Name: Sanchit Monga

Activity 1 – using File Encryption and File Compression

1. (20 points) What type of encryption method does Bit Locker utilize, which method is the most secure and why?
   BitLocker uses Advanced Encryption Standard (AES) as its encryption algorithm with configurable key lengths of 128 or 256 bits.
   AES is one of the most secure method of encryption. It is most secure because it is considered more mathematically efficient and elegant cryptographic algorithm and it has options for various key lengths. It allows you to choose 128-bit, 192-bit or 256-bit making it exponentially stronger than the other methods.

   (20 points) Cite references used for researching this question. References from Wikipedia are unacceptable and will not be accountable.
   https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-security-faq
   https://www.toptenreviews.com/secure-encryption-methods
   https://blog.syncsort.com/2018/08/data-security/aes-vs-des-encryption-standard-3des-tdea/

2. (5 points) What are the four compression methods 7-Zip utilizes?

   The four compression methods that 7zip utilizes are : LZMA,LZMA2, PPMd and BZip2.

   (5 points) Cite references used for researching this question. References from Wikipedia are unacceptable and will not be accountable.
   https://superuser.com/questions/432025/different-compression-methods-in-7zip-which-is-best-suited-for-what-task

3. (10 points) Which one of the four compression methods is the best from a security perspective?

   LZMA2 is the most secure method of compression and uses AES 256 for the encryption.

   (10 points) Cite references used for researching this question. References from Wikipedia are unacceptable and will not be accountable.
   https://security.stackexchange.com/questions/100650/how-secure-is-7z-encryption

4. (10 points) What was the noticeable differences with the Encrypt file names option checked and unchecked?

The checked was compressed twice and the uncheck was compressed just once. The checked contains the unchecked directory which is compressed and has the file inside it. We need to enter the password twice to open the checked.

(20 points) Explain why this may be useful from a security perspective. Include a screenshot with the appropriate answer.