CS 5460: Computer Security I
Fall 2019
Assignment 3
Total Marks: 75

Assume that you are a member of the cybersecurity team in an organization, who are planning to develop a new cryptographic hash function, and thus, invited prototype from team members. Your prototype might not be ready yet for a real-life deployment, but is expected to demonstrate your readiness to be a part of cutting-edge project on new hash function development. So, the prototype should clearly reflect your *knowledge* and *creativity*.

Deliverables for the Prototype:

1. Pseudocode (or circuit diagram) of your cryptographic hash function.
2. Written explanation of how your algorithm satisfies the properties of cryptographic hash function.
3. Implementation of the algorithm using any programming language of your choice. Your programs need to have required input fields and mechanism to show the output.

Submission and Demonstration

- You will need to submit the noted deliverables including a working version of your code through email to GTA of this course (Manazir Ahsan, email: manazir.ahsan@aggiemail.usu.edu) before **11:59 PM on Thursday, October 17**. If needed, add additional instructions for running the code in a 'Read Me' file.

- One submission is required from each group (all group members need to be cc'd in the submission email). See Late Submission Policy in course syllabus.

- The subject-line of the email: **CS 5460: Assignment 3 Submission: <Group Name>**

- Each group, with all members present, will need to demonstrate the code on **Monday, October 21**. Attendance during demonstration is required. A student will not receive any marks for the assignment if he/she fails to attend the demonstration.