рисунок 2. Ввод персональных данных отправителя



The screenshot shows the 'Review Certificate Parameters' step of the Certificate Creation Wizard. The window has a dark header with a back arrow icon, a red icon, and the title 'Certificate Creation Wizard'. The main area is white with the heading 'Review Certificate Parameters' in blue. Below the heading is a paragraph: 'Please review the certificate parameters before proceeding to create the certificate.' There is a box containing the following details: Name: Artyom, Email Address: rozhkovartyom@yandex.ru, Comment: to communicate with Egor, Key Type: RSA, Key Strength: 2,048 bits, and Certificate Usage: Sign, Encrypt. Below this box is a checkbox labeled 'Show all details' which is checked. At the bottom right are two buttons: 'Create Key' and 'Cancel'.

← Certificate Creation Wizard

Review Certificate Parameters

Please review the certificate parameters before proceeding to create the certificate.

Name: Artyom

Email Address: rozhkovartyom@yandex.ru

Comment: to communicate with Egor

Key Type: RSA

Key Strength: 2,048 bits

Certificate Usage: Sign, Encrypt

☒ Show all details

Create Key Cancel

Рисунок 3. Обзор параметров сертификата

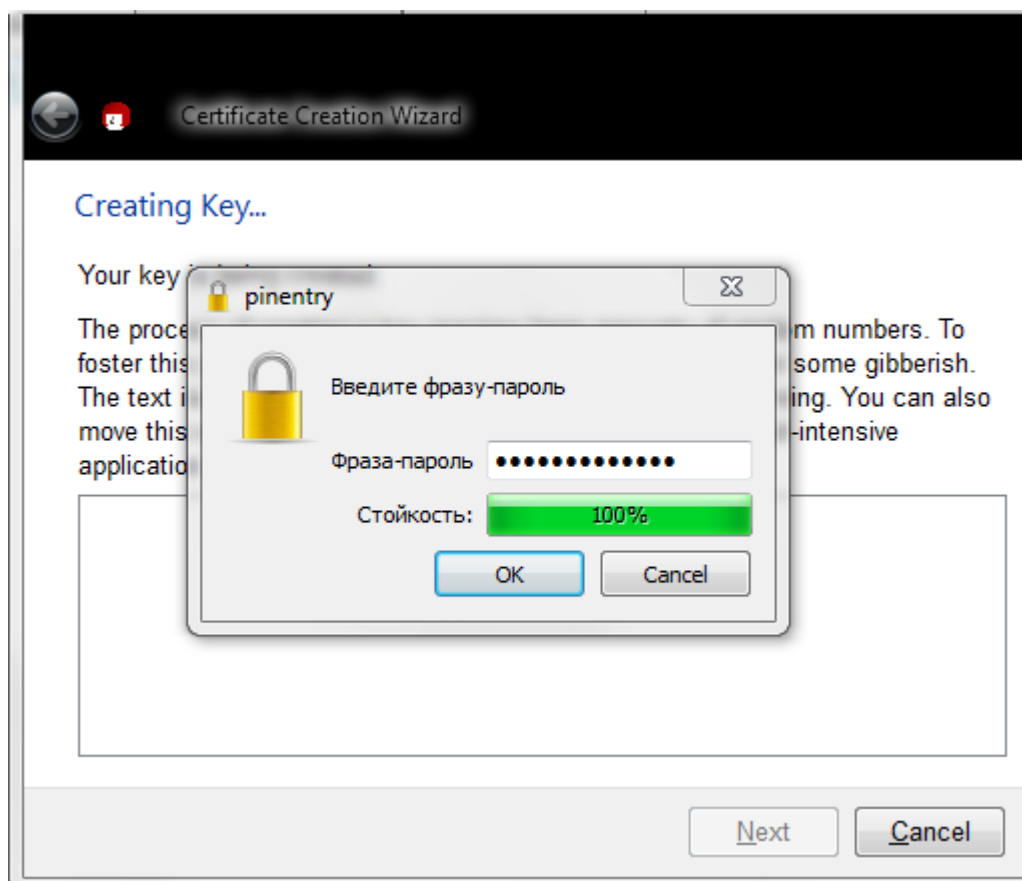


Рисунок 4. Ввод пароля, необходимого при создании ЭЦП отправителем либо дешифрации шифрованных посланий получателем

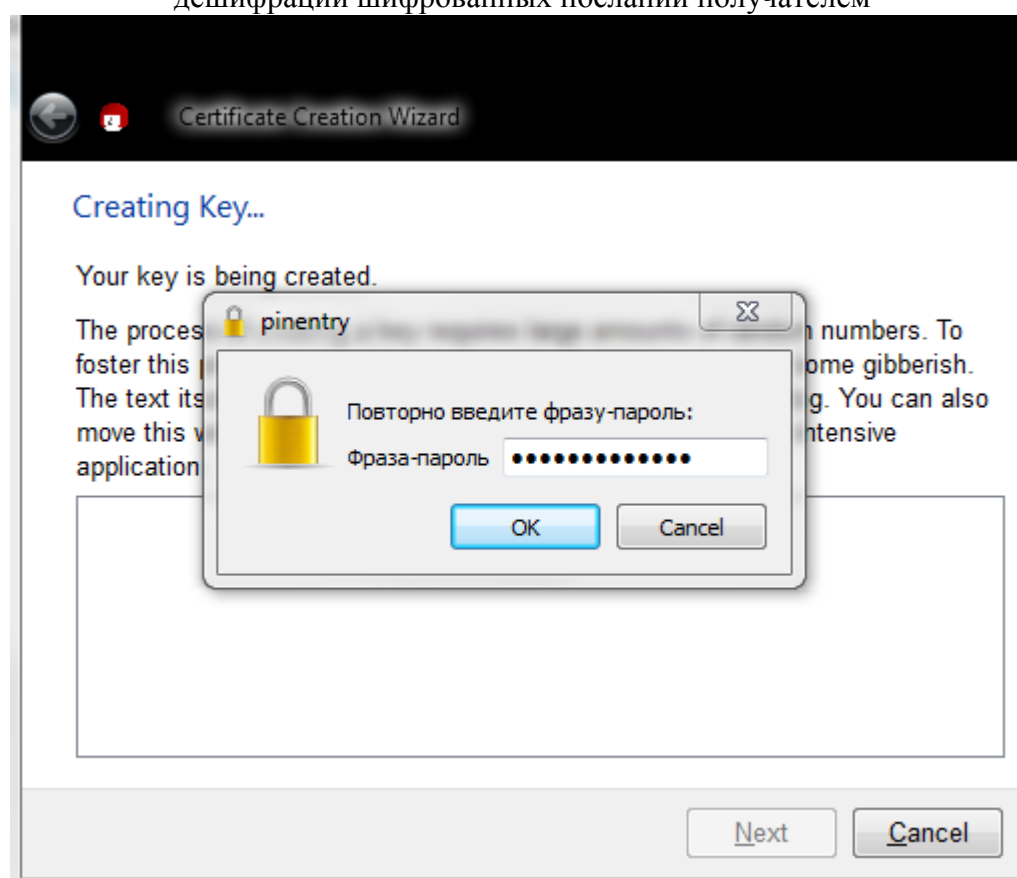


Рисунок 5. Подтверждение пароля, необходимого при создании ЭЦП отправителем либо дешифрации шифрованных посланий получателем

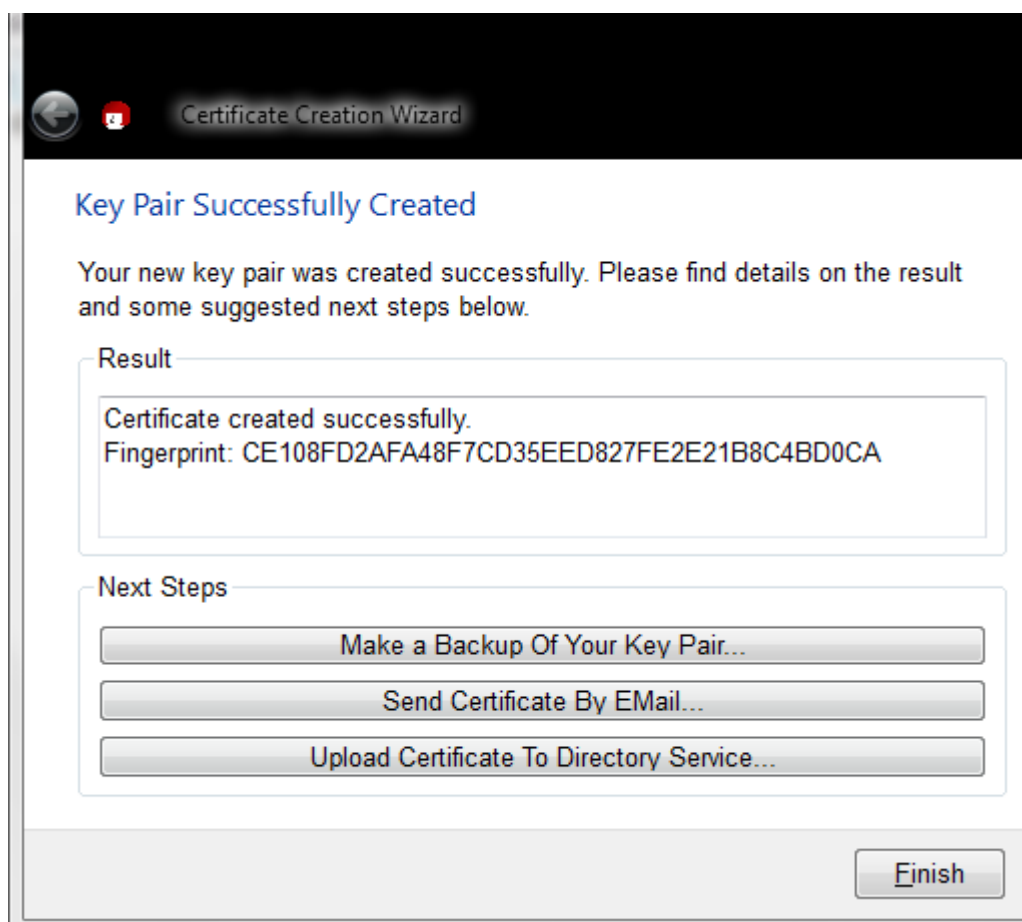


Рисунок 6. Сертификат создан

Обмен сертификатами и их сертификация

Чтобы получатель мог дешифровать сообщение отправителя, он должен сначала передать отправителю свой сертификат.

Поскольку выбран сертификат OpenPGP, его сертификация на стороннем сервере не производится. Участникам взаимодействия рекомендуется подтвердить подлинность сертификатов друг друга после обмена ими (создать «сеть доверия»).

В данном случае получатель и отправитель сверили первые символы в названии сертификата отправителя по телефонной связи и убедились в том, что они одинаковы. Таким образом, оба получили подтверждение того, что сертификат не подменён при передаче через почтовый сервер.

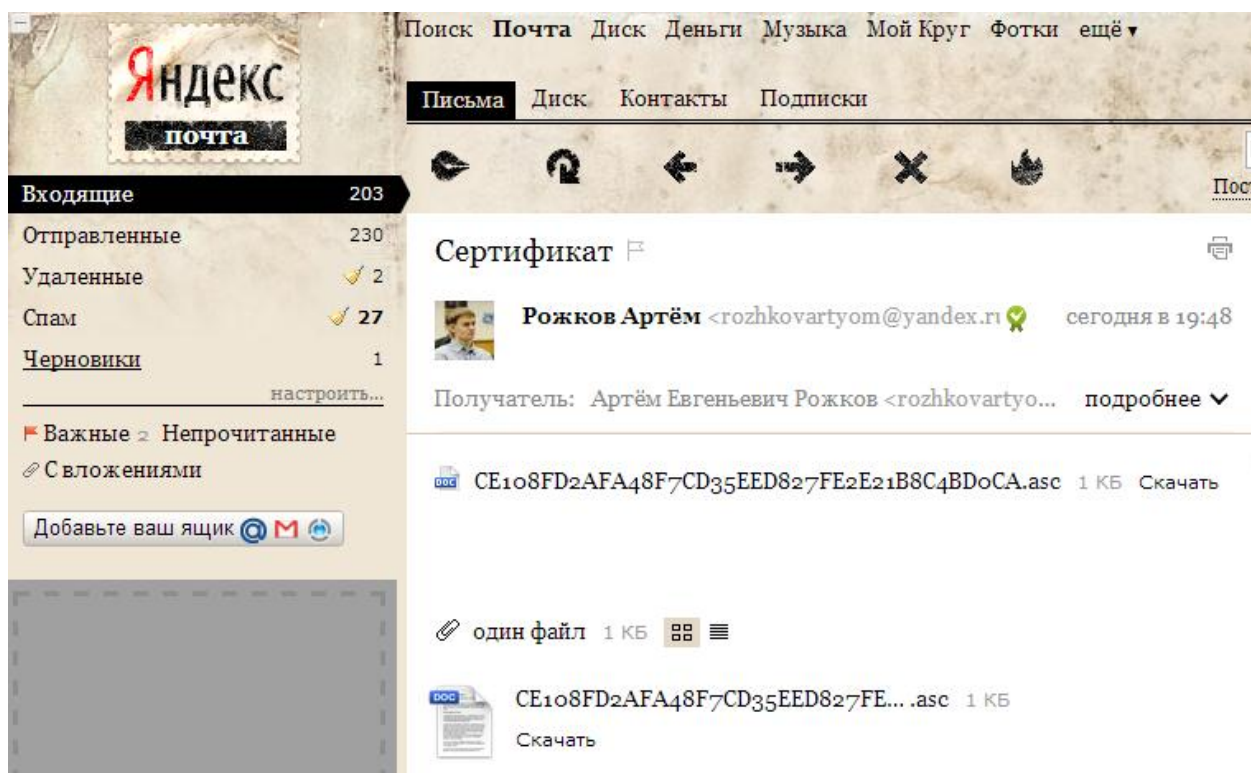


Рисунок 7. Сертификат передан получателю отправителем по электронной почте

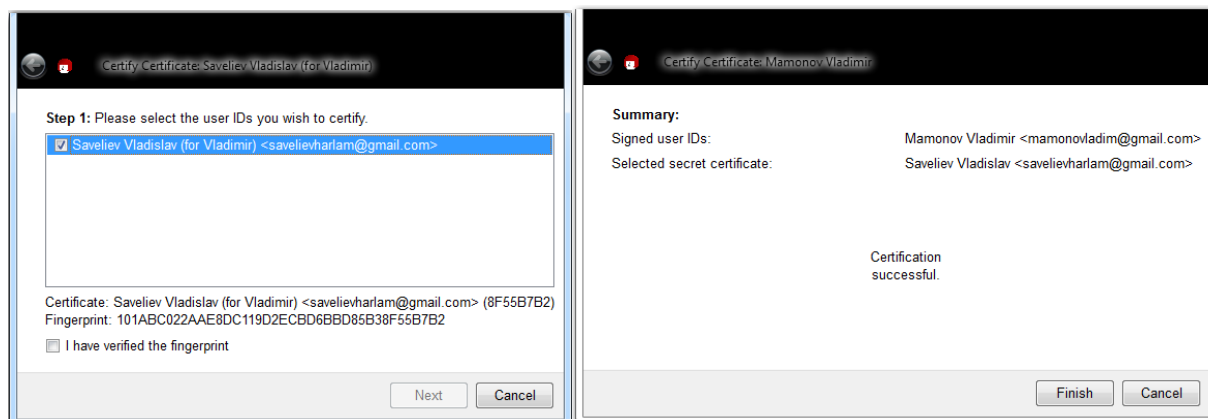


Рисунок 8. Получатель подтверждает подлинность сертификата отправителя своим сертификатом

Подписание документа

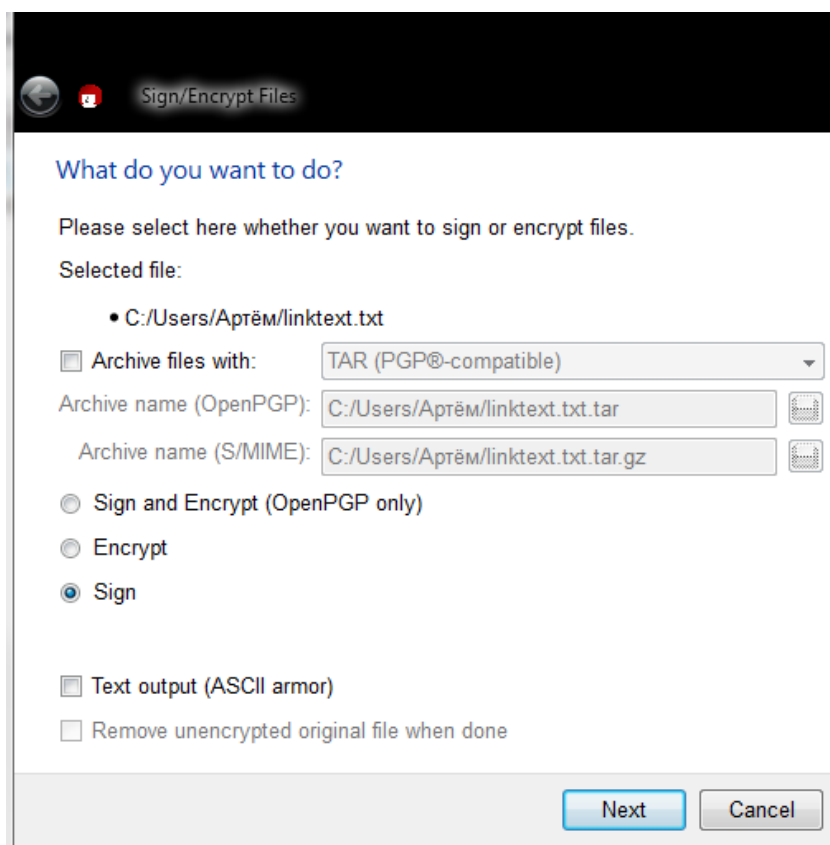


Рисунок 9. Отправитель начинает создание файла подписи для документа linktext.txt

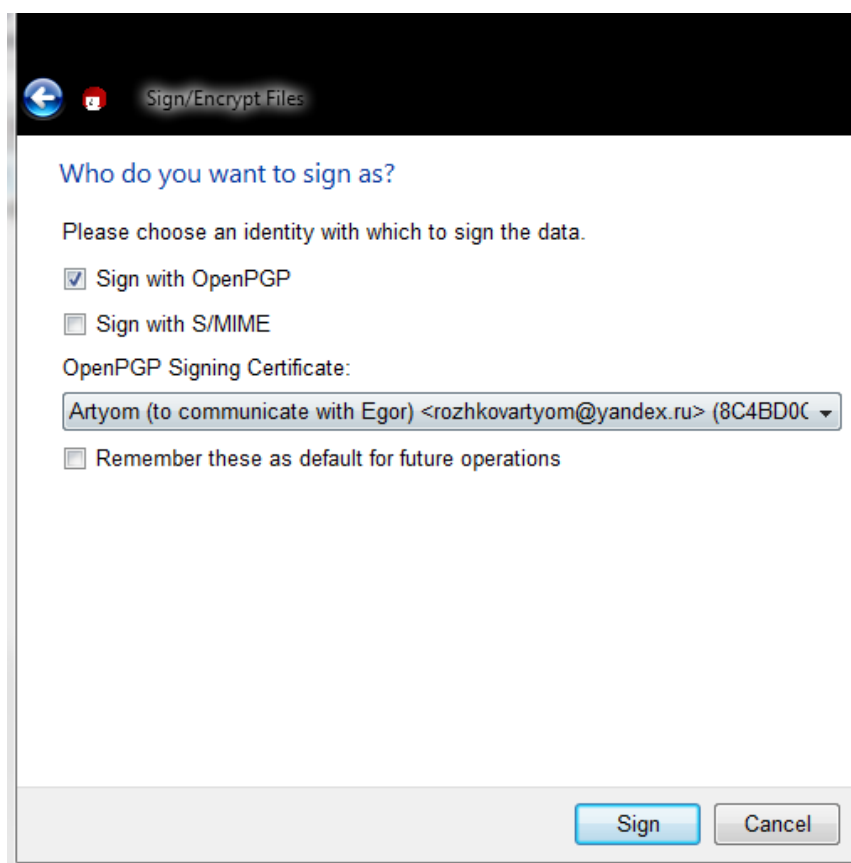


Рисунок 10. Для подписи отправитель применяет свой сертификат

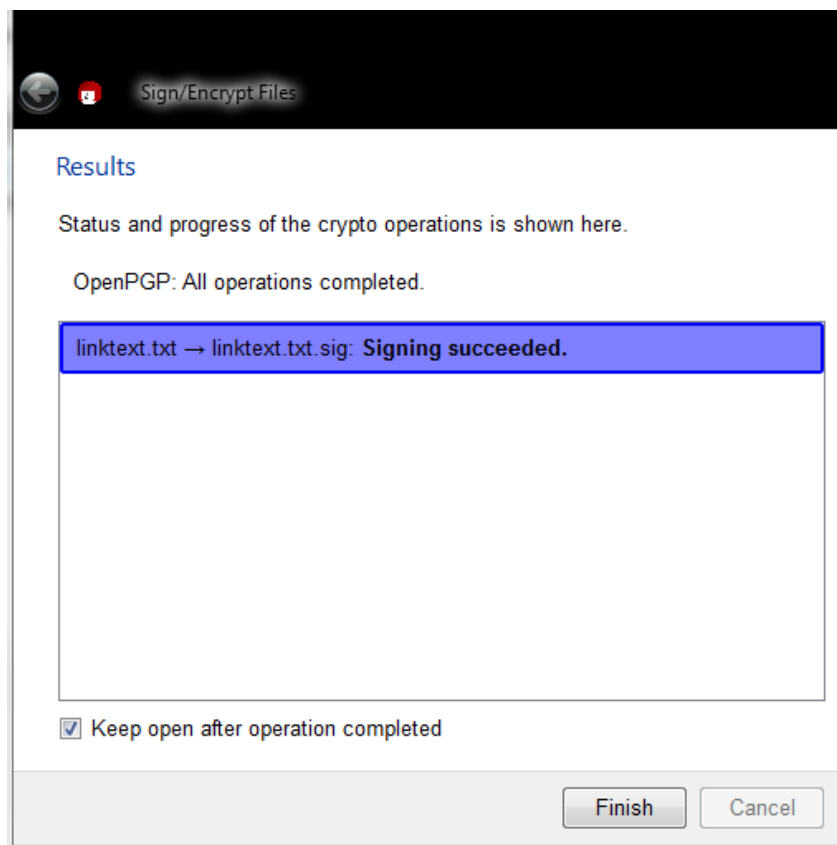


Рисунок 11. В директории исходного документа успешно создан файл подписи

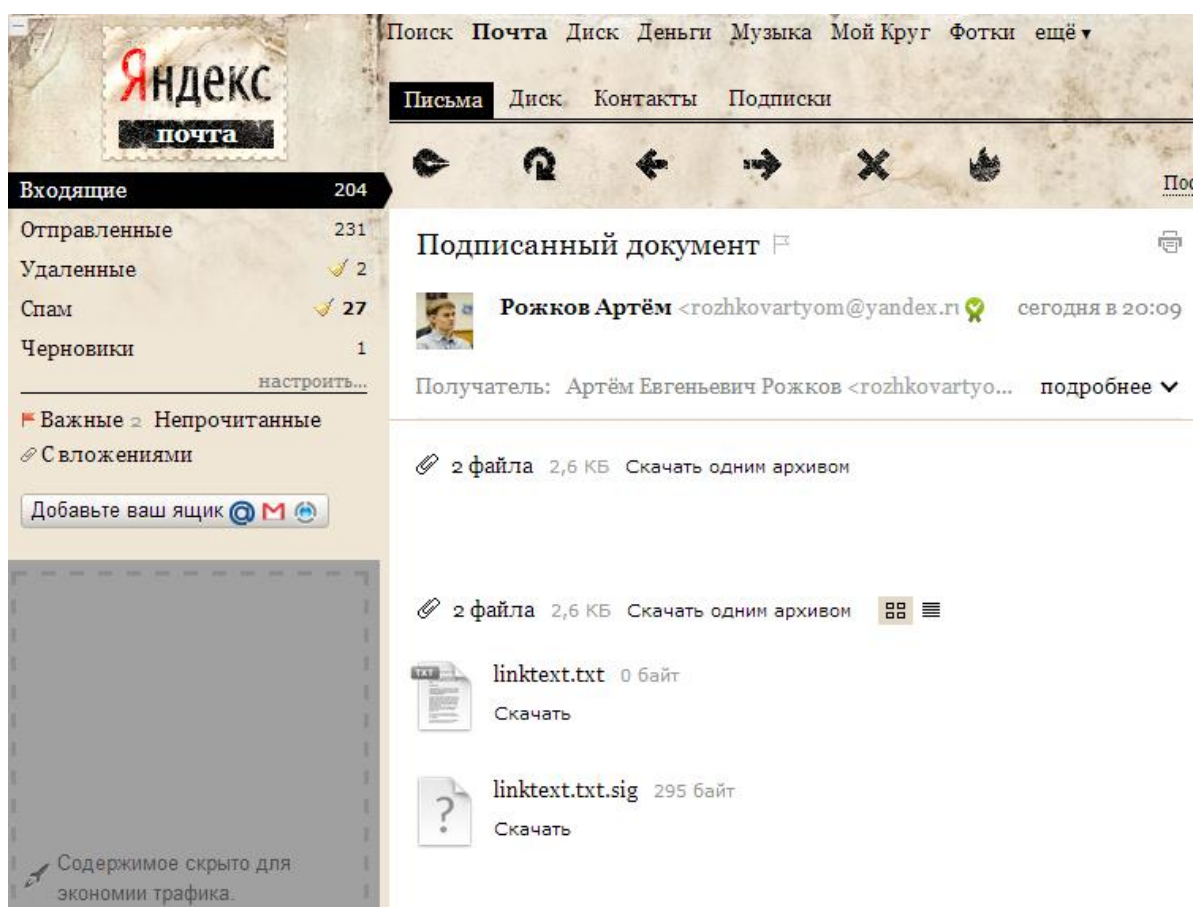
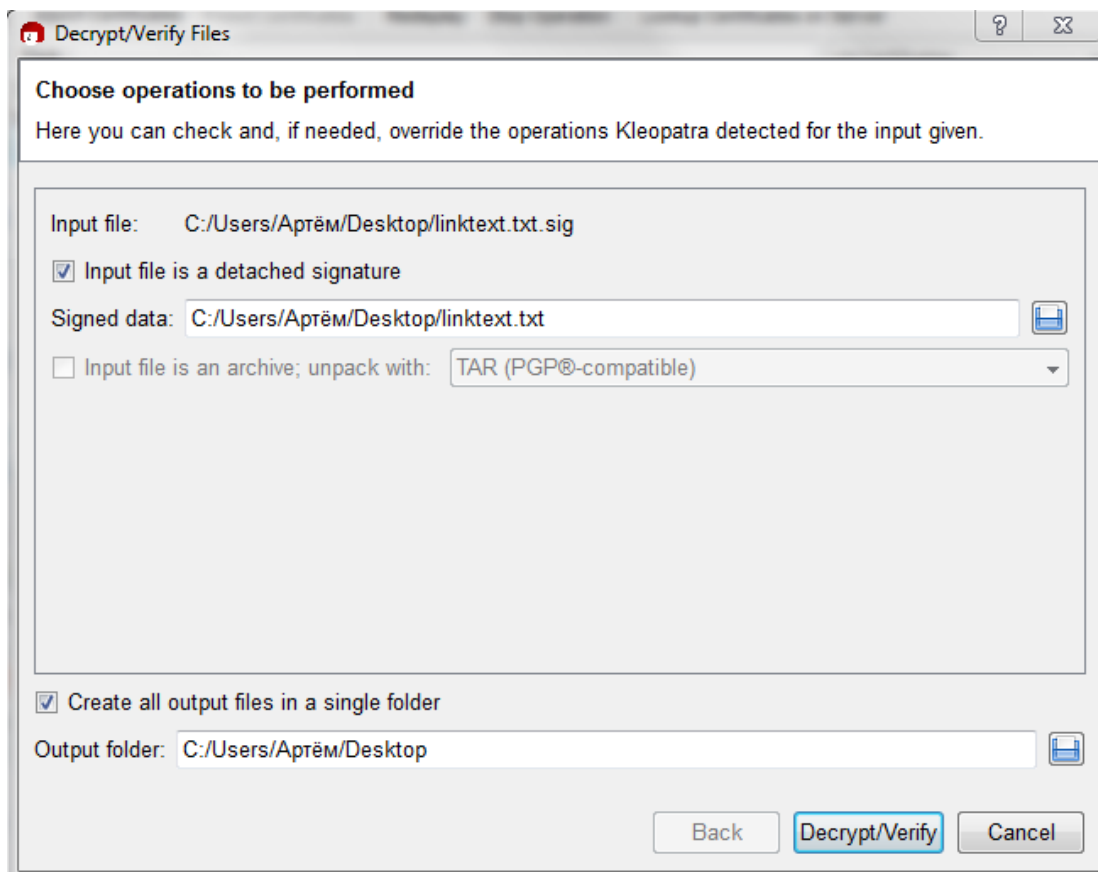
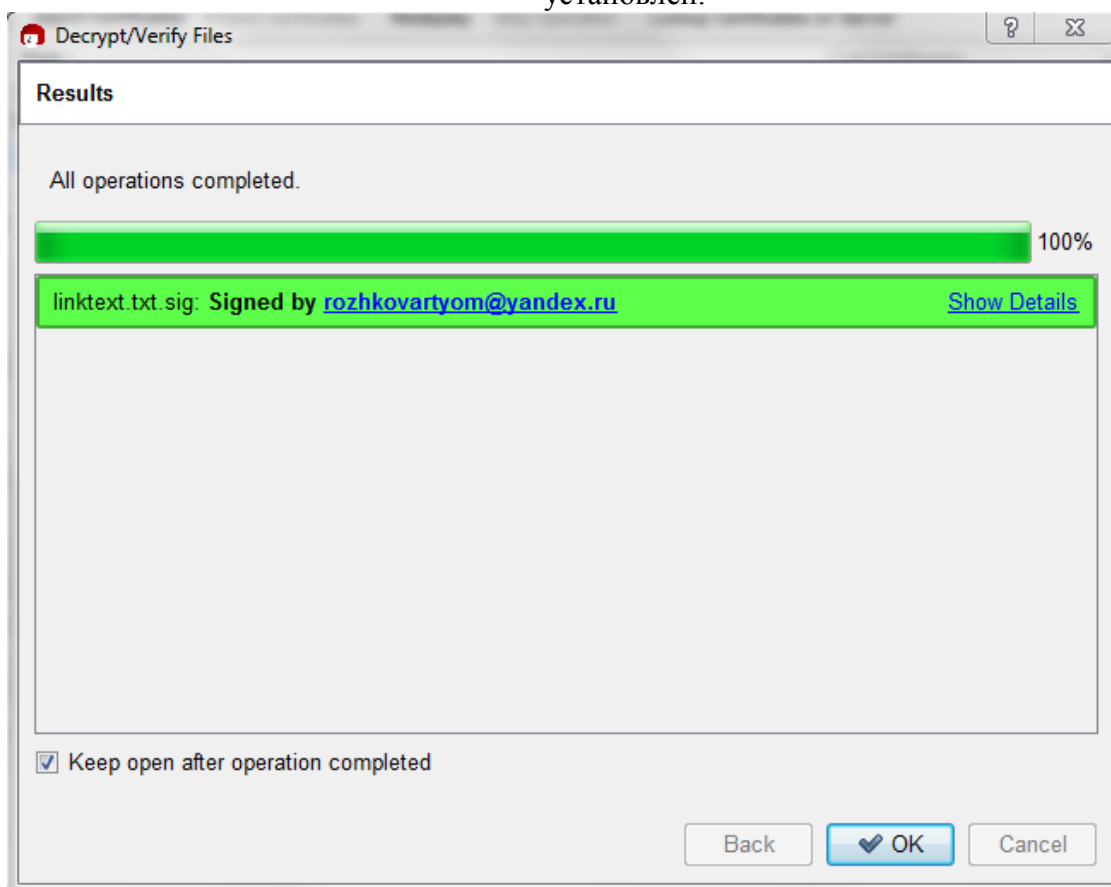


Рисунок 12. Отправка документа и его ЭЦП получателю через электронную почту



13. Результат проверки подписи получателем – подпись достоверна, отправитель установлен.



14. Результат проверки подписи получателем – подпись достоверна, отправитель установлен.

Следующий рисунок показывает, что правка документа злоумышленником «уничтожает» подпись (делает её недостоверной), таким образом подделать авторство документа практически невозможно.

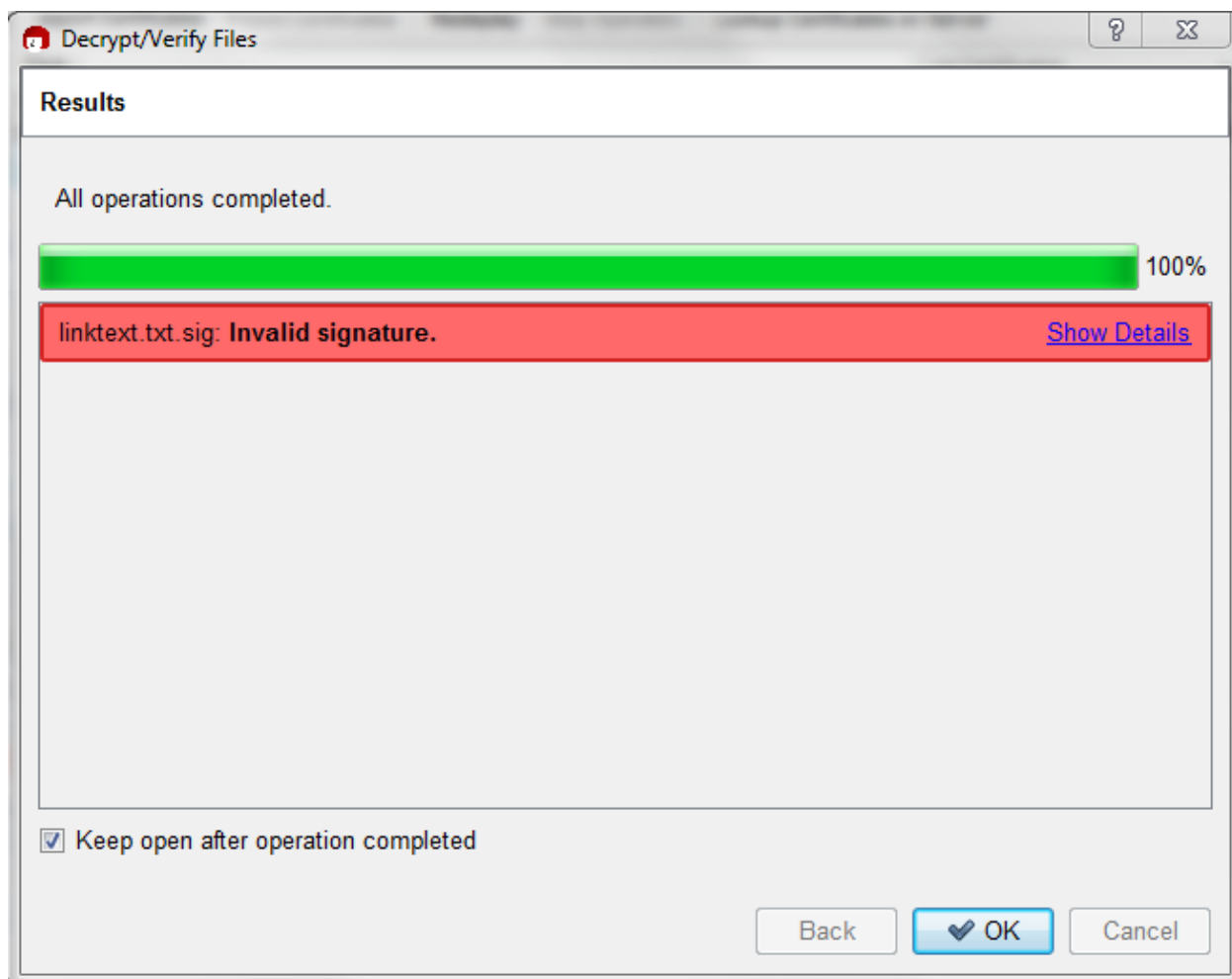


Рисунок 15. Результат проверки подписи после правки исходного документа

Шифрование документа

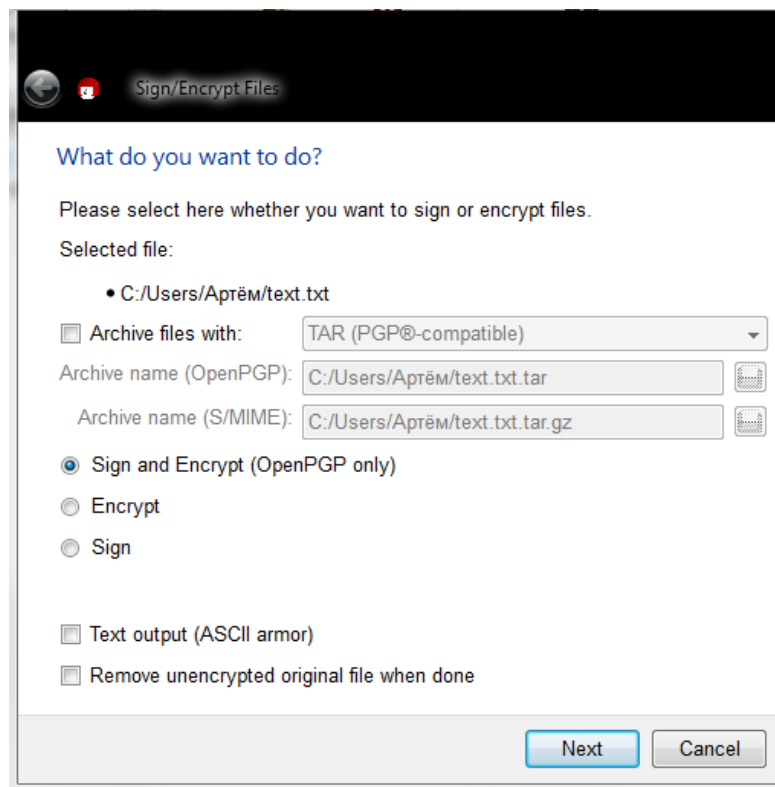


Рисунок 16. Отправитель шифрует некоторый файл, помимо этого подписывает

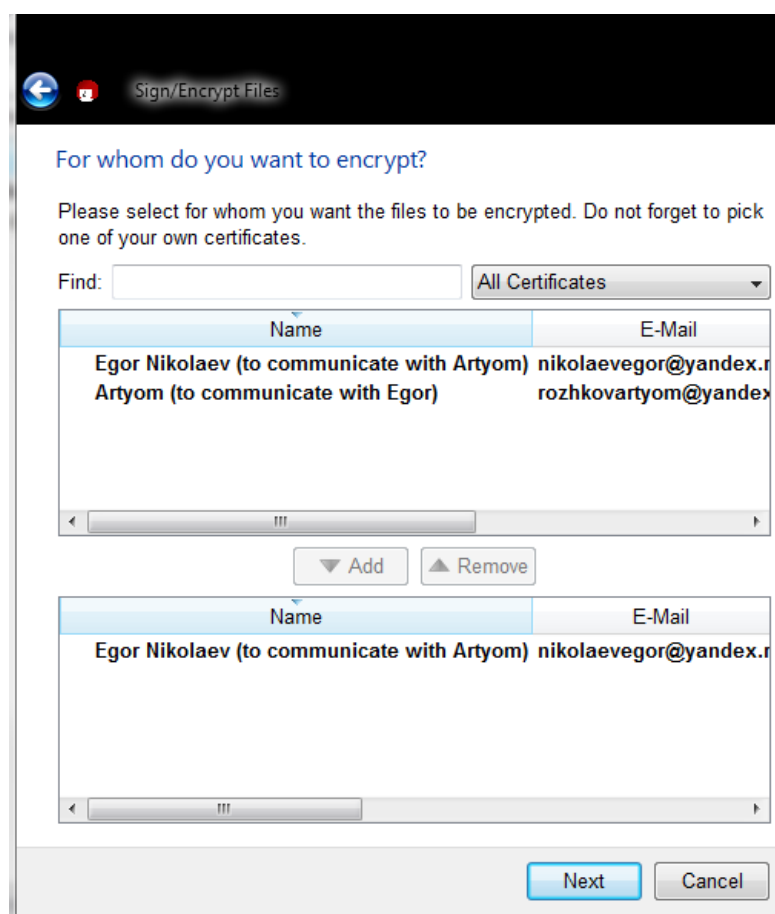


Рисунок 17. Указываются сертификаты, создатели которых могут дешифровать создаваемый файл

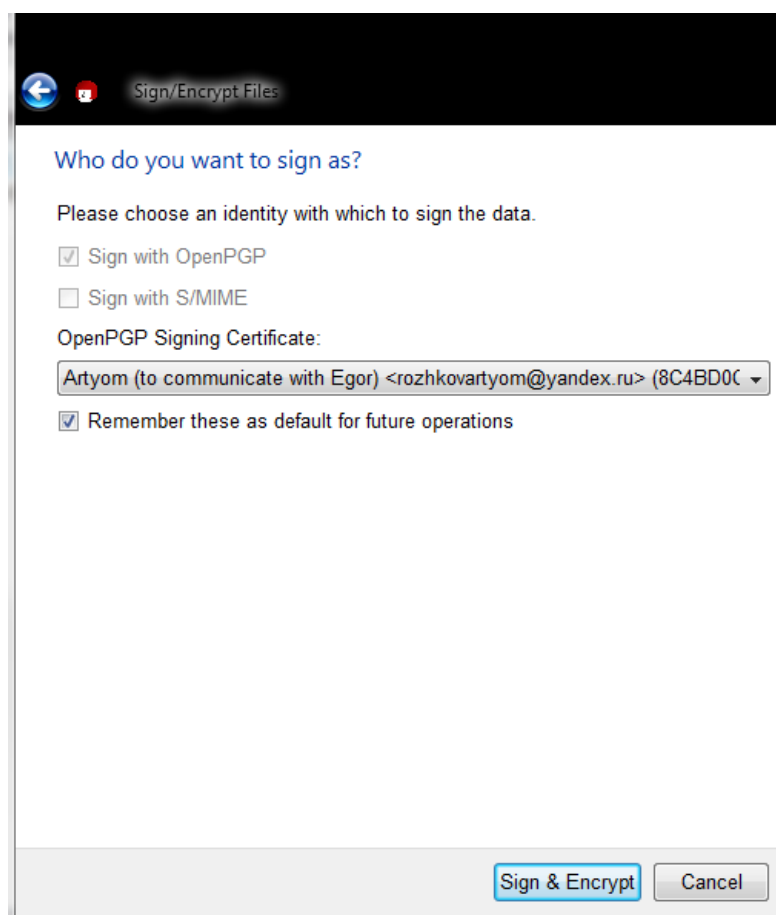


Рисунок 18. Отправитель подписывается своим сертификатом. (Этот этап отсутствует при шифровании без подписания)

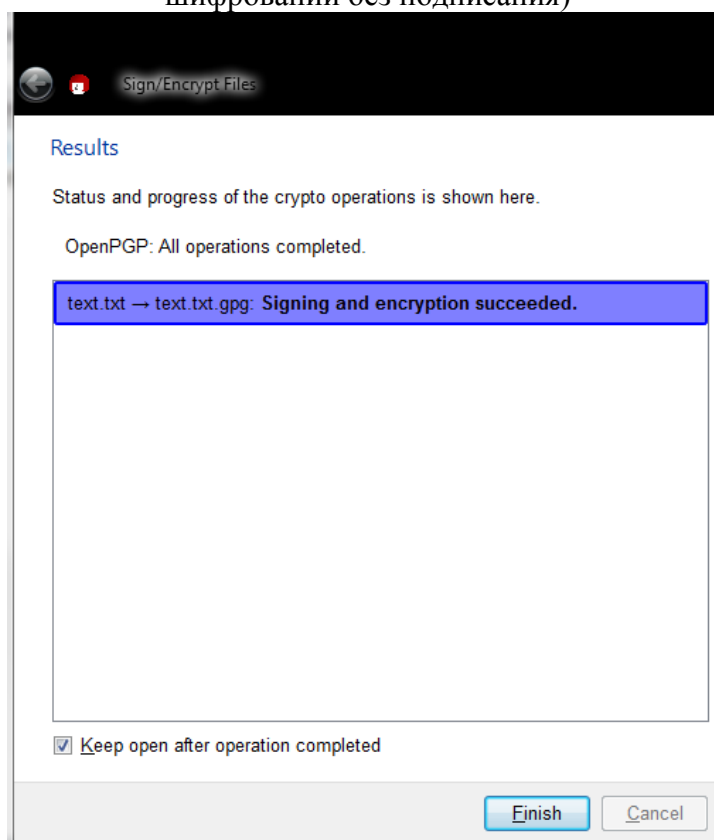


Рисунок 19. Операция создания шифрованного текстового файла завершена.

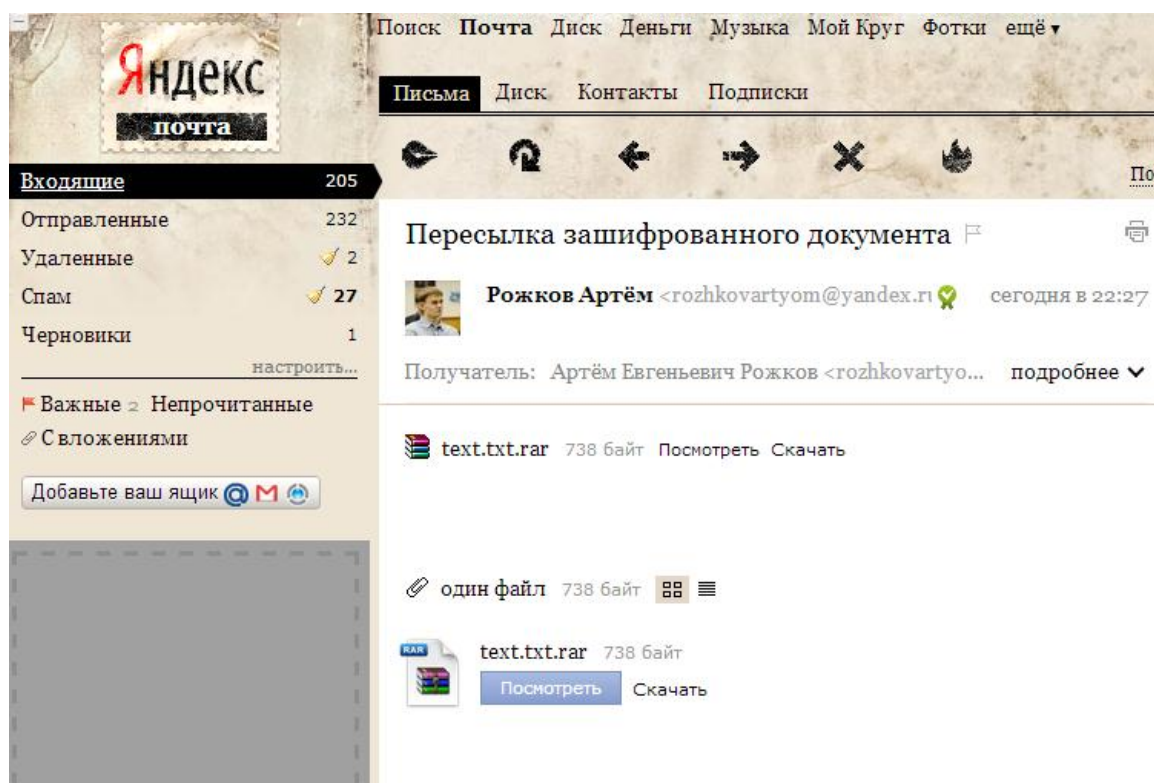


Рисунок 20. Передача файла получателю по электронной почте

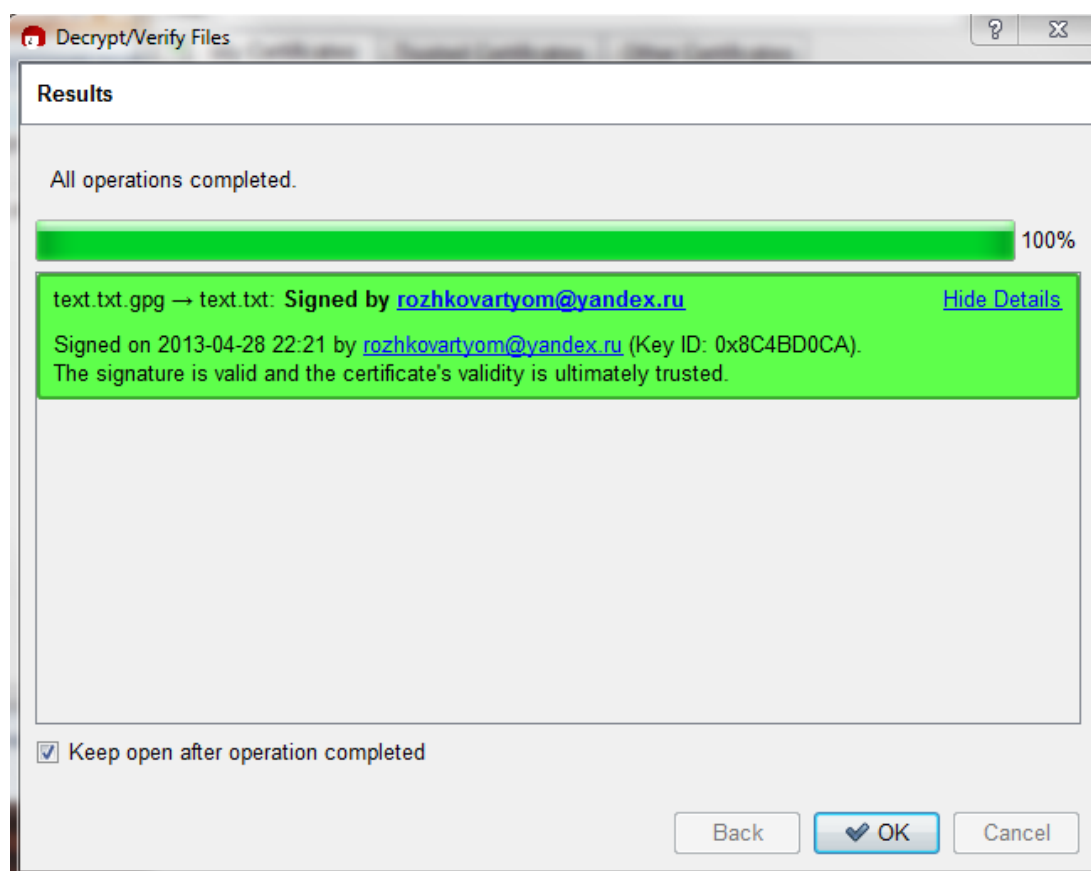


Рисунок 21. Получатель успешно восстановил файл; создатель идентифицирован

Примечание: На стороне получателя при дешифрации программа может не спросить пароль от сертификата получателя, если уже сделала это ранее для другой операции.

Выводы

Мы освоили программный продукт *gpg4win* для создания цифровой подписи и криптозащиты *gpg*. Благодаря удобному графическому интерфейсу процесс шифрования/подписания и расшифровывания/проверки подписи данных проходит очень просто.

Тем не менее, пользователю стоит позаботиться о том, чтобы в его отсутствие никто не мог получить доступ к ПК с целью подписания сообщения «активированным» сертификатом или кражи экспортированного в файл секретного ключа.