Project Code: CYBER1-CodeVersion
Client: Scalable Algorithms for Data Science Laboratory (SCADS)
Contact Person: Tashi Stirewalt, tashi.stirewalt@wsu.edu
Preferred Meeting Method: Online or in-person
Preferred Meeting Frequency: Weekly
Scope: 3-4 students

Abstract and Motivation: This project aims to create a tool for generating multiple versions of a given C/C++ or Python source code file. Each version will perform the same function but have a different code structure. The tool will utilize a mechanism such as a non-deterministic graph algorithm to model the probability of code mutations and use a genetic algorithm to create and test code mutations iteratively. The tool's role in cybersecurity is vital as it will be crucial in identifying and comprehending the polymorphic behavior of malware code to make signature-based detection methods more robust to structural changes.

Outcome:

- A system that employs non-deterministic and genetic algorithms to model and generate code mutations.
- Documentation for cybersecurity professionals to effectively utilize the tool.

Expectations from students:

- Programming Skills: Proficiency in C/C++ and Python programming languages.
- Algorithm Knowledge: Familiarity with non-deterministic algorithms.
- Cybersecurity Interest: An interest in cybersecurity and malware analysis.
- Research Skills: Ability to analyze and interpret data to evaluate the tool's effectiveness.

Resources from client:

- Hardware: Access to computing resources for running the algorithms.
- Software: Software tools and libraries required for development.
- Data: Sample source code files for testing and validation.
- Support: Guidance and feedback from cybersecurity experts.