ECE Information and Network Security
Exam 1 solutions
Spring 2006

Short Answer:

1. Note that $n_1 = p_1 q_1$, and $n_2 = p_2 q_2$ for primes p_j and q_j. Since $\gcd(n_1, n_2) \neq 1$, we have that $\gcd(n_1, n_2)$ is a shared factor of both n_1 and n_2. Hence, they share a factor and it is trivial to factor both n_1 and n_2, e.g. by $n_1/\gcd(n_1, n_2)$.

2. If the public encryption exponent e is chosen such that $m < n^{1/e}$, then observe that $m^e < n$. Thus, decrypting $c = m^e \pmod{n}$ can be trivially accomplished by taking the normal e-th root of c.

3. See the book.

4. $x = 10$ since $51 * 10 = 510 \equiv 10 \pmod{100}$.

Challenge Questions:

1. Let c_A and c_B be the outputs of the two machines. Then $c_A - c_B = 0 \pmod{p}$ but $c_B - c_A = 1 \pmod{q}$. Therefore $gcd(c_A - c_B, n) = p$, and $q = n/p$.

2. (a) The keys $K_1, \ldots, K_{16}$ are all the same (all 1's). Decryption is accomplished by reversing the order of the keys to $K_{16}, \ldots, K_1$. Since the K_i are all the same, this is the same as encryption, so encrypting twice gives back the plaintext.

(b) The key of all 0's , by the same reasoning.

3. (a) Assume we have a large number arithmetic library, and a means to generate the digits of e. Simply start by grabbing the first 5 digits of e, (27182), and call this n. Now, divide n by all whole numbers less than $\sqrt{n}$ (use a for loop). If you find any division with out a remainder, then n is not prime, and you move to the next 5 digits. In this case 27182 is divisible by 2, so you move on to $n = 71828$, and then on to $n = 18281$ and so on, each time trying to divide by all numbers less than $\sqrt{n}$.

(b) One can obtain the digits of e via the Taylor expansion $e^x = 1 + x + x^2/2 = x^3/3 + \cdots$. Or, one could use a non-technical approach and search the web, find the digits, download it to a file and use that as the starting point, e.g.

$$2.718281828459045235360287471 \cdots$$