Problem Set 5

Part One

1. The "key" for an ADFGVX cipher consists of some arrangement of the 26 letters of the alphabet as well as the digits 0 through 9 in a six-by-six grid, plus a keyword used to determine how certain columns of ciphertext are rearranged at the appropriate point in the enciphering process. Suppose you know that a keyword of length 4 has been used. How many distinct "keys" are there in this case? (Hint: The keywords KNOT and BENT have the same effect on the column rearrangement, so you should treat them as identical in your count of keys.)

2. On page 199, Singh describes efforts to foil any frequency analysis conducted on the Navajo code alphabet. Certain common letters were represented by multiple code words. The letters A and N each had three possible code words, and the letters U, D, and L had two each. How many different ways were there to express the word GUADALCANAL in the Navajo code alphabet?

Part Two

During class on November 8th, we determined that the RSA encryption scheme needs to meet the following three conditions in order to be considered secure and reliable. (The numbered steps referenced below refer to the steps in the RSA process as described on the handout from class that day.)

Condition 1. In Step 4, we should always be able to find a value for d regardless of our choices for p, q, and e.

Condition 2. The value for x calculated in Step 9 should always equal the value of x that Bob selects in Step 6.

Condition 3. The number m needs to be very difficult for Eve to factor.

Here are the three relevant theorems I distributed on the second handout in class that day:

Theorem 1. If a and b are relatively prime, then there exist numbers s and t such that $as + bt = 1$.

Theorem 2. Let p and q be distinct primes. For any integer a,

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

where k is any positive integer.

Theorem 3. The number of prime numbers less than or equal to n is approximately equal to $\frac{n}{\ln n}$ for large values of n.

Theorem 4. For any integers a and b and any positive integer m,

$(a \text{ MOD } m)^b \text{ MOD m} = a^b \text{ MOD } m$.

[In other words, you can apply the MOD operator, raise to the *b* power, then apply the MOD operator again… or you can raise to the *b* power, then apply the MOD operator once.]

The following questions ask you to connect the dots between these conditions and theorems.

3. Use Theorem 1 to prove that Condition 1 is satisfied.

4. Use Theorems 2 and 4 to prove that Condition 2 is satisfied.

5. This is a two-part question.

    a. What does Theorem 3 tell you about the difficulty involved in factoring *m*?

    b. What assumptions did you make in your answer to part (a)?