



CYENG 312: Trusted Operating System (OS) – Fall 2022: Assignment 1

Instructor: Dr. Shayan (Sean) Taheri

Note – Cheating and Plagiarism: Cheating and plagiarism are not permitted in any form and cause certain penalties. The instructor reserves the right to fail culprits.

Deliverable: All your responses to the assignment questions should be included in a single compressed file to be uploaded in the Gannon University (GU) – Blackboard Learn environment.

Question 1. Consider the following algorithms:

- Banker
- Dining Philosopher's
- File Allocation
- First-Come, First-Served Scheduling
- Lamport's Bakery
- Multiple-Level Queues Scheduling
- Page Replacement
- Priority Scheduling
- Producer Consumer
- Round Robin Scheduling
- Shortest Remaining Time
- Shortest-Job-Next Scheduling

1-A. Provide comprehensive explanations for the algorithms through research.

1-B. Write their computational flows and draw their flowcharts.

1-C. Determine real-world applications of these algorithms.

1-D. Implement the fastest version of the Banker Algorithm using the C++ programming language.

Question 2. Consider the following algorithms:

- Advanced Encryption Standard
- Blowfish
- Data Encryption Standard
- Diffie Hellman Key Exchange
- Elliptic Curve Cryptography
- Message-Digest
- Rivest-Shamir-Adleman

- Secure Hash
- Triple Data Encryption Standard

2-A. Provide comprehensive explanations for the algorithms through research.

2-B. Write their computational flows and draw their flowcharts.

2-C. Determine real-world applications of these algorithms.

2-D. Specify high-level/overall difference(s) between the algorithms mentioned in Questions 1 and 2.

2-E. Implement the fastest version of the Advanced Encryption Standard Algorithm using the C++ programming language.

Question 3. Read the research papers available in your assignment package and show your understanding for each in one paragraph (i.e., a paragraph has at least five lines with the font size of 12 in here).

- Huang, C., Tan, Y., Duan, G., Chen, Z., Zhang, B., Deng, P., Zhang, Q., Sun, J., Chen, H., Xiao, G. and Liao, Q., 2021, December. A Coverage-Guided Fuzzing Framework for Trusted Execution Environments. In 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys) (pp. 775-782). IEEE.
- Alharbi, F., Zhou, Y., Qian, F., Qian, Z. and Abu-Ghazaleh, N., 2022. Dns poisoning of operating system caches: Attacks and mitigations. IEEE Transactions on Dependable and Secure Computing, 19(4), pp.2851-2863.