1 Work Plan

1.1 Literature review

Duration: ?

This stage will involve reviewing the research into producing near collisions with SHA1. This may also extend into producing a review around full collisions of SHA1.

SHA1 has been selected due to its vulnerability. Methods for producing collisions have been known for a long time and it seems the algorithm is on its way out of mainstream use.

1.2 Formulation specific research questions

Duration: ?

Questions may currently involve:

- What is the probability of producing near-collisions with SHA1?
- What would be the complexity in storage and computation?
- Can such near-collisions be generated e.g. using the university's high-performance computing facilities?

Further questions may be added using information gained from already performed research.

1.3 Implementing near-collision code

Duration: ?

This section will involve the actual implementation of code using knowledge gained through the literature review. This may be pre-existing code manipulated to work on the university's HPC cluster.

1.4 Determining metrics for measuring experiments

Ways to measure the progress of a project

1.5 Experimentation stage

Duration: ?

This stage will involve running experiments to gain complexity data. This may involve working on further research and validating results.

1.6 Thesis/Paper writing

Duration: ?

This will involve the creation of a ˜70 page dissertation alongside a condensed paper for submission to a journal

2 Delivery Plan

2.1 Literature Review

This will be the process defined in Section 1.1.

2.2 Relevant code

This section may change but it will be any code used to produce near collisions. Section 1.3 in the Work plan contains details on this section.

2.3 Experiment Results

2.4 Thesis

2.5 Paper