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

Handout 11
September 25, 1997

Solutions to Problem Set 3

Reminder: Please type up your problem sets. The TA will deduct points from future problem sets if they are not typed up. You may add things you could not type by hand (pictures, complex symbols).

Problem 3-1. Messages Which Equal Their Encryptions

We have $m \in Z_n^*$ such that

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

where E is the RSA encryption function with public modulus $n = pq$ and public encryption exponent e. This is the same as claiming

$$m^e \equiv m \pmod{n}$$

We now analyze it in terms of p and q seperately.

$$\begin{aligned} m^e \bmod n &= m \bmod n \\ m^e \bmod n \bmod p &= m \bmod n \bmod p \\ m^e \bmod p &= m \bmod p \\ m^e &\equiv m \pmod{p} \end{aligned}$$

The same is true mod$q$.

We now proceed to figure out how many messages like that exist. We know a generator exists for p, which we shall call g. We know that for all $m \in Z_p^*$, there exists x such that $g^x \equiv m \pmod{p}$. We also know that $a^x \equiv a^y \pmod{n}$ if and only if $x \equiv y \pmod{\phi(n)}$. We can therefore compute:

$$\begin{aligned} m^e &\equiv m \pmod{p} \\ (g^x)^e &\equiv g^x \pmod{p} \\ g^{xe} &\equiv g^x \pmod{p} \\ xe &\equiv x \pmod{\phi(p)} \\ xe &\equiv x \pmod{p-1} \\ x(e-1) &\equiv 0 \pmod{p-1} \end{aligned}$$

Finally, Corollary 33.22 claims $ax \equiv b \pmod{n}$ has $d = gcd(a, n)$ solutions or none at all. Since we know of at least one solution ($x = 0$), we believe there are $gcd(e-1, p-1)$ solutions.

By similar means, we discover there are $gcd(e-1, q-1)$ solutions for the same question $\pmod q$.

Now, We need to extend back to $\pmod n$. First, we note that each solution in $\pmod p$ maps to q solution in $\pmod n$, which gives us $q * gcd(e-1, p-1)$ potential messages in $\pmod n$. Again similar arguments can be made for the $\pmod q$ part. So, if we put all the messages together, we get a pool of $p * q * gcd(e-1, p-1) * gcd(e-1, q-1)$ to choose from.

HOWEVER, we know, by the Chinese Remainder Theorem, that there exists a uniqe mapping for $\pmod n$ and the "vectors" formed by the $\pmod p$, $\pmod q$ combinations. Whatever properties we compute in $\pmod n$ still hold in the "vector" and vice versa. So, given any solution we found in $\pmod p$, and any solution we found in $\pmod q$, we can map to a solution in $\pmod n$. This is a unique one-to-one mapping, so overlaps can't exist.

The total number of possible pairs is $gcd(e-1, p-1) * gcd(e-1, q-1)$, and thus we get our solution.

Problem 3-2. Common Modulus Systems

We have:

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

We also know that $gcd(e_a, e_b) = 1$. First, we know that we can plug these into the Extended Euclid computation to yield constants (a, b) such that:

$$e_a a + e_b b = gcd(e_a, e_b) = 1$$

Finally, we know we can compute the following:

$$\begin{aligned} M^{xe_a} &= {C_a}^x \\ M^{e_a+e_b} &= C_a C_b \\ M^{xe_a+ye_b} &= {C_a}^x {C_b}^y \\ M^{ae_a+be_b} &= M^1 \end{aligned}$$

We know that one of (a, b) will be negative. Assume without loss of generality that it is a. We can't really compute M to the power of a negative number, BUT we can use Extended Euclid again to find the inverse of $C_a = {C_a}^{-1}$. Then, we simply compute:

$$M = ({C_a}^{-1})^{-a} {C_b}^b$$