Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 7
September 25, 1997

Problem Set 3

This problem set is due on *Thursday, October 2, 1997* at the end of class. Late homeworks will *not* be accepted.

Mark the top of each sheet with your name, 6.857, the problem set number, and the date. Type up your solutions, and be clear. Points may be deducted if your TA has problems understanding your solution.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

Problem 3-1. Messages Which Equal Their Encryptions

Show that the number of plaintexts m in Z_n^* such that

$$E(m) = m \pmod{n},$$

where E is the RSA encryption function with public modulus $n = pq$ and public encryption exponent e, is equal to

$$\gcd(e-1, p-1) * \gcd(e-1, q-1)$$

Hint: consider what happens mod p and mod q separately. Take logarithms (where the base is a generator mod p, or mod q)

Problem 3-2. Common Modulus Systems

Alice and Bob are very good friends. In order to save time, they agree to simply find one good pair of primes p, and q, and therefore use the same public modulus $n = pq$. Of course, to not have any confusions over who signed which message and to prevent, they select different exponents e_a and e_b.

Show that in this system, it is possible to decrypt a message M sent to both of them if $\gcd(e_a, e_b) = 1$. That is, given:

$$\begin{aligned} C_a &\equiv M^{e_a} \pmod{n} \\ C_b &\equiv M^{e_b} \pmod{n} \end{aligned}$$

an adversary can compute M.