Math 223, Spring '09
Homework 12, due Wednesday, May 13

(1) What is the ciphertext that is produced when RSA encryption with public key $(e, n) = (3, 2669)$ is used to encrypt the message $BESTWISHES$? Use the protocol $A = 00$, $B = 01$, ..., $Z = 25$ and break your message up into blocks of length 4.

(2) Suppose a cryptanalyst discovers a plaintext block P that is not relatively prime to the enciphering modulus $n = pq$ used in an RSA cipher. Show that the cryptanalyst can factor n. (Hint: Recall that $P \leq n$.)

(3) Recall that one of the issues in RSA decryption is that it requires the use of Euler's Formula with base P, where P is a plaintext block, and modulus n, without knowing if $gcd(P, n) = 1$. Show that it is extremely unlikely that this is not the case by showing that the probability that P and n are not relatively prime is $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. Thus if both p and q are larger than 10^{100}, the probability that $gcd(P, n) \neq 1$ is less than 10^{-99}. (Recall that the probability of an event occurring is the number of ways it can occur divided by the total number of possible events.)

(4) Recall that if we know the factorization of $n = pq$, then $\phi(n) = (p-1)(q-1)$ is easy to compute. In this problem, you will show that knowing n and $\phi(n)$ leads to the factorization of n. Thus factoring n is a problem of the same complexity as finding $\phi(n)$.

(a) Show that $p + q = n - \phi(n) + 1$.

(b) By using the fact that $q = n/p$, show that p satisfies the quadratic equation $p^2 + (\phi(n) - n - 1)p + n = 0$.

(c) Deduce that p and q are

$$p = \frac{(n - \phi(n) + 1) + \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}$$

$$q = \frac{(n - \phi(n) + 1) - \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}$$

(5) (a) Suppose the length of each block in an RSA cipher is precisely the length of the numerical equivalent of each letter. How could this cipher be broken?

(b) The exponent $e = 2$ should never be used in an RSA public key. Why?

(6) One instance of how RSA can be subverted is when there is a *common modulus protocol failure*, which means that two parties are using the same modulus n but different exponents e for encryption. Show that the plaintext of a message sent to each of these two parties can be recovered from the ciphertext messages if the exponents are relatively prime.