Enigma Project Plan

Adam Mulligan

October 3, 2011

1 Goal

The goal of this project is to display an understanding cryptographic systems based on prime numbers and related number theory by producing a number of utilities that implement cryptographic standards, and also produce a final application that utilises these standards to provide a product or service that could be used for secure communications.

2 Main objectives

1. RSA Encryption
   (a) Produce a set of command line utilities that:
      i. Generate RSA keys and stores/outputs them
      ii. Encrypts binary data using these keys
      iii. Decrypts enciphered data using these keys
      iv. Possibly include signing
2. DES or AES
   (a) Produce a set of command line utilities that implement RSA as above, but:
      i. Encrypt and decrypt using symmetric cryptography
      ii. Share the key using RSA
3. GUI Application
   (a) Produce a fully-fledged application that:
      i. Allows [at least] two users to communicate with text
      ii. (?) Allows users to send files to each other during chat
      iii. Text and files should be encrypted using methods in Points 1 and 2

3 Secondary objectives

1. Attacks
   (a) Consider attacks on RSA and other crypto algorithms, such as integer factorisation, and attempt to implement them
2. Numerical experiments
3. Look in to using other encryption algorithms