# Project progress report 2

Student name: Ayush Keshar Prasai

Student name: Ronit Ashok Maheshwori

Student name: Jalay Shah

Student name: Virajsinh Jeetendra Sinh Rahevar

Unit: COIT20265

Unit mentor: Mohammed Mohammed

Unit coordinator: Fariza Sabrina

# Introduction

This progress report lists the progress made from the project plan derived previously on the project in terms of technical contributions. The information in this progress report depicts the depth of the progress made and the contributions everyone made towards forging the contents of the actual project plan.

# GitHub link:

https://github.com/ayush12198371/Quantum-Safe-Cryptography-Mitigating-Vulnerabilities-in-Post-Quantum-Era.git

# Technical Artefacts:

|  |  |
| --- | --- |
| Student | Technical artefact |
| 1. Ayush Keshar Prasai | -review of the KEM algorithm, NTRU, Rainbow literature |
| 1. Ronit Ashok Maheshwori | -literature of NTRU  -implementation |
| 1. Jalay shah | -literature of Rainbow  -implementation |
| 1. Virajsinh Jeetendra Sinh Rahevar | -literature of KEM  -implementation |

# Task completed

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| s/n. Tasks from the Project Plan | Deliverables | Student contribution | Start-Date of completion | Task progress |
| 1. Research post-quantum computational ability. |  | Virajsinh Jeetendra Sinh Rahevar/ Jalay Shah | 30/07/2024-05/08/2024 | 80% |
| 1. Outline post-quantum computational limit. |  | Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 30/07/2024-05/08/2024 | 80% |
| 1. Research present day computational ability | -vulnerability  -risks from threat actors | Ayush keshar Prasai/ Ronit Ashok Maheshwori | 10/07/2024-14/07/2024 | 80% |
| 1. List present day algorithms. | -present day cryptography  -algorithms in use | Jalay Shah/Ayush Keshar Prasai | 14/07/2024-16/07/2024 | 80% |
| 1. Outline present day computational limit. | -widely accepted vulnerabilities | Ronit Ashok Maheshwori/ Ayush keshar Prasai | 16/07/2024-19/07/2024 | 80% |
| 1. Compare present day computational limit to post-quantum computational ability. | limitation of modern computers  -post-quantum vulnerabilities list | Ronit Ashok Maheshwori/ Jalay Shah | 19/07/2024-23/07/2024 | 80% |
| 1. Review of the tasks completed | Draft documentation | Ronit Ashok Maheshwori/ Jalay Shah/ Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 24/07/2024-05/08/2024 | 40% |
| 1. Project Plan | Documentation | Ayush Keshar Prasai | 19/07/2024-24/07/2024 | 100% |
| 1. Progress report | Documentation | Ayush Keshar Prasai | 24/07/2024-05/08/2024 | 100% |
| 1. System implementation | System | Ronit Ashok Maheshwori/ Jalay Shah/ Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 05/08/2024-  20/08/2024 | 50% |
| 1. Draft report | Documentation | Ayush Keshar Prasai | 20/08/2024-  26/08/2024 | 100% |
| 1. Derive risk associated with present algorithms relating to post-quantum ability. | Documentation | Jalay Shah/Ayush Keshar Prasai | 26/08/2024-  01/09/2024 | 100% |
| 1. Identify and outline vulnerabilities in present computational ability and cryptographic techniques. | Documentation | Ronit Ashok Maheshwori | 01/09/2024-  03/09/2024 | 100% |
| 1. Explain the need for transition from present cryptographic techniques in relation to risk. | Documentation | Ayush Keshar Prasai | 03/09/2024-  05/09/2024 | 100% |
| 1. Propose such transition. | Documentation | Virajsinh Jeetendra Sinh Rahevar | 05/09/2024-  06/09/2024 | 100% |
| 1. Literature review | review | Ronit Ashok Maheshwori/ Jalay Shah/ Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 06/09/2024-  09/09/2024 | 100% |
| 1. System implemetation | Implementation drafts | Ronit Ashok Maheshwori/ Jalay Shah/ Ayush Keshar Prasai/ Virajsinh Jeetendra Sinh Rahevar | 06/09/2024-  09/09/2024 | 20% |
| 1. Progress report 2 | report | Ayush Keshar Prasai | 09/09/2024-  12/09/2024 | 100% |

# Change from the project plan

As the project progresses, some of the key tasks assigned have been required to change in addition to the team member for this project group. With equally assigned tasks and expected outputs, the addition of team members has led to tasks being reassigned and scheduled to another completion date. Furthermore, some of the new tasks that were in priority were added to the lists of tasks and slotted in front of the scheduled tasks to be completed and presented first such as system implementation.

1. Schedules:

Due to added scope from the project plan, the schedule of the tasks completed were changed drastically where approximately 12 days were added to the existing schedule and spent on system implementation, draft and literature review.

1. Tasks:

The tasks added to the existing schedule were:

|  |  |  |
| --- | --- | --- |
| Task | Description | deliverable |
| 1. Literature review | -literature review was performed on an existing topic relating to the topic undertaken where ample number of algorithms were reviewed, and some were chosen in relevance to the topic. | -relevant algorithm forging  -implementation draft |
| 1. System implementation | -implementation of such algorithms were done and portrayed to show quantum cryptography techniques and vulnerabilities | -system implementation |

# Issues and challenges

Some of the issues faced by the team while working on the tasks are:

1. Scheduling conflicts.
2. Ineffective communication.
3. Failure to publish technical artefacts on scheduled time.
4. Ineffective communication.
5. Inadequate backup strategies.

Some of the challenges of this project were:

1. Non-existent background knowledge.
2. Low morale.
3. Problem dumping.
4. Ineffective reviews.

# Addressing challenges:

Challenges were addressed when:

1. Collaboration techniques were re-imagined and interpreted.
2. Backups were tracked back.
3. Excessive amount of time was spent on researching literature topics.

# Priority tasks

|  |  |  |
| --- | --- | --- |
| tasks | Student1 | Student 2 |
| 1. Implementation | Ayush keshar Prasai/jalay shah | Virajsinh Jeetendra Sinh Rahevar/ronit maheshwori |
| 1. Proposing transition | Ayush keshar Prasai/jalay shah | Virajsinh Jeetendra Sinh Rahevar/ronit maheshwori |