KTH Royal Institute of Technology
School of Computer Science and Communication

El Gamal Mix-Nets and Implementation of a Verifier

SA104X Degree Project in Engineering Physics

Carl Svensson carlsven@kth.se & Erik Larsson erikl3@kth.se
Supervisor: Douglas Wikström

A mix-net is a cryptographic protocol based on public key cryptography which enables untraceable communication through a collection of nodes. One important application is electronic voting where it enables the construction of systems which satisfies many voting security requirements, including verifiability of correct execution. Verificatum is an implementation of a mix-net by Wikström.

This report concerns the implementation of a verifier and evaluation of the implementation manual for the Verificatum mix-net. The purpose of the document is to enable third parties to convince themselves that the mix-net has behaved correctly without revealing any secret information. It was possible to implement a simple version of the verifier using the document and some test vectors generated by the mix-net. While the document is complete regarding content there still exist some possibilities for further clarification to make it comprehensible to a larger audience.