CS 554 Homework #3

Due: Tuesday, March 15
Alexander Powell

1. In mod n arithmetic, the quotient of two numbers r and m is a number q such that $mq = r \bmod n$. Given r, m, and n, how can you find q? How many qs are there? Under what conditions is q unique? [Hint: $mq = r \bmod n$ iff there is an integer k such that $qm + kn = r$. Divide by $\gcd(m,n)$.]

   Solution: To find q, start by dividing r by m mod n. To do so, divide r by m, and let's call the quotient x and the remainder r_1. Next, divide n by m and let's call the quotient y. Also, lets call the remainder of this division r_2. From here, solve for a where $r_1 + a \times r_2$ is a multiple of n. Finally, q is calculated using the following equation.

   $$q = x + a \times y$$

   Also, q will be unique if n is a prime number, excepts for when $m = 0$.

2. For what type of number n is $\phi(n)$ largest (relative to n)?

   Solution: $\phi(n)$ is largest for prime numbers since all numbers from 1 to $n-1$ are relatively prime to n is n is prime.

3. For what type of number n is $\phi(n)$ smallest (relative to n)?

   Solution: $\phi(n)$ is smallest for a number containing the max possible number of prime factors.

4. Is it possible for $\phi(n)$ to be bigger than n?

   Solution: No, it is not possible for $\phi(n)$ to be bigger than n because the max value of a totient function occurs when n is prime and the value of the function is $n-1$.

5. In section 6.4.2 Defenses Against Man-in-the-Middle Attack, it states that encrypting the Diffie-Hellman value with the other side's public key prevents the attack. Why is this the case, given that an attacker can encrypt whatever it wants with the other side's public key?

   Solution: This is the case because the person conducting the attack isn't able to decrypt the Diffie-Hellman values that are sent to them. Therefore, they won't be able to compute the shared message.

6. In RSA, is it possible for more than one d to work with a given e, p, and q?

   Solution: It's important to note that d is the multiplicative inverse of e mod $(p-1) \times (q-1)$. This means that d is unique modulo $(p-1) \times (q-1)$. Also, since e has a multiplicative inverse, then we know $gcd(e,(p-1) \times (q-1)) = 1$. Therefore, there's only one element in $Z_{(p-1)\times(q-1)}$ that yields 1 when multiplied by e. So, it is not possible for more than one d to work with a given e, p, and q?

7. In RSA, given that the primes p and q are approximately the same size, approximately how big is $\phi(n)$ compared to n?

   Solution: We know that $\phi(n) = (p-1) \times (q-1)$. By expanding out this binomial, we get $pq - p - q + 1$, which is the same as $n - 2 \times \sqrt{n}$. This can be written as the product $n\left(1 - \frac{2}{\sqrt{n}}\right)$.

8. What is the probability that a randomly chosen number would not be relatively prime to some particular RSA modulus n? What threat would finding such a number pose?

Solution: The probability that a number is not relatively prime to n can be written as

$$\frac{(pq-(p-1)(q-1))}{pq} = \frac{(p+q-1)}{pq} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$$

This is a threat because if such a number was found it could lead to a factorization of n from which it would be possible to figure out $\phi(n)$ as well as the multiplicative inverse of any public key mod $\phi(n)$. It would also give the attacker the ability to find the private key of a key pair.

9. Suppose Fred sees your RSA signature on m_1 and on m_2 (i.e. he sees m_1^d mod n and m_2^d mod n). How does he compute the signature on each of m_1^j mod n (for positive integer j), m_1^{-1} mod n, $m_1 m_2$ mod n, and in general $m_1^j \times m_2^k modn$ (for arbitrary integers j and k)?

   Solution: The signature of m_1^j mod n for any j positive integer can be computed by $(m_1^d)^j$ mod $n = (m_1^j)^d$ mod n.

   The signature of m_1^{-1} is $(m_1^{-1})^d$ mod $n = (m_1^{-d})$ mod $n = (m_1^d)^{-1}$ mod n. This can be calculated by finding the multiplicative invserse of m_1^d mod n using Euclid's algorithm.

   The signature of $m_1 \times m_2$ is $(m1 * m2)^d$ mod $n = ((m1)^d$ mod $n) * (m2^d$ mod $n)$ mod n.

   Finally, to compute the signature for $m_1^j \times m_2^k modn$ (for arbitrary integers j and k), we know that if $j < 0$ then $j = -1 * -j$, where $j < 0$. Therefore the signature of m_1^j can be computed using the signature of m_1^{-j} and the signature of m_1^j can be computed using the signature of m_1^{-j}. Continuing from this, we can compute the signature of m_2^k because we already know how to compute the signature of m_1^j and m_2^k.

10. This problem illustrates the point that the Diffie-Hellman protocol is not secure without the step where you take the modulus; i.e. the "Indiscrete Log Problem" is not a hard problem! You are Eve, and have captured Alice and Bob and imprisoned them. You overhear the following dialog. Bob: Oh, let's not bother with the prime in the Diffie-Hellman protocol, it will make things easier. Alice: Okay, but we still need a base g to raise things to. How about $g = 3$? Bob: All right, then my result is 27. Alice: And mine is 243. What is Bob's secret x_B and Alice's secret x_A? What is their secret combined key? (Don't forget to show your steps.)

    Solution: First of all, we know $g = 3$, Bob's result is 27, and Alice's result is 243. So, we can write $B = 27 = 3^3$ and $A = 243 = 3^5$. So, we now know that $x_B = 3$ and $x_A = 5$. Also, their secret combined key is

    $$243^3 = 27^5 = 14348907.$$

11. See attached java code.