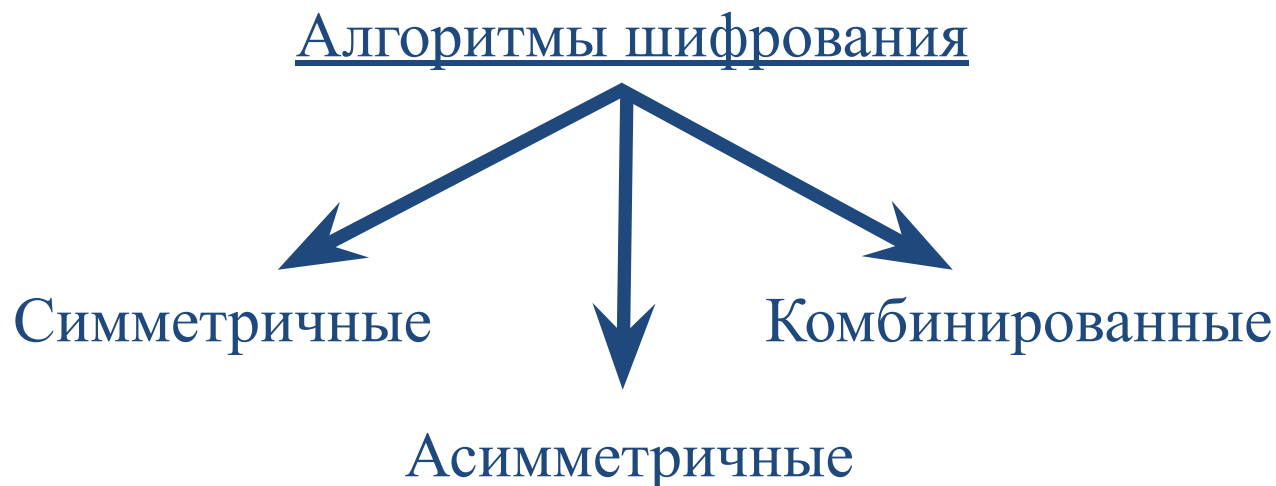


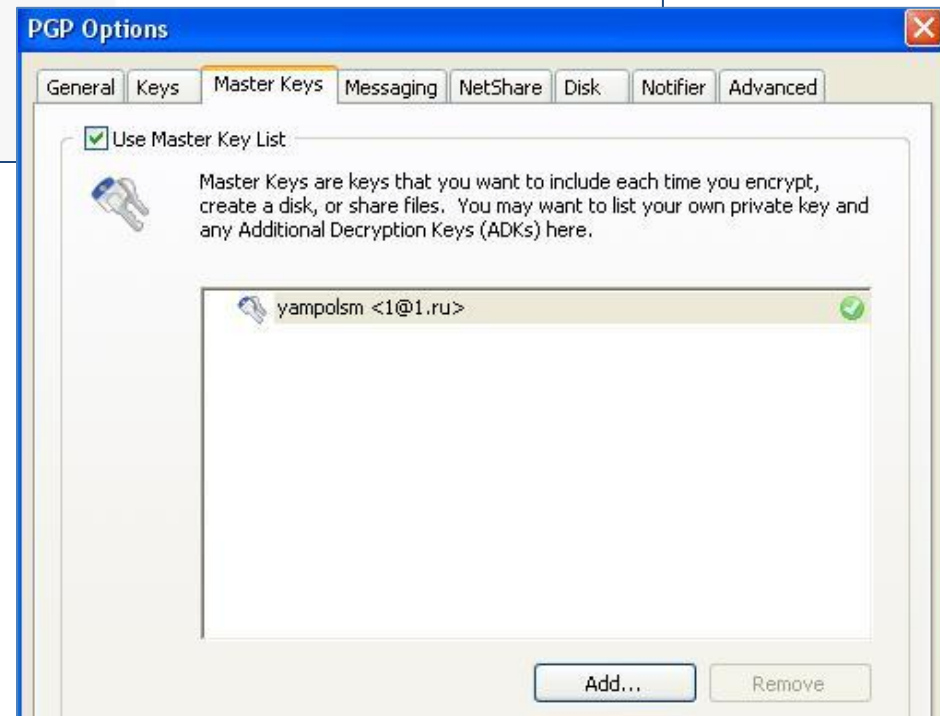
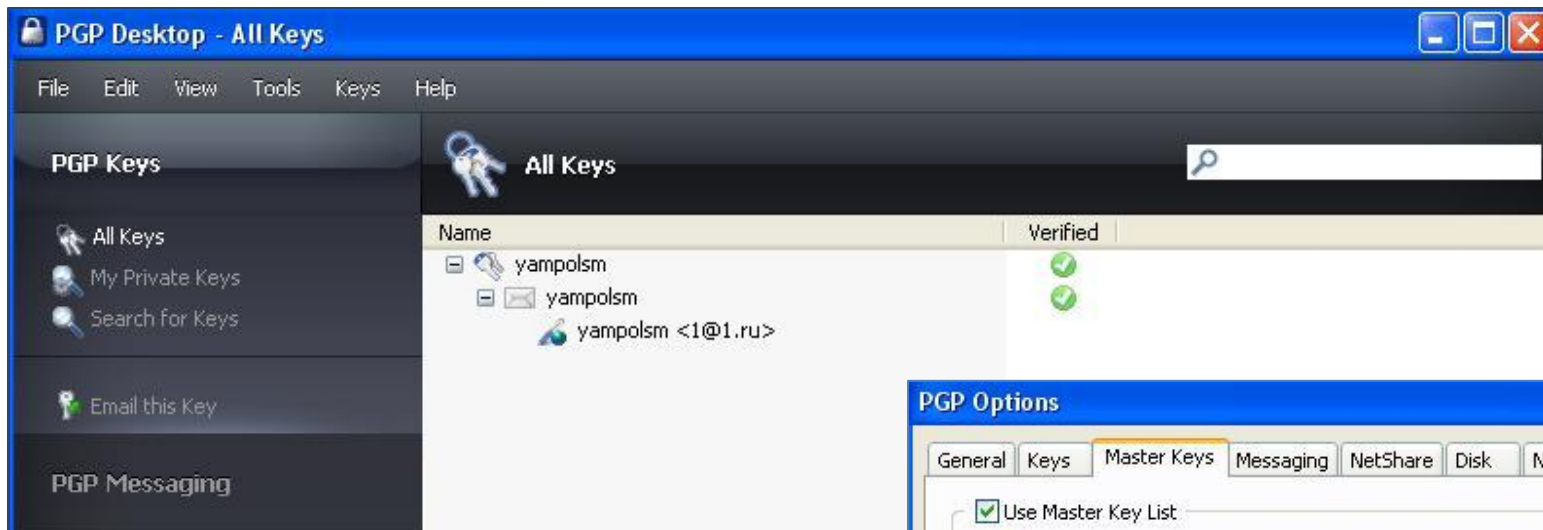
Лабораторная работа
по дисциплине
«Методы и средства защиты
компьютерной информации»

Тема: «Изучение технологии асимметричного шифрования информации и применения электронно-цифровой подписи»

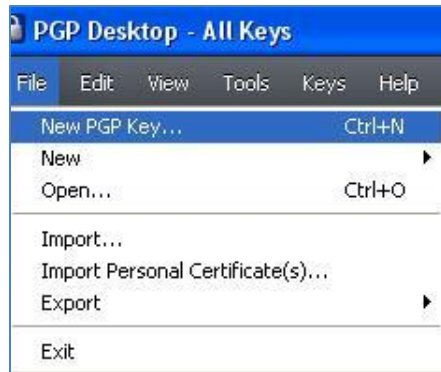
- Шифр - это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования



PGP (Pretty Good Privacy) – это программа, предназначенная для шифрования конфиденциальной информации и применения электронно-цифровой подписи



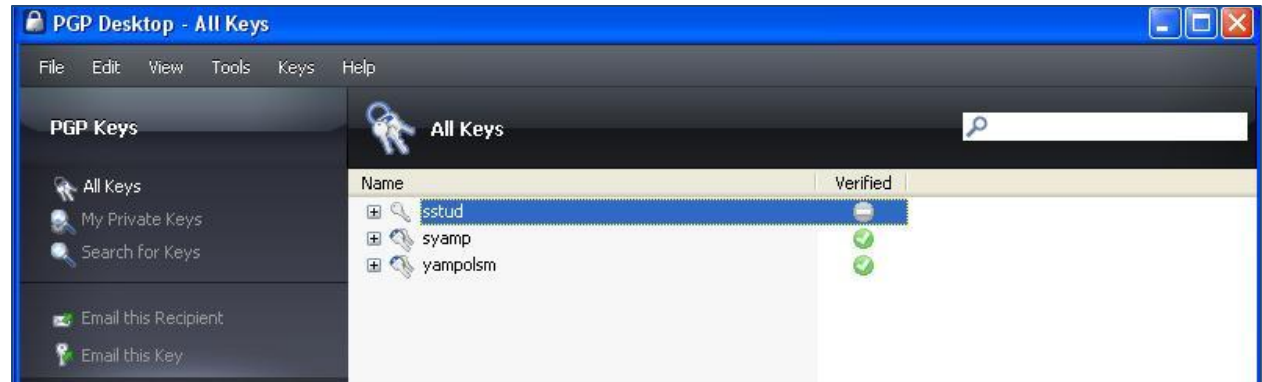
Главный ключ программы



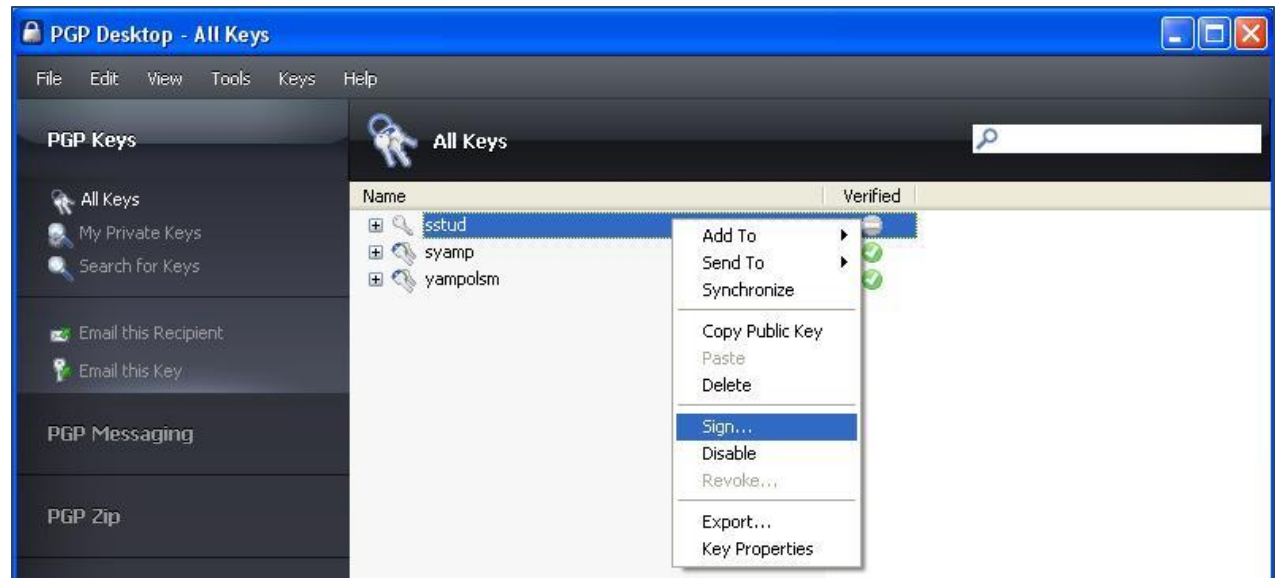
- Создание пары сеансовых ключей для организации сеанса связи



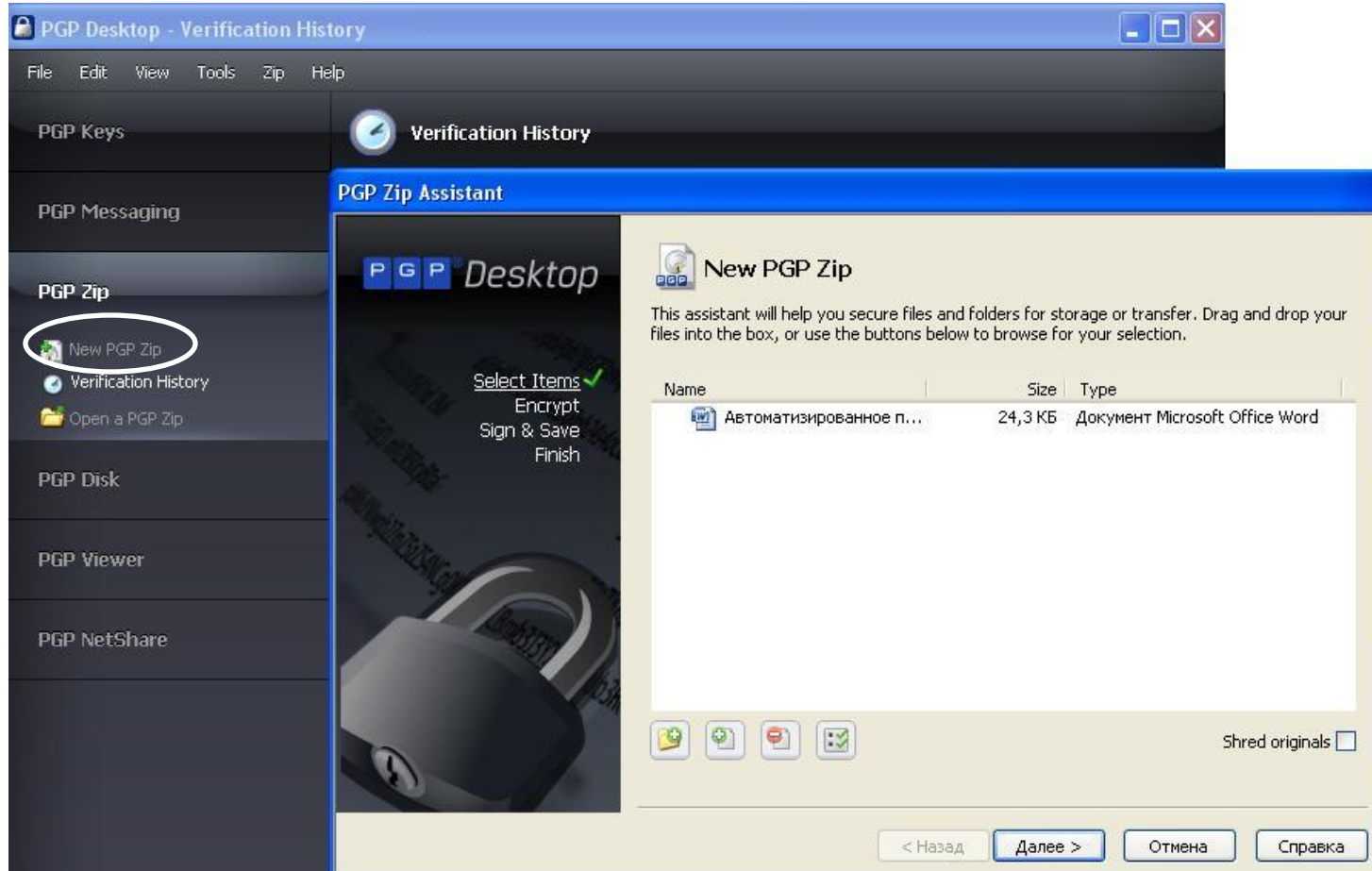
• Экспорт и импорт открытых ключей



• Подпись открытых ключей



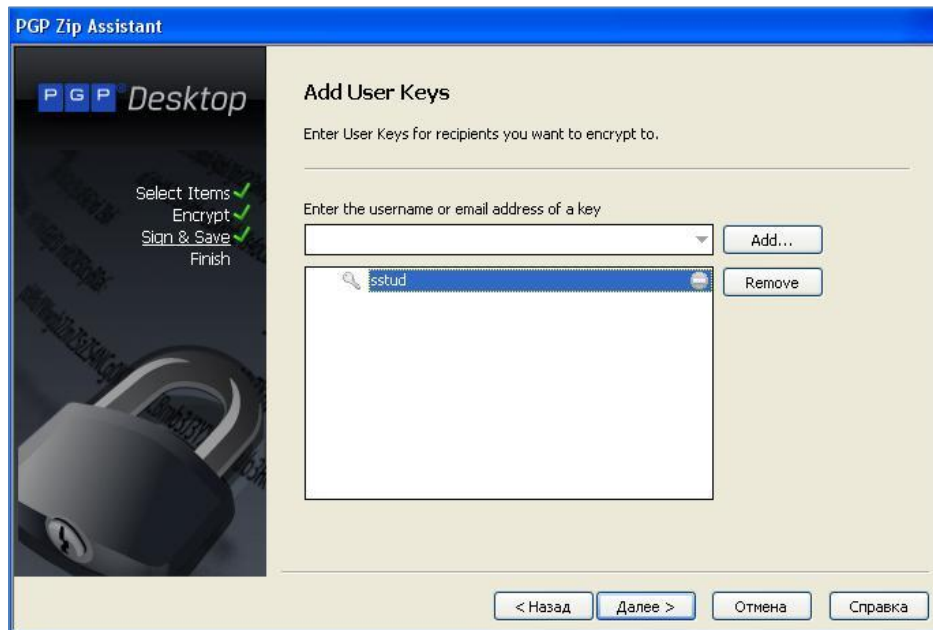
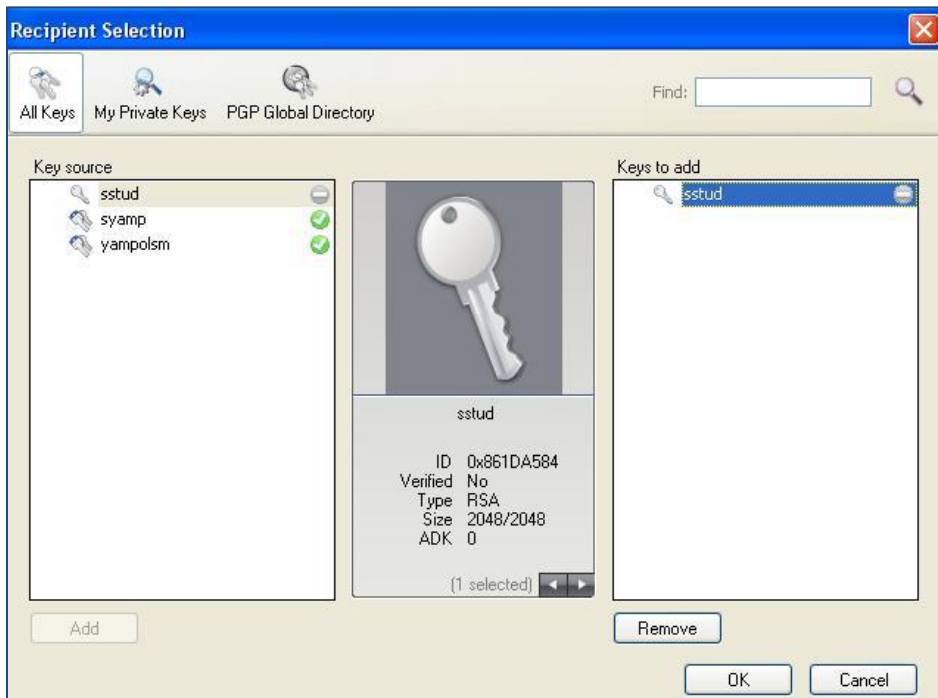
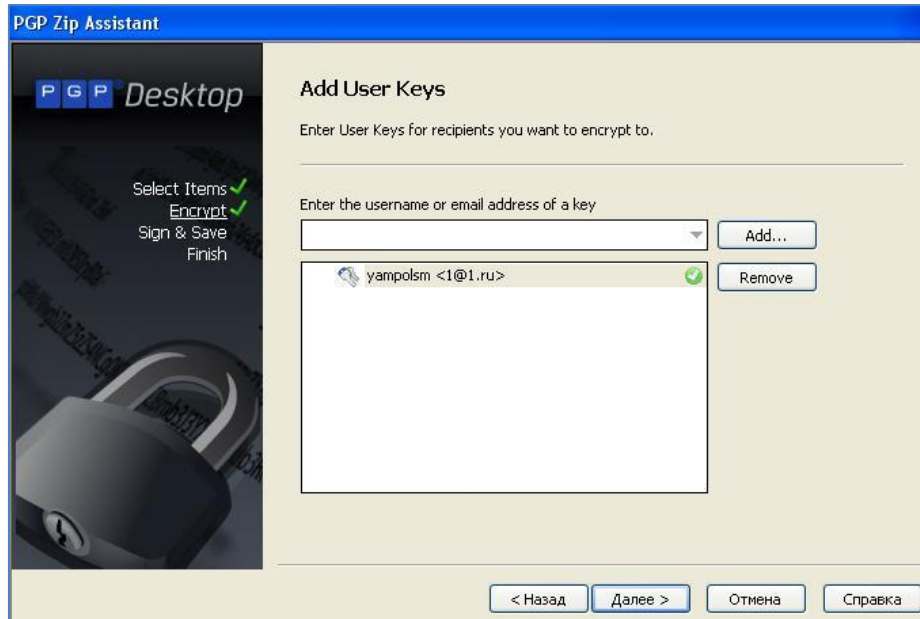
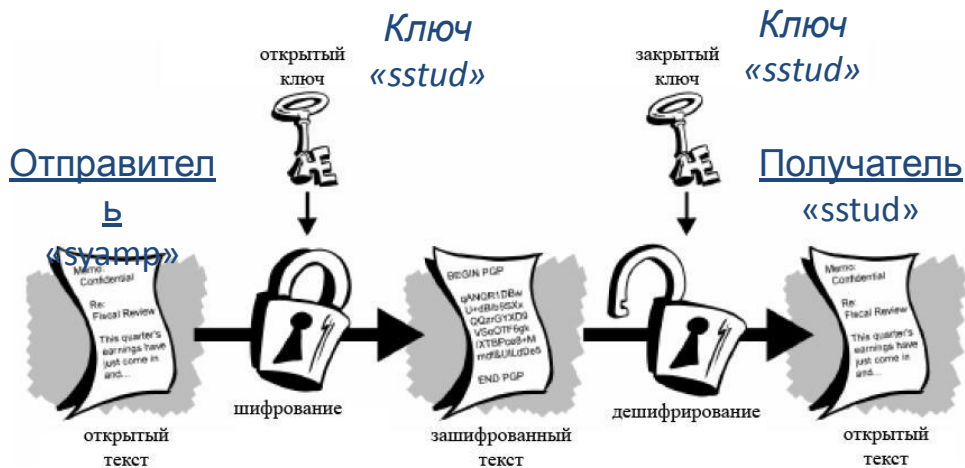
- Выбор файла (папки) для шифрования информации



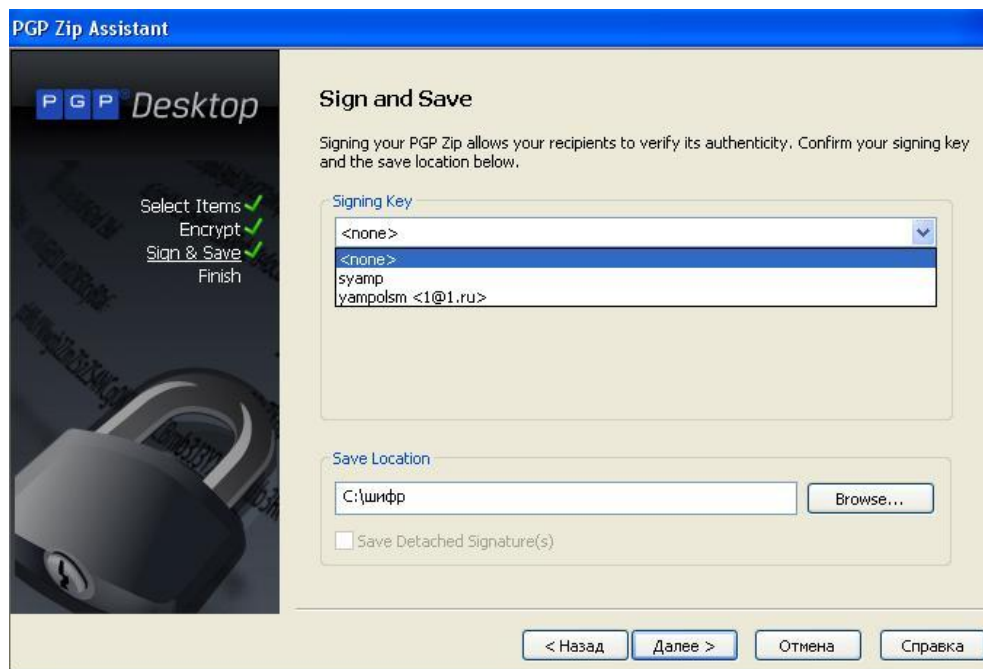
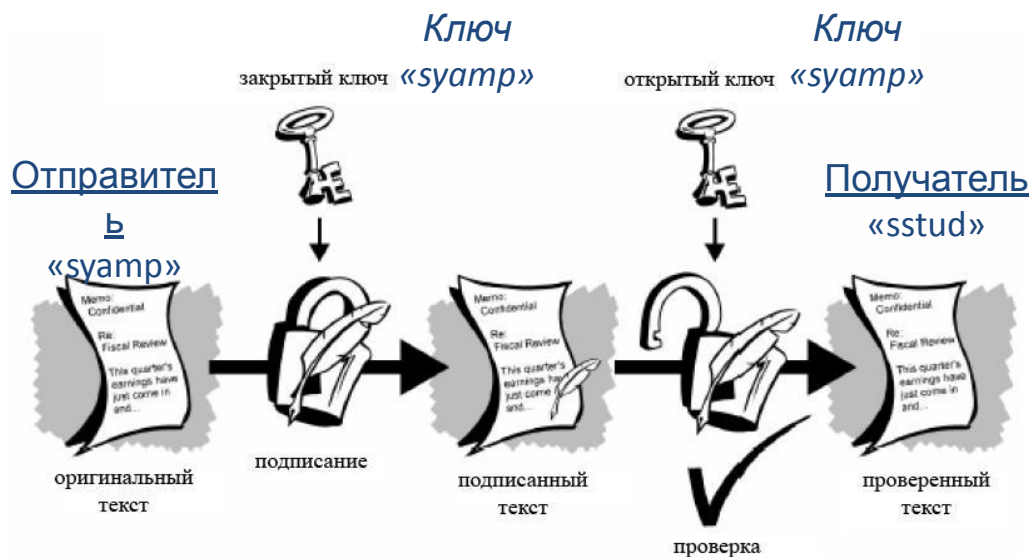
- Выполнение шифрования информации и электронно-цифровой подписи



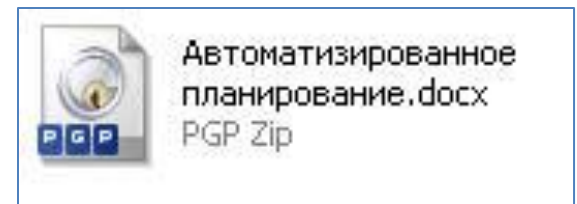
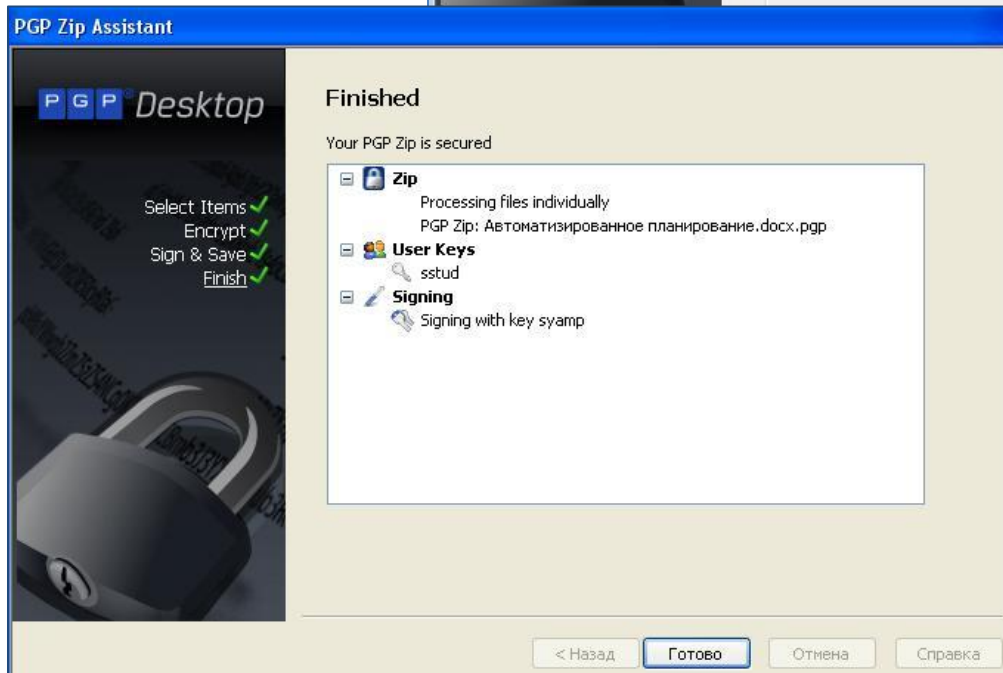
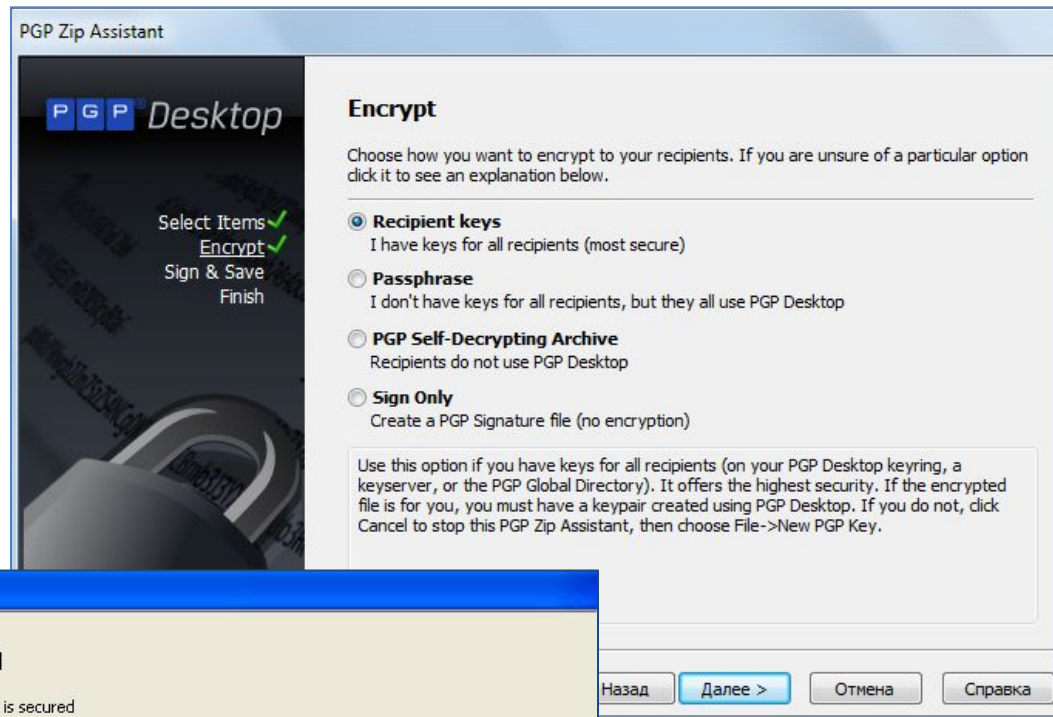
● Выбор ключа для шифрования информации



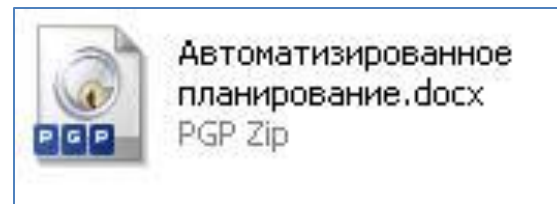
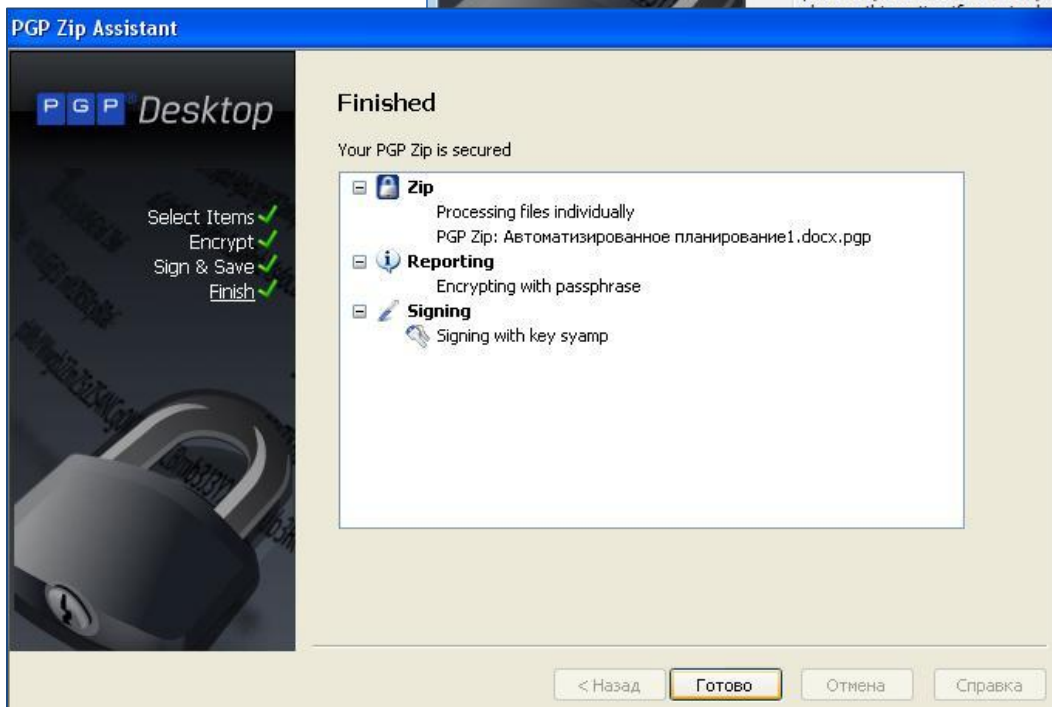
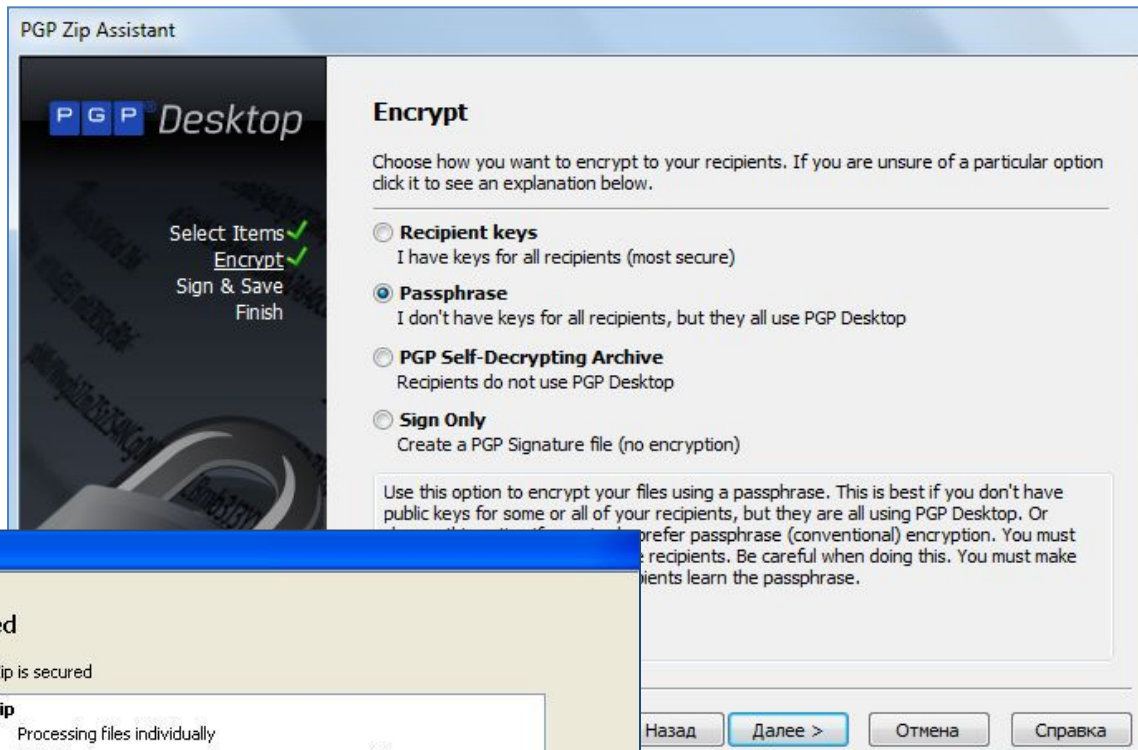
● Выбор ключа для электронно-цифровой подписи информации



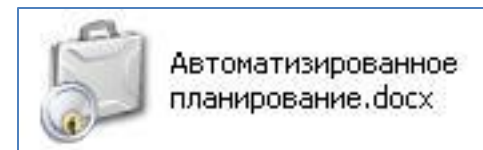
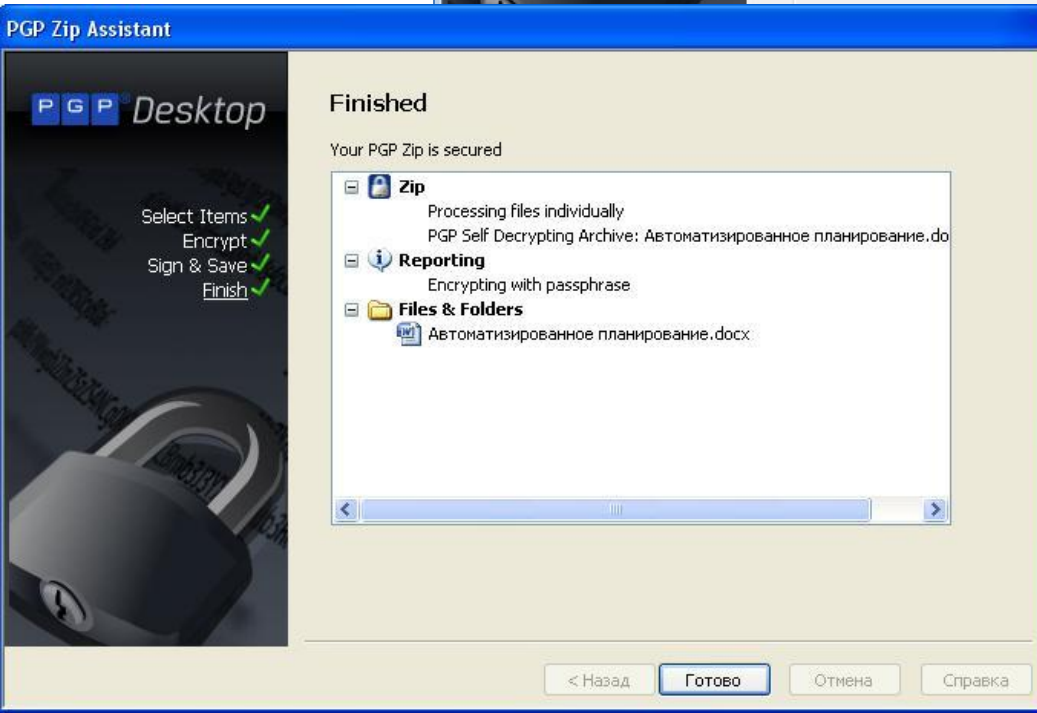
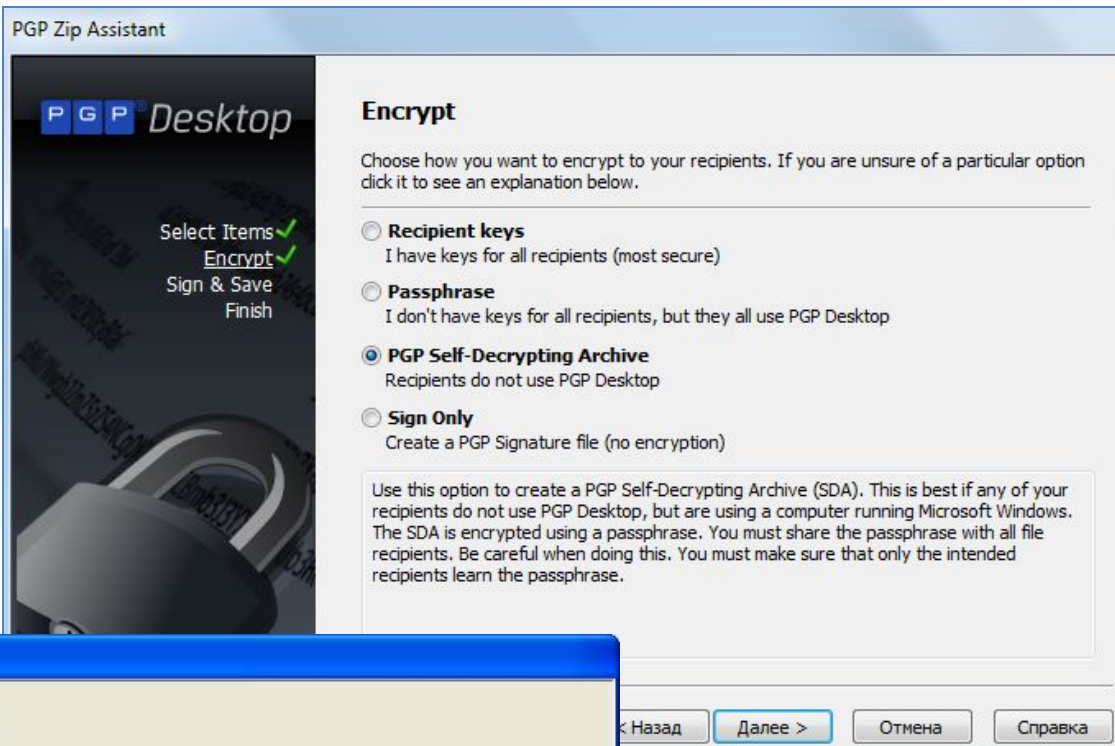
● Результат шифрования информации и электронно-цифровой подписи



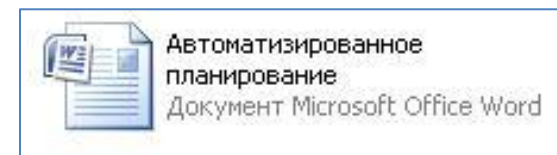
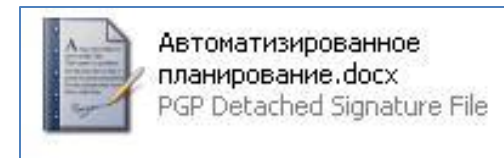
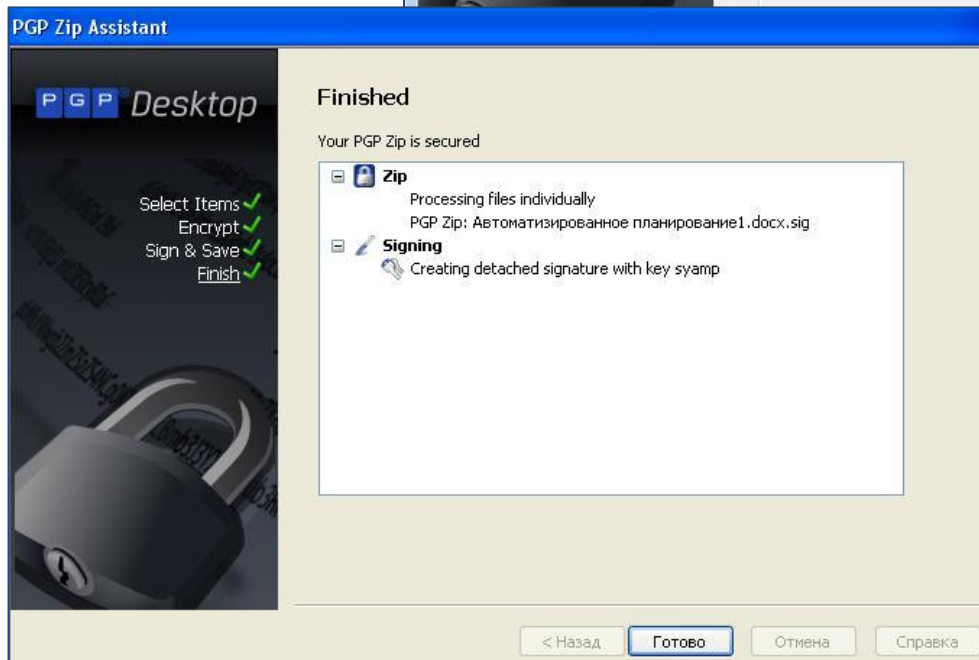
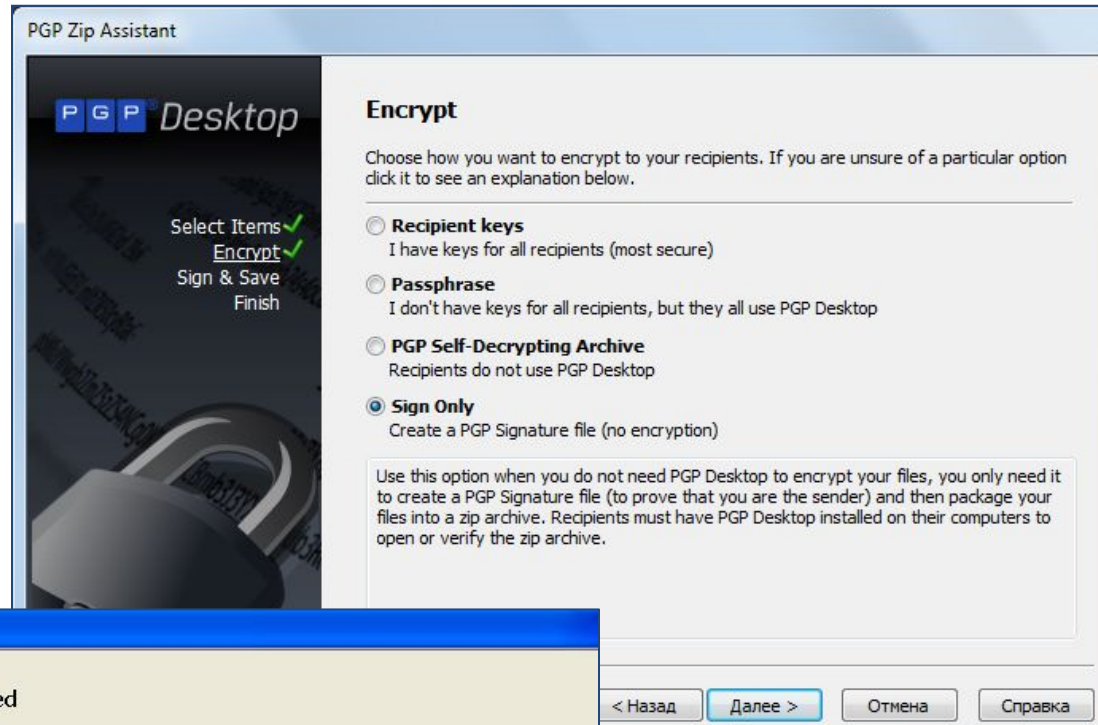
● Результат шифрования информации парольной фразой и электронно-цифровой подписи



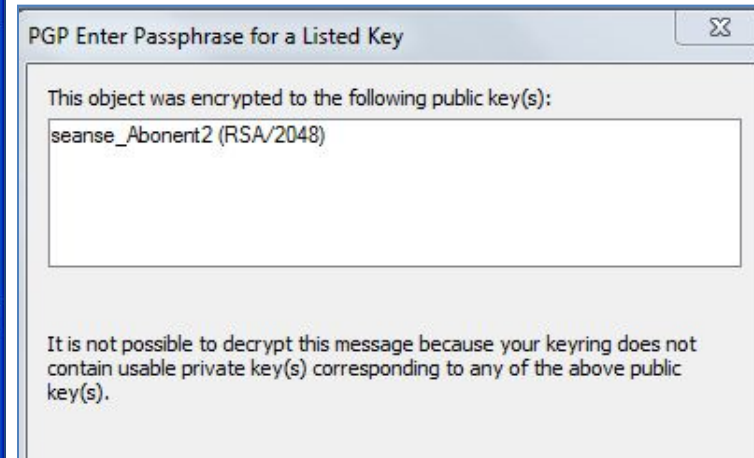
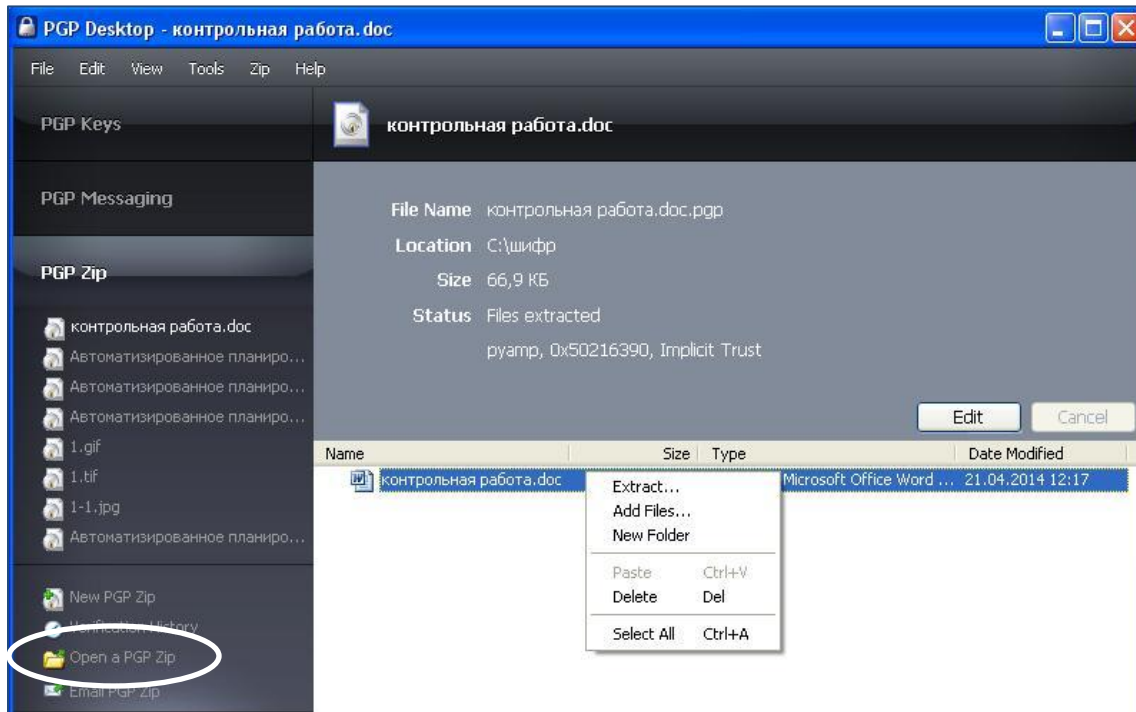
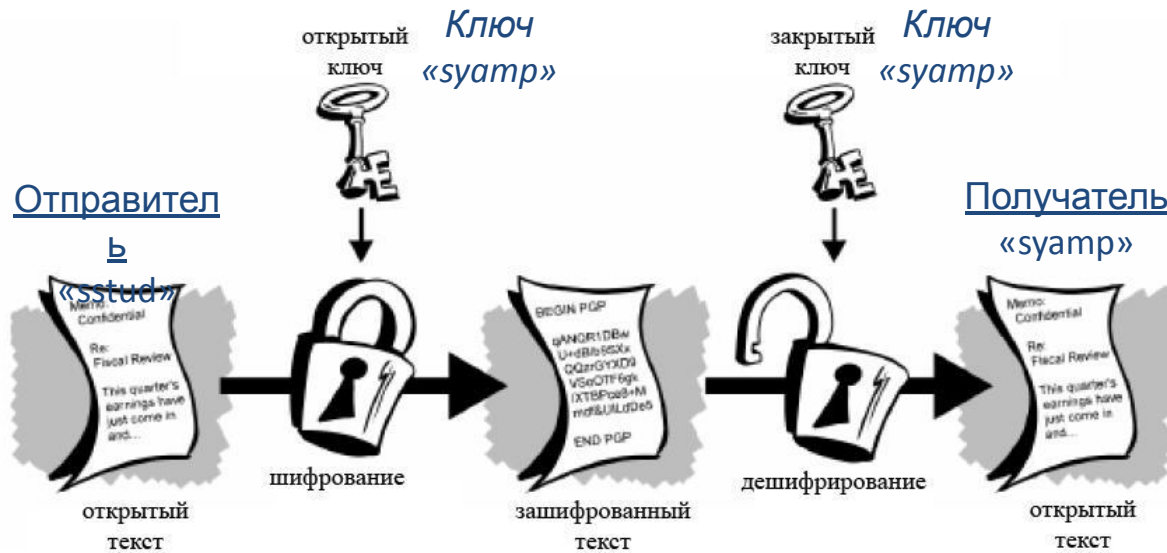
● Результат создания архива информации



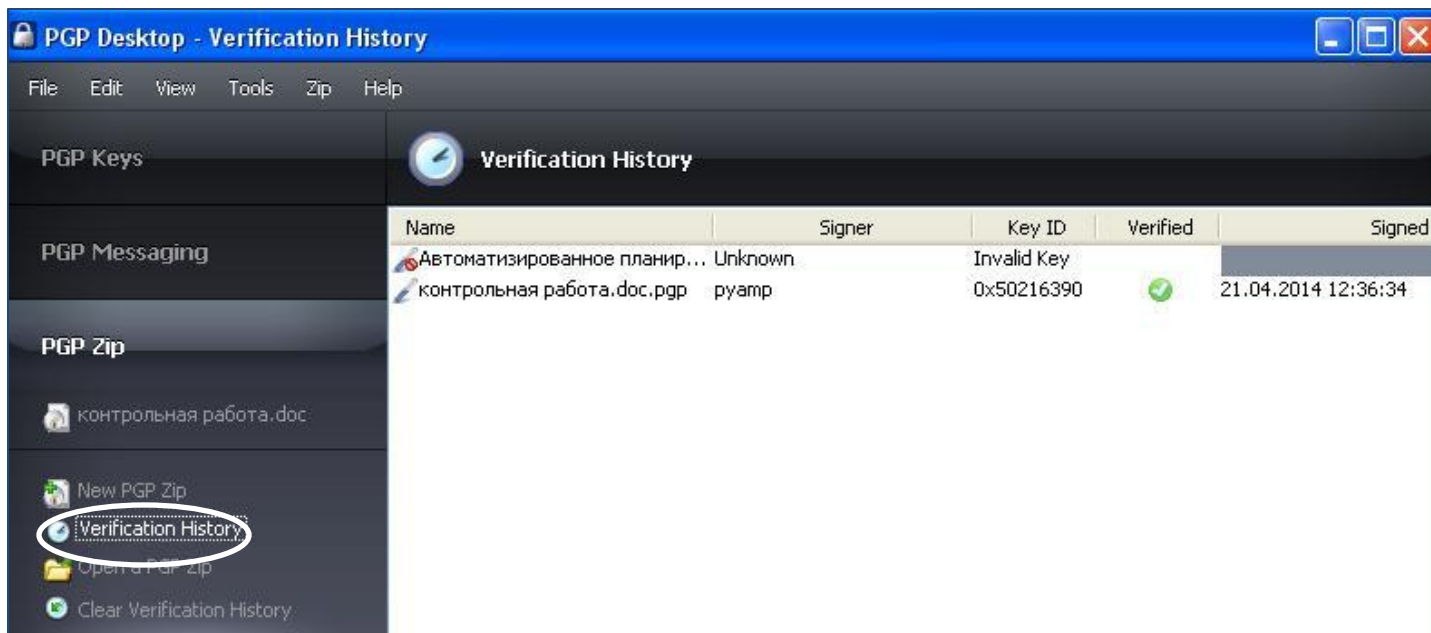
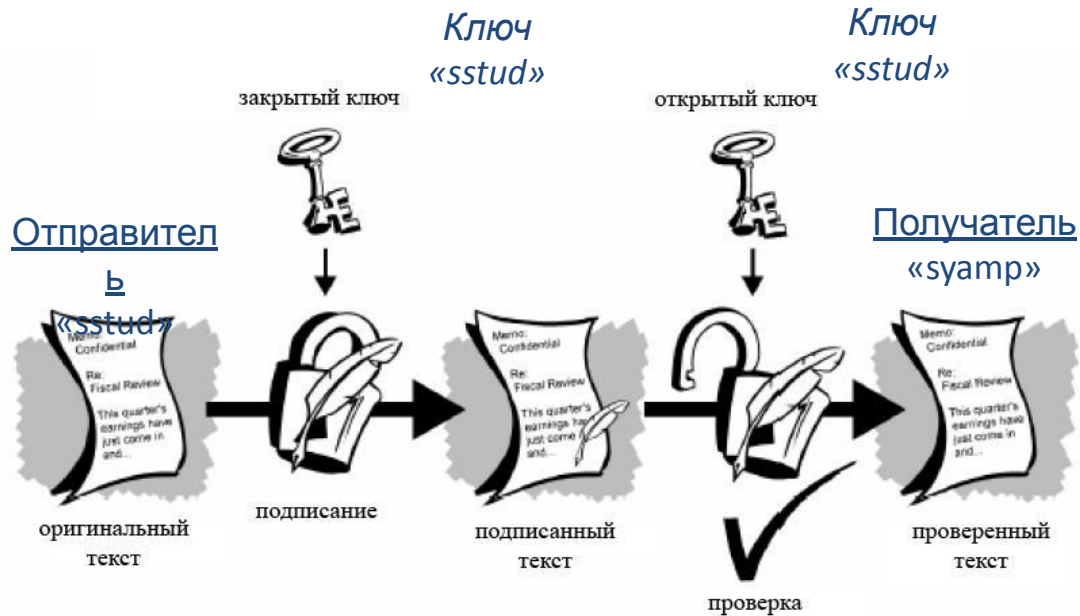
● Результат электронно-цифровой подписи



• Дешифрирование информации



● Проверка электронно-цифровой подписи



● Задание

1. Создать главный ключ программы
2. Создать пару сеансовых ключей для организации сеанса связи
3. Экспортировать открытую часть сеансового ключа
4. Импортировать открытую часть сеансового ключа преподавателя
5. Зашифровать и подписать любой текстовый файл
6. Передать преподавателю зашифрованный файл и открытую часть своего сеансового ключа. Проверить с преподавателем правильность использования ключей.
7. Проверить целостность подписи преподавателя.
8. Внести изменения в файл преподавателя и убедиться в нарушении целостности подписи

Спасибо за
внимание !