# Cryptography

## Programming 6

**Ex 1** Implement an RSA encryption/decryption algorithm in two versions: one that uses *Chinese remainder algorithm* (CRT) and the second one "regular". Generate keys using openssl, set the security parameter to 256 (see NIST SP800-57).

To find $p, q$ use: *openssl rsa -noout -text -in privkey.pem*.

Compare efficiency of both implementations.

**Ex 2 (for algorithmic track)** Add key generation to your RSA implementation. Compare efficiency of encryption/decryption for various pairs of $e, d$.

Implement Wiener's attack on low exponent (see: `http://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf`). Your implementation will be tested: on input $\langle N, e \rangle$ your program should return $d$ (assuming that $d < \sqrt[4]{N}/3$.

**Ex 2 (for security track)** Add key generation to your RSA implementation. Implement Kocher's Timing attack.

**Ex 3 (for security track)** Implement Fault Attack on CRT implementation.