SEC 540 – Project Proposal
November 27, 2020

❖ **Project Title:** Missile Launcher System.

❖ **Team Members:**

- Muhammad Basurrah: 201564030
- Hussain Alrajjal: 201550190

❖ **Topic:** Number Theory

❖ **Abstract:**

In this project, the goal is to assure that a certain missile will not be launched if all five generals have consensus to launch it. The value S is an extremely large secret integer used to unlock a missile system. Each general will have a key where the combination of them all will unlock the key, thus, it will be launched.

❖ **Requirements/Options:**

(a) Design a cryptosystem that solves this problem using the Chinese remainder theorem.

(b) If one of the lieutenant generals also becomes incapacitated, can the other four launch the missiles? Estimate the time they need to launch the missiles without the information held by incapacitated lieutenant using the big-O notation in terms of N.

(c) Design another cryptosystem in which any three of the five lieutenants can agree to launch the missiles.

(d) Implement your design in (c) and test it with large integer N. Report the approximate size of N that can be handled by your implementation.

(e) If only two lieutenants agree to launch the missiles, estimate the time they need to succeed using the big-O notation in terms of N.

(f) Generalize this system for 10 lieutenants where any set of k lieutenants can work together to launch the missiles, where $2 < k < 10$. (Note: a set of $k - 1$ of them should not be able to unlock the system). Such a setup is called a k threshold system for sharing a secret. Implement the design and report the approximate size of N that can be handled by your implementation. [Optional for individuals]