Math 116 Y. X. Zhang Midterm Exam Solutions Fall 2015

1 (25(5) pts.)

Consider the following cryptosystem. Bob generates p and q, big integers, and $M = pq - 1$. Bob then generates $c = aM + p$ and $d = bM + q$ for some random positive integers a and b. Bob finally computes $N = (cd - 1)/M$. Bob publicizes the public key (N, c) and keeps (d, p, q, M) private. Alice encrypts any integer m by computing $mc \pmod{N}$.

1. (5(1) pts) Show that N is a well-defined integer.

   We have $(cd - 1) = (ab)M^2 + (aq + pb)M + pq - 1 = (ab)M^2 + (aq + pb)M + M$, which is divisible by M.

2. (10(2) pts) Bob claims he can decrypt a ciphertext m' by computing $m'd \pmod{N}$. Why does this work?

   We know a correctly-sent ciphertext m' equals mc for some message m. Thus, $m'd = mcd \pmod{N}$. Since $cd = NM + 1$, modulo N we have $mcd = m * 1 = m \pmod{N}$.

3. (10(2) pts) You are Eve. Show that you can break this cryptosystem.

   Since $cd = NM + 1$, we have $\gcd(N, c) = 1$. This means Eve can use the extended Euclidean algorithm to find some d' such that $cd' = 1 \pmod{N}$. Then Eve obtains the message from ciphertext m' by computing $m'd'$, and by the previous problem this recovers the ciphertext.

(This is meant to be a review of basic modular arithmetic, Euclidean algorithm stuff, and the fact that we do not need the exact key to decrypt

(similar to the ClumpyCrypto homework). While it is not necessary that $d = d'$**, it is still true that** $mcd' = m \pmod N$**, so Eve can decrypt any message.)**.

2 (25(5) pts.)

1. (10(2) pts) Compute the last digit of 7^{7^7}. Do not just do pattern recognition – use concepts you learned in class.

   Computing the last digits of an integer is finding the integer modulo 10. We know $\gcd(7, 10) = 1$, so Euler's theorem tells us $7^{\phi(10)} = 1 \pmod{10}$. We know that $\phi(10) = (1/2)(4/5)(10) = 4$, so it suffices to look at $7^7 \pmod 4$, which is $(-1)^7 = 3 \pmod 4$, so the last digit of 7^{7^7} is equal to the last digit of 7^3, which is 3.

   (Pattern recognition gives a 4-periodic pattern quickly. However, the point of this exercise is to think of things in terms of modular arithmetic and Euler Phi function. This way, you know how to do things like find the last two digits of something (you want to then look at $\phi(100)$ in the exponent).).

2. (15(3) pts) Show that you can compute $n!$ for a big integer n in $O(n^2 \log^2(n))$ time. (Hint: be careful if your method generates something that is $O(n \log^2(n))$.)

   We can compute $n!$ by doing $n - 1 = O(n)$ multiplications, starting from 1 end ending at n. In each multiplication, the new number we are multiplying by is bounded above by n and thus have $\log(n)$ length. The other number (the current product) is at most n^{n-1} (since we have multiplied together at most $(n-1)$ numbers, each of which is at most n), which has length bounded above by $n \log(n)$. We know that multiplying a length-m and a length-n integer takes $O(mn)$ time, so each of these operations take at most $n \log^2(n)$ time. Since we do $O(n)$ multiplications, we only need a total of $O(n^2 \log^2(n))$ time.

   (It is easy to assume that the two numbers are both $\log(n)$ length and forget that the current product we keep in memory can get very big. Everything

else comes to fundamental understanding of big O as we did in lecture and review.)

3 (25(5) pts.)

1. (15(3) pts) Prove that if p and q are odd primes, then $a^{\frac{(p-1)(q-1)}{2}} = 1 \pmod{pq}$ if a shares no factor with pq.

   We know that $a^{\frac{p-1}{2}}$ is a well-defined integer k since $2|(p-1)$, so by Fermat's Little Theorem $a^{\frac{(p-1)(q-1)}{2}} = k^{q-1} = 1 \pmod{q}$ because k is not divisible by q (as a is not divisible by q). Similarly, this quantity is $1 \pmod{p}$, meaning it is $1 \pmod{pq}$ by the Chinese Remainder Theorem.

   (You can also directly use the theorem (3.1) that we covered in class if you remember the content correctly, from which this is a direct consequence.)

2. (10(2) pts) Prove that in RSA, for a fixed public key (N, e), where $N = pq$ and p and q are odd primes, the possible private key d that Bob uses to decrypt is not unique (modulo $\phi(N)$).

   To decrypt in RSA, Bob only needs that d satisfies $(m^e)^d = m^{de} = m \pmod{N}$ for appropriate m, which is satisfied exactly when $m^{de-1} = 1 \pmod{N}$. However, the first part of this problem shows that $m^{\frac{(p-1)(q-1)}{2}} = 1 \pmod{N}$. Just adding $(p-1)(q-1)/2$ to a d that works, for example, would obtain a different d' that also works modulo $\phi(N) = (p-1)(q-1)$. Thus, there must be at least 2 keys that could have worked.

   (This is why it makes sense to talk about "decryption exponents" in RSA, instead of "the" decryption exponent/key.)

4 (25(5) pts.)

!!! MID-BOSS !!!

This problem concerns square roots again.

1. (15(3) pts) Suppose we have the equation $x^2 = a \pmod{p^e}$, where p is prime, $e > 0$ is an integer, and p does not divide a. If we have at least one solution for x, show that we have exactly 2. (you may assume we did the case $e = 1$, which was done in homework. Hint: look at $(x + b)(x - b)$, where b is a solution)

   Suppose a has at least one square root b. This means $-b$ is also a square root, as $b^2 = (-b)^2$. Thus, we know $x^2 = a = b^2 \pmod{p^e}$, or $(x + b)(x - b) = kp^e$ for some integral k. Suppose x were a third root not equal to $\pm b \pmod{p^e}$. This is equivalent to p^e not dividing either factor on the left, so we must have at least one power of p in both factors. This means $p|(x + b)$ and $p|(x - b)$, which implies $p|(x+b+x-b)$, or $p|2x$, a contradiction as p does not divide $a = x^2$.

   (Slightly tricky, but there are several ways of getting a contradiction once you think about what the third root can take and there is no fancy theorem. Meant to be the hardest problem.).

2. (10(2) pts) Let p, q, r be prime, and a not divisible by any of these primes. How many square roots of a modulo (p^2qr^3) are there, if we have at least one square root?

If we have at least one square root x, then $x^2 = a \pmod{p^2}$, $\pmod{q}$, and $\pmod{r^3}$. The first part of this problem shows us that a has exactly two roots modulo each prime power, since we know there is at least one. All $2^3 = 8$ ways of picking a square root for each prime power combines into a unique integer modulo p^2qr^3 by the Chinese Remainder Theorem, so there are 8 roots.

(Just standard CRT, hopefully comboing with the homework problem where you show things have 4 square roots modulo pq. If you understood that problem, this is a natural continuation.)