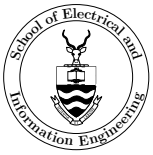

School of Electrical and Information Engineering
University of the Witwatersrand, Johannesburg
ELEN3015 – Data and Information Management

Laboratory 6: Public Key Cryptography - RSA

1 Objective

Objective of the lab: The objective of this lab is to give the student some practical exposure to the concepts and theory of public key cryptography and RSA algorithm presented in class.

2 Requirements

Note: This lab requires some preparation, in terms of theoretical background as well as the use of the tools (use of the D-Lab, Matlab, the m-files, etc.). Students who are unable to do the lab because they have not prepared will be asked to leave.

Instructions, source material and preparation required:

- You are required to do all the preparation needed to implement the algorithms beforehand.
- Lab partners must operate in groups of two (and no larger) and may help each other during the lab but each should use his/her unique messages or codewords in all the exercises and write his/her own lab report.

Report: The report will take the form of the following group of files which should all be attached to a single email:

- An answer sheet (in Word or PDF format) with your name and your lab partner's name and student numbers, the date and experiment number, and your results for the various questions.
- All the m-files used in the lab.

3 Outcomes

1. Key Generation
   - Generate two large primes, p and q, by using one of these two primality test algorithms, Solovay-Strassen test or Rabin-Miller test. Check whether the primality test is working by 'isprime()' function. (Two primes are less than 2^{32}, if use Matlab.)
   - Calculate $m = pq$ and $\phi(m) = (p-1)(q-1)$.
   - Randomly choose public key s (of an appropriate size). Check if s is coprime of $\phi(m)$.
   - Use extended Euclidean algorithm to get private key h. Check if $sh \equiv 1 \pmod{\phi(m)}$
2. RSA Encryption and Decryption
   - Generate 1000 numbers and encrypt them with public k. Record the processing time.
   - Decrypt these 1000 encrypted numbers and verify the algorithm. Record the processing time.