Lab 8. Encrypting Files using 7-Zip

What is encryption?

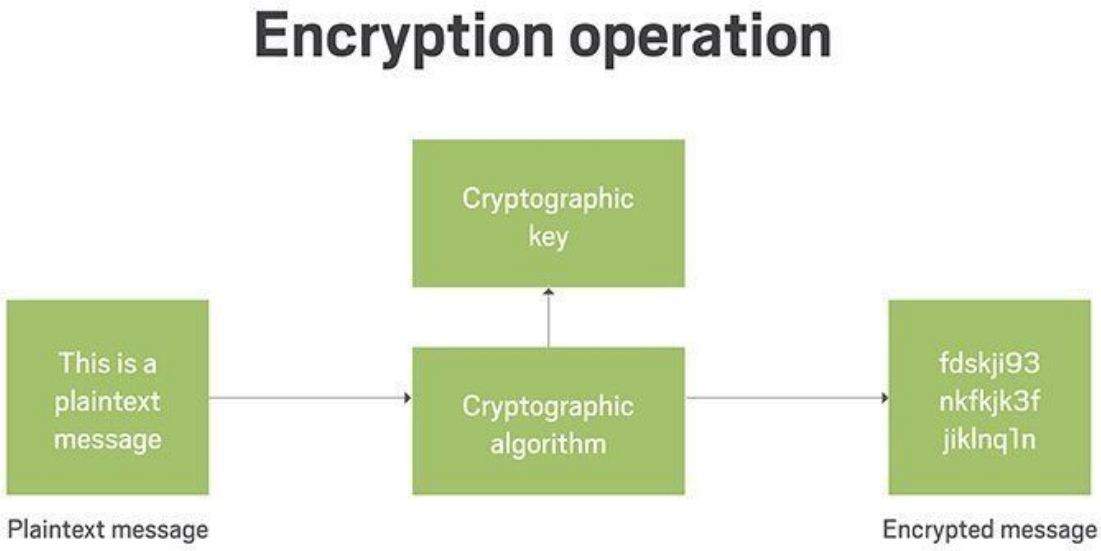
- In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. One can apply encryption to any type of data.
- Decryption is the reverse. The process takes the jumbled text and returns it to the original order.

Unencrypted (plain text) message: `Your secret code is: let-me-in`
Encrypted message: `QyCzt5d7rlS0apOMLRqVFnIZl7EqKC/cpwiQPbvfgTA=`

Try now

1. Go to: http://www.online-toolz.com/tools/text-encryption-decryption.php
2. Copy the encrypted message above and paste it in the "**Encrypted Text**" box (under Decryption)

How does it work?



There are two primary components to encryption:

1. Encryption algorithm
2. Encryption key

The **encryption algorithm** tells the computer how to encrypt the text. For example, a simple algorithm might shift all characters to spots to the right. The letter ‘a’ becomes ‘c’, ‘d become ‘f’, and ‘z becomes ‘b’. Or, it might swap characters. The letter ‘q’ becomes 8 and the letter ‘n’ becomes z. To decrypt the message, the computer needs to know the algorithm.

The **encryption key** is a random string of text or bits that the encryption algorithm uses to encode the data. The encryption key is usually very long. The encrypted data is secure and cannot be understood by anyone without the key.

Sometimes, a **passphrase** is used along with the encryption key. The passphrase is just a key used to encrypt the encryption key. Using a passphrase allows someone to store the encrypted data and encryption key together.

Here is a sample encryption key used SSL on websites (a website using HTTPS). You can generate RSA keys of various sizes: https://8gwifi.org/rsafunctions.jsp

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAtsr44N6SoJx+zKUW6Cy4woAY+utyCFoYQy9sk/in0BZqSBcX
A7x6R9FBkng6SwKL7h6r2mm5jxHzvItwwl5LPE0yEpimZgmTzZY/weDwow6+HHJ1
qLiNX6524oWho7OCZ1qU4HgPDgwdztz/lJXVd0hIAfrWtq6AzfWwcsdzWwsipDhs
NyPDI/h/A/JpvVH0tsO92Edc9YZcumlULnhuhXZkOx7Pav5ZBgN1tvg+94Zl4dd2
GrUTyvRpzS3OOr/d62HuG8f+4cMkg/k5NbQQo8GvxTLtJ2UovlywxQ95pB0uBQ57
6Vk2ToV6h+qfWgJnGn3Mwe8cvnDRpF6OVwPpCQIDAQABAoIBADdW8cwadie72UOZ
```

```
g3rc9z6jS2zD1S0kIY5NkECoGh4MezbCDsypxhdyCbkPPw6wga6giITCV1QyKild
ydB+faaO9Gbe4hmoMqAeKcVHlXK4JuQz3t0qqlpaVlG0BUCrOwKRUNs4Xc5x6qBT
FellB1BqiKpYx6Jc6E/yXu4Q5iKclBDmvkcrLBs0uhmuH5Rds2PU4pWjqykh2hVC
5tl2PKn8DIhjqETjK+H4wOlmDbZYUQSkNUIphZkYp/fNKIFmi4dT5v7EenPlGDpE
7NSJDwfaXB46gEWqLBj6jVdtLUjwD/61ypSNHpWfGYOx3orkJPOT5tWylwif0Hc1
yocNEBECgYEA6TdPI1yD0jKTpQFalejahcSwWbR4l1t/RmVil0lZ4Ln5a/7K7qsL
MLXMFGyoT4M3GP9Ya8gJpHBk45KqG+5JUCL9Myp/CyedxD4nxonJBpM9d8+Fzxmy
cLKISWsuZIr/B8VWcNe2jSSSmRj32wsmYdUoiKNNaUzbeVmHLnuPm10CgYEAyKaW
lvRVc3kyGhDwFzNtBi7HYHFmiNiURv/KxzZdoglBqaqNSTBqeHZZHyzu++ZyEW4j
TebfGZhi8fI+2CkYs5Ar4Jiz4sFj4zDCWcN+GHcFvCouhhW3wQZCo6HX1cIFWf28
51zwTobQCrlqwfnL/BZ5CiQBrHyG11tJ7UjPFZ0CgYA0Hk4rQuOat/7S40iRM+aR
+nDGu1QvzxzUaJft41CYrjcVcW18hPENQ7OF5PqAOny3s2jZPW0aOJvzV7V4ZHox
1H/tTVPy9DmHv7Q35Fbuhz03Z0MqEz4TfXKDpdZKVd3EqM82jJ6ZUFEKsc/CPe2n
83EJiCUmoSxzJBTXyHlBaQKBgQDHGTY4F75q1Im4f7Ic83RtPCGuOxgpFe8b/Fk0
D2gdjt3PA2MqipY7bgPFAYsp/WKWlRkHBd2+wgz8Uwm06CKQmrBPLnbgvFDncMyI
0YjfscrJCXocppQtPo8FW2SVwO4ae8LkOL5izTbGTXH3hGy6eXola9EVXINYUkcq
4qJJqQKBgGnxfSDH8WrMQ1yMVuw0Snm0ux32iuL9KTN6JM3dBlPYTFxsTPC4iBxf
zEQWiuWeVshRpcLkxWC/8M6d8BHelDHwkCbhuCZSYDyo1HOD1dFC9Y3cCRowi1TP
rpj+PSAxMsYHbkJ1LWBlWF1u64H6sjAYnxrVX6Cxwr4b3XGkK0P4
-----END RSA PRIVATE KEY-----
```

Public vs Private Key

Encryption keys usual come in pairs, **public** and **private**. The private key used to unlock the public key, which then reveals the data.

- A **public key** is like the lock on your apartment or car. Everyone knows that it is there. People can look at it and inspect it. They can't get in because they don't the correct key.
- A **private key** is like the key on your keyring. You use it to open the door to your apartment. Anyone with a copy of your key can open your door.

You will find the BilimEdtech SSH (secure shell) **public key** used to access a virtual private server (VPS) on their website:
https://resources.bilimedtech.com/ssh-keys/install-publi-key1.sh

- Whoever installs that key will give BilimEdtech access to their server.
- No one except those at BilimEdtech has the private key.

Why would they do this? This allows the instructors to help the students with their VPSs if they have a problem doing the laboratory assignments for Cloud Computing. The students do not need to give anyone the password to their server. They only need to install the public key. A student can remove the public key anytime they want. Their password stays safe.

Applications use private and public keys to talk to each other. You generate a public key when you install WhatsApp. This key identifies your WhatsApp. You can read more at
https://www.pcrisk.com/internet-threat-news/10240-whatsapp-encryption-explained

Your Tasks

You are going to use 7-Zip to encrypt files. 7-Zip uses the same encryption algorithm to encrypt and decrypt files. Since 7-Zip files do not store encryption keys separately, any application that reads a `.7z` file can open an encrypted 7-Zip file. The way you will protect your file is by using a passphrase, which prevents the application from reading the key to your file.

Before you begin

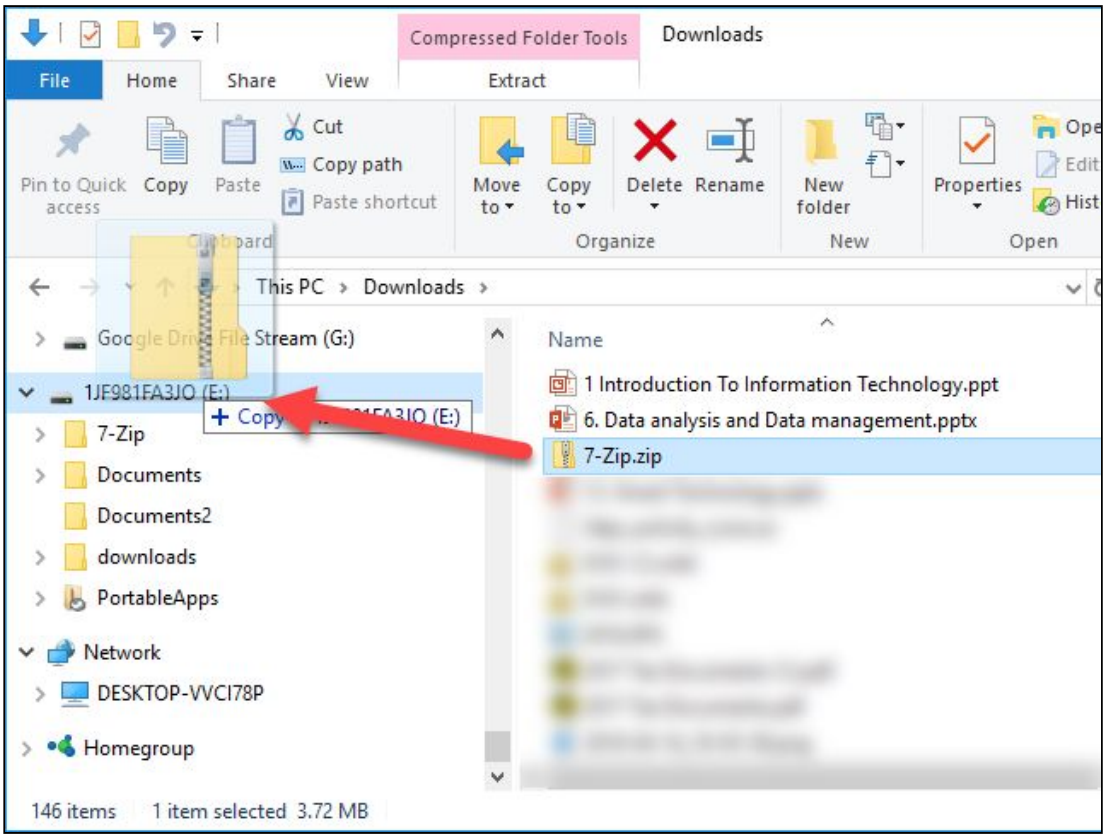
Think about the files you have on your flash drive.

1. What happens if you lose the drive or forget it in the computer lab. Do you have any personal information or embarrassing information?
2. Would you want to have additional files accessible on your flash drive but you are afraid of others accessing that data?
    a. For example, a file containing your passwords or bank information
3. What might you want to encrypt?

Task 1: Download 7-Zip

7-Zip is a free compression and encryption tool. Anyone can download and use it. You can install it on your computer or you can use it as a portable app from your flash drive. To simplify the process, we prepared a copy of the portable version ready for you to use.

1. Insert your flash drive into the computer
    a. If you do not have a flash drive, then use the Downloads folder
2. Download the portable version of 7-Zip
    a. This version works without an installer.
    b. You can extract it and run the application directly.
3. Copy the file from the downloads folder your flash drive

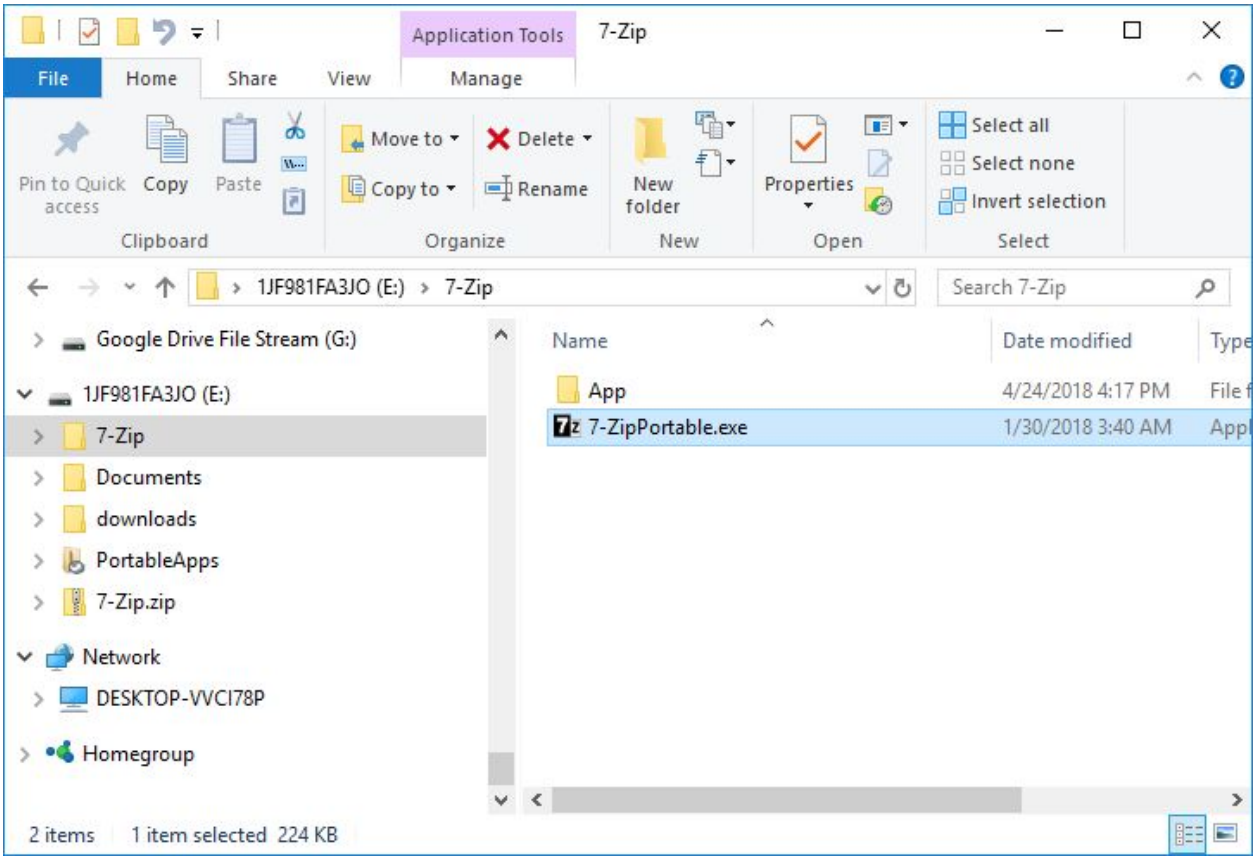


4. Extract `7-Zip.zip` to a folder called `7-Zip`.
    a. Ask your instructor or friend if you need help with this step
5. Open the `7-Zip` folder
6. You will see a file called `7-ZipPortable.exe` and a folder called `App`.

Task 2: Decrypt a File

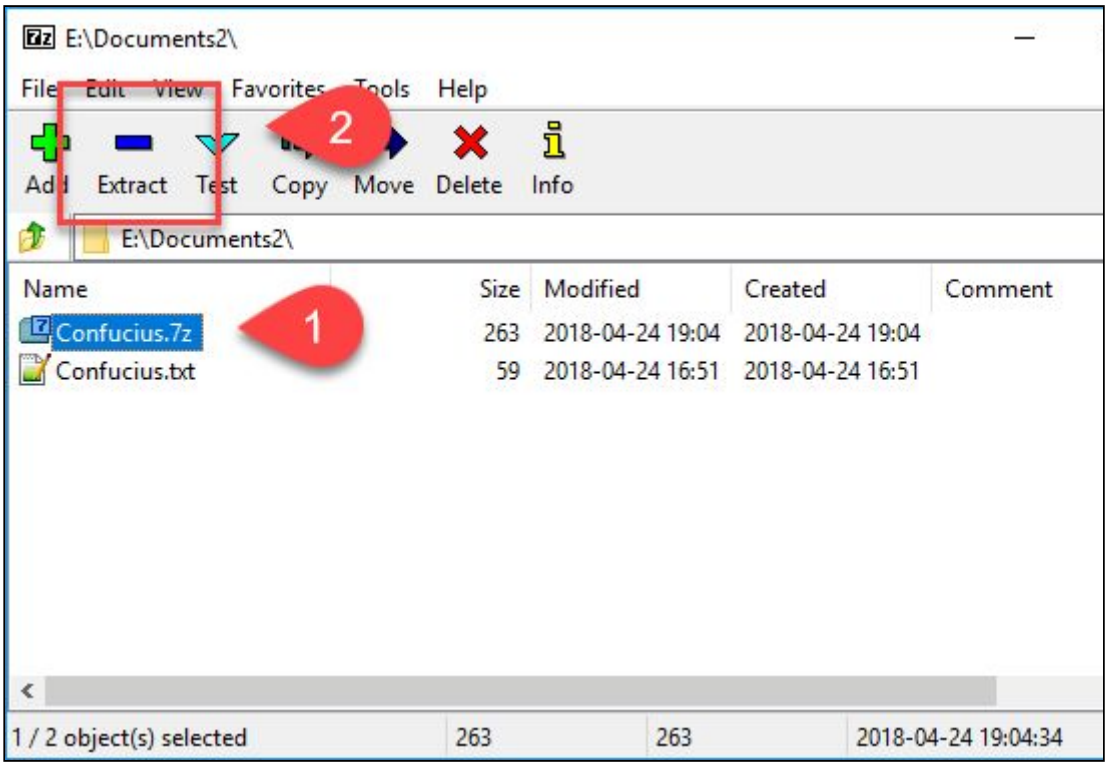
Now that you have 7-Zip on your flash drive, you can use it encrypt and decrypt files on any Windows computer!

1. Open the project folder on Google Drive.
2. Download the instructor example 7-zip file (`Confucius.7z`)
3. Save file `Confucius.7z` to your flash drive
4. Go to the 7-Zip folder. Double click on `7-ZipPortable.exe`



5. Using 7-Zip, browse to your file
6. Click on the file to select it

7. Click the **Extract** button (or right-click and choose extract)



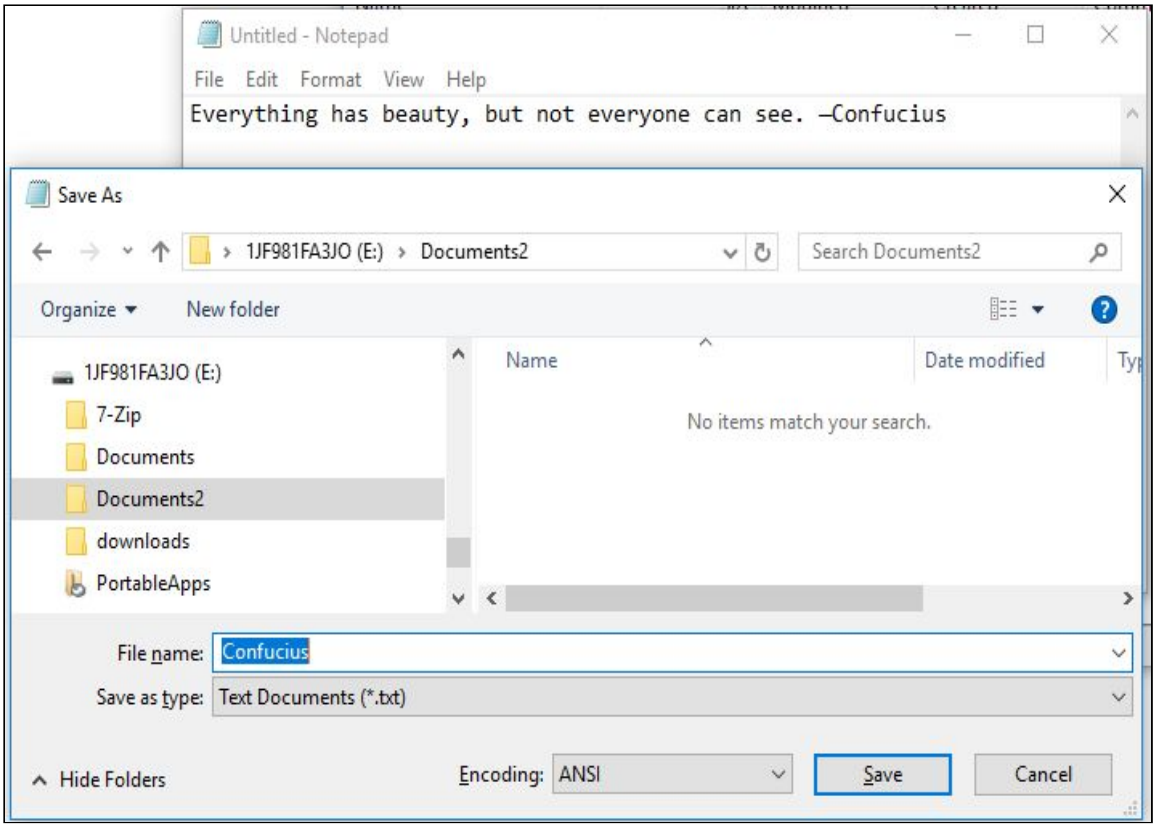
8. Verify the file will extract to your flash drive (or preferred destination)
9. Type in the password: `Confucius says...`
10. Press the OK button

11. Browse to the folder where you extracted the file
12. Open the file
13. Show the file contents to your instructor

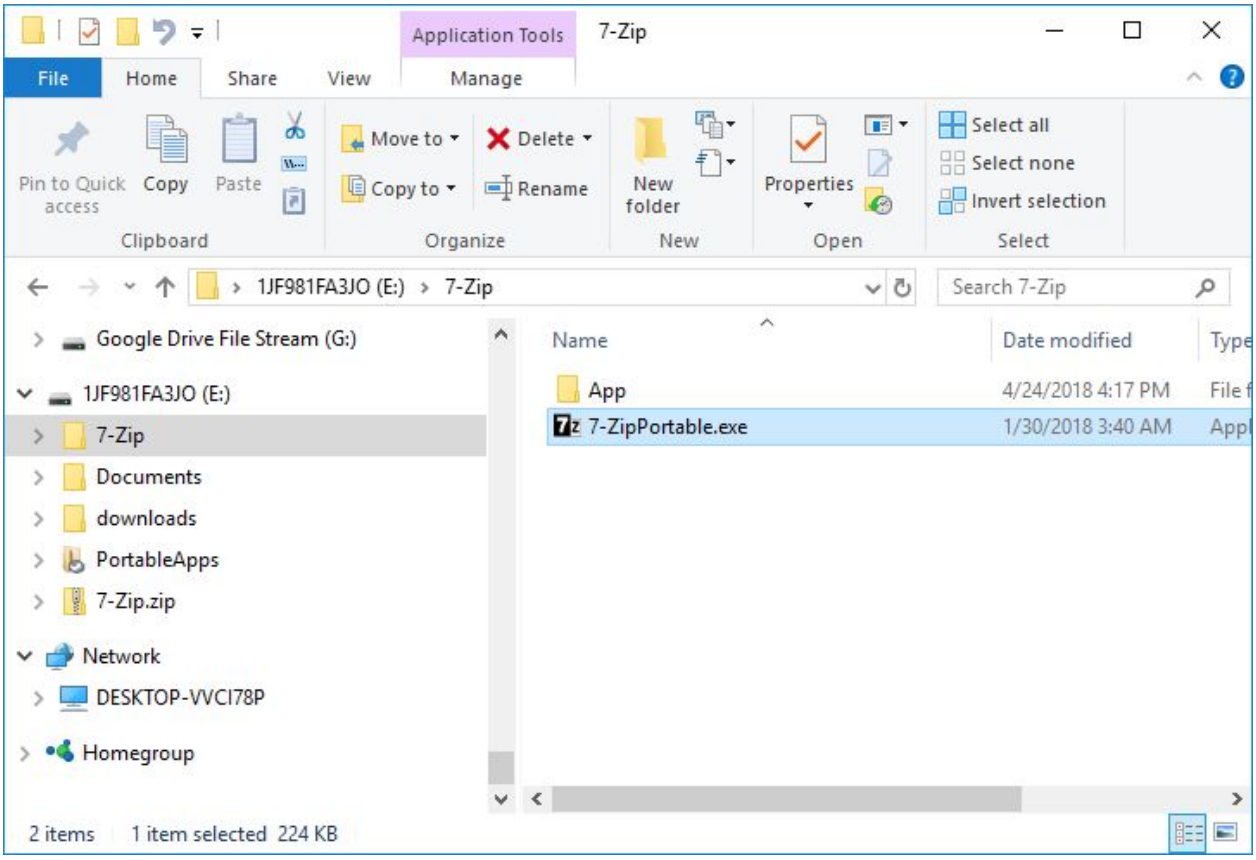
Task 3: Encrypt a File

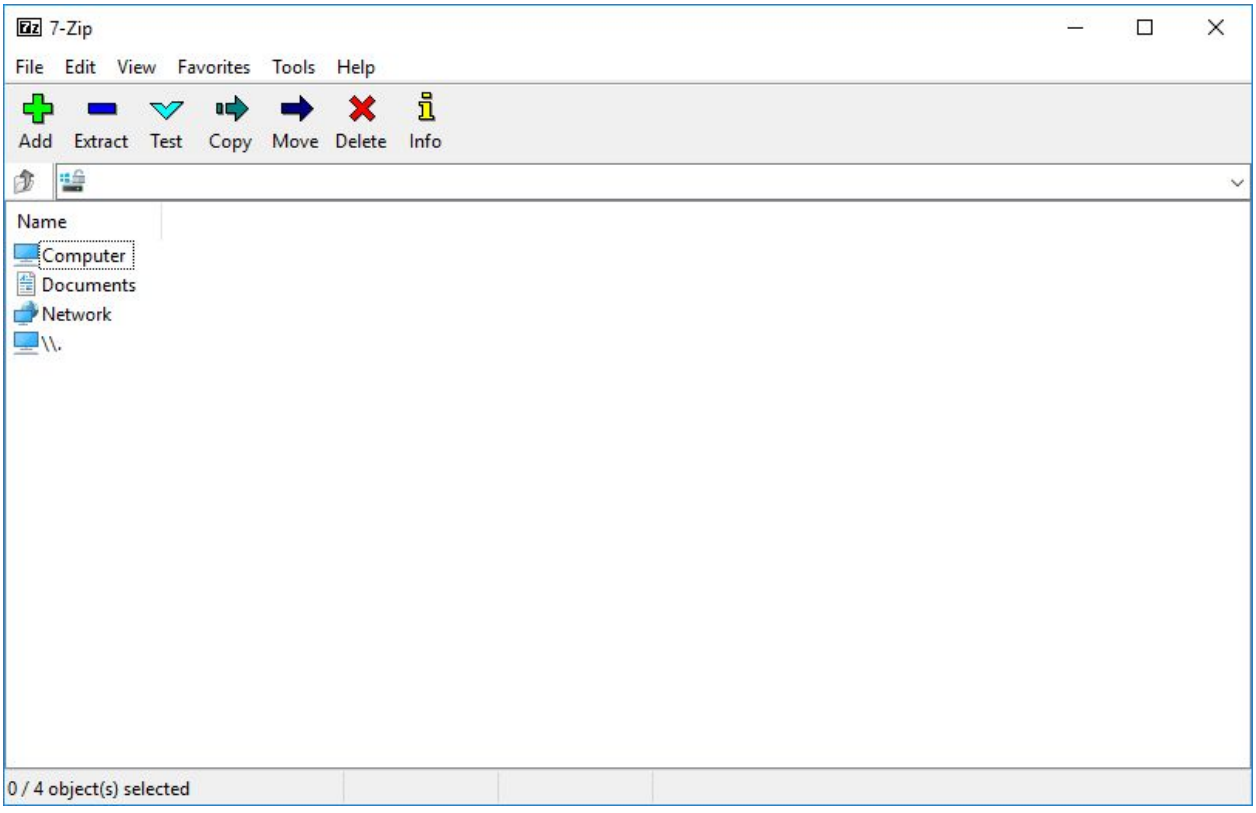
You can encrypt a single file, multiple files, or an entire folder! We will encrypt a single file.

1. Create a new file using Microsoft Word or Notepad.
2. Type a favorite quote or inspirational saying
3. Save the file with your name to your flash drive. (e.g., jill.txt)

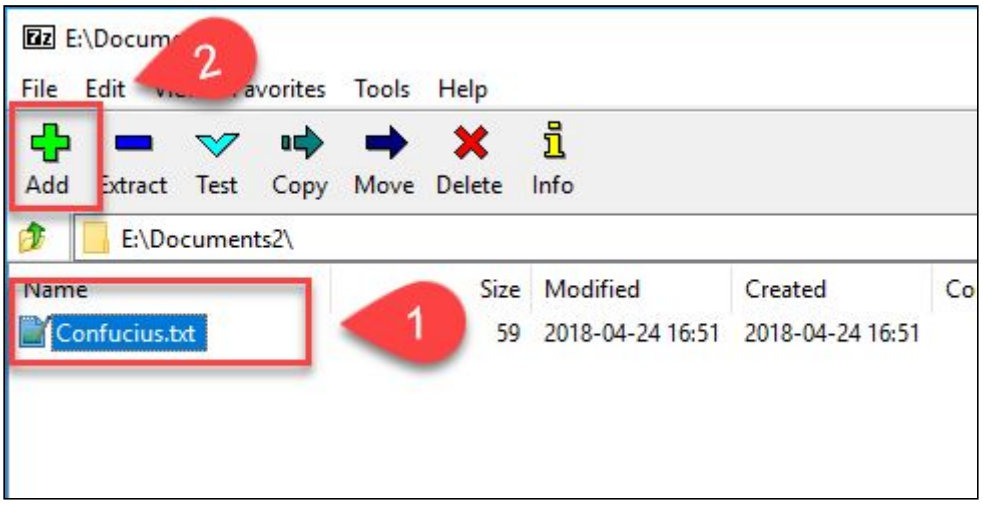


4. Go to the 7-Zip folder. Double click on `7-ZipPortable.exe`

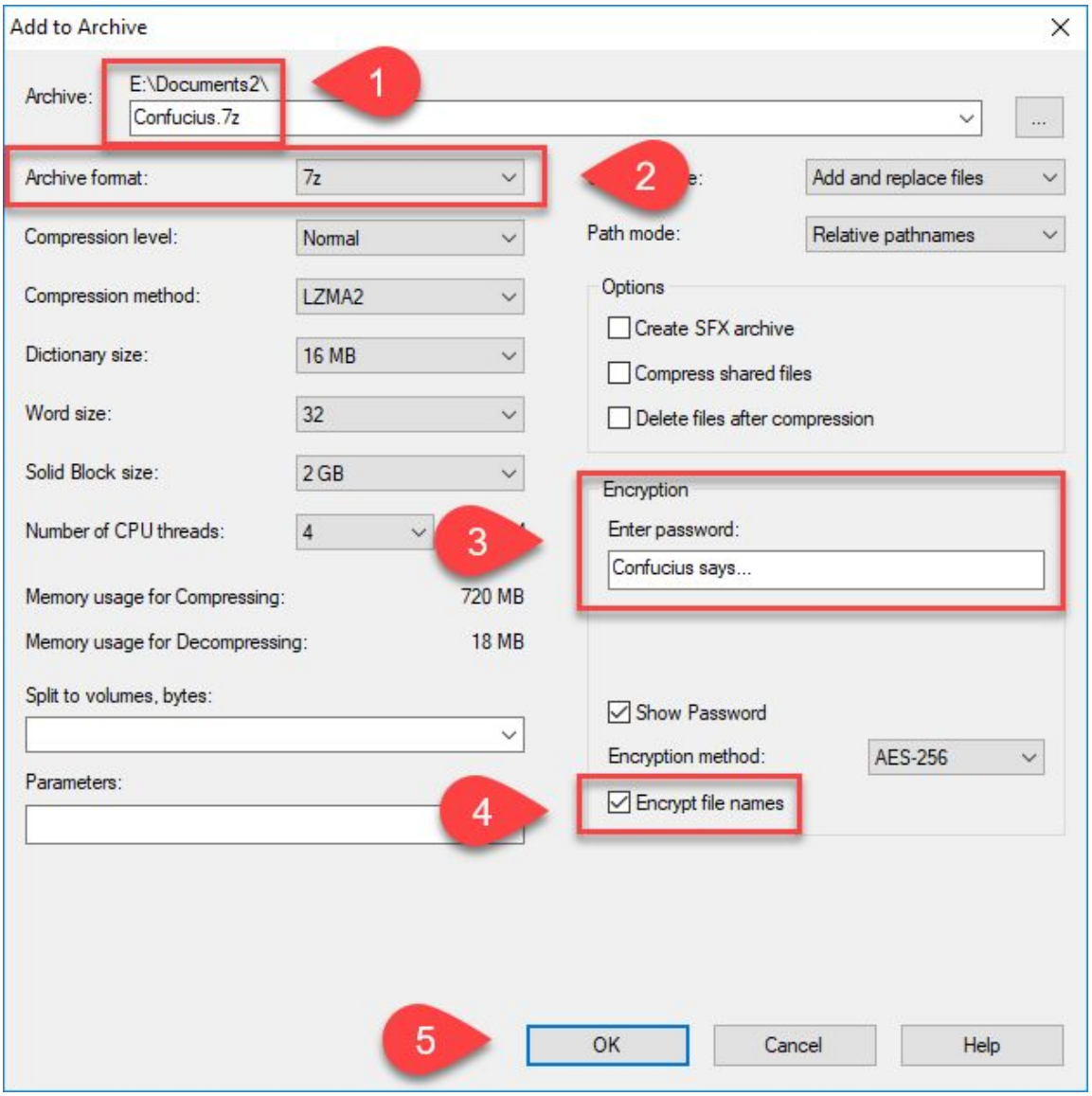




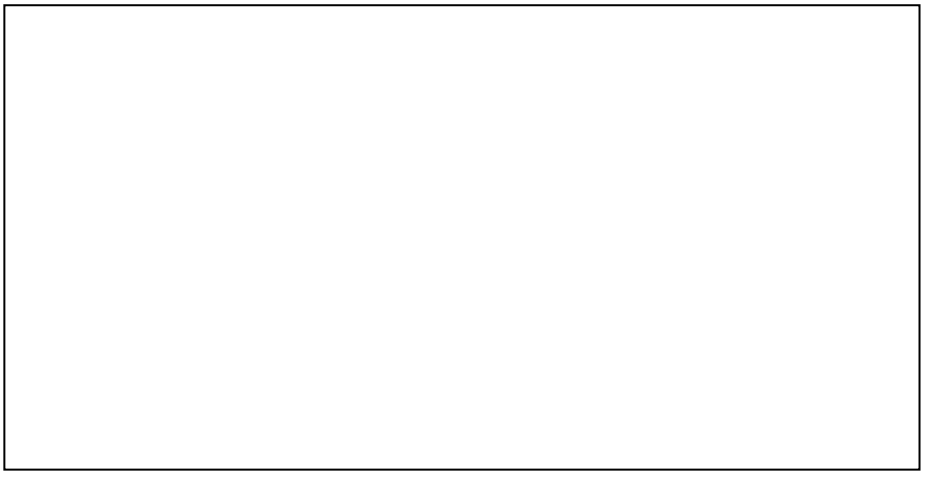
5. Using 7-Zip, browse to your file
6. Select it and then click on the **Add** button



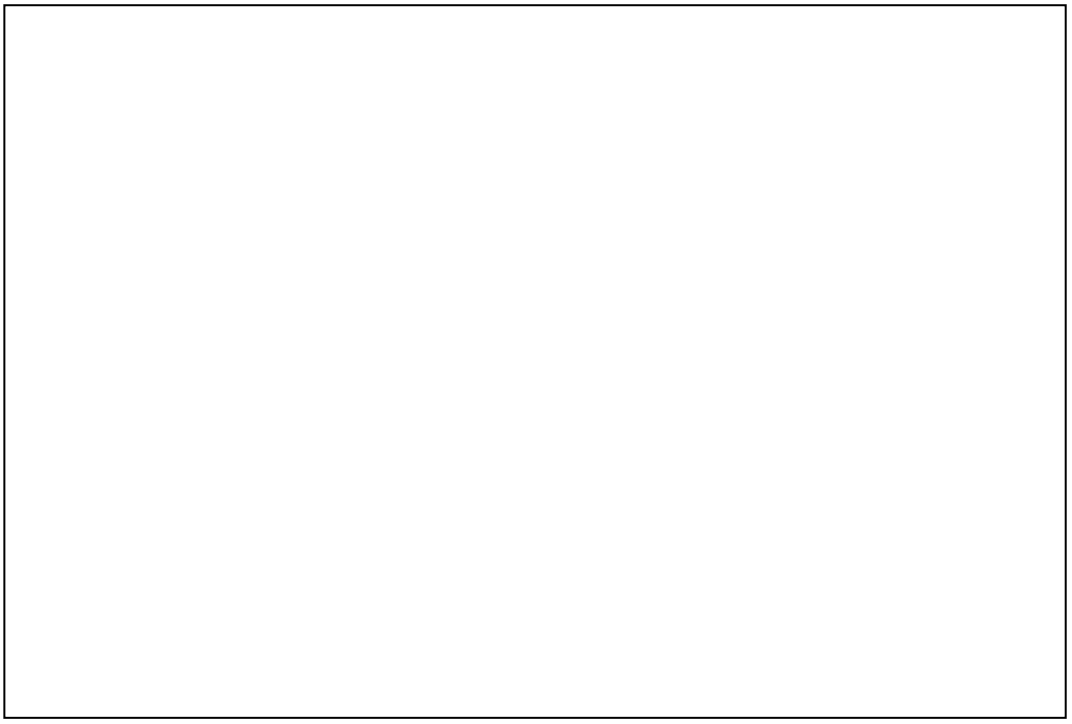
7. The archive format should already be set to 7z.
    a. If not, change it now
8. Enter a password
    a. Normally you would want a secure or strong password.
    b. For this assignment, please use your name or a simple object
    c. Examples: Jimmy; clock; 16:38; yellow pen; sunny today;
9. Check the **Encrypt file names** checkbox
    a. This prevents others from looking at the contents of the 7z file without a passphrase
10. Press the **OK** button

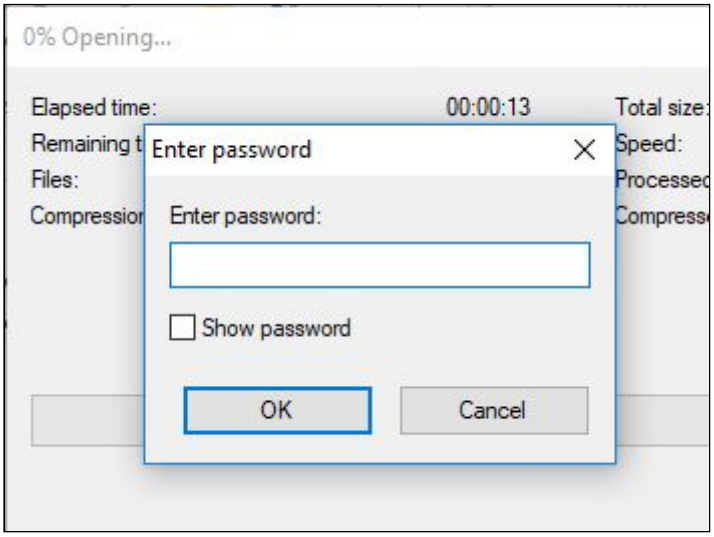


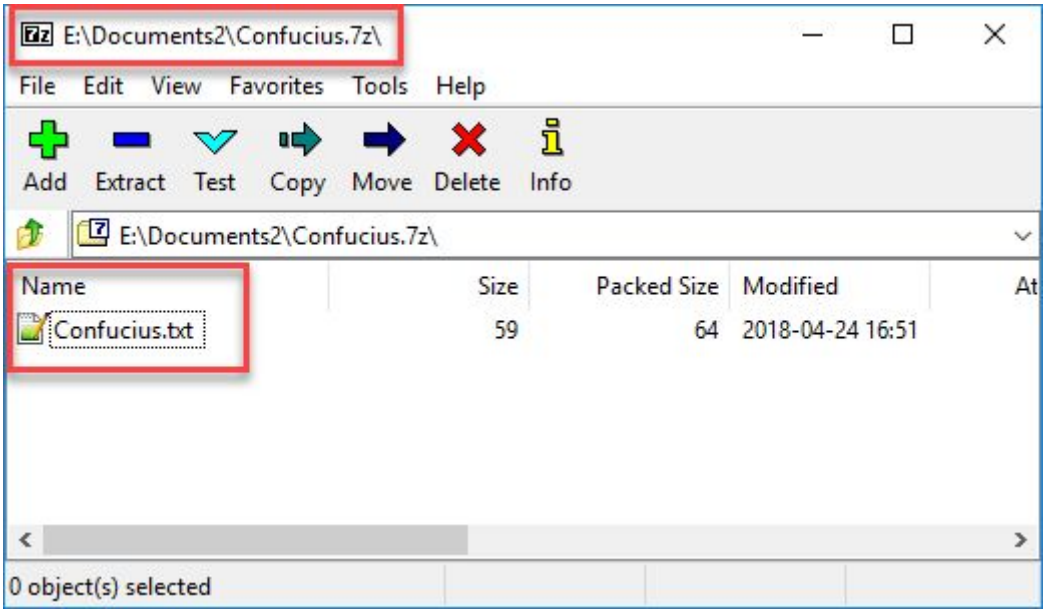
11. Look in the folder (or the location you saved the 7z file



12. Open the 7z file to verify your passphrase works.







13. To get lab credit, follow the submission guidelines from your instructor

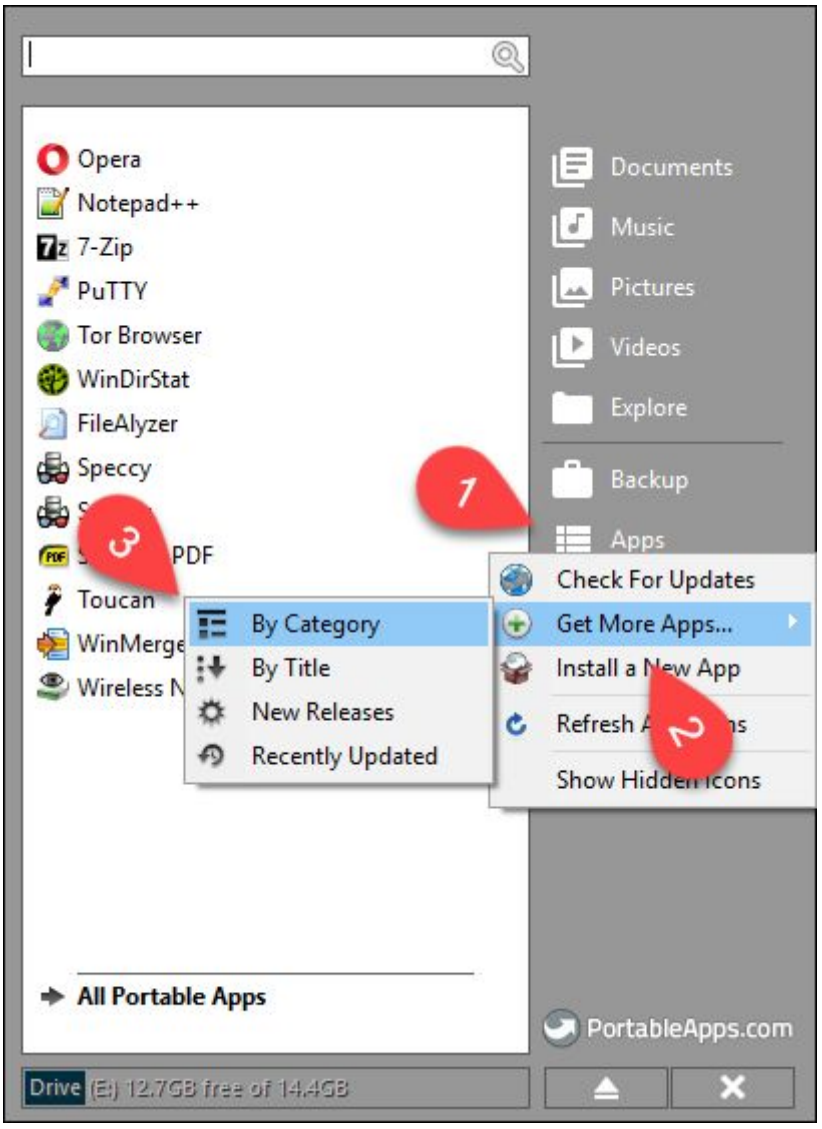
On Your Own

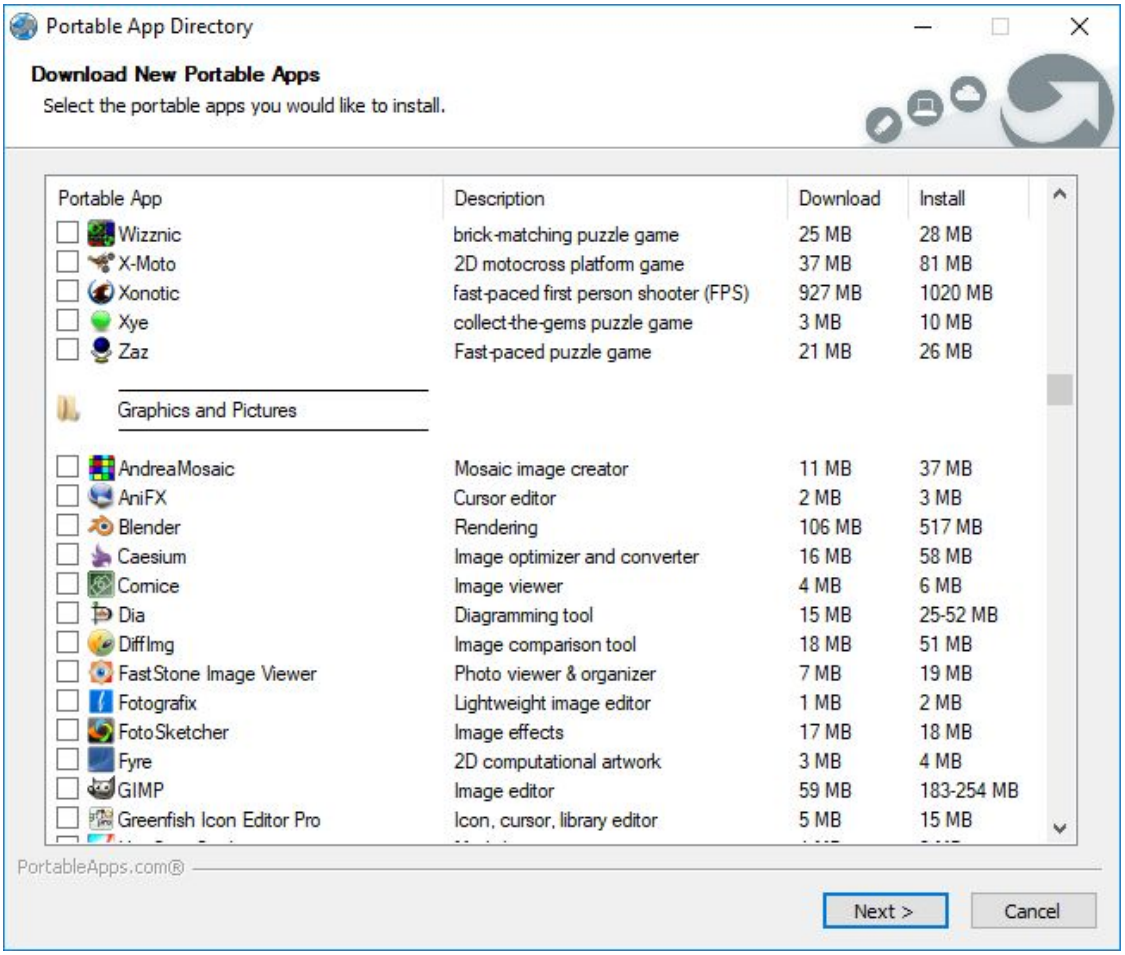
How will you use 7-zip? Perhaps you could encrypt most of the files on your flash drive you rarely use. You can extract one or more files at any time.

PortableApps.com

Portable 7-Zip is one of many portable applications that you can run from your flash drive.

1. Go to https://portableapps.com/ and install the application launcher on your flash drive
2. 7-zip is a default application
3. Browse the list of portable apps https://portableapps.com/apps
4. Once you find some apps, you can install them from the PortableApps launcher


Opera
Notepad++
7-Zip
PuTTY
Tor Browser
WinDirStat
FileAlyzer
Speccy
Toucan
WinMerge
Wireless N
Documents
Music
Pictures
Videos
Explore
Backup
Apps
1
2
3
Check For Updates
Get More Apps...
Install a New App
Refresh A
Show Hidden Icons
By Category
By Title
New Releases
Recently Updated
All Portable Apps
PortableApps.com
Drive (E:) 12.7GB free of 14.4GB



7-Zip for your Desktop

1. On your own computer, you can download and install 7-Zip https://www.7-zip.org/download.html
2. The desktop version gives you contents menu shortcuts