Problem Set 5

1. Suppose you receive the following ciphertext from a colleague who enciphered her message using the Vigenère Cipher with the keyword USAF:

   J S R F H G I F C K T O J P W I X E X M A O S

   When you attempt to decipher the message, you suspect that your colleague made a mistake when applying the keyword technique. What mistake did she make and what is the correct plaintext message?

2. Use the ADFGVX cipher to encipher the following plaintext message using the grid and keyword given below.

   Plaintext: to sleep perchance to dream

   Grid:

	A	**D**	**F**	**G**	**V**	**X**
A	n	g	c	1	p	v
D	h	m	u	k	0	i
F	x	r	2	b	z	5
G	8	a	w	q	7	j
V	s	9	3	o	4	d
X	6	f	t	l	y	e

   Keyword: HAMLET

3. 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.
   a. 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.)
   b. Suppose you know that the length of the keyword is 4, 5, or 6. How many distinct "keys" are there in this case?

4. 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?