Project Ragnarok: Post-Quantum Cybersecurity with Lightning data

Group Members:

- Joanna Zhang (zhangj2022@my.fit.edu)
- Gianni Bubb (gbubb2022@my.fit.edu)
- Aidan Nelappana (anelappana2021@my.fit.edu)

Advisor: Dr. Bhattacharyya, sbhattacharyya@fit.edu

Client: Dr. Bhattacharyya, sbhattacharyya@fit.edu

Date(s) of Meeting(s) with the Client for developing this Plan: Jan 15, 2026, and Jan 20, 2026: gaining a better understanding of the project and receiving the previous project's repository.

Goal and Motivation

Project Ragnarok will be built off and extend the efforts of Project Thor, which was an attempt to remedy the pitfalls of current psuedo-random number generation. Its goal was to create a web application to generate encryption keys with a non-deterministic process to improve security and entropy. As the name suggests, Project Thor picked lightning data to achieve less predictable natural randomness. Cryptography needs to constantly evolve in order to secure data. We believe this idea can be extended into the post-quantum age where many of our current cryptosystems are vulnerable to such attacks. These two aspects will work together to revolutionize cryptography.

For our project we will improve the encryption algorithm of the existing system and ensure there is high entropy. The user will be able to protect against quantum-computer-aided attacks. The lightning database will be secure.

Approach (key features of the system)

The user can generate cryptographic keys that are generated with a non-deterministic process via a website.

- The user will be able to use encryption that is resistant to quantum-assisted attacks by utilizing a newly developed cryptographic algorithm. Since there is currently no fully functional, large-scale quantum computer, the security of the algorithm is evaluated theoretically based on existing literature, mathematical proofs, and simulations that model potential quantum attack scenarios. This approach allows us to assess the algorithm's resilience against known quantum algorithms while remaining consistent with current technological limitations.
- The user will be able to access random numbers through a python API. The previous project wanted to implement a better way to access their generated keys. The API will improve the ease of accessing and implementation of generated keys. The database will be updated continuously with new data.

- The previous project implemented an elementary way of entropy maximization without any guaranteed theoretical backing. We want to improve upon the random number generation by using mathematical formulations to prove that these random numbers are truly random and meet the NIST standards. This will ensure that the project will be of use to computer scientists and cryptography researchers.

Novel features/functionalities
Post quantum encryption is still not a standard feature of current cryptosystems.

Algorithms and tools
Previous encryption schemes developed and post-quantum encryption algorithms approved by NIST.

Technical Challenges
We do not have a good understanding of how cryptography works and how these systems are developed. We also must understand how post-quantum cryptography works.

- Basic cryptography and post-quantum cryptography.
- Measuring and Maximizing Entropy
- Python APIs
- Securing Databases

Milestone 1 (Feb 23): itemized tasks:

1) Compare and select technical tools
   a) Project THOR's implemented AES encryption
   b) NIST Post-Quantum Cryptography
      i) Lattice
      ii) Multivariate
      iii) Hash-based
      iv) Supersingular elliptic curve isogeny
   c) Securing Database
      i) Planning & Scope Definition
      ii) Information Gathering
      iii) Threat Modeling & Risk Analysis
      iv) Vulnerability Identification
      v) Vulnerability Analysis & Validation
      vi) Exploitation
      vii) Privilege Escalation & Post-Exploitation
      viii) Security Controls Testing
      ix) Reporting & Documentation
2) Provide demos to using chosen options to show:
   a. Importing raw data to database
   b. Display data from database to user on web browser

c. Small presentation detailing the entropy found in the data set thus far.

3) Resolve technical challenges
   a. Create cloud-based server environment for application testing
   b. Setting up backend option to add raw data to database
   c. Designing our key generator using a well-known algorithm
   d. Maximizing the entropy of the random numbers generated .
4) Compare and select collaboration tools for software development, documents/presentations, communication, task calendar
   a) Software development: GitHub
   b) Documents/presentations: Google Drive (Docs and Slides)
   c) Communication: Discord Server, Text messaging
   d) Task Calendar: Google Calendar
   e) Create Requirement Document
5) Create Design Document
6) Create Test Plan

Milestone 2 (Mar 30): itemized tasks:

a) Have all of the math finalized
b) Implement a basic python API
c) Implement the basic PQ algorithms
d) Have test for maximizing the entropy of the random numbers
e) Remediation & Fixes Database security

Milestone 3 (Apr 20): itemized tasks:

a) Retesting / Verification Database security
b) Guarantee the random numbers satisfies the NIST standards

Task matrix for Milestone 1

Task	Aidan	Gianni	Joanna
Compare and select Technical Tools	NIST PQ	Python API	Database Security
"hello world" demos	Basic NIST implementation	Basic python API	Run the old project
Resolve Technical Challenges	Measuring entropy	Setting up the cloud-based server and backend	Identify potential threats, attack surfaces, and high-value assets; prioritize risks based on impact and likelihood
Compare and select Collaboration Tools	Establish private discord server	Establish Git repository, Google Drive	Establish text messaging group chat
Requirement Document	Write 33%	Write 33%	Write 33%
Design Document	Write 33%	Write 33%	Write 33%
Test Plan	Write 33%	Write 33%	Write 33%

Approval from Faculty Advisor

"I have discussed with the team and approve this project plan. I will evaluate the progress and assign a grade for each of the three milestones."

Signature: ______________________________________ Date: _______________________