***Anthony Gimei***

Exercise 1 – Cryptography

Download and install gpg4win (Cleopatra)

<https://www.gpg4win.org/>

(Mac users: <https://gnupg.org/download/>)

(you don’t have to donate, select $0)

BEFORE running the install, verify the hash value of the downloaded file:

|  |
| --- |
| SHA256 checksums (<https://www.gpg4win.org/package-integrity.html> )  0cf87835a914cb6fd1bcb32e8beee995b5da35c513f627356685c389df1be6cb gpg4win-3.1.4.exe |

certutil -hashfile <file path/file name> SHA256

|  |
| --- |
| C:\Users\gimeia1\Documents\DATA\CSCC\cscc\_cyber\_security\_II>certutil -hashfile gpg4win-3.1.4.exe SHA256  SHA256 hash of file gpg4win-3.1.4.exe:  0cf87835a914cb6fd1bcb32e8beee995b5da35c513f627356685c389df1be6cb  CertUtil: -hashfile command completed successfully. |

QUESTION 1: Why do you verify the hash? What should you do if the hash does not match?

***To verify the integrity of the downloaded file. That it actually originated from the author of the file and has not been changed.***

Create a PERSONAL key pair

Use your name and CSCC email

Under Advanced, set the expiration date to Jan 1 2019.

When setting your password, DO NOT FORGET it. Write it down for the rest of the upcoming exercises.

QUESTION 2: What does this password protect?

***Protects against having someone alter the key.***

Click through to finish key creation.

You should see your key in the Cleopatra Window. Right click and click on “Details”.

Click on Export. Copy the ASCII armored text to a text file on your USB drive.

Copy the “Fingerprint” value and email it to me ([kking83@cscc.edu](mailto:kking83@cscc.edu))

***Fingerprint: CBEC 71A5 CF07 3D41 7339 7FF0 6589 43FE E8B0 C761***

NOTE: I need to have all your fingerprints back no later than noon on 11/5 so I have time to create the next exercise.

This completes the first exercise.