CIS 3362 Homework #2 - Both Groups

Assigned: Wednesday, September 16, 2015
Due Date: Check Webcourses

Directions: Please complete these questions with no computer programs. You may use a calculator but please clearly write out all of the set up for your calculations as most of the grade is based on the set up and not the answer itself. Please submit a .pdf file via WebCourses before the due date/time posted there.

1) Given that the encryption function for an affine cipher in a language with 65 alphabet characters is f(x) = (24x + 11) % 65, determine the corresponding decryption function. Please show all of your work.

2) Encrypt the following message below using the affine cipher function, f(x) = (9x + 17) % 26.

```
PACKMYBOXWITHFIVEDOZENLIQUORJUGS
```

3) Consider a language with an alphabet size of 165. How many possible affine cipher keys could there be for this language?

4) You are attempting to break an affine cipher (in English). You believe that the ciphertext 'G' maps to the plaintext letter 'e' and that the ciphertext 'P' maps to the plaintext 't'. Determine the **decryption** function used based on these two pieces of information.

5) Let M = $\begin{pmatrix} 8 & 17 \\ 7 & 9 \end{pmatrix}$. Determine M^{-1}, the corresponding decryption for the Hill cipher with an encryption key of M.

6) Encrypt the plain text "COMPUTERS" with the Hill cipher using the encryption key $\begin{pmatrix} 4 & 1 & 3 \\ 5 & 9 & 7 \\ 15 & 1 & 2 \end{pmatrix}$.

7) What is the index of coincidence of the following set of letters: 15 As, 45 Bs, 40 Cs, 60 Ds, 40 Es? For full credit, please express your answer as a **fraction in lowest terms.**

8) The following ciphertext was encrypted using the Vigenere cipher with the keyword "FORK": GFVKPTRCYTFYI. What was the original plaintext?

9) Using the Extended Euclidean Algorithm determine 80^{-1} mod 153. Please answer with an integer in between 0 and 152, inclusive.

10) Encrypt the message "90210WASMYFAVORITESHOW" using the ADVGFX cipher with the square shown below and the keyword "PRIESTLY".

	A	D	F	G	V	X
A	K	Q	C	7	U	G
D	V	D	1 (# one)	N	M	0
F	J	P	5	6	F	Z
G	9	R	B	T	3	H
V	E	I (letter I)	W	2	X	4
X	L (letter L)	S	8	O (letter O)	Y	A

11) The following ciphertext was created using the Playfair cipher with the keyword “KNIGHTS” and the padding character X. What is the corresponding plaintext? (Note: The ciphertext is broken up into digraphs for convenience.)

```
NM LY GA FE FJ BQ PK WL AS LP FT ZY
```