# Exercise 1.1: Shift cipher

Convert the following cipher text back into plain text using a method of your choice:

Jrypbzr gb gur jbeyq bs pelcgbtencul! Gur zrffntr lbh ner ernqvat vf pbqrq hfvat EBG13. Guvf vf n xvaq bs Prnfne fuvsg, hfvat n guvegrra ebgngvba. Va gur rneyl qnlf bs gur arg, guvf jnf cbchyneyl hfrq nf gur rneyl vagrearg'f rdhvinyrag bs hcfvqr-qbja jevgvat.

Frr gur yvax sbe zber vasb:

uggc://jjj.fvzbafvatu.arg/Gur\_Oynpx\_Punzore/pnrfne.ugzy

# Exercise 1.2: Substitution

Convert the following cipher text back into plain text using grammatical and frequency analysis:

Search online for a frequency generator and use this website to decode it: https://spyrosoft.com/tools/manual-cipher-decoder.html

Don’t use an automatic solver.

What is the first line of the speech, who said it and when?

Ipxn Svuvvbf bf vku Htwvbe vx Vpbusvu bf vku Tqpbtvbe, tf bpxf elpvtbf kts quseufquq tepxss vku Exfvbfufv. Hukbfq vktv wbfu wbu tww vku etjbvtws xi vku tfebufv svtvus xi Eufvptw tfq Utsvupf Ulpxju. Ztpstz, Hupwbf, Jptclu, Abufft, Hlqtjusv, Huwcptqu, Hlektpusv tfq Sxibt, tww vkusu itnxls ebvbus tfq vku jxjlwtvbxfs tpxlfq vkun wbu bf zktv B nlsv etww vku Sxabuv sjkupu, tfq tww tpu slhruev bf xfu ixpn xp tfxvkup, fxv xfwd vx Sxabuv bfiwlufeu hlv vx t aupd kbck tfq, bf ntfd etsus, bfeputsbfc nutslpu xi exfvpxw ipxn Nxsexz. Tvkufs twxfu - Cpuueu zbvk bvs bnnxpvtw cwxpbus - bs ipuu vx quebqu bvs ilvlpu tv tf uwuevbxf lfqup Hpbvbsk, Tnupbetf tfq Ipufek xhsupatvbxf. Vku Plssbtf-qxnbftvuq Jxwbsk Cxaupfnufv kts huuf ufexlptcuq vx ntou ufxpnxls tfq zpxfcilw bfpxtqs ljxf Cupntfd, tfq ntss uyjlwsbxfs xi nbwwbxfs xi Cupntfs xf t setwu cpbuaxls tfq lfqputnuq-xi tpu fxz vtobfc jwteu. Vku Exnnlfbsv jtpvbus, zkbek zupu aupd sntww bf tww vkusu Utsvupf Svtvus xi Ulpxju, ktau huuf ptbsuq vx jpu-unbfufeu tfq jxzup itp hudxfq vkubp flnhups tfq tpu suuobfc uaupdzkupu vx xhvtbf vxvtwbvtpbtf exfvpxw. Jxwbeu cxaupfnufvs tpu jpuatbwbfc bf futpwd uaupd etsu, tfq sx itp, uyeujv bf Eguekxswxatobt, vkupu bs fx vplu qunxepted.

# Exercise 2: One Time Pad

Once the instructor has demonstrated modular arithmetic with a modulus of 26, use the One Time Pad below to encrypt a short message and pass it to your contact. Decrypt your partner’s message as well.

zjgwh rktcz fclhy

wnrlt ehdks fqfck

nuvbg zuzxm acsus

sguqc epweo kanvn

bowhy apxyo yuvdp

aloux puciz warxc

# Exercise 3: Enigma

Following a demo of the Enigma machine by the instructor, use the machine to send an encrypted message to your partner.

# Setup

* Set up the Enigma machine using the settings of the day below
  + Wehrmacht UKW - B Enigma machine
  + Walzenlage ist V, III, I (Rotors to use and the order)
  + Ringstellung ist 06,22,14 (setting for each ring - before you put them in)
  + Steckerverbinungen ist AD, BZ, UX, NK, EV (match pairs of letter on the plug board)
  + Kenngruppen ist 16,14,11 (PNK ) (Daily message setting - with the Enigma closed set the three rotors to start here)

# Day settings

* Choose a 3 letter code – don’t make any changes to the Enigma machine yet
* Type your 3 letter code twice and record the 6 letters below – (this is Part A)

……………………………………………………………………………………………………………………………………………………………

# Encrypting your message

* Now change your rotor start positions to the 3 letter code (from Part A)
* Encrypt your message recording the ciphertext below – (this is Part B)

……………………………………………………………………………………………………………………………………………………………

* Write down the 6 letters from Part A first, followed then by the remaining letters from Part B on a piece of paper, separating Part B into chunks of 4 letters at a time
  + E.g. XXXXXX (part a) XXXX XXXX XXXX XXXX (part b)
* Forward this paper to your partner for them to decrypt
* Decrypt the message they pass to you

……………………………………………………………………………………………………………………………………………………………

# Exercise 4: Hashing

In this exercise use Cain, WinMD5 and Hashkiller.co.uk to calculate and compare hash results.

1. Go to Windows start -> Programs -> Cain.
2. Once Cain is open accept any warnings, and click Tools -> Hash Calculator
3. When the hash calculator type in the word “**Cisco**” (without quotes) and note the MD5 value created.

1. Next open WinMD5 and create an MD5 hash of Message1.txt
2. Paste the MD5 checksum value below

…………………………………………………………………………………………………………………………

1. The using WinMD5 create a MD5 hash of the Message1\_upd.txt file
2. Paste the MD5 checksum value below

…………………………………………………………………………………………………………………………

There are numerous online websites that can compare user-provided hashes against a database of stored hashes. In this instance we will be using <http://www.hashkiller.co.uk/>, which claims to provide over hundreds of Billions of MD5 hashes within its database.

1. Enter the hashes you generated in tasks 1 and 2 and place the plaintext results below

Message1txt content = ………………………………………………

Message1\_upd.txt content = ……………………………………..

1. Notice that there is a vast difference in the hash values and yet the plaintext is nearly identical apart from capitalisation one letter.
2. Generate an MD5 hash of message 2.txt

…………………………………………………………………………………………………………………………..

1. Using <http://www.hashkiller.co.uk/>, search for a match of the resulting hash. What is the result and why do you think this is the case?

1. For validation purposes you may wish to compare the results by hashing the above files using SHA1 instead, you can do this using Cain and other online tool such as <http://www.sha1-online.com/>
2. How do SHA1 hashes of the same file compare with MD5?

# Exercise 5: Certificates

In this exercise, you will be researching the possibility of purchasing a 2-year SSL certificate for use on your e-commerce web site. Your instructor will provide you with the name of the certificate authority to investigate. Prepare your answers for class discussion.

* Your instructor will give you the name of a certificate authority to investigate. Record that information below
* Locate their main home page and record the URL below
* Do they offer an SSL certificate for an e-commerce web site?
* What is the price for a 2-year SSL certificate?
* Do they offer an EV certificate? If so how much is it?
* What additional features are available when purchasing a standard domain or EV certificate? What does the authority add to the bundle?
* What difference will an EV certificate have for your business?
* Locate a web site that has an EV certificate installed and record that site below

# Exercise 6: Analysing TLS traffic

In this lab you are using Wireshark to investigate TLS traffic on the network.

In order to answer the questions below you will need to investigate the packet information and packet details of the communication using column filters in the packet list (top pane) and expansion of the dissectors in the packet details (middle pane).

* Open the Ex6\_samplehttps PCAP file using Wireshark
* What are the IP addresses of the two devices?
* What is the name of page the client is visiting?
* Using the Client Hello packet - what is the first-choice cipher suite offered by the browser?
* Using the Server Hello packet - what is the cipher suite agreed for this conversation?
* Which (fictional) Certification Authority issued the certificate used by the site?
* What is the name of page the client is visiting over TLS?
* Can you read the content of the page?

# Exercise 7: Using PGP for encrypted messages

In this exercise, you will install and configure PGP software and then share your public key. After creating a message, you will use your private key to help encrypt your message for your partner to decrypt using your shared public key.

## Generate and share key

* Install Portable PGP using PortablePGP-setup.exe and follow the instructions to create a Private and Public key pair. **Run the program as Admin (right click the icon and select “Run as Administrator”)**
* **Select Generate a new key pair – the 1st icon**
* Do not use real email addresses or personal details, this is just for practice
* Use a key size of 1024 bits and choose a simple password you will remember – accept the warning
* Once created you will notice both a new public and private key pairing – note the prefix for this key pair will match e.g. [0xE7108819]
* **Select your** **public key** and **export it using the Save icon**. Name it in the format *FirstnameLastInitial.key* e.g. John Doe would have *johnd.key*. Upload it to the Instructor share/web server – the instructor will write this address on the whiteboard

## Obtain Partner key and import

* Download the shared public key for your partner from the same shared location and add this into Portable PGP using the **Import** icon above the Public Keys pane
* Your partner will perform the same exercise and import your public key into their Portable PGP application. You both now have each other’s public keys, so messages subsequently encrypted using your own private key can be decrypted by your partner with the public key you have shared

## Creating an encrypted message

* Select the **encrypt** option, leave the **encrypt text** radio button selected and type your message
* **Select** the **target drop down box** and **select** your **partners public key** to encrypt the message and press the **encrypt** button
* **Save** this as a text file using the naming convention of securemessageforX where X is your partners name and upload this message to the classroom share
* Inform your partner that their encrypted message is now available

Continued…

## Decrypting your partners message

* Download the message encrypted for you by your partner
* Open the file using notepad and copy the entire contents to the clipboard – the message should say **begin PGP** etc… followed by non-readable content
* **Select** the **decrypt** option in Portable PGP and copy the contents of the clipboard into the **decrypt ASCII armoured text file** area and press **decrypt**
* Enter your passphrase if you chose one earlier, otherwise just press **OK**
* A Text Editor window will appear showing the decrypted message

# Exercise 8: File and disk encryption using VeraCrypt

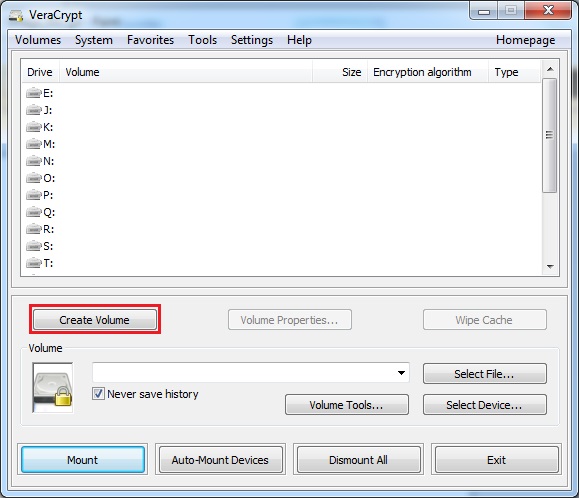
In this exercise you will be using VeraCrypt to create a new virtual drive within C:\ and mount this new volume as drive letter M:\ .

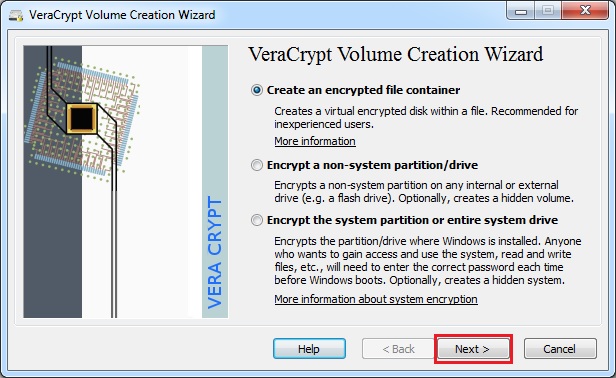
All files saved to this new location will be encrypted.

Part 1 – Create a folder to hold your encrypted volume

Part 2 – Install VeraCrypt

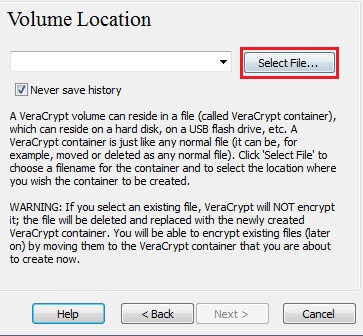
Part 3 – Create mount and use a VeraCrypt volume

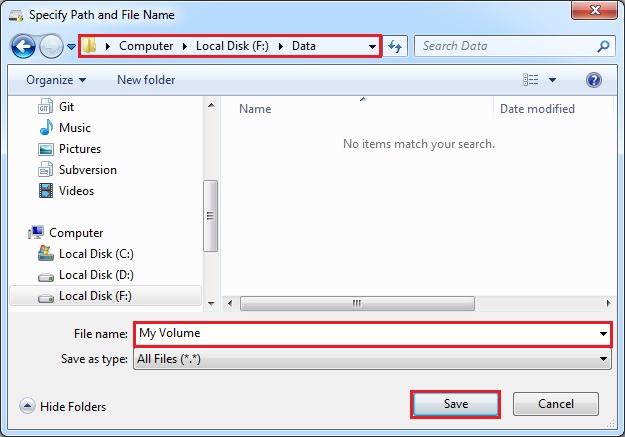
* Anywhere on your desktop right-click and select New -> Folder. Name the folder “Data”
* Install VeraCrypt using the default settings
* Run VeraCrypt and select create volume

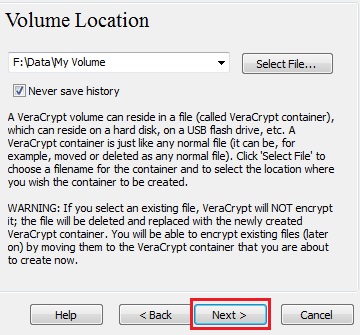


* In this step you need to choose where you wish the VeraCrypt volume to be created. A VeraCrypt volume can reside in a file, which is also called container, in a partition or drive. In this lab we will choose the first option and create a VeraCrypt volume within a file
* Select standard VeraCrypt volume

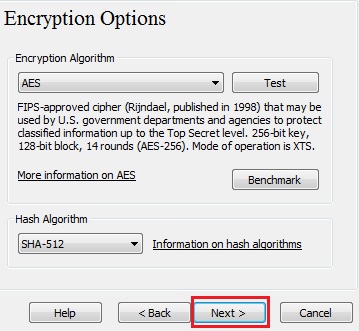


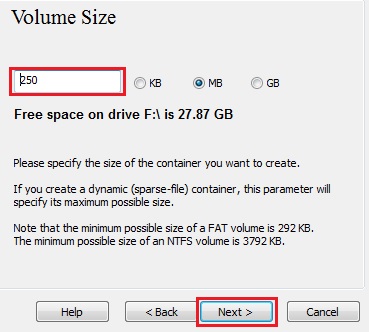


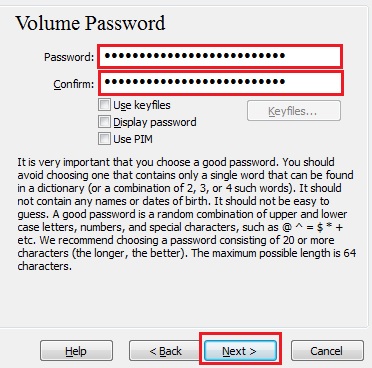
* In this step you have to specify where you wish the VeraCrypt volume (file container) to be created. Note that a VeraCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step
* Click **Select File**. The standard Windows file selector should appear (while the window of the VeraCrypt Volume Creation Wizard remains open in the background)  
    
    
  
* Create the VeraCrypt volume in the folder **Data** that you created earlierand the filename of the volume (container) will be ***My Volume***(your screenshot may have a different path). You may, of course, choose any other filename and location you like (for example, on a USB memory stick). Note that the file *My Volume*does not exist yet – VeraCrypt will create it
* IMPORTANT: Note that VeraCrypt will *not*encrypt any existing files (when creating a VeraCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be *lost*, *not*encrypted). You will be able to encrypt existing files (later on) by moving them to the VeraCrypt volume that we are creating now
* Click **Save**. The file selector window should disappear.
* Select the desired path (where you wish the container to be created) in the file selector. Type the desired container file name in the **File name**box

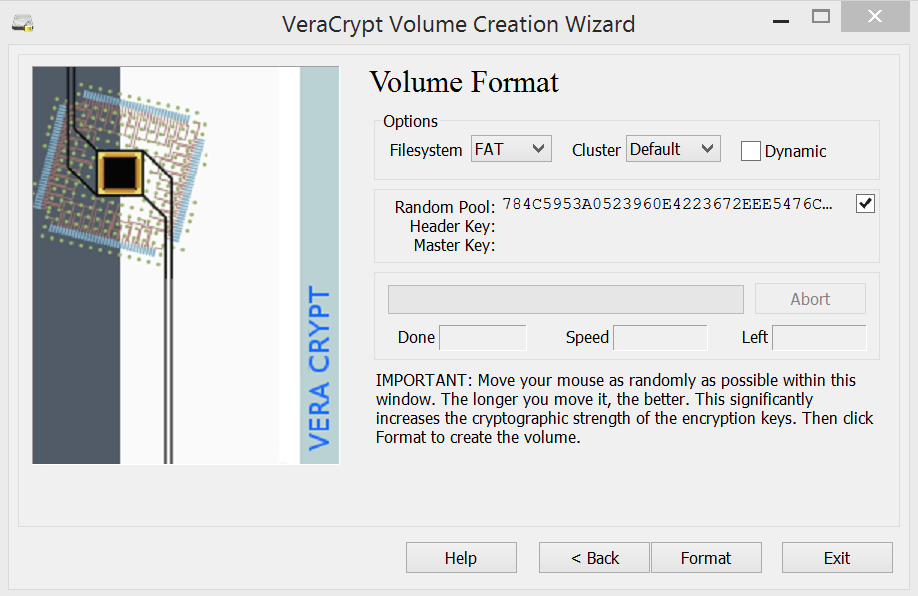
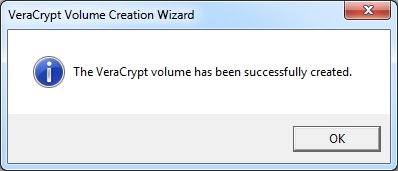
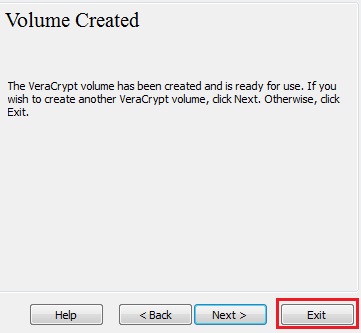
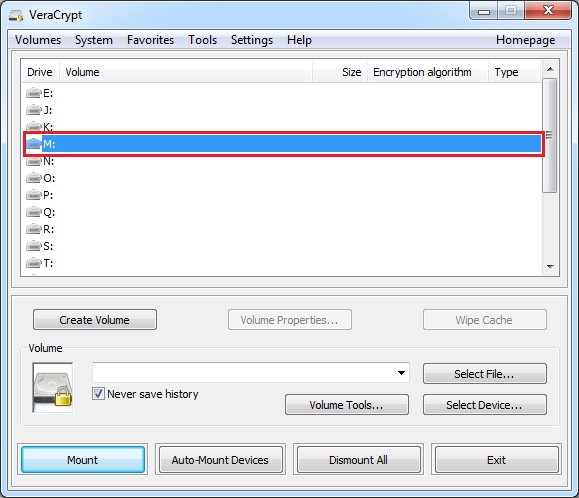


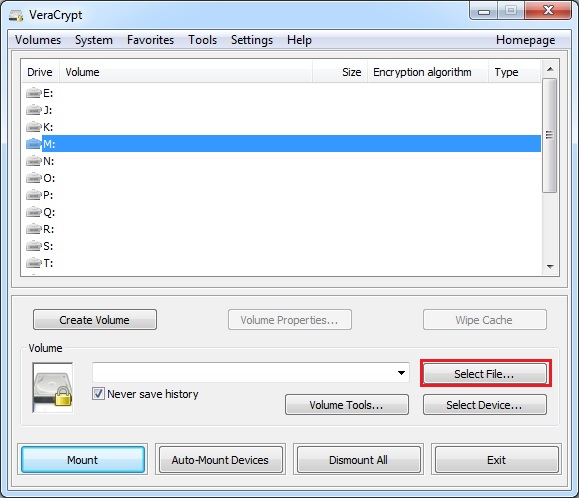
* In the Volume Creation Wizard window, click **Next**  
    
  .

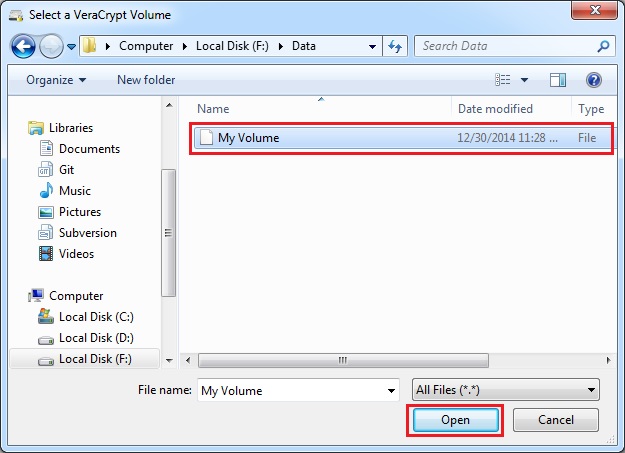
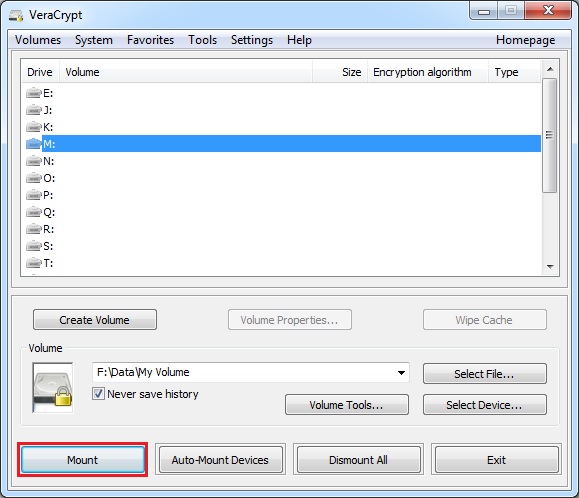
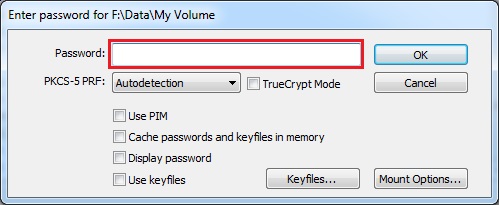
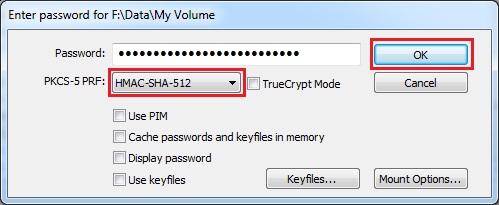
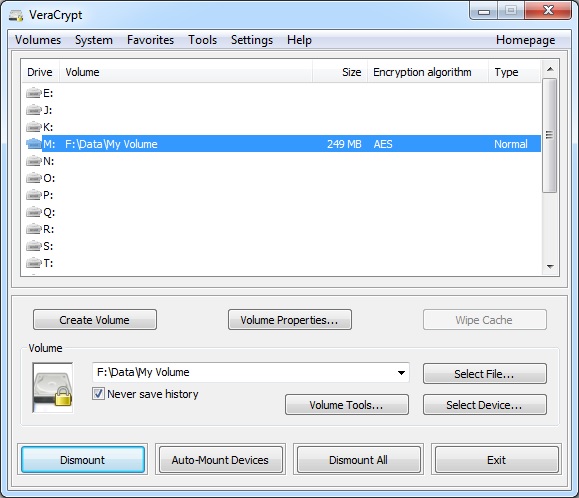


* Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next**(for more information, see chapters [*Encryption Algorithms*](https://veracrypt.codeplex.com/wikipage?title=Encryption%20Algorithms) and [*Hash Algorithms*](https://veracrypt.codeplex.com/wikipage?title=Hash%20Algorithms))
* Next, we specify that we wish the size of our VeraCrypt container to be 250 megabytes. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**



* This is one of the most important steps. Here you have to choose a good volume password. Read carefully the information displayed in the Wizard window about what is considered a good password. Select **Next**
* Move your mouse as randomly as possible within the Volume Creation Wizard window at least for 30 seconds. The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security). Select **Format**  
    
  
* Volume creation should begin. VeraCrypt will now create a file called *My Volume*in the folder F*:\Data\*(as we specified in Step 6). This file will be a VeraCrypt container (it will contain the encrypted VeraCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:
* Click **OK**to close the dialog box.
* We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click **Exit**. The Wizard window should disappear.
* In the remaining steps, we will mount the volume we just created. We will return to the main VeraCrypt
* Select a drive letter from the list (for example use M:). This will be the drive letter to which the VeraCrypt container will be mounted



* Click **Select File**. The standard file selector window should appear
* In the file selector, browse to the container file and select it. Click **Open**(in the file selector  
  window). The file selector window should disappear  
    
    
  
* In the main VeraCrypt window, click **Mount**. Password prompt dialog window should appear
* Type the password in the password input field
* Select the PRF algorithm that was used during the creation of the volume (SHA-512 is the default PRF used by VeraCrypt). If you don’t remember which PRF was used, just leave it set to “autodetection” but the mounting process will take more time. Click **OK** after entering the password
* VeraCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), VeraCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted
* We have just successfully mounted the container as a virtual disk M:  
  The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written
* If you open a file stored on a VeraCrypt volume, for example, in media player, the file will be automatically decrypted to RAM (memory) on the fly while it is being read
* Now access your M: drive from Windows Explorer and create a file to test the volume

# Exercise 9: Bitcoin

In this exercise we will view and identify a historic Bitcoin transaction related to the infamous Silk Road. Next, you will be asked to manually track the movement of Bitcoins to the owner’s wallet, and finally view a list of unconfirmed transactions and research why some transactions take longer to be confirmed than others.

# Researching Bitcoin transactions

Bitcoin was used as the main method of currency for purchasing goods and services on the infamous Silk Road. In this exercise look at the infamous transaction between the owner Dread Pirate Roberts (DPR) and his contact Red and White.

Visit this page and read about DPR and how he used bitcoin to pay for services:

<https://arstechnica.com/tech-policy/2015/02/the-hitman-scam-dread-pirate-roberts-bizarre-murder-for-hire-attempts/>

Locate the Bitcoin wallet address that DPR used to pay Red and White for his services.

How much money did DPR agree to pay Red and White initially for the hit?

Look up the transaction:

* <https://www.blockchain.com/>

What is the current value of the 1670 BTC transaction and how does this compare to the value at the time?

Why is there a transaction for 132.64 bitcoins?

Why is this refund address different to the original addresses used to pay the recipient?

# Track the movement of Bitcoin to the Silk Road Wallet

In this exercise, manually track the movement of Bitcoin from DPR to the Silk Road wallet.

Start at the payment:

* <https://blockchain.info/address/1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS>

Then move through the following payments:

1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS

1BG9jDV3pA1MsJUnvRyWuA2b7PfGd4MZaw

12h6TzwPNBvDnppbsqpyXwW4oo5UUKaKSa

1EG9HJG9aGqzgGujfNQMiNbyqpKnFxafvE

1AHki5AbZYiz4fHkGSTVKN3T1Tv5PwZpnh

15TEAwEMxVS3BK718HhwgJg7nxwyJ2ib9y

Finish at the Silk Road Wallet:

* https://blockchain.info/address/1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a

# Viewing unconfirmed transactions

View unconfirmed bitcoin transactions using Firefox or Chrome:

* <https://blockchain.info/unconfirmed-transactions>

Research the Blockchain.info website’s FAQ and answer the following question:

What can you do to increase the likelihood that your transaction will be used as part of a block and thus become confirmed?

# Exercise 10: Steganography

In this exercise you will be using Cryptapix to hide an image within another image:

1. Install Cryptapix by double clicking the cpx32.exe file in the exercise folder
2. Go online, download any image and add it to the folder with the two batman files.
3. In Cryptapix file manager navigate to the exercise folder.
4. In Cryptapix select image file batman.bmp at the bottom.
5. In Cryptapix select “Stego”, insert and browse to the new image you just download.
6. Insert the image into Batman.bmp and save the new image as batman-hidden
7. To reverse the process select the batman-hidden -> “Stego” -> “Extract”
8. Are there any differences between batman.bmp and batman-hidden?
9. Now repeat the exercise but this time **open** the batman.jpg file
10. Are there any obvious differences now?