Homework 5

Section 1.6:

9. If the number of digits in a block is greater than the number of digits in either of the chosen primes, we will be unable to decode it uniquely. For example, if you encode 123 or 246, in both cases we will get 0. When we try to decode 0, we don't know from which number it came; it could be either 123 or 246.

12. Because our cryptographer foolishly used primes low enough for us to factor their product, we, the cryptanalysts, know that they are 3 and 29. Thus, we can calculate $\phi(87) = \phi(3)\phi(29) = 2(28) = 56$. This tells us that $x^{(56n+1)}$ is congruent to x mod 87, so all we have to do is solve the linear diophantine equation $19a - 56n = 1$ using the Euclidean algorithm, which gives us $a = 3$. Now, we know that for each block B of the message, we have been sent B^19, so using our key we calculate $(B^19)^3 = B^{(56+1)} = B$ mod 87. So, to decode the message, we just have to cube each block. $04^3 = 64$ and $10^3 = 43$ mod 87, so the encoded message is 6443, or FOOD.

13. The exact same technique described above solves this problem as well; only the numbers are different. The message is JOHN.

The other assignments:

1. Find the primes p and q if pq=4,386,607 and $\phi(pq) = 4,382,136$. Explain the method you have used.

   We use the fact that $\phi(pq) = (p-1)(q-1)$, so by solving the system of quadratic equations: $\begin{cases} pq = 4386607 \\ (p-1)(q-1) = 4382136 \end{cases}$ we can find the two primes 3019 and 1453.

2. Are there any numbers n such that $\phi(n) = 14$. Explain!

   We write n as the product of powers of primes $n = p_1^{k_1} \cdots p_m^{k_m}$ where $p_1 < p_2 < \cdots < p_m$ and each k_i is positive. Then $\phi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_m^{k_m-1}(p_m - 1) = 14$. Thus there is a prime p_i with $p_i - 1 = 7$ or 14. Then $p_i = 8$ or 15 but both of them are not prime which contradicts to our assumption that p_i is a prime. So there is no such n.

3. Find the remainder at division of 3^{1000} by 35.

   Since 3 and 35 are relatively prime and $\phi(35) = 24$, Euler' Theorem gives $3^{24} \equiv 1 \mod 35$. So $3^{1000} \equiv 3^{16}(3^{24})^{41} \equiv 3^{16} \equiv 81^4 \equiv 11^4 \equiv 121^2 \equiv 16^2 \equiv 11 \mod 35$.

4. Suppose that a cryptanalyst discovers a message P that is not relatively prime to the enciphering modulus n=pq used in a RSA cipher. Show that the cryptanalyst can actually factor n.

   Let us suppose our clever cryptanalyst knows that P and n are not relatively prime. Then one of either p or q must divide both P and n; without loss of generality, let us assume it's q. Then $P = kq$ for some k. Using the Euclidean algorithm, our cryptanalyst buddy can easily find the GCD of P and n, which will be q; then, dividing n by q, he gets p, and the factorization is complete.