# Криптография

# Модуль 19

# Криптография

*Криптография – искусство и наука сокрытия информации в формате, не доступном для прочтения посторонним человеком.*

## Постановка задачи

Способность защищать и обеспечивать безопасность информации имеет жизненно важное значение для роста электронной коммерции и развития Интернета. Сегодня люди стремятся обеспечить безопасность работы средств связи и передачи данных в различных областях деятельности. Шифрование данных играет важную роль в этом процессе. Например, банки по всему миру используют методы шифрования для обработки финансовых транзакций, которые включают в себя перевод крупных сумм денежных средств из одного банка в другой. Банки также используют методы шифрования для защиты ПИН-кода своих клиентов во время проведения операций в банкомате. Существует также много компаний и даже торговых центров, которые продают все виды товаров (от цветов до бутылок вина) через Интернет. При этом все транзакции совершаются с помощью кредитных карт и безопасных интернет-браузеров с использованием методов шифрования. Клиенты, которые совершают покупки через Интернет, хотят быть уверенными в том, что соединение является безопасным, отправляя информацию о своей кредитной карте и других финансовых данных через глобальную сеть. Это возможно лишь с использованием надежных методов шифрования. Когда вы получите должность специалиста в области этичного хакинга и тестирования на проникновение, ваш IT-директор будет поручать вам шифровать данные с помощью различных алгоритмов шифрования в целях защиты данных организации.

## Цель работы

В ходе выполнения лабораторной работы вы научитесь шифровать данные и работать с ними, а также:

- использовать команды шифрования/дешифрования;
- создавать хеши и контрольные суммы файлов.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

## Среда

Для выполнения лабораторной работы вам понадобятся:

■ Компьютер под управлением **Window Server 2012;**

■ Веб-браузер и доступ в Интернет.

## Время выполнения

50 мин.

## Криптография

Криптография – это практика и изучение **сокрытия** информации. Современная криптография находится на пересечение таких дисциплин, как математика, информатика и электротехника. Термин «криптография» до недавнего времени считался синонимом термина «шифрование» – преобразования исходных данных в нечитаемый формат.

## Задачи

Перечень рекомендуемых лабораторных работ, которые могут Вам в изучении криптографии:

■ Шифрование данных с помощью **HashCalc.**

■ Шифрование данных с помощью **MD5 Calculator.**

■ Шифрование данных с помощью **Advance Encryption Package.**

■ Шифрование данных с помощью **TrueCrypt.**

■ Шифрование данных с помощью **CrypTool.**

■ Шифрование и дешифрование данных с помощью **BCTextEncoder.**

■ Шифрование данных с помощью **Rohos Disk Encryption.**

## Анализ

Проанализируйте и запишите результаты выполненной лабораторной работы. Выскажите свое мнение по поводу методов безопасности и уязвимости данных.


# Шифрование данных с помощью Hash Calc

*Программа HashCalc позволяет вычислять множество хешей, контрольных сумм и HMAC для файлов, текста и HEX-строк. Она поддерживает хеш-функции MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, а также хеш, используемый в инструментах eDonkey и eMule.*

## Постановка задачи

Ноутбуки, содержащие ценные данные, часто подвергаются краже. Чтобы зашифровать загрузочный диск необходимо создать ключ для дальнейшего запуска операционной системы и получения доступа к носителю. Как результат, шифруются все данные системы, включая файлы, папки и операционную систему. Это наиболее целесообразно, когда обеспечение безопасности системы на физическом уровне не гарантировано. Например, в случаи использования портативных или настольных компьютеров, которые  При правильной реализации шифрование обеспечивает повышенный уровень защиты данных, поскольку зашифрованные данные не могут просматриваться или иным образом обнаруживаться посторонними лицами в случае кражи, потери или перехвата данных. Чтобы стать экспертом в области этического хакинга и тестирования на проникновение, вы должны понимать процесс шифрования данных с использованием алгоритмов шифрования.

## Цель работы

В ходе выполнения лабораторной работы вы научитесь шифровать данные и работать с ними, а также:

- использовать команды шифрования/дешифрования;
- создавать хеши и контрольные суммы файлов.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

## Среда

Для выполнения лабораторной работы вам понадобятся:

- Программа **HashCalc** расположена в **D:\CEH-Tools\CEHv8Module 19Cryptography\MD5 Hash Calculators\HashCalc.**

■ Чтобы скачать последнюю версию HashCalc, перейдите по ссылке:
http:/Avww.slavasott.com/hashcalc/
■ При использовании **последней версии программы**, скриншоты в лабораторной работе могут отличаться.
■ Следуйте инструкциям мастера установки.
■ Запустите программу под управлением **Windows Server 2012.**
■ Для запуска программы необходимы права администратора.

## Время выполнения

10 мин.

## Обзор хеша

HashCalc – это быстрый и простой в использовании калькулятор, который предлагает на выбор 13 самых популярных хеш-функций и контрольных сумм для дайджеста файловых сообщений, и вычисления контрольной суммы.

## Задачи

1. Запустите меню **Start**, наведя курсор мыши на нижний левый угол рабочего стола.

HashCalc можно также скачать по ссылке: http://www.slavasoft.com


Рис. 1.1: Windows Server 2012— Рабочий стол

2. Нажмите на иконку **HashCalc,** чтобы открыть окно программы.

Интерфейс HashCalc создан для простых операций: перечисление входных данных и результатов.

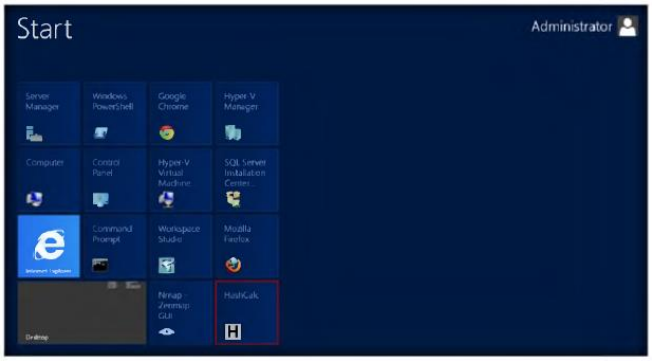


рис. 1.2: Windows Server 2012 — Программы

3. На экране появится главное окно **HashCalc,** как показано на следующем рисунке.
4. Из выпадающего списка **Data Format** выберите **File.**

Хеш-алгоритмы поддерживают три формата входных данных: файл, текст и HEX-строку.

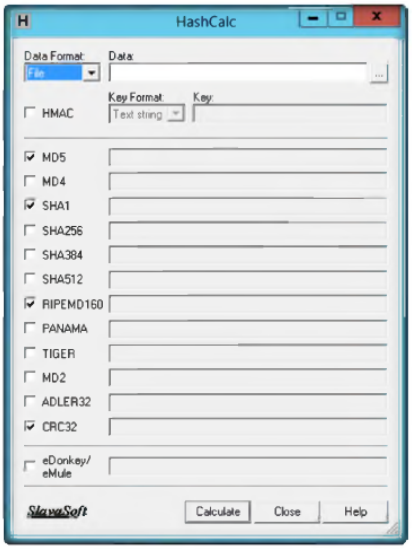


Рис. 1.3: Главное окно HashCalc

5. Введите / выберите данные для вычисления.
6. Выберите необходимый **алгоритм хеширования**, установив флажки.
7. Нажмите кнопку **Calculate.**

Программа HashCalc используется для создания зашифрованного текста.

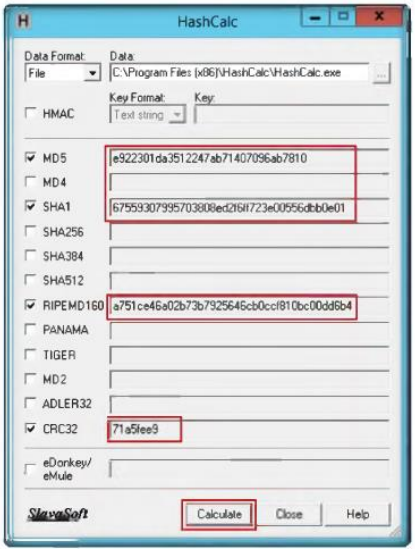


Рис. 1.4: Создание хеша для выбранной хеш-строки

# Анализ

Запишите все значения хеша, MD5 и CRC для дальнейшего использования.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| HashCalc | **Output:** Generated Hashes for<br>▪ MD5<br>▪ SHA1<br>▪ RIPEMD160<br>▪ CEC32 |

# Вопросы

1. Определите, как вычислять несколько контрольных сумм одновременно.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |


# Шифрование данных с помощью MD5 Calculator

*MD5 Calculator – простая программа, которая позволяет вычислить MD5-хеш файла, в том числе больших файлов (несколько ГБ). Она имеет индикатор хода выполнения процесса и текстовое поле, из которого можно скопировать MD5-хеш в буфер обмена.*

## Постановка задачи

Сегодня существует необходимость защищать данные от «посторонних глаз». В электронную эпоху информация, которая могла бы принести пользу, повышать осведомленность группы или отдельных лиц, может быть использована против них самих. Промышленный шпионаж среди высококонкурентных предприятий заставляет прибегнуть к принятию серьезных мер безопасности. К тому же желающие сохранить свободу личности перед лицом правительства, могут также пожелать зашифровать определенную информацию во избежание преследования. На самом деле, метод шифрования и дешифрования данных относительно прост. Алгоритмы шифрования используются для шифрования данных и безопасного хранения системных файлов от посторонних глаз. Чтобы стать экспертом в области этического хакинга и тестирования на проникновение, вы должны понимать процесс шифрования данных с помощью алгоритмов шифрования.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

## Цель работы

В ходе выполнения лабораторной работы вы научитесь шифровать данные и работать с ними, а также:

- использовать команды шифрования/дешифрования;
- вычислять значение MD5 выбранного файла.

## Среда

Для выполнения лабораторной работы вам понадобятся:

- Программа **MD5 Calculator** расположена в **D:\CEH-Tools\CEHv8Module19 Cryptography\MD5 Hash Calculators\MD5 Calculator**

■ Чтобы скачать последнюю версию **MD5 Calculator,** перейдите по ссылке: http://www.bullzip.com/products/md5/info.php
■ При использовании **последней версии программы**, скриншоты в лабораторной работе могут отличаться.
■ Следуйте инструкциям мастера установки.
■ Запустите программу под управлением **Windows Server 2012.**
■ Для запуска программы необходимы права администратора.

## Время выполнения

10 мин.

## MD5 Calculator

MD5 Calculator – это простая программа для **расчета и сравнения** файлов по алгоритму MD5. Несмотря на свою простоту, она дает быстрые и точные результаты.

## Задачи

1. Чтобы найти MD5-хеш любого файла, нажмите правой кнопкой мыши на файл и выберите **MD5 Calculator** из контекстного меню.

Контрольная сумма MD5 используется для создания MD5-хеша.

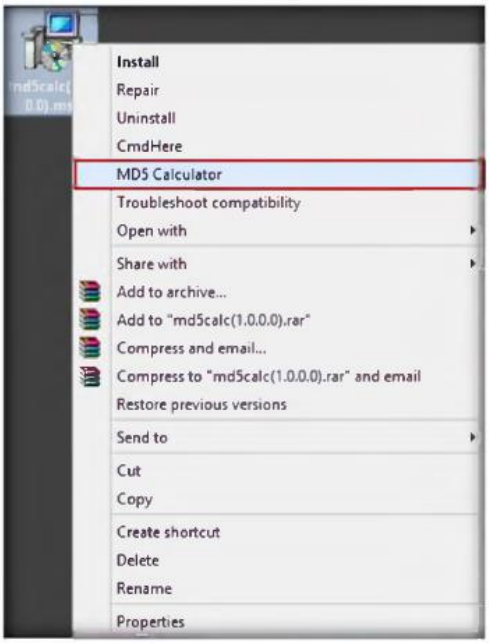


Рис. 2.1: Опция MD5 в контекстном меню

2. Программа **MD5 Calculator** показывает MD5 дайджест выбранного файла.

**Примечание:** Вы также можете выбрать любой файл для вычисления его MD5-хеша. Чтобы произвести вычисление, нажмите кнопку **Calculate**.

MD5-хеш (или контрольная сумма) функционирует в качестве компактного цифрового отпечатка файла.

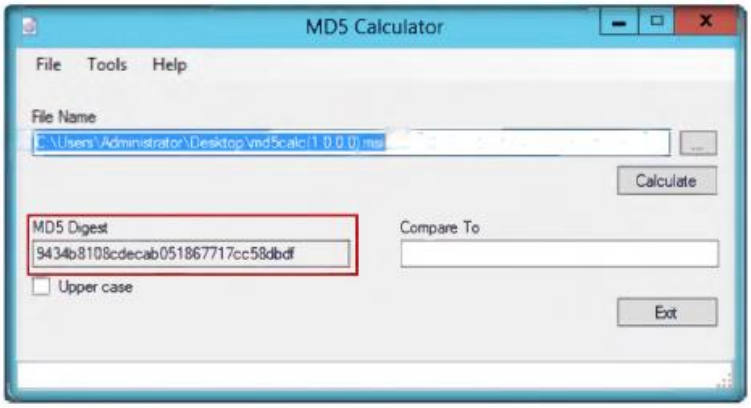


Рис. 2.2: Генерация MD5 для выбранного файла

## Анализ

Проанализируйте и запишите результаты выполненной лабораторной работы.

ПРИ ВОЗНИКНОВЕНИИ ДОПОЛНИТЕЛЬНЫХ ВОПРОСОВ, ОБРАТИТЕСЬ К ВАШЕМУ ПРЕПОДАВАТЕЛЮ.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| MD5 Calculator | **Output:** MD5 Hashes for selected software |

## Вопросы

1. Приведите пример аналогов программы **md5sum**, позволяющей вычислять значения контрольных сумм?
2. Является ли калькулятор MD5 (алгоритм по построению дайджеста сообщения 5) широко используемой криптографической хеш-функцией со 128-битным хеш-значением?

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |


# Шифрование данных с помощью Advanced Encryption Package

*Программа Advanced Encryption Package наиболее примечательна своей гибкостью. С ее помощью вы можете не только зашифровать файлы в целях их защиты, но и создать версии файлов, которые не нуждаются в дешифровании с помощью Advanced Encryption Package или другого программного обеспечения.*

## Постановка задачи

Основными методами, которые обеспечивают безопасность и защиту данных, являются шифрование и дешифрование. Большинство систем используют блочные шифры такие как AES (симметричный алгоритм блочного шифрования), однако их реализации, а также реализация других криптографических алгоритмов подвержены атакам по сторонним каналам. Эти атаки позволяют злоумышленникам извлекать секретные ключи из устройств путем пассивного мониторинга энергопотребления и других побочных каналов. Применение контрмер необходимо в таких приложениях, где атаки по побочным каналам представляют серьезную угрозу. К ним относятся несколько военных и аэрокосмических приложений, в которых информация о программе, секретные данные, алгоритмы и секретные ключи хранятся в файлах, физическая защита которых не может быть гарантирована. Чтобы стать экспертом в области этического хакинга и тестирования на проникновение, вы должны научиться работать с файлами зашифрованных данных.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

## Цель работы

В ходе выполнения лабораторной работы вы научитесь шифровать данные и работать с ними, а также:

- использовать команды шифрования/дешифрования;
- вычислять зашифрованное значение выбранного файла.

## Среда

Для выполнения лабораторной работы вам понадобятся:

- Программа **Advanced Encryption Package** расположена в **D:\CEH-Tools\CEHv8Module 19 Cryptography\Cryptography Tools\Advanced EncryptionPackage**
- Чтобы скачать последнюю версию **Advanced Encryption Package,** перейдите по ссылке: http://www.secureaction.com/encryptionpro/

■ При использовании **последней версии программы**, скриншоты в лабораторной работе могут отличаться.
■ Следуйте инструкциям мастера установки.
■ Запустите программу под управлением **Windows Server 2012.**
■ Для запуска программы необходимы права администратора.

## Время выполнения

10мин.

## Advanced Encryption Package

Програма **Advanced Encryption Package** включает в себя инструмент **File Shredder**, который предназначен для удаления файлов. Она также интегрируется с **Windows Explorer**, позволяя использовать контекстное меню проводника и исключить перекрытие экрана другим окном.

## Задачи

1. Запустите меню **Start**, наведя курсор мыши на нижний левый угол рабочего стола.

Advance Encryption Package можно также скачать по ссылке: http://www.secureaction.com


Рис. 3.1: Windows Server 2012— Рабочий стол

2. Нажмите на иконку **Advanced Encryption Package,** чтобы открыть окно программы.

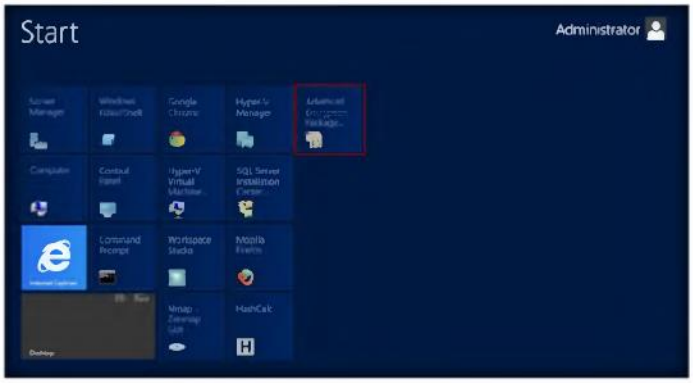


FIGURE 3.2: Windows Server 2012 – Apps

3. На экране появиться окно пробной версии программы **Register Advanced Encryption Package 2013**. Нажмите кнопку **Try Now!**.

Программа Advance Encryption Package проста в использовании для новичков.


Рис. 3.3: Окно активации

4. На экране появится главное окно программы **Advanced Encryption Package**, как показано на следующем рисунке.

Advanced Encryption Package – программа симметричного шифрования, которая включает в себя три блочных шифра: AES-128, AES-192 и AES-256.

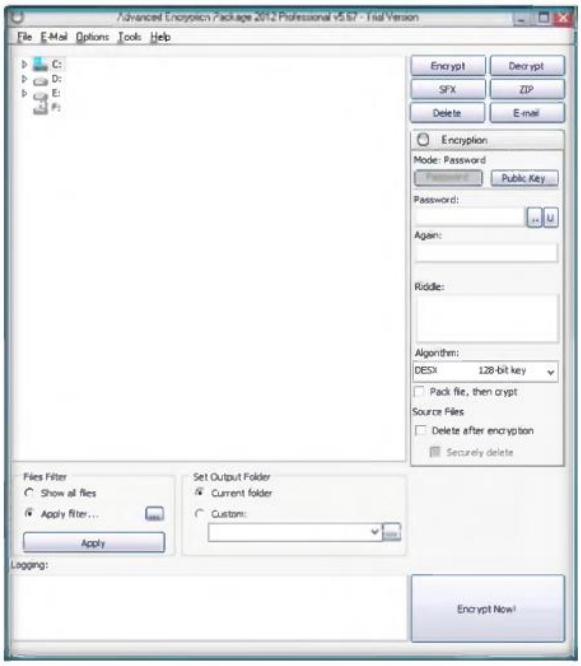


Рис. 3.4: Окно приветствия Advance Encryption Package

5. Выберите образец файла для шифрования. Файл находится в **D:\CEHTools\CEHv8Module19Cryptography\Cryptography Tools\AdvancedEncryptionPackage**.

6. Нажмите кнопку **Encrypt**. После необходимо будет ввести пароль. Введите пароль в **поле Password**, а затем повторите ввод пароля в поле **Again**.

7. Нажмите кнопку **Encrypt Now!**.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

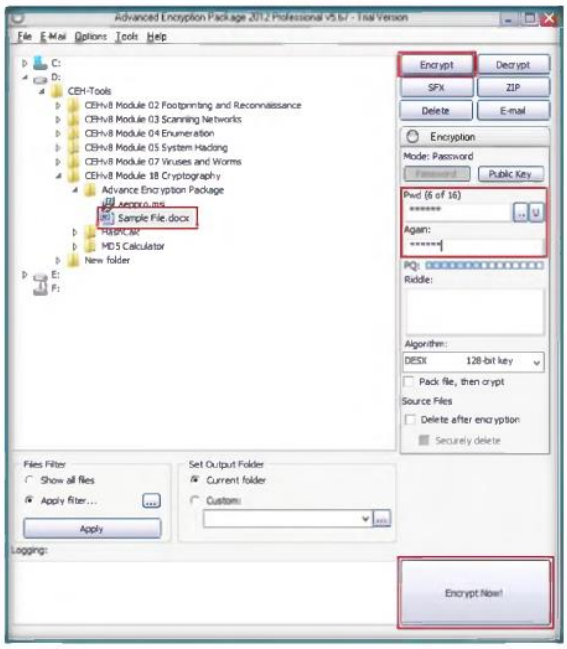


Рис. 3.5: Окно приветствия Advance Encryption Package

8. Место расположения зашифрованного образца файла соответствует месту расположения исходного файла, как показано на следующем рисунке.

Программа создает зашифрованные самораспаковывающиеся файлы для отправки в качестве вложений электронной почты.

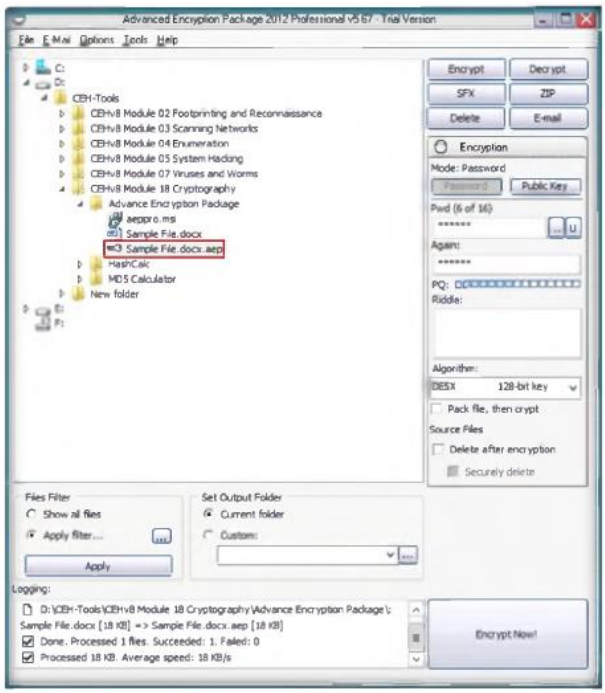


Рис. 3.6: Шифрование выбранного файла

9. Выберите зашифрованный файл, чтобы расшифровать его. Нажмите кнопку **Decrypt**; после необходимо будет ввести пароль.
10. Нажмите кнопку **Decrypt Now!**.

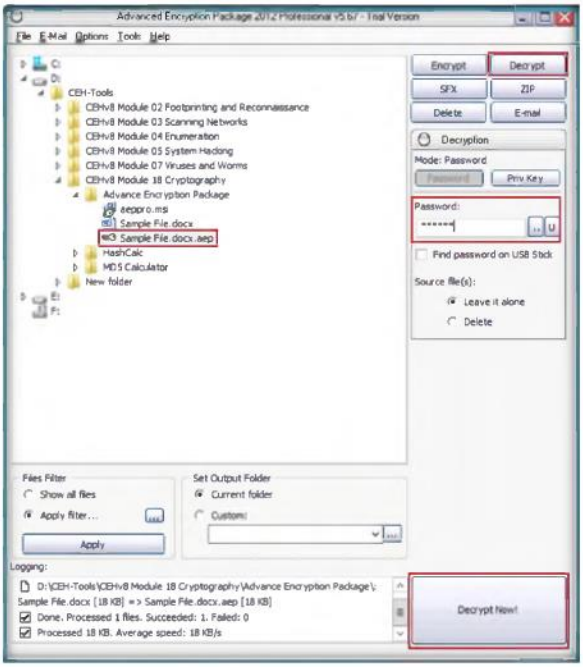


Рис. 3.7: Расшифровка выбранного файла

## Анализ

Проанализируйте и запишите результаты выполненной лабораторной работы.

ПРИ ВОЗНИКНОВЕНИИ ДОПОЛНИТЕЛЬНЫХ ВОПРОСОВ, ОБРАТИТЕСЬ К ВАШЕМУ ПРЕПОДАВАТЕЛЮ.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Advance Encryption Package | **Output:** Encrypted simple File.docx.ape |

## Вопросы

1. Какой алгоритм использует программа Advanced Encryption Package для защиты конфиденциальных документов?
2. Есть ли другой способ защитить приватный ключ, кроме пароля?

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |


# Шифрование данных с помощью TrueCrypt

*TrueCrypt – это компьютерная программа для создания и поддержки зашифрованных данных диска «на лету» (устройство хранения данных). Шифрование «на лету» означает, что данные автоматически вводятся или дешифруются прямо перед загрузкой или сохранением, без какого-либо вмешательства пользователя.*

## Постановка задачи

CiTx – это компания с миллиардным оборотом, которая не хочет искушать судьбу, рискуя конфиденциальной информацией о партнерах, клиентах и финансах, хранящимися на ее ноутбуках. Компания CiTx не может допустить утечку всех данных к кому-либо из своих конкурентов, поэтому она прибегла к полному шифрованию диска, чтобы защитить свои данные от посторонних глаз. Полное шифрование диска шифрует все данные в системе, включая файлы, папки и операционную систему. Это наиболее целесообразный подход, если невозможно обеспечить физическую безопасность системы. Для шифрования и дешифрования данных в целях их защиты используется один или несколько криптографических ключей.

## Цель работы

В ходе выполнения лабораторной работы вы научитесь шифровать данные и работать с ними, а также:

- использовать команды шифрования/дешифрования;
- создавать виртуальный зашифрованный диск с файлом.

**Инструменты лабораторной работы доступны в D:\CEHTools\ CEHv8 Module 19 Cryptography**

## Среда

Для выполнения лабораторной работы вам понадобятся:

- Программа **TrueCrypt** расположена в **D:\CEH-Tools\CEHv8 Module 19Cryptography\Disk Encryption Tools\TrueCrypt**
- Чтобы скачать последнюю версию **TrueCrypt,** перейдите по ссылке: http://www.truecrypt.org/downloads
- При использовании **последней версии программы**, скриншоты в лабораторной работе могут отличаться.
- Следуйте инструкциям мастера установки.

■ Запустите программу под управлением **Windows Server 2012.**
■ Для запуска программы необходимы права администратора.

## Время выполнения

10 мин.

## TrueCrypt

TrueCrypt – это бесплатна программа с открытым исходным кодом для шифрования «на лету». С ее помощью можно создать виртуальный зашифрованный диск в виде файла или зашифровать раздел диска, или все устройство хранения.

## Задачи

1. Запустите меню **Start**, наведя курсор мыши на нижний левый угол рабочего стола.


Рис. 4.1: Windows Server 2012— Рабочий стол

TrueCrypt можно также скачать по ссылке: http://www. truecrypt.org

2. Нажмите на иконку **TrueCrypt,** чтобы запустить окно программы.

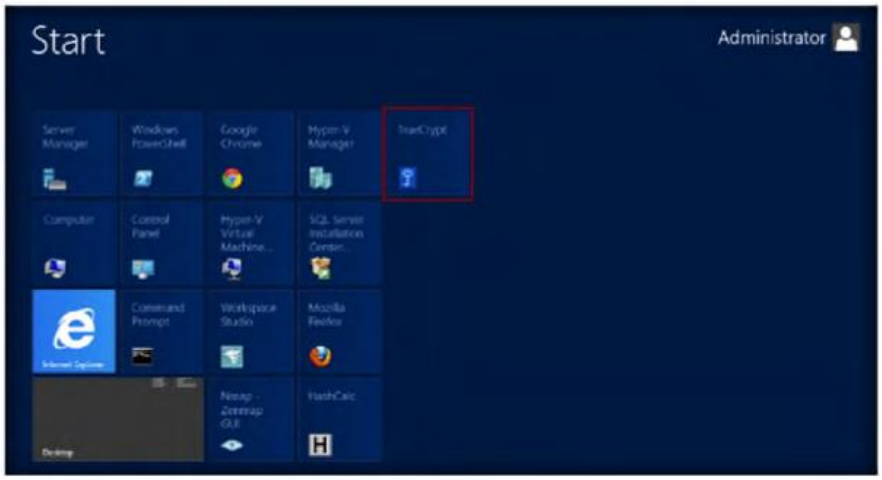


Рис. 4.2: Windows Server 2012 – Программы

TrueCrypt – программа для шифрования «на лету». Она бесплатная, а ее исходный код находится в открытом доступе.

3. На экране появится главное окно программы **TrueCrypt**.
4. Выберите том (диск) для шифрования, и нажмите кнопку **Create Volume**.

TrueCrypt позволяет создавать скрытую операционную систему, существование которой невозможно подтвердить.

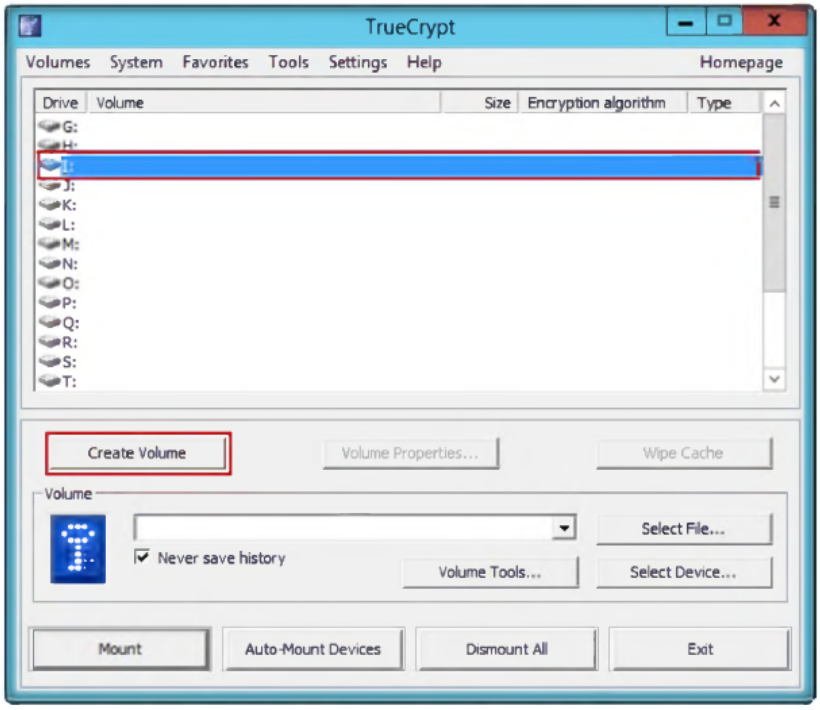


Рис. 4.3: Главное окно TrueCrypt с опцией Create Volume

5. На экране появится окно **TrueCrypt Volume Creation Wizard**.
6. Выберите опцию **Create an encrypted file container**, которая создаст виртуальный зашифрованный диск в файле.

ВАЖНО: TrueCrypt не будет шифровать существующие файлы (при создании файлового контейнера TrueCrypt). Если вы выберете существующий файл на этом шаге, он будет перезаписан и заменен вновь созданным томом (поэтому перезаписанный файл будет утерян, а не зашифрован). Вы сможете зашифровать существующие файлы (позже), переместив их в том TrueCrypt, который мы создаем сейчас.

7. По умолчанию выбран параметр **Create an encrypted file container**. Чтобы продолжить, нажмите кнопку **Next**.

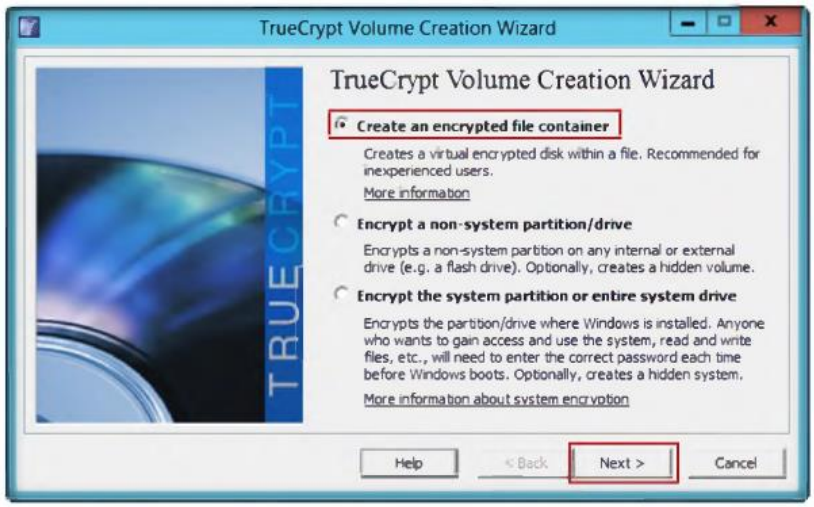


Рис. 4.4: TrueCrypt Volume Creation Wizard-Create Encrypted File Container

8. На следующем шаге мастера установки выберите тип тома.
9. Выберите **Standard TrueCrypt volume,** чтобы создать **обычный том** TrueCrypt.
10. Чтобы продолжить, нажмите кнопку **Next**.

Внимание! После копирования существующих незашифрованных файлов на том TrueCrypt необходимо безопасно удалить (стереть) исходные незашифрованные файлы с помощью программных инструментов (многие из них бесплатны).


Рис. 4.5: TrueCrypt Volume Creation Wizard-Volume Type

11. На следующем шаге мастера установки появится окно **Volume Location**.
12. Нажмите кнопку **Select File...**

TrueCrypt придерживается концепции правдоподобного отрицания.

*В криптографии к правдоподобному отрицанию принято относить возможность отрицания самого факта шифрования или возможность предъявления ключа шифрования, который расшифровывает лишь отвлекающие несекретные данные.


Рис. 4.6: TrueCrypt Volume Creation Wizard-Volume Location

13. На экране появится селектор файла Windows. Окно **TrueCrypt Volume Creation Wizard** останется открытым в фоновом режиме.
14. Выберите **место размещения**; укажите имя файла в поле **File name** и нажмите кнопку **Save**.

TrueCrypt использует режим XTS для зашифрованных разделов диска, дисков и виртуальных томов.

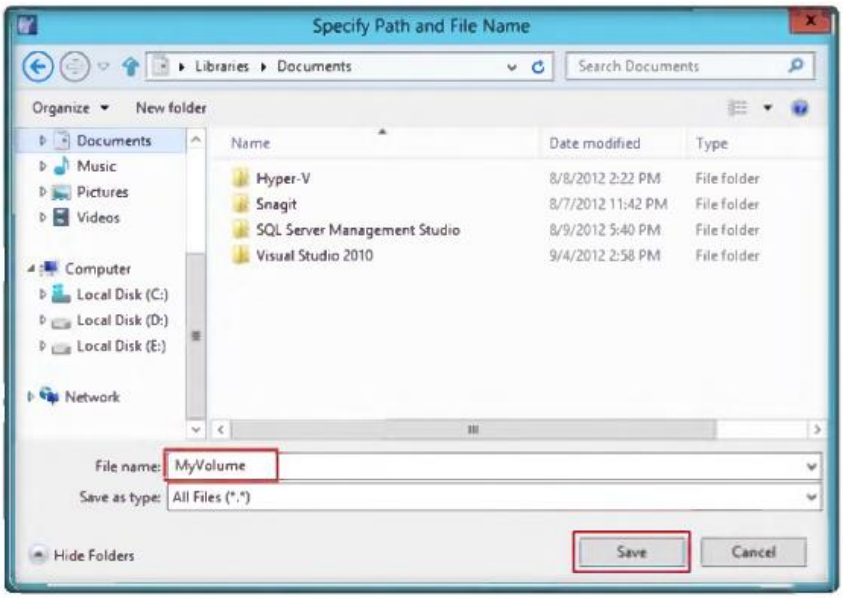


Рис. 4.7: Windows Standard - Окно Specify Path and File Name

15. После сохранения файла, вы вернетесь к окну **Volume Location**. Чтобы продолжить, нажмите кнопку **Next**.

Тома True Crypt не содержат заголовков файлов, а их содержимое ничем не отличается от случайных данных.

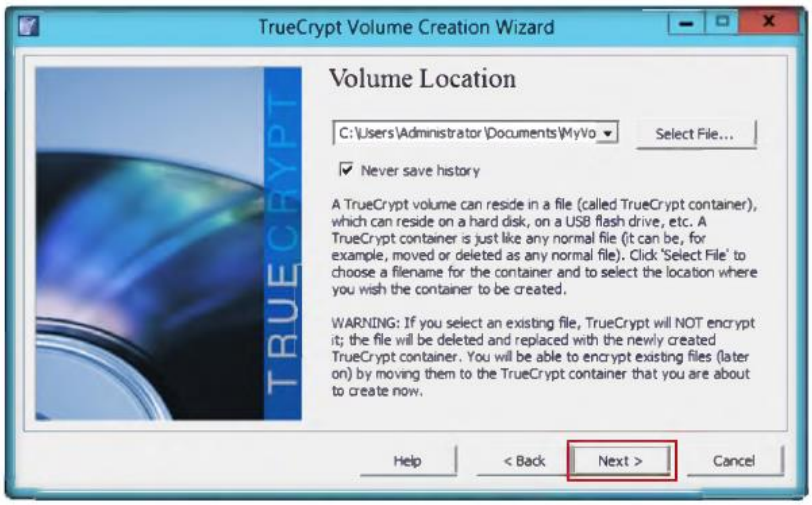


Рис. 4.8: TrueCrypt Volume Creation Wizard - Окно Volume Location

16. На следующем шаге мастера установки появится окно **Encryption Options**.

17. Выберите алгоритм шифрования **AES** и алгоритм хеширования **RIPEMD-160;** нажмите кнопку **Next**.

TrueCrypt использует следующие алгоритмы хеширования:
- RIPEMD-160;
- SHA-512;
- Whirlpool.

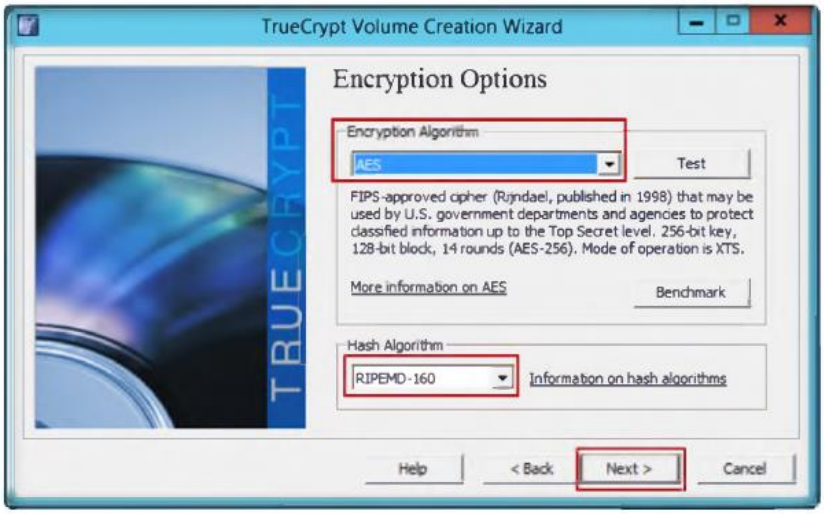


Рис. 4.9: TrueCrypt Volume Creation Wizard - Окно Encryption Options

18. На следующем шаге мастера установки появится окно **Volume Size**.
19. Задайте размер зашифрованного тома в **2** МБ и нажмите кнопку **Next**.

Примечание: Кнопка Next станет активной при условии, что пароли в обоих полях ввода будут одинаковыми.

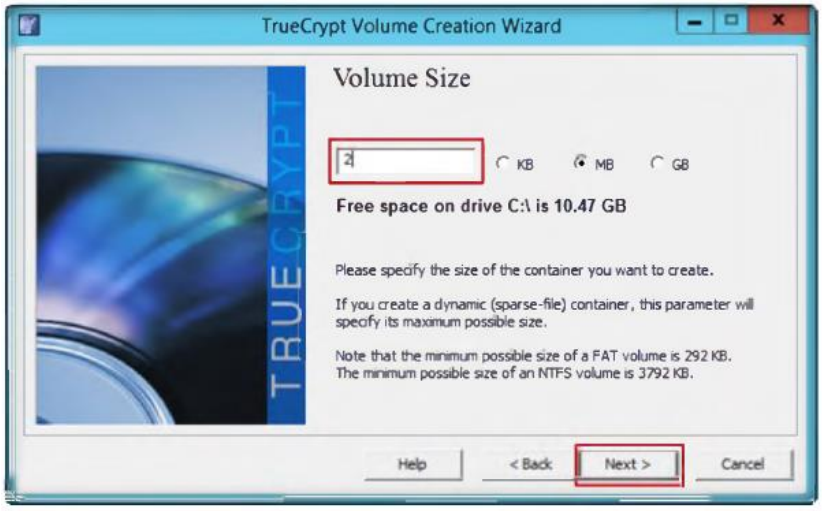


Рис. 4.10: TrueCrypt Volume Creation Wizard-Окно Volume Size

20. На экране появится окно **Volume Password**. Внимательно прочтите информацию, отображенную в окне мастера установки, касательно надежности пароля.
21. Введите надежный пароль в первое поле ввода, повторно введите его в поле **Confirm** и нажмите кнопку **Next**.

Чем дольше вы будете двигать мышью, тем лучше. Это действие значительно увеличивает криптографическую стойкость шифрования.


Рис. 4.11: TrueCrypt Volume Creation Wizard - ОкноVolume Password

22. На экране появится окно **Volume Format**. Выберите из выпадающего списка **Filesystem** систему **FAT**, а значение **Cluster** установите **Default**.
23. Перемещайте указатель мыши в окне **Volume Creation** мастера установки не менее 30 секунд для генерации случайных данных, которые помогут увеличить стойкость шифрования.
24. Нажмите кнопку **Format**.

Зашифрованные тома TrueCrypt не имеют характерных подписей или строк идентификатора. Они состоят из набора случайных данных.

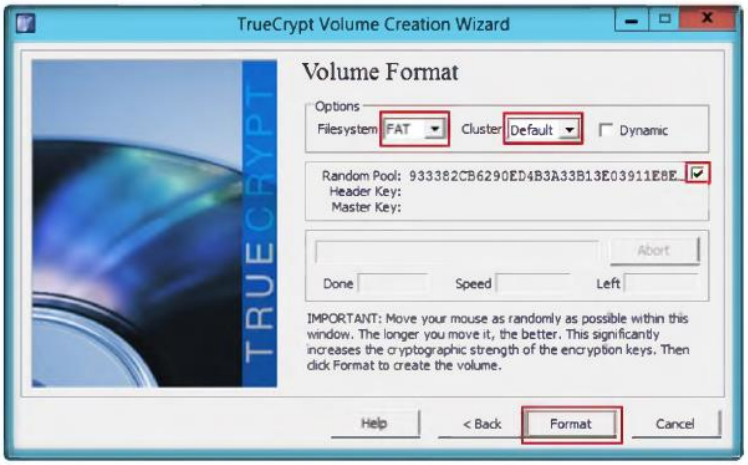


Рис. 4.12: TrueCrypt Volume Creation Wizard - Окно Volume Format

25. После нажатия кнопки **Format** начнется создание диска. Программа **TrueCrypt** создаст файл под названием **MyVolume** в указанной папке, который будет зависеть от контейнера TrueCrypt (файл будет содержать зашифрованный том TrueCrypt).
26. Время создания диска зависит от его размера. После его завершения появится следующее диалоговое окно.


Рис. 4.13: TrueCrypt Volume Creation Wizard- Диалоговое окно Volume Successfully Created

27. Чтобы закрыть диалоговое окно, нажмите кнопку **OK.**
28. Создание тома TrueCrypt успешно завершено (файлового контейнера).
29. В окне мастера установки **TrueCrypt Volume Creation**, нажмите кнопку **Exit**.


Рис. 4.14: TrueCrypt Volume Creation Wizard- Окно Volume Created

30. Чтобы смонтировать том в системе, запустите программу **TrueCrypt**.
31. В главном окне программы **TrueCrypt**, нажмите кнопку **Select File...**

Если злоумышленник имеет физический доступ к компьютеру, то TrueCrypt не может обеспечить защиту данных.