**Math 115F Fall 2014 – Problem Set 5**

1. Consider the affine cipher *y* = (*mx* + *b*) MOD 26, where *x* is an integer between 0 and 25 representing a letter in the plaintext, *y* is an integer between 0 and 25 representing the corresponding letter in the ciphertext, and *m* and *b*are constants, each integers between 0 and 25.
	1. During our class discussion of the affine cipher problem on Problem Set 4, we noted that *m*=9, *b*=11 and *m*=22, *b*=11 both satisfy the condition that the plaintext “ac” corresponds to the ciphertext “LD.” Which one of these solutions doesn’t actually work as an affine cipher? Why not?
	2. How many unique affine ciphers are there? Justify your answer.
2. 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.)
3. 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?
4. Recall that the Friedman Test for estimating the length of a keyword used in a Vigenère cipher involved calculating the probability that two randomly chosen letters in the ciphertext are identical. Suppose (for simplicity’s sake) that we have an alphabet consisting of four letters, V, G, N, and R. Also suppose that we have a sample of ciphertext consisting of 56 letters: 12 Vs, 16 Gs, 10 Ns, and 18 Rs. If we were to select two of these letters at random, what’s the probability that they would be identical?
5. On a certain multiple-choice exam, there are five questions, each with four choices. Bubba has not studied for the exam at all and decides to guess answers at random. What is the probability that…
	1. The first question he gets right is the 5th question?
	2. He gets all questions right?
	3. He gets at least one question right?
6. Suppose a certain cipher machine has a plugboard, like the Enigma machine, in which pairs of letters (A--Z) can be connected via cables. Two such cables are provided with the machine, and both must be used for the machine to work.
	1. How many different plugboard settings are there in which one cable connects two letters in the first half of the alphabet (A-M) and the other connects two letters in the second half (N-Z)?
	2. How many different plugboard settings are there in which the letters A and Z are connected, either to each other or to other letters?