

STUDENT ACTIVITY 4.3: UNDERSTAND ENCRYPTION

MTA Course: 10753 Windows Operating System Fundamentals

Topic: Understand encryption

File name: 10753_WindowsOS_SA_4.3

Lesson Objective

4.3: Understand encryption. *This objective may include but is not limited to:* understanding BitLocker, encrypting file systems (EFS), and compression.

Resources, software, and additional files needed for this lesson:

- A workstation with Microsoft Windows 7 Professional or Enterprise edition installed
 - The workstation should have two user accounts.
- Alternative option:
 - A virtual machine with Windows 7 Professional or Enterprise edition installed

Directions to the student:

Complete the following hands-on activities. Answer any questions as you work through the activity. Note that the screenshots in the activity may look different from your system. Request assistance from the instructor as needed.

Encrypting a folder and file

1. Authenticate into your system using the first user account provided by your instructor.
2. Open Windows Explorer. Double-click your secondary logical drive (if available; otherwise, double-click your system drive).
3. Click the New Folder button on the menu bar and name the folder **Secret**.
4. Right-click the Secret folder and select Properties.
5. Click the General tab and then click Advanced.
6. In the Advance Attributes window, select the Encrypt Contents To Secure Data checkbox.

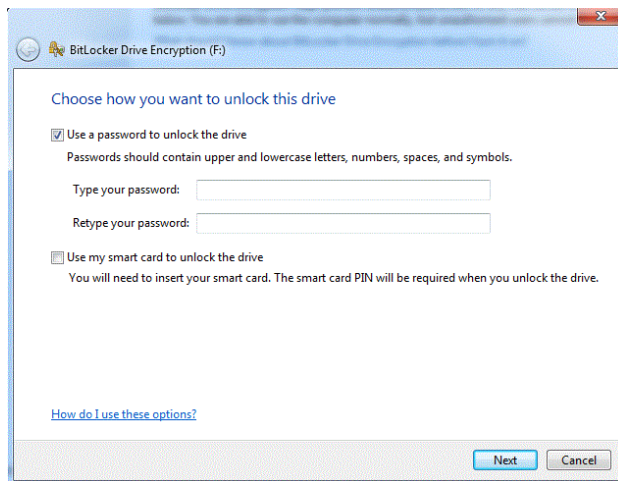
7. Click OK to close the Advance Attributes window and then click OK to close the folder Properties dialog box.
8. What color is the Secret folder?
 - a. _____
9. Open the Secret folder.
10. Create a new text document and name it Private.
11. What is the color of the Private file?
 - a. _____
12. Open the Private file and type **Confidential**. Save and close the file.
13. Click the back arrow to get back to the root of the drive.
14. Create a new text document and name it **Public**.
15. Open the Public file and type **Hello World**. Save and close the file.
16. Copy the Public file to the Secret folder.
17. Open the Secret folder.
18. What color is the Public file?
 - a. _____
19. What does that mean?
 - a. _____
20. Close Windows Explorer.
21. Log out and log on again with the second user account provided by your instructor.
22. Open Windows Explorer and navigate to the Secret folder.
23. Open the Private file. Did the file open? ____ Yes ____ No
24. Open the Public file. Did the file open? ____ Yes ____ No
25. Return to the root of the drive. Open the Public file that you first created.
26. Did the file open? ____ Yes ____ No
27. Log out and log back on with the first user account.
28. Navigate to the Secret folder. Use what you have learned to encrypt this folder. Repeat those same steps and remove the encryption.
29. Do you have the option to decrypt the contents of the folder? ____ Yes ____ No

30. What is the color of the Secret folder?

a. _____

Enabling BitLocker To Go

1. Be sure that you are logged on as a user that is a member of the Administrators group.
2. Click Start, Control Panel, System and Security, and then BitLocker Drive Encryption.
3. Choose your secondary volume to secure and click Turn On BitLocker. This will start the BitLocker setup, as shown here.



4. Select Use A Password To Unlock The Drive: Specify the password as: **Pa\$\$w0rd**
5. Choose to save the recovery key and save the recovery key to your desktop and then click Next.
6. Click Start Encrypting. The time it will take to encrypt will vary based on the size of your volume.
7. Using Windows Explorer, navigate to that volume once the encryption process is finished.
8. Create a new text document named **MySecureText**. Were you able to do this? ____ Yes
____ No
9. Using what you have learned, return to the BitLocker Drive Encryption console in Control Panel.
10. Locate the volume that you have just secured. Click Manage BitLocker.

11. List the options that are available to manage.

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____

12. Click Close to exit the Options page.

13. When your drive has finished encrypting, log off your system.

14. Log back onto your system and open the encrypted drive.

15. Did it open successfully? ____ Yes ____ No

16. Right-click the encrypted drive, select Unlock Drive, and provide the password that you used to lock the drive.

17. Open the BitLocker Drive Encryption console and click Turn Off Bitlocker.
Acknowledge the warning by clicking Decrypt Drive.

18. Have your instructor verify your answers.