

Fundamentals of Information Technology Security
CSEC 1110
Lab 05

- Contact your instructor with your questions about the assignments.
- The student must insure all the answers are free from any malware.
- The student must ensure all answers are legal as defined by the class syllabus.
- All parts of your answers must be neat and easy to read.
- Paragraphs are at least four properly constructed English sentences.
- Embedding documents within documents does not work with the D2L Bright Space assignments.
- Plagiarism will not be tolerated.
- Unless noted, all lab sections must be done as unprivileged login.
- Labeling answers is highly recommended.

5. Lab05: Encrypting Files

- 5.1. Upload each answer to the D2L Bright Space Assignment section 5.1 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
 - 5.1.1. Run a password-cracking program against the following passwords. Some of these passwords are from <https://www.weforum.org/agenda/2024/07/popular-passwords-cybercrime-digital-safety/>
 - 5.1.1.1. !Password123
 - 5.1.1.2. Aa123456
 - 5.1.1.3. UNKNOWN
 - 5.1.1.4. Admin123
 - 5.1.1.5. An eight-character password of your choice
 - 5.1.1.6. Odnltmotd5dbguaseo
 - 5.1.1.7. "A honu dancing with Snuffy"
 - 5.1.2. Provide a report of the password cracking program results for each password and execution time. You may stop working on a password after eight hours.
 - 5.1.3. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 5.2. Upload each answer to the D2L Bright Space Assignment section 5.2 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
 - 5.2.1. On host01, calculate the computer hash utilizing two different computer hash algorithms for ten different files. Identify the operating system.
 - 5.2.2. Copy the ten files from host01 to host02.
 - 5.2.3. On host02, calculate the computer hash utilizing two different computer hash algorithms for ten different files. Identify the operating system.
 - 5.2.4. Create a table(s) comparing the results of all the computer hash calculations between both hosts.
 - 5.2.5. Provide an explanation of the results shown in the table(s).
 - 5.2.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 5.3. Upload each answer to the D2L Bright Space Assignment section 5.3 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
 - 5.3.1. Provide directions for successfully encrypting at least ten files using symmetric encryption. Include any necessary citations for your directions. Each step, mouse click, and answer must be in a separate sentence or bullet point.
 - 5.3.2. Provide evidence of successfully encrypting at least ten files using symmetric encryption.
 - 5.3.3. Provide evidence of successful decryption of all the encrypted files
 - 5.3.4. Identify the encryption algorithm and strength for this section.
 - 5.3.5. Provide at least one sentence explaining why you selected the algorithm.
 - 5.3.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 5.4. Upload each answer to the D2L Bright Space Assignment section 5.4 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.

- 5.4.1. Provide directions for creating a key pair using only gpg programs. Each step, mouse click, and answer must be in a separate sentence or bullet point.
- 5.4.2. Provide directions for verifying the digital signature using only gpg programs. Each step, mouse click, and answer must be in a separate sentence or bullet point.
- 5.4.3. Provide directions for encrypting a message using only gpg programs.
- 5.4.4. Provide directions for decrypting a message using only gpg programs.
- 5.4.5. Provide directions for encrypting a file using only gpg programs.
- 5.4.6. Provide directions for decrypting a file using only gpg programs.
- 5.4.7. Provide at least one sentence explaining why you selected the algorithm.
- 5.4.8. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.