Cryptology 2008
(Home work 3)

April 15, 2008

- Due on Tuesday, April 25, midnight.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.
- Each problem bear 10 points.
- **You can use any programming language, even a very high-level language like MAPLE. Or you can use any other publicly available library for long integer arithmetic. Email me your programs with the results at debrup@cs.cinvestav.mx please put Crypto-HW3 as the subject**

1. Implement the Miller Rabins primalility test.
2. Using the algorithm above generate two 128 bit strong primes.
3. Generate the public and secret keys for RSA using the product of the above primes as the modulus.