Assignment 5: RSA

1 Implementation

You are to implement RSA. Use your entropy gathering implementation for the public key generation. Use `libgmp` for computations with large numbers. You should provide three programs. The first program creates a new RSA key and writes public and private keys to two files (given as first and second argument respectively). The second program encrypts a (short) message (read from stdin, written to stdout) given the filename of the public key. The third program decrypts a (short) message (read from stdin, written to stdout) given the filename of the private key. Measure the execution time of each of the three operations and include the time in a comment at the beginning of each file.

2 Submission

You must submit the implementations to your subversion repository to the directory `courses/comp3704/s2009/$USER/p5/`. Do not include generated files. The submitted files should be called:

- `create.c`
- `encrypt.c`
- `decrypt.c`
- `Makefile`

You must check that the submitted code compiles by invoking `make`. Verify that the output of your program matches the expected output using your own testcases.