Iteration 1 Report - Leonid Lygin

Intro

- **Student name**: Leonid Lygin.
- **Topic**: brute-force assistance for asymmetric encryption.
- **Supervisor**: Phillip Braun.
- **Iteration number**: 1.

Initial plan

Initially, the plan for this iteration was “researching existing methods on the topic and providing a summary on them”.

Actual work done

Several attack vectors for asymmetric cryptography were analysed and summed up.

References to results

Bundled document (`vectors.pdf`) contains the summary of attack vectors on asymmetric crypto and further research directions.

Current issues

The resulting vector would probably change into designing a process to produce specific EC parameters with backdoors, which would look like normal parameters, but would allow the attacker to crack the encryption with significantly less effort that plain brute-force.

Plan for the next iteration

Initial plan for the next iteration was to compare performance for brute-force, but it seems that a more interesting approach would be to design some “nice” EC parameters with backdoors, so plan for the next week would be to research them more comprehensively, and maybe experiment with some known weak curves