CIS 3362 Test #1: Classical Cryptographic Schemes

Date: 9/19/2014

Name : ____

1) (8 pts) What is the index of coincidence of the following set of letters: 20 As, 50 Bs, 40 Cs, 60 Ds, 30 Es? For full credit, please express your answer as a **fraction in lowest terms.**

____

2) (10 pts) The following ciphertext was encrypted using the Vigenere cipher with the keyword "FORK": GFVKPTRCYTFYI. What was the original plaintext?

____

3) (10 pts) Encrypt "CRYPTOGRAPHY" using the shift cipher with an encryption key of 7.

____

4) (15 pts) Using the Extended Euclidean Algorithm determine 65^{-1} mod 147. Please answer with an integer in between 0 and 146, inclusive. **Note: most of the credit will be for the steps of the algorithm and not the final answer.**

5) (15 pts) Encrypt the message "ON9192014ATTACKWITH2ARMIES" using the ADVGFX cipher with the square shown below and the keyword "SOUTH".

	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

5) (10 pts) Consider an affine cipher with the encryption function f(x) = (19x + 12) mod 26. What is the corresponding decryption function?

6) (12 pts) Consider a Hill cipher for Spanish, where the letters are assigned values from 0 to 29, inclusive. If the encryption key is $\begin{pmatrix} 11 & 15 \\ 4 & 7 \end{pmatrix}$ for the cipher, what is the corresponding decryption key. **Remember, the relevant mod value is mod 30, NOT mod 26.**

8) (6 pts) You are working on decrypting a ciphertext that was created using the substitution cipher in English. You are certain that your mappings for the ciphertext letters W, O and G are correct. You are also certain that the ciphertext letters H, J, Q, U and Y map to the plaintext letters R, S, T, L and N, but you don't have any information about the one to one mappings within these sets of five letters. Given this information and no other restrictions, how many possible keys could there be? Please leave your answer in a product of factorials.

____

9) (12 pts) 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
```

____

10) (2 pts) The world's busiest airport, Hartsfield-Jackson Atlanta International Airport is named after which two former mayors of Atlanta?

________________ and __________________

Scratch Page – Please clearly mark any work on this page you would like graded.