Something Awesome Proposal:
(Mostly) Weekly Crypto Challenge

Youhan Cheery (z3417483)

16 March 2017

1 Introduction

- Completing a weekly cryptography challenge found on *http://cryptopals.com/*
- I have some theoretical understanding of cryptography (through MATH3411 - Information, Codes and Ciphers). However I have no experience actually applying the theory that I learned.
- I would like to undertake the weekly challenges, of which there are about 6-7 sub-challenges in each of these.
- The weekly topics include:
    1. Basics
    2. Block cryptography
    3. Block and stream cryptography
    4. Stream crypto and randomness
    5. Diffie-Hellman
    6. RSA and DSA
    7. Hashes
    8. Abstract algebra
- I would then like to compile the work that it takes to solve these problems in a separate report for future students' use.
- As I am currently working on a thesis, I imagine I will go through periods of inactivity depending on the state of my thesis. To prevent going through long periods of inactivity on the cryptography challenges, I will outline the theory of the modules involved in the report prior to undertaking the challenge. I don't think this in itself is trivial, but I'm fairly certain it will take a lot less time than the challenges.

2 Plan

Assuming the project will begin from week 4, that leaves me approximately 10 weeks (including the break week) for the due date. Cryptopals claims that the difficult increases further down the line, which on the surface seems true given the topic titles. As such, having a 2 week buffer to handle more complex challenges seems reasonable.

I am not under the impression I will be able to complete everything. However I will definitely attempt to, and will blog as I go along.