Assignment 1, Due Date 24-01-15

I Use of OpenSSL

(a) Use Open SSL to generate an RSA public key-private key pair for different key sizes. What is the value of e (encryption key)? What is the size of p, q and the decryption key. Show one set of n, p, q, e, d.

(b) How is input text converted to bits before being encrypted? What is base-64 encoding and why is it used here?

(c) Determine experimentally the block size used for different key sizes. Is padding used and how?

(d) With key size = 1000, encrypt a bit string of 5000 zeros. Display the output.

(e) Study the OpenSSL source code for RSA and identify the optimization used in decryption/encryption. (More info will be updated soon)

II Question 8, Chapter 6 of the text.

III Question on Firebug, etc. – to appear soon.