FIRST meeting document

Name	NTRUP Post Quantum Cryptography
Date	09/11/2019
Student	Smeallie. Aran
Admin	1. Meeting Times: Every two weeks at 9am on Wednesday 2. Meeting scheduling. Email me at crypjt@gmail.com at the start of the week if you want to meet. 3. Write up in LaTeX 4. Keep a glossary and bibliography from the start 5. Diary of what you did. Especially what didn't work. 6. Project deadline March 20th 2020. 7. PLEASE NOTE: The last meaningful feedback on your thesis will be given one week before the ORIGINAL project deadline. You should submit any drafts before this date. 8. Project Credits □ 15
Work plan	Main Idea: Post-quantum Crypto To understand and implement the NTRU algorithm Ten to investigate the post Quantum proposal Fundamentals: Work through the papers below and get a handle on • Why RSA is vulnerable to a Quantum Computer • What the PQC competition is about • The idea of NTRU and how it differs from RSA • What makes it PQ resistant • Produce a Java prototype of NTRU • Produce a Java prototype of the NTRU KEM

	Describe and explain them in your write up. Implement (Paying attention to Extras below) them in Python/Java and gather some data. (Including the inevitable problems that arise) Present your results.
References	• Stinson – Cryptography NTRU system • Post Quantum Cryptography ISBN 978-3-540-88701-0 • https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf • https://pqcrypto.org/ • https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
Current Action points.	1. 2. 3. 4.