Exercises due November 8th, 2005 1:30pm.

Exercise 1. We define a public key encryption scheme \((G, E, D)\) to be secure if it satisfies the following conditions:

**Validity** For every possible message \(x\), if \((e, d) \leftarrow \mathcal{G}(1^n)\) then \(D_d(E_e(x)) = x\).

**Security** There exist super-polynomial functions \(T, \epsilon\) such that for every two messages \(x, x'\), and every \(T(n)\)-sized adversary \(A\),

\[
\left| \Pr_{(e,d) \leftarrow \mathcal{G}(1^n)}[A(e, E_e(x)) = 1] - \Pr_{(e,d) \leftarrow \mathcal{G}(1^n)}[A(e, E_e(x')) = 1] \right| < \epsilon(n)
\]

where this probability is over the coins of both \(G\) and \(E\).

It is not hard to see that if we have a public-key encryption scheme for one bit messages (e.g., \(x\) is either 0 or 1) then we can use it to have an encryption scheme for arbitrarily long messages.

Consider the following assumption:

**Axiom 3: Factoring Blum Integers is hard.** There exist super-polynomial function \(T, \epsilon\) such that for every \(T(\ell)\)-sized adversary \(A\), if \(P\) and \(Q\) are independently chosen random primes between 1 and \(2^\ell\) with \(P, Q = 3 \pmod{4}\) and \(N = P \cdot Q\) then the probability that \(A(N) = P \circ Q\) (i.e. \(A\) outputs the factorization of \(N\)) is less than \(\epsilon(\ell)\).

Give a full proof that if Axiom 3 is true then there exists a secure public key encryption scheme for one bit messages.

**Hint:** Start by proving formally that the modified Rabin collection is a trapdoor permutation if factoring Blum integers is hard. Then use the Goldreich-Levin hardcore bit theorem to construct an encryption scheme. You will probably find parts of your answer to Exercise 1 of the previous handout useful. In particular, you can use in your answer the Goldreich-Levin lemma without proving it.