**1. Цель работы**

Изучить принципы работы средств симметричного шифрования.

**2. Порядок проведения работы**

2.1. Изучить лекционный материал (разделы [2.1-2.4](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter2_1.html))  
2.2. Изучить теоретический материал по лабораторной работе  
2.3. Выполнить задание на лабораторную работу.   
2.4. Ответить на контрольные вопросы.

**3. Задание на лабораторную работу**

3.1. Создать текстовый файл  
3.2. Зашифровать и впоследствии расшифровать подготовленный файл с помощью программ Mooseoft Encrypter 3.0, Invisible Secrets Pro, Cryptomania.

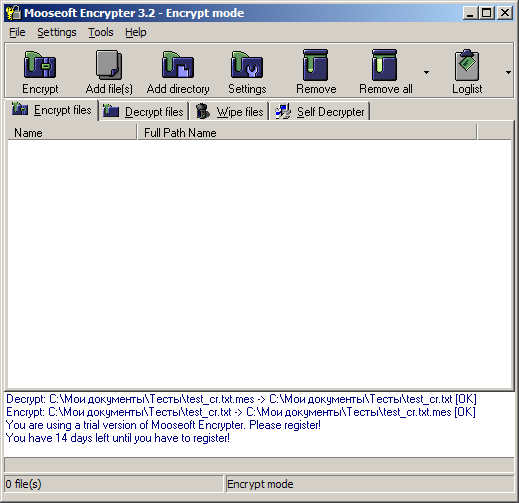
**4. Теоретический материал и практические аспекты**

Криптография является наиболее существенным элементом любой системы, предназначенной для защиты конфиденциальной информации. Для выполнения данной лабораторной работы необходимо знание учебного материала в объеме пп. [2.1-2.4.](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter2_1.html)

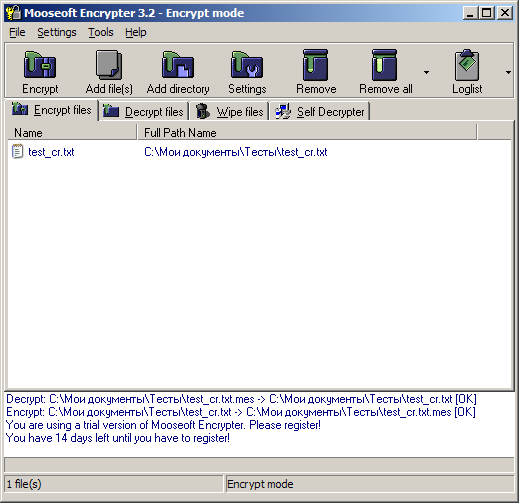
Современные программные средства предлагают достаточно большой выбор криптоалгоритмов высокой стойкости.

**ПРОГРАММА MOOSEOFT ENCRYPTER 3.0**

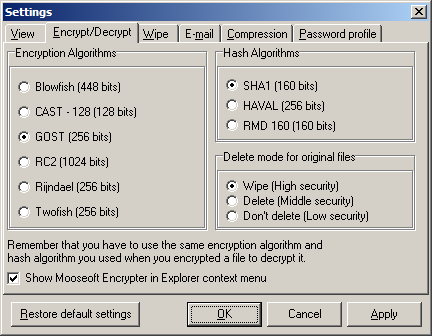
Данная программа позволяет осуществлять шифрование файлов по алгоритмам Blowfish, Cast128, Cast256, GOST, IDEA, MARS, Misty1, RC2, RC5, RC6, Rijndael и Twofish.



Для шифрования файла необходимо ввести его имя (для шифрования всего каталога необходимо ввести имя каталога) с помощью кнопок "Add file(s)" и "Add directory":



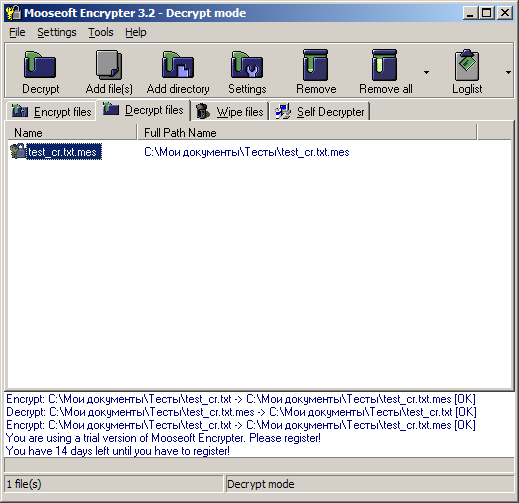
Для настройки параметров шифрования (прежде всего, алгоритмы шифрования и хеширования для преобразования введенного пароля в криптографический ключ нужной размерности служит вкладка Settings:



Собственно шифрование происходит при нажатии кнопки Encrypt. Здесь необходимо ввести пароль для шифрования (в нижнем поле показано качество вводимого ключа) и выбрать каталог, куда будет помещен результат:



Аналогичным образом производится расшифрование файла. Выбирается имя файла для расшифровки:



Для расшифрования необходимо ввести правильный пароль:



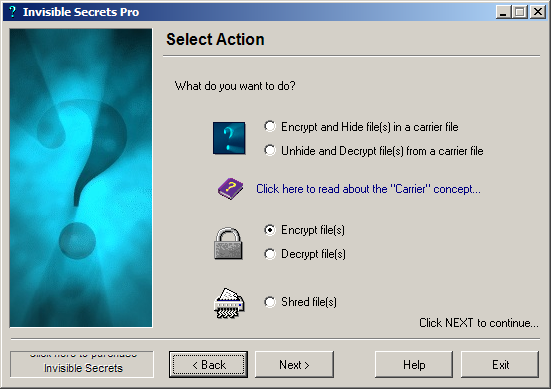
Загрузить программу Mooseoft Encrypter 3.0: [Mooseoft Encrypter 3.0.exe](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\Mooseoft%20Encrypter%203.0.exe)

Просмотреть видеозапись работы с программой: [encrypter.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\encrypter.avi)

**ПРОГРАММА INVISIBLE SECRETS PRO**

Эта программа обладает различными возможностями, в том числе и шифрует файлов с помощью алгоритмов Blowfish, Twofish, RC4(tm), GOST, Cast128.

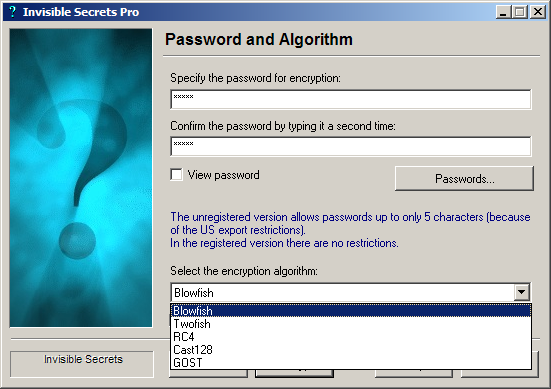
Для шифрования выберем соответствующий пункт меню:



Затем добавим файлы и каталоги, которые должны быть зашифрованы:

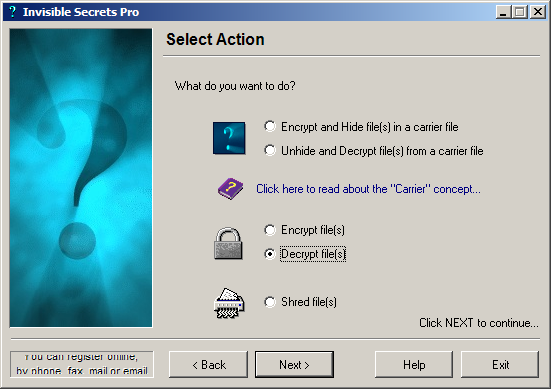


Задаем пароль и выбираем алгоритм шифрования:

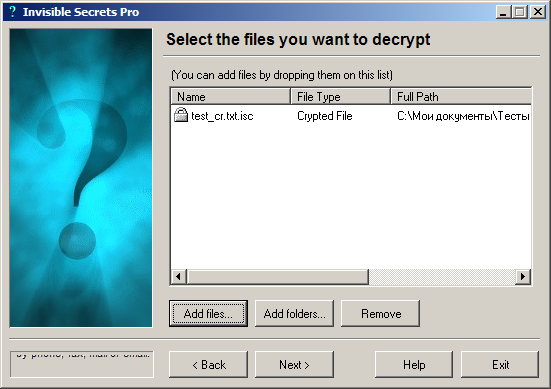


После этого файл будет зашифрован.

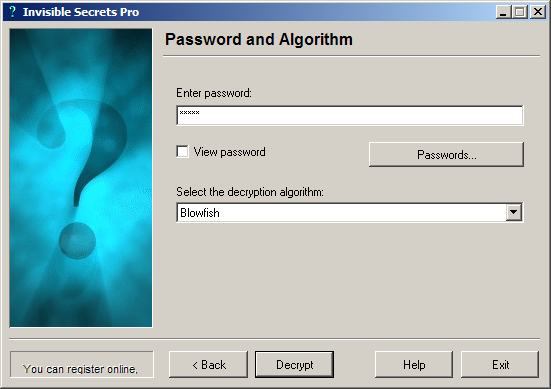
Теперь расшифруем полученный зашифрованный файл:



Выберем зашифрованный файл:



Введем пароль и выберем нужный алгоритм шифрования:



После этого файл будет расшифрован.

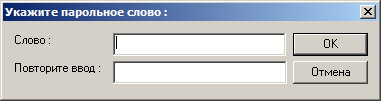
Загрузить пробную версию программы [Invisible Secrets Pro: etispro.exe](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\etispro.exe)

Просмотреть видеозапись работы с программой: [isp.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\isp.avi)

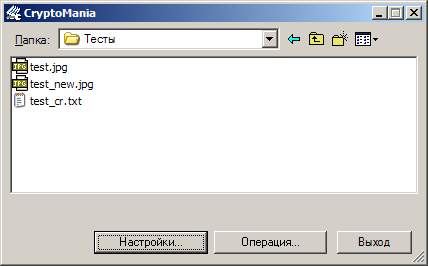
**ПРОГРАММА CRYPTOMANIA**

Российская разработка Cryptomania входит в комплекс средств защиты VIPNet. Она предназначена для шифрования файлов по российскому стандарту шифрования ГОСТ №28147-89.

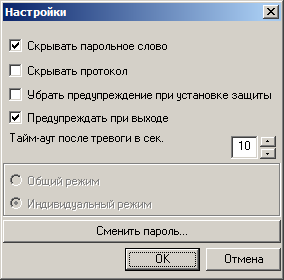
При входе в систему требуется ввести пароль, который по умолчанию будет использован в дальнейшем для шифрования и расшифрования данных:



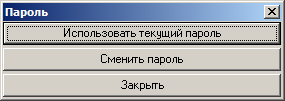
Далее необходимо выбрать файлы для шифрования:



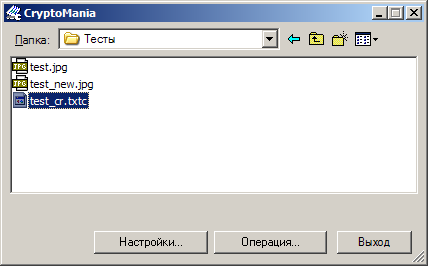
При этом можно изменить настройки по умолчанию (в том числе и пароль):



При выборе файла будет запрошен вариант использования пароля:



В результате файл будет зашифрован и получит измененное имя путем добавления символа "с" к разрешению:



Расшифрование производится аналогично.

Загрузить пробную версию программы Cryptomania: [Cryptomania 2\_0.exe](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\Cryptomania%202_0.exe)

Просмотреть видеозапись работы с программой: [cryptomania.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\cryptomania.avi)

