

CIS 3362 Exam #1
September 25, 2015

Last Name: _____ , **First Name:** _____

1) (10 pts) Encrypt the plaintext QUICKFOXES using the Shift Cipher with a key of 17.

2) (10 pts) Calculate the index of coincidence of the following set of letters:

30 As, 20 Bs, 50 Cs, 60 Ds, 40 Es

3) (10 pts) You believe a ciphertext has been encrypted using the Vigenere cipher with a keyword with a length in between 5 and 8 letters, inclusive. You've written a brute force program that can try every possible string and determine whether it's the proper key. Your program can check one million keys per second on this ciphertext. How long will your program take to try all keys in this case?

4) (10 pts) Decrypt the ciphertext PVWMAMKOBUXGAZXMFIL. It was encrypted using the Vigenere cipher with the keyword "TRAIN" .

5) (15 pts) Consider an affine cipher for a language with an alphabet size of 67 with the encryption function: $f(x) = (24x + 43) \% 67$. Determine the corresponding decryption function.

6) (12 pts) The ciphertext ERMREZCEQPVR was encrypted using the Playfair cipher with the keyword CALCULATOR. Determine the corresponding plaintext.

7) (9 pts) Encrypt the plaintext TICTACTOE using the Hill cipher with they key: $\begin{pmatrix} 3 & 1 & 18 \\ 8 & 9 & 19 \\ 21 & 11 & 15 \end{pmatrix}$.

8) (15 pts) Encrypt the plaintext THESECRETKEYWORDIS9345MQ using the ADFGVX cipher with the ADFGVX square shown below and the keyword ELECTION.

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

9) (8 pts) When the Germans added two new scramblers to the Enigma, they effectively increased the size of the look up table that had to be created by a multiplicative factor of 10. If the Germans added yet one more scrambler, how many times bigger would the look up table be than right before that one scrambler was added?

10) (1 pt) Name one type of food item on Del Taco's menu. _____

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