CIS 3362 Homework #6 Solutions

Number Theory, RSA

1) What is the prime factorization of 589449600? (Hint: 97 is a factor of the given number.)

$589449600 = 100 \times 5894496 = 2^2 5^2 (2^5)(184203) = 2^7 5^2 3^2 (20467) = 2^7 3^1 5^2 97^1 211^1$

2) What is φ(589449600)?

$\varphi(589449600) = \varphi(2^7 5^2 3^1 97^1 211^1) = (2^7 - 2^6)(3^2 - 3^1)(5^2 - 5^1)(97^1 - 97^0)(211^1 - 211^0)$

$= 64 \times 6 \times 20 \times 96 \times 210 = 154828800$

3) Using Fermat's Theorem, determine 3456^{25178} mod 2099.

Note: Fermat's Theorem says that $1357^{2098} \equiv 1 \bmod 2099$. (4 pts)

$3456^{25178} \equiv 1357^{25178} \equiv (1357^{2098})^{12}(1357^2)$
$\equiv 1357^2$ (due to Fermat's Theorem)
$\equiv 1841449$
$\equiv 626 \bmod 2099$

4) Using Euler's Theorem, determine 13^{6051} mod 2664.

Note: $\varphi(2664) = \varphi(2^3 3^2 37^1) = (2^3 - 2^2)(3^2 - 3^1)(37^1 - 37^0) = 4 \times 6 \times 36 = 864$. Thus, Euler's theorem says that $13^{864} \equiv 1 \bmod 2664$. (2 pts)

$13^{6051} \equiv (13^{864})^7 (13^3) \bmod 2664$
$\equiv (13^3) \bmod 2664$, due to Euler's Theorem
$\equiv 2197 \bmod 2664$

5) In an RSA scheme, p = 13, q = 31 and e = 127. What is d?

n = 13 x 31 = 403
φ(n) = 12 x 30 = 360

gcd(360, 127) = 1

360 = 2 x 127 + 106
127 = 1 x 106 + 21
106 = 5 x 21 + 1
106 – 5(127 – 106) = 1
106 – 5(127) + 5(106) = 1
6(106) – 5(127) = 1
6(360 – 2x127) – 5(127) = 1
6 x 360 – 12x127 – 5x127 = 1
6x360 – 17x127 = 1
d ≡ -17 ≡ 343 mod 360, so d = 343.

6) One of the primitive roots (also called generators) mod 29 is 2. There are 11 other primitive roots mod 29. One way to list these is 2^{a1} mod 29, 2^{a2} mod 29, … 2^{a12} mod 29, where 0 < a1 < a2 < … < a12. (Note: it's fairly easy to see that a1 = 1, since 2 is a primitive root.) Find the values of a10, a11 and a12 and the corresponding values 2^{a10} mod 29, 2^{a11} mod 29, and 2^{a12} mod 29.

The list $a_1, a_2, \ldots, a_{12}$, is simply the list of values relatively prime to 28. In essence, if g is a generator, it's easy to see that g^x is NOT a generator if x and 28 share a common factor. For example, if x = 6, then $(g^6)^{14} = g^{84} \equiv (g^{28})^3 \equiv 1$ mod 29. In general, for any x that shares a common factor with 28, we see that 28/c, where c is that common factor is an exponent we can raise g^x to, to obtain 1. Thus, the values of a_{10}, a_{11} and a_{12} are 23, 25, and 27, respectively, as none of these shares a common factor with 28, and they are the last three numbers with that property in [1, 28]. Thus, the values we seek are 2^{23}, 2^{25} and 2^{27} mod 29. We can calculate the first and easily obtain the last two from the first:

$2^{23} = 8388608 \equiv 10$ mod 29, thus
$2^{25} = 2^{23}2^2 \equiv 10(4) \equiv 40 \equiv 11$ mod 29
$2^{27} = 2^{25}2^2 \equiv 11(4) \equiv 44 \equiv 15$ mod 29.

7) In the Diffie-Hellman Key Exchange, let the public keys be p = 29, g = 19, and the secret keys be a = 11 and b = 13, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share?

Alice sends Bob $19^{11} \equiv (19^5)^2 19 \equiv 21^2(19) \equiv 27$ mod 29
Bob sends Alice $19^{13} \equiv (19^{11})(19^2) \equiv (27)(361) \equiv 3$ mod 29

Secret Key = $(19^{13})^{11} \equiv 3^{11} \equiv 15$

8) In El Gamal, Alice chooses $Y_A = \alpha^{XA} \bmod q$. Bob, who is sending a message, calculates a value $K = Y_A^k$, where k is randomly chosen with $0 < k < q$. Is it possible that for different choices of k, Bob will calculate the same value K, or will each unique value of k be guaranteed to produce a different value for K? Give a brief rationale for your answer.

Yes, it's possible that for two different k's, the same K will be produced. Consider if Alice chooses X_A that shares a common factor with q – 1. (Since q is a large prime, there are several possible choices, as q – 1 is even.) As an example, let $X_A = 2c$. Consider some integer $k < (q – 1)/2$ and another integer $k' = k + (q – 1)/2$. Consider the two values of Y_A and Y'_A calculated in these scenarios:

$$Y_A = \alpha^{X_A k} \bmod q$$

$$Y'_A = \alpha^{X_A(k+\frac{q-1}{2})} \equiv \alpha^{X_A k}\alpha^{X_A(\frac{q-1}{2})} \equiv \alpha^{X_A k}\alpha^{2c(\frac{q-1}{2})} \equiv \alpha^{X_A k}\alpha^{c(q-1)} \equiv \alpha^{X_A k} \bmod q,$$

via Fermat's Theorem, since that last term is 1 mod q.

If X_A shares no common factors with q – 1, this is NOT possible.

9) Write a program that prompts the user to enter an integer, n, in between 1 and 10^{12} and calculates φ(n).

Attached program is phi.c. Note: I just used long long in C, which suffices since I never square a number in this program.

10) Using your program from question 1, write a program that determines if (a) an input value in between 1 and 10^{12} is prime, and (b) if so, asks the user to enter an integer in between 1 and the prime number minus 1 and determines if that value is a primitive root. Your program should work as follows:

Calculate each unique prime factor q_i of p – 1, and calculate $x^{(p-1)/qi} \bmod p$ for each q_i. If none of these are equal to 1, then x is a primitive root.

Attached program is primroot.c. Note: I had to do some trickery (rewrite modular multiplication) to avoid overflow errors when multiplying two terms greater than 10^9.

11) A primitive root, α, of a prime, p, is a value such that when you calculate the remainders of α, α^2, α^3, α^4 , ... , α^{p-1}, when divided by p, each number from the set {1, 2, 3, ..., p-1} shows up exactly once. Prove that a prime p has exactly φ(p-1) primitive roots. In writing your proof, you may assume that at least one primitive root of p exists. (Normally, this is the first part of the proof.) (Note: This question is difficult, so don't feel bad if you can't figure it out.)

We assume that g is a primitive root of p.

Now, consider each of the terms g^1 mod p, g^2 mod p, …, g^{p-1} mod p. We know that this sequence is a permutation of the values in the set {1, 2, 3, …, p-1}, and that $g^{p-1} \equiv 1$ mod p.

Due to the cyclic behavior, we see that $g^n \equiv 1$ mod p if and only if $n \equiv 0$ mod (p-1). Namely, we can only achieve 1 as a result when exponentiating g when raising it to a power that is a multiple of (p-1).

Now, consider an arbitrary term on the list, g^i mod p, and trying to see if it is a generator. We would want to find the smallest k such that $(g^i)^k \equiv 1$ mod p. This is equivalent to finding the smallest positive value of k such that $ik \equiv 0$ (mod p-1) as previously discussed. The key observation is that if gcd(i, p-1) = 1, then the only way the statement is true is if k | (p-1). In order for this to be true and k to be positive, the minimal value of k that satisfies the requirement is k = p -1, meaning that if gcd(i, p-1) = 1, then g^i is also generator mod p. Alternatively, if this gcd isn't 1, we can see that there will be a solution for k to the equation that's smaller than p-1. (Namely, let k = $\frac{p-1}{gcd(i,p-1)}$. If you plug this in for k, we see that the gcd can completely divide into i, revealing that ik is a multiple of p-1.)

Thus, the total number of generators is equal to the total number of values i for which gcd(i, p-1) = 1. By definition, this value is just φ(p-1).

12) Alice and Bob are using Diffie-Hellman to exchange a secret key. They are using the prime number p = 1234577 and the generator g = 1225529. Alice picks a secret value a and sends g^a = 654127 to Bob. Bob picks a secret value b and sends g^b = 221505 to Alice. What is the secret key they share?

We need to find a and b, which aren't given in the question. We can find these via brute force. Attached is the python program, q12DH.py, which does this. Here are the results of the program:

a = 356700
b = 923747
g^{ab} = 606771

13) Decrypt the following message:

204298354508286797413 50
260227996268125919805 67
305721142249215613443 99
141804248336734145620 55
195392829833936761423 12

These 5 blocks of cipher text were created with a set of RSA public keys that follow:

n = 43767782750765499923141
e = 986321785648512635467

When you decrypt, you'll initially get numbers, but those numbers can be converted into blocks of 16 letters each.

This looks very, very hard. But, I made it easier by picking a prime number for one of the secret keys that was very small. If you run trial division upto 10,000,000, that one of the divisors is less than 10,000,000. From there, we can calculate φ(n) and d. The attached Java program (DecryptRSA.java) does this and outputs the following:

p = 4433237
q = 9872646725353393
phi = 43767772878118770136512
d = 41311939691347620167587

When you decrypt using d, you get the following message:

OMWHQKCBJQUFPJPF

HIDDEN IN FIRE DEVC BY ARUPS OFICE LIFT UP RED ITEM TO GET MSG AND DO WHAT IT SAYS

Actually, there was no message there, there was just a prize for the first person who got there! (You'll notice that the first block was gobblety gook…the last four blocks are fine.)