Math 1350 Quiz 5 - August 4, 2010

(4 points) Name: Solutions

1. You want to be able to send and receive messages using the RSA Public Key Cryptosystem. You choose primes $p = 11$ and $q = 19$, and so $m = 209$.

   (a) (5 points) Your value of n is 180. Factor n completely into its prime factors.

   We can use that $n = 10 \cdot 18$ to factor it. $n = 2 \cdot 5 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \cdot 5$.

   (b) (6 points) You choose $e = 29$. Find your decryption key d using the Euclidean Algorithm.

   Hint: We need e and d to be multiplicative inverses modulo what number?

   We need e and d to be inverses mod $n = 180$, so we use the Euclidean Algorithm to compute $\gcd(180, 29)$.

$$\begin{aligned} 180 &= 6 \cdot 29 + 6 \\ 29 &= 4 \cdot 6 + 5 \\ 6 &= 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

   Substituting backwards, we see:

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (29 - 4 \cdot 6) = 5 \cdot 6 - 29 \\ &= 5(180 - 6 \cdot 29) - 29 = 5 \cdot 180 - 31 \cdot 29 \end{aligned}$$

   This gives us $d \equiv -31 \equiv 149 \pmod{180}$, i.e. $d = 149$.

   (c) (3 points) Suppose someone sends you a message including the number 33. In order to decrypt this number, you need to compute a power of 33. What is the number you must compute, including the modulus?

   We need to compute $33^{149} \pmod{209}$.

   (d) (7 points) Show how to use successive squaring to compute the number from part (c). You do not need to multiply out the numbers, simply show which numbers you would need to compute.

   We could compute $33^2, 33^4, 33^8, 33^{16}, 33^{32}, 33^{64}$, and 33^{128}. all mod 209. Alternately, we could compute the same powers of 3 and 11 separately. After that, since $149 = 128 + 16 + 4 + 1$, we would multiply $33^{128} \cdot 33^{16} \cdot 33^4 \cdot 33 \pmod{209}$ to get our decrypted letter.