Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

Кафедра электронных приборов

Локальные компьютерные сети

Методы шифрования информации

Методические указания к лабораторной работе
для студентов направлений «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

2012

Агеев Евгений Юрьевич

Методы шифрования информации = Локальные компьютерные сети: Методические указания к лабораторной работе для студентов направлений «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства» / Е.Ю. Агеев; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Томский государственный университет систем управления и радиоэлектроники, Кафедра электронных приборов. - Томск : ТУСУР, 2012. - 15 с.

Целью настоящей работы является изучение аспектов безопасности компьютерных сетей: секретность передачи информации, которая обеспечивается защитой информации в электронном документе с помощью его шифрования, и электронная подпись, т.е подтверждение личности отправителя в электронном сообщении с помощью специального механизма цифровой подписи

Предназначено для студентов очной и заочной форм, обучающихся по направлению «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства») по курсу «Локальные компьютерные сети»

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и
радиоэлектроники»

Кафедра электронных приборов

УТВЕРЖДАЮ
Зав.кафедрой ЭП
_____С.М. Шандаров
«___» _____ 2012 г.

Локальные компьютерные сети

Методы шифрования информации

Методические указания к лабораторной работе
для студентов направлений «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

Разработчик

_____Е.Ю. Агеев
_____2012 г

2012

СОДЕРЖАНИЕ

1 Введение

В первые десятилетия существования локальных компьютерных сетей, они использовались в основном исследователями и университетскими работниками. В то время вопрос безопасности и защиты информации от несанкционированного доступа не стоял так остро, так как информация в университетском сообществе в основном не имеет коммерческого характера. С внедрением компьютерных сетей в работу большинства организаций и компаний вопрос защиты информации приобрел большую остроту. Дело в том, что электронные документы, в отличие от обычных, бумажных, могут быть легко подделаны, так как копия любого электронного документа ничем не отличается от оригинала.

В общем случае проблемы безопасности компьютерных сетей могут быть разделены на четыре составляющих:

- Секретность передачи информации. Секретность обеспечивается защитой информации в электронном документе с помощью его шифрования;
- Аутентификация (проверка личности) при вступлении двух субъектов в контакт посредством компьютерной сети. Позволяет определить с кем вы разговариваете, прежде чем предоставить собеседнику доступ к секретной информации или вступить с ним в деловые отношения;
- Электронная подпись. Подтверждение личности отправителя в электронном сообщении с помощью специального механизма цифровой подписи;
- Обеспечение целостности сообщения. Нарушение целостности указывает на возможную попытку несанкционированного доступа к передаваемой информации.

В лабораторной работе изучаются два аспекта из вышеперечисленных: шифрование и электронная подпись.

2 Теоретическая часть

2.1 Общие понятия

Традиционная криптография (наука шифрования) использовала для операции шифрования методы с одним секретным ключом (рис. 2.1).

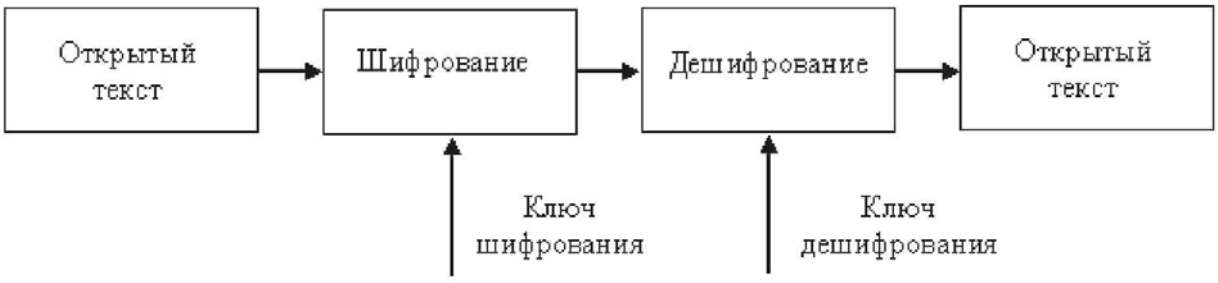

Рисунок 2.1 - Процесс шифрования-дешифрования с одним секретным ключом

И для шифрования и для обратной операции в этом случае используется один и тот же ключ, и именно он является главным секретом шифровальщика. Число известных методов шифрования не так велико и о том, как они работают, могут знать не только шифровальщики, но и потенциальные взломщики. Однако, если злоумышленнику не известен используемый секретный ключ (даже если он определит длину такого ключа), он будет вынужден перебирать все возможные комбинации цифр, пока не наткнется на верную. Вероятность такого случайного подбора быстро уменьшается с увеличением длины ключа. Казалось бы, достаточно взять достаточно длинный ключ, чтобы обеспечить надежную защиту информации. Пример одного из международных стандартов шифрования, основанных на использовании длинного секретного ключа – стандарт DES (Data Encryption Standard) и его модификации. Однако, слабым местом всех методов шифрования с использованием одного секретного ключа, является необходимость передачи самого секретного ключа одним участником обмена секретной информацией другому. В процессе передачи ключа он может быть получен злоумышленником и тогда вся процедура шифрации окажется бесполезной. Вероятность перехвата ключа возрастает с увеличением числа лиц, вовлеченных в процесс обмена секретной информацией, каждому из которых необходимо получить секретный ключ.

В 1976 г. ученые-криптографы из Стенфордского университета Диффи и Хеллман предложили метод шифрования с использованием двух различных ключей, получивший название **шифрования с открытым ключом**. В основе их метода лежат свойства некоторых математических функций. Один из ключей – **закрытый** используется для расшифровки сообщения, а для шифрования сообщения применяется другой ключ – **открытый**. Он получил такое название, т.к. его можно передавать совершенно свободно, не беспокоясь о его защите, ведь из открытого ключа невозможно получить закрытый, а значит и расшифровать зашифрованное сообщение. Для закрытого же ключа вполне можно обеспечить высокую степень защиты, т.к. его не нужно никуда передавать. Иногда используется другое название этого метода – **асимметричное шифрование**, в отличие от симметричного, использующего один и тот же ключ. В случае использования метода шифрования с открытым ключом, два участника переговорного процесса обмениваются своими открытыми ключами, после чего они могут шифровать сообщения, отправляемые друг другу с помощью своих открытых ключей (рис. 2.2).

Рисунок 2.2 - Процесс шифрования с открытым ключом

Прочитать зашифрованное сообщение сможет только владелец соответствующего закрытого ключа, то есть адресат сообщения. Т.к. при кодировании использовался открытый ключ адресата, даже тот кто его зашифровал не сможет выполнить расшифровку, ведь закрытого ключа адресата у него нет. Примером алгоритма шифрования с открытым ключом может служить RSA, назван по имени авторов-разработчиков – Rivest, Shamir, Adleman. Метод RSA основан на чрезвычайной сложности задачи нахождения делителей для больших чисел. Алгоритм решения до сих пор неопределен, поэтому задача решается только непосредственным перебором всех чисел, а для больших чисел это требует огромных вычислительных мощностей.

Алгоритм шифрования с открытым ключом позволяет создавать **цифровые подписи** – аналог обычной подписи. В этом случае при шифровании информации о владельце подписи (например, его имени и фамилии) используются два ключа – собственный закрытый ключ и открытый ключ адресата (рис. 2.3).

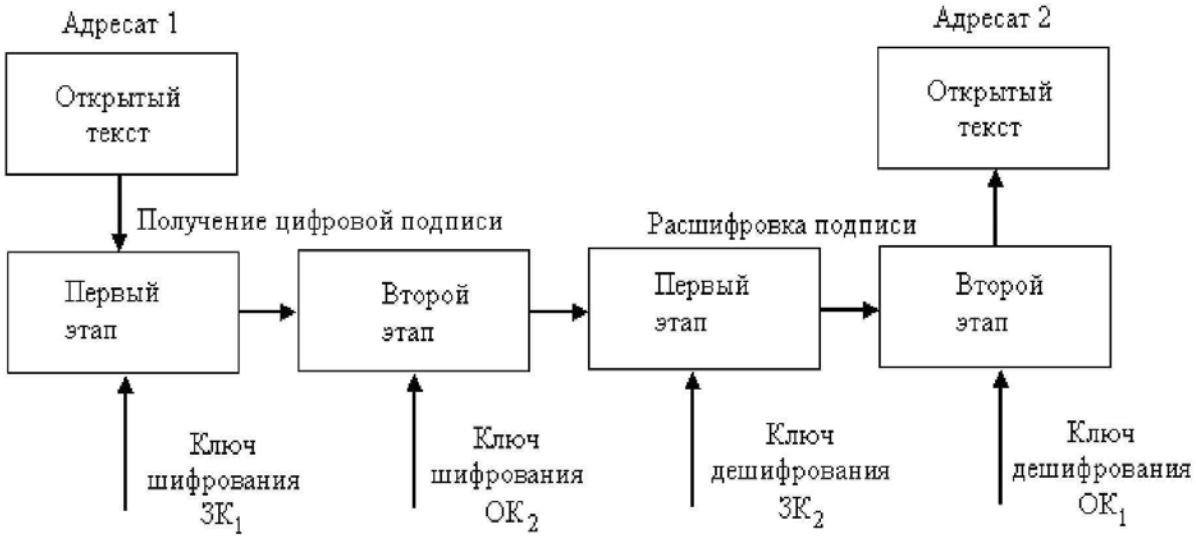

Рисунок 2.3 - Механизм формирования цифровой подписи

Так как открытый и закрытый ключ выполняют взаимно обратные операции, получатель сообщения, зашифрованного таким образом, может расшифровать его, проверив подлинность закрытого ключа отправителя, а значит и самой подписи. Электронный документ, объединяющий цифровую подпись, вместе с соответствующим открытым ключом, получил название **цифрового сертификата**.

2.2 Контрольные вопросы

1. Что такое открытый ключ, поясните механизм работы шифрования с открытым ключом.
2. Что такое цифровая подпись.
3. Кем была создана программа PGP.
4. Почему программа PGP обеспечивает очень высокую степень защиты зашифрованных файлов.
5. Что такое электронный сертификат, может ли электронный сертификат создаваться с помощью программы PGP.
6. Изменяется ли размер текстового файла после шифрования его с помощью программы PGP, как изменяется, почему.
7. Для чего выполняется процедура обмена открытыми ключами между двумя участниками секретных переговоров.
8. Удаленный сервер перед отправкой в ваш адрес зашифрованной веб-странички присылает вам сообщение с просьбой принять сертификат, зачем это делается. Что будет в том случае, если вы согласитесь принять сертификат, если откажетесь.
9. Почему защита информации и безопасность особенно важна при использовании электронных документов.
10. В чем недостаток традиционной системы шифрования с использованием симметричного ключа.

3 Экспериментальная часть

3.1 Задание на работу

Работа выполняется группами по два-три человека. Каждый член группы должен:

1 Создать пару ключей для использования шифрации с открытым ключом;

2 Выполнить экспорт своего открытого ключа и передачу его всем членам группы;

3 Выполнить шифрацию произвольного сообщения для каждого члена группы и отправку зашифрованного сообщения адресатам;

4 Каждый член группы выполняет дешифрацию сообщений, полученных от своих корреспондентов.

3.2 Методические указания по выполнению работы

Использование программы PGP (версия 6.5.8) для шифрования данных

Программа PGP (Pretty Good Privacy – довольно хорошая секретность) разработана Филиппом Циммерманом и является свободно распространяемой программой. Несмотря на это, в отличие от некоторых коммерческих программ, программа PGP обеспечивает очень высокую степень защиты данных за счет использования алгоритмов шифрования с открытым ключом и применения ключей с длиной 1024 бит и более.

После установки программы в операционной системе Windows, в системном трее появляется иконка ^, а в списке программ - вкладка PGP (рис. 3.1).

Рисунок 3.1 – Вкладка программы PGP в меню «Пуск/Все программы».

Управлять программой можно и через меню, и через щелчок по иконке. Работа в программе делится на три этапа:

1. Создание пары ключей и обмен открытыми ключами с корреспондентами;
2. Шифрация сообщений и документов;
3. Дешифрация сообщений и документов

Создание пары ключей и обмен открытыми ключами

Для начала работы необходимо создать пару ключей: открытый (public) и закрытый (privat). Выбирая пункт PGPKeys, мы открываем окно программы для работы с ключами шифрования (рис. 3.2).

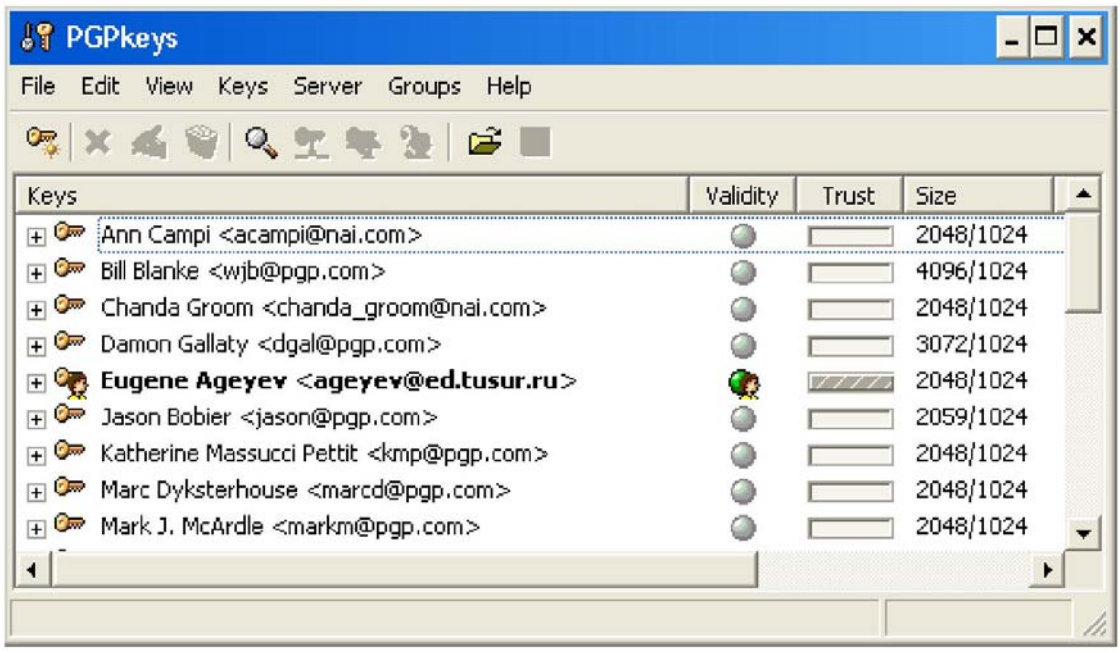

Рисунок 3.2 – Окно программы PGP для создания и управления параметрами ключей шифрования

Выбор в этом окне пункта меню Keys/New Key… (рис.3.3) запускает мастер, позволяющий в несколько шагов создать пару ключей на основе индивидуальной информации (имени, адреса электронной почты) и символьного пароля.

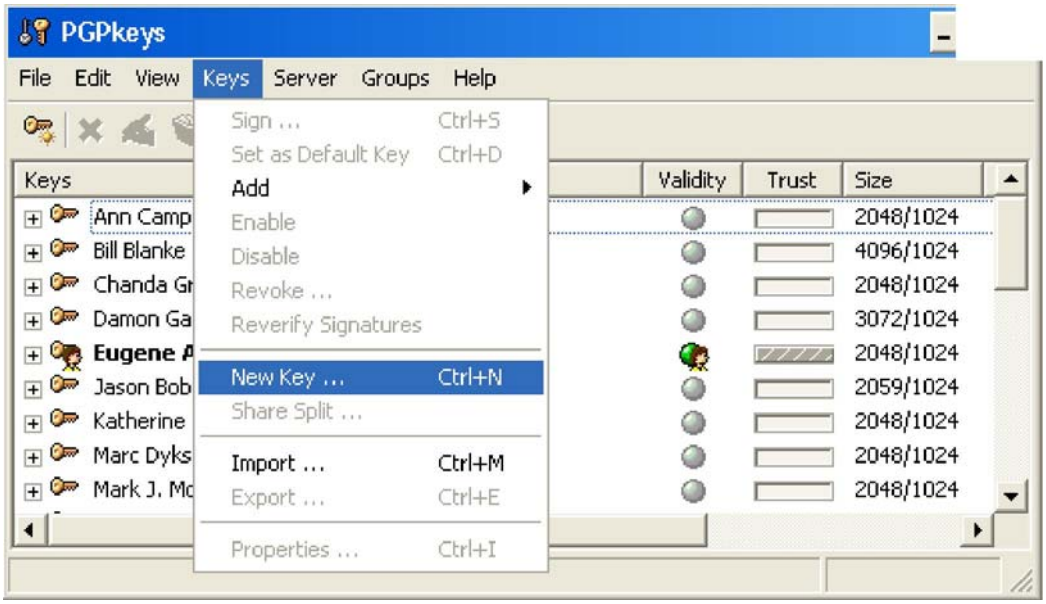

Рисунок 3.3 – Запуск мастера создания новой пары ключей

Обмен ключами можно осуществлять с помощью специального сервера, надежность которого не вызывает сомнений (пункт Server в меню окна PGPKeys) или путем прямой передачи ключа, которую можно осуществить, выполнив экспорт ключа в виде текстового файла, и передав его своим корреспондентам любым путем: электронной почтой, копированием и т.п. Экспорт открытого (public) ключа можно выполнить через меню Keys/Export… или контекстное меню (контекстное меню Export… вызывается правой клавишей мышки, установленной на строку окна программы с вновь созданной парой ключей).

Получив каким-либо из способов открытый ключ, корреспондент должен импортировать его в программу (меню Keys/Import), после чего он сможет его использовать для шифрования сообщений для того адресата, который передал ему этот ключ.

Шифрация сообщений и документов

Процесс шифрования несложен и может быть выполнен двумя способами.

Способ 1. Выбором команды PGPTools при щелчке мышкой по иконке PGP в системном трее или в окне меню программы (рис. 4). При этом открывается окно PGPTools программы PGP (рис. 7). Щелчок мышкой на второй слева пиктограмме в этом окне открывает окно выбора файла (или группы файлов) для шифрования.

Рисунок 3.4 – Создание зашифрованного сообщения(файла) с помощью панели PGPTools

После завершения выбора файла открывается окно выбора корреспондента (рис. 3.5). Этот выбор выполняется двойным щелчком по строке с выбранным пользователем или перетаскиванием этой строки в окно Recipients. Соответствующий открытый ключ для указанного пользователя будет использован автоматически в процессе шифрования. Зашифрованный файл имеет расширение «pgp».

В этом же окне можно задать традиционный (Conventional), более простой, способ шифрования с использованием парольной фразы, установив флажки в строках Conventional Encryption или Self Decrypting Archive. Алгоритм шифрования с открытым ключом в этом случае не используется и для расшифровки сообщения его получатель должен будет узнать парольную фразу, которая использовалась при шифровании.

Флажок Wipe Original позволяет выполнить шифрование с одновременным удалением оригинала файла, а при установке флажка Text Output в результате шифрования создается зашифрованный файл текстового формата с расширением «asc».

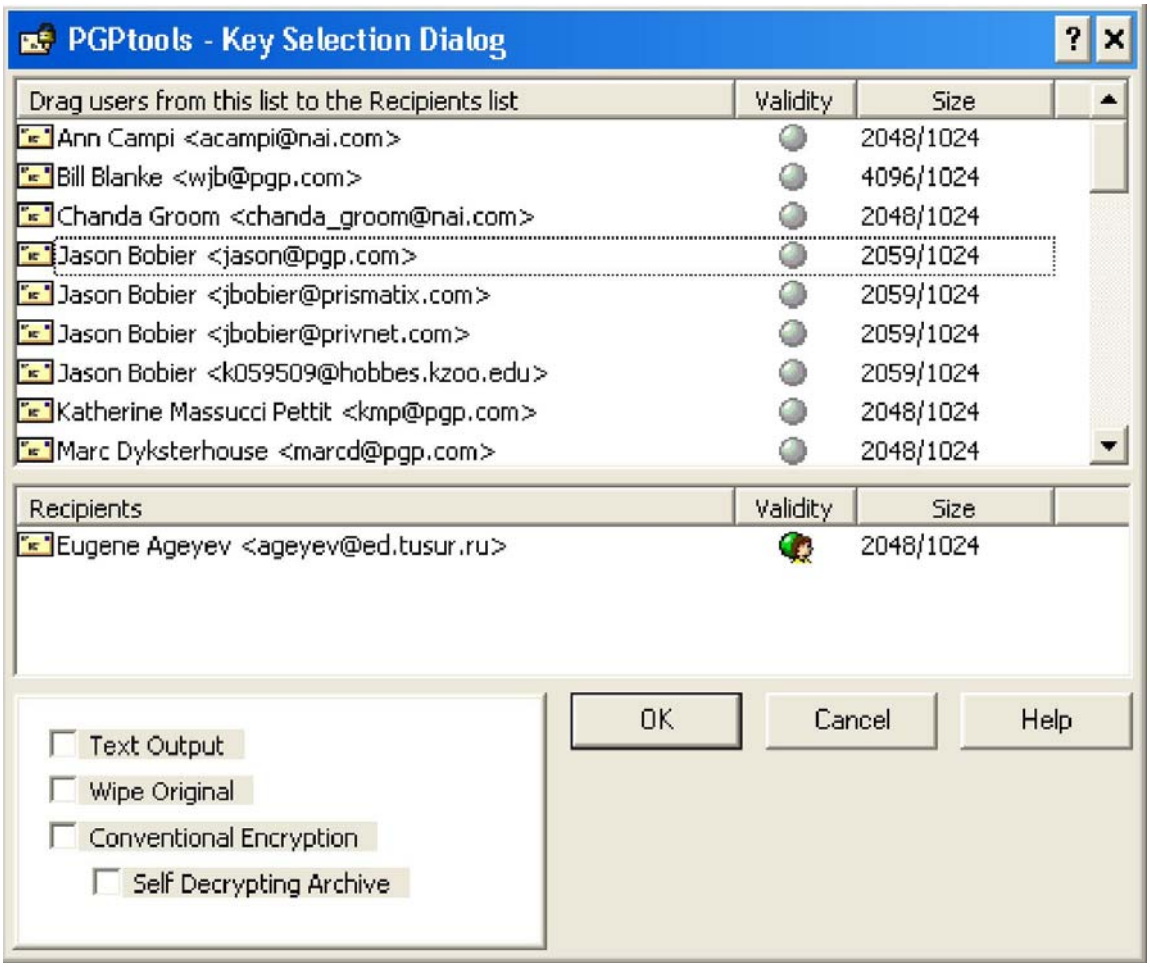

Рисунок 3.5 – Окно выбора корреспондента и открытого ключа для шифрации

Второй способ шифрования файла – с помощью контекстного меню, появляющегося при выборе файла в окне «Проводника» и нажатии правой клавиши мышки (рис. 3.6).

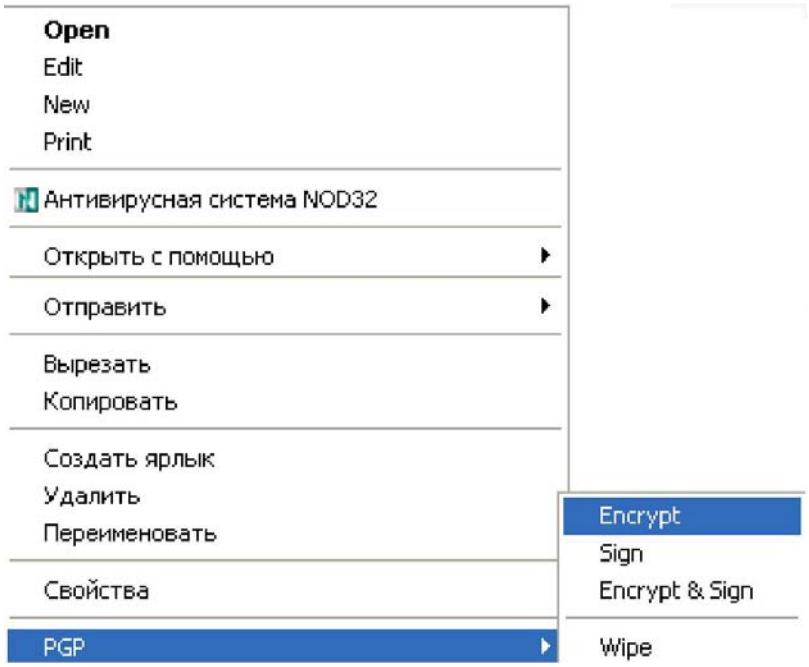

Рисунок 3.6 – Шифрование файла (группы файлов) с помощью контекстного меню

Поскольку выбор файла в этом случае уже выполнен, сразу происходит переход к окну выбора ключа шифрации (рис. 3.5).

Дешифрация сообщения или файла

Для расшифровки файла, его получатель просто выполняет двойной щелчок левой кнопкой мышки на файле. Это действие вызывает окно ввода пароля, использованного при создании пары из открытого и закрытого ключей (рис. 3.7).

Рисунок 3.7 – Окно ввода пароля при расшифровке файла

Ввод корректного пароля запускает процесс дешифрации, в результате которого получается расшифрованный исходный файл.

3.3 Содержание отчета

Каждый студент должен представить преподавателю отчет по лабораторной работе, которой должен содержать:

1. Титульный лист.
2. Введение.
3. Результаты выполнения задания.
4. Список используемой литературы.

Рекомендуемая литература

1. Аппаратные средства локальных сетей: энциклопедия / М. Гук. - СПб. : Питер, 2005. – 572 с. - ISBN 5-8046-0113-X :

2. Компьютерные сети: Принципы, технологии, протоколы : учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. : Питер, 2006. - 960 с. - ISBN 5-469-00504-6

3. Сетевые операционные системы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538[6] с. : - ISBN 5-272-00120-6 :

4. Локальные сети, модемы, интернет: ответы и советы / сост. : И. Грень. - Минск : Новое знание, 2004. – 350 с. : ил. - ISBN 985-475-059-0 : экз – 49.

5. Локальные компьютерные сети: конспект лекций по курсу "Локальные компьютерные сети" для студентов специальности 200300 / Е. Ю. Агеев; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра электронных приборов. - Томск : ТУСУР, 2007. - 103 с.

Учебное пособие

Агеев Е.Ю.

Методы шифрования информации

Методические указания к лабораторной работе
по дисциплине «Локальные компьютерные сети»

Усл. печ. л. _____Препринт
Томский государственный университет
систем управления и радиоэлектроники
634050, г.Томск, пр.Ленина, 40