Quantum Cryptography: Summer of Science 2024

Harshil Solanki
Roll number: 23B1016
Mentor: Raunak Gupta

May 24, 2024

Learning Objectives

- I see the Summer of Science project as an opportunity to gain insights into the way research is done and how material is presented and organised, while learning new skills and knowledge of Cryptography.
- Particularly, in relation to the topic, I want to dive deep into the prospects of Quantum Cryptography, the work that is done by Scientists till now and all that can possibly be done in the future.
- I want to familiarise myself with the evolving Quantum technology and gain insights into how Mathematics can be used to incorporate it with Cryptography.
- In the end, it's all to fulfill my curiosity and explore the horizons of Science.

References

- Cryptography and Network Security 3rd Edition - Atul Kahate, McGraw Hill Education (India) Private Limited
- Cryptography and Network Security: *Principles and Practice* 7th Edition - William Stallings, Pearson
- Elementary Number Theory 7th Edition - David M. Burton
- Quantum Computation and Quantum Information - Michael A. Nielsen and Isaac L. Chuang
- Quantum Cryptography and Secret-Key Distillation - Gilles Van Assche

PLAN OF ACTION

Week 1	Mathematical Foundation: (Advanced) Number Theory and Introduction to Cryptography
Week 2	Classical Cryptography: Historical Ciphers, Symmetric Key Cryptography, Assymetric Key Cryptography
Week 3	Cryptographic Hash Functions, Digital Signatures and Public Key Infrastructure
Week 4	Cryptographic Protocols and Information Theory
23^{rd} June	Mid-Summer Report Submission
Week 5	Advanced Cryptographic Concepts: Elliptic Curve and Lattice-based Cryptography
Week 6	Quantum Computing Basics
Week 7	Quantum Cryptography: Quantum Key Distribution (QKD) and Post-Quantum Cryptography
Week 8	Insights into new possibilities
23^{rd} July	End-Summer Report Submission