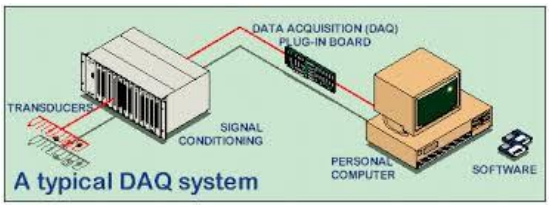

CS6305.001 Data Security and Privacy for Practitioners

Assignment 3:

Due back on Friday, February 17, 2023 at 11:00pm.

The following is from syllabus:

No e-mail submissions are accepted. No late submissions are accepted. So, please plan accordingly, do not leave your submissions to the last minute. If you encounter a problem during elearning submission, please contact 24/7 elearning Help IMMEDIATELY. This help is available 24/7 at:

eLearning Help URL: http://www.utdallas.edu/elearning/eLearningHelpdesk.html
eLearning Help Phone: 1 866 588 3192

Any submission that is missed will be graded with a zero. Please do not insist for exceptions.

Purpose: Demonstrate the ability to understand violation of privacy in Windows systems, also in cryptographic protocols.

Question 1 (25 POINTS) This question requires a Windows OS. Demonstrate the execution of Encrypting File System (EFS) on a file, then on a folder. Cut and paste the encrypted file from encrypted folder into an unencrypted folder. Can you access the file now or not? Please provide screenshots for each stage as an evidence for your work. You can watch the short video about the execution of EFS, attached to this assignment.

Question 2 (25 POINTS) Demonstrate the execution of full disk encryption via BitLocker. Does your computer have Trusted Platform Module (TPM) chip? Are you doing software encryption or hardware encryption? Why? Please provide screenshots for each stage as evidence for your work. You can watch the short video about the execution of BitLocker, attached to this assignment.

Please note: For questions 1 and 2, if your computer cannot access EFS or BitLocker please use one of the following options:

1. You can try one of the following compatible third party disk encryption tools instead. Make sure to execute the tool of your choice fully, including your step by step screenshots:
   - Jetico BestCrypt Volume Encryption https://www.jetico.com/downloads
   - TrueCrypt https://sourceforge.net/projects/truecrypt/files/

- Another freely available disk encryption tool you find. Please provide the name of your tool clearly and also provide your resource website.

2. BitLocker comes along with the Windows 10 Education edition which is available to our students via their UTDallas Azure Dev Tools for Teaching (formerly known as Imagine) account. So, you can download the Windows 10 Education edition from UTDallas Azure Dev Tools for Teaching portal, then run the BitLocker on that OS.

3. You can use a friend's computer to run EFS and BitLocker, but these should be executed on a separate file of yours, and each student should submit individual work.

Question 3 (50 POINTS) XOR is a special function that is frequently used in cryptographic algortihms, thanks to its performance – as it can be implemented with a logic gate that makes it extremely fast-, also its unique property as explained in the example below.

Assuming both message and key sizes are 4-bits each:

```
Message                 = 1011
Key                     = 1111
C= Message XOR Key      = 0100

C XOR Key               = 1011  Voila! Original message is recovered!
```

Assume the following cryptographic protocol introduced to verify that both sender and received are in possession of the same cryptographic key by incorporating XOR operation: Sender creates a message which is a random bit sequence with the same length as the key, performs encryption by XORing the message he generated and the key, then sends the resulting bit sequence over the network to the receiver. The receiver, upon receipt of this XOR result from the sender, XORs the incoming bit sequence with his key and sends the resulting bit sequence back to the sender. The sender checks whether the bit sequence he received is equal to the original message he had generated. If they match, it means that both sender and receiver has the same key.
As is, this scheme is vulnerable to MIM (Man In the Middle) attack. Demonstrate how a MIM attack can successfully be performed on this protocol. Assume **arbitrary 8-bit length only** for each bit sequence mentioned in the protocol. Please explain each step as much as you can.

If you are submitting multiple files, please create a ZIP file of all your files and use the following naming convention for your ZIP file:

CS6305-Assignment<number>-<FirstName><LastName>.zip.

So, student John Smith will name his 1st assignment zip file as:

CS6305-Assignment1-JohnSmith.zip

If you are submitting a single file, please name your file as:

CS6305-Assignment1-JohnSmith.doc or .pdf, etc.

Good luck.