CIS 3362 Quiz #1: Shift, Affine, GCD, Substitution, Vigenere Solution

1) (5 pts) Encrypt the plaintext "THIRD" using the shift cipher with a key equal to 15.

T	H	I	R	D
19	7	8	17	3
15	15	15	15	15
--------	--------	--------	--------	--------
34	22	23	32	18
8	22	23	6	18
I	W	X	G	S

I W X G S

Grading: 1 pt per letter, just grade the answer.

2) (6 pts) The encryption keys for an Affine Cipher with alphabet size 26 are a = 11, b = 13. What are the corresponding decryption keys? (Credit given for work but formula sheet should be used appropriately.

Swap x and y in the formula for the affine to get:

$x \equiv (11y + 13)\ mod\ 26$ **Grading: 1 pt**

$11y \equiv (x - 13)\ mod\ 26$ **Grading: 1 pt**

Look on the reference sheet to see that 11^{-1} mod 26 is 19.

$19(11y) \equiv 19(x - 13)\ mod\ 26$ **Grading: 1 pt**

$y \equiv 19x - 247\ mod\ 26$ **Grading: 1 pt**

$y \equiv 19x + 13\ mod\ 26$

a = 19 , b = 13 (Grading: 1 pt for each of these, so if they answer 19, -247 5 out of 6)

3) (12 pts) Determine 107^{-1} mod 243. Show your work and give a final answer in between 0 and 242, inclusive.

First do the Euclidean Algorithm:

243 = 2 x 107 + 29
107 = 3 x 29 + 20
29 = 1 x 20 + 9
20 = 2 x 9 + 2
9 = 4 x 2 + 1

Grading: 3 pts total to here

Now, run the Extended Euclidean Algorithm:

9 – 4 x 2 = 1

Grading : 1 pt

9 – 4(20 – 2 x 9) = 1
9 – 4 x 20 + 8 x 9 = 1
9 x 9 – 4 x 20 = 1

Grading: 1 pt

9(29 – 1 x 20) – 4 x 20 = 1
9 x 29 – 9 x 20 – 4 x 20 = 1
9 x 29 – 13 x 20 = 1

Grading: 1 pt

9 x 29 – 13(107 – 3 x 29) = 1
9 x 29 – 13 x 107 + 39 x 29 = 1
48 x 29 – 13 x 107 = 1

Grading: 1 pt

48(243 – 2 x 107) – 13 x 107 = 1
48 x 243 – 96 x 107 – 13 x 107 = 1
48 x 243 – 109 x 107 = 1

Grading: 1 pt

Take this equation mod 243 to get

$-109 \times 107 \equiv 1\ (mod\ 243)$

Grading: 2 pts

It follows that $107^{-1} \equiv -109 \equiv 134\ (mod\ 243)$

Grading: 1 pt to extract -109
1 pt to map to 134

<u>134</u>

4) (10 pts) A substitution cipher can be stored in a character array of size 26, where code[i] stores the cipher text letter corresponding to the ith letter of the alphabet with i ranging from 0 to 25. For example, if code started “TQEB...”, then the plaintext letter ‘A’ would map to the ciphertext letter ‘T’, the plaintext letter 'B’ would map to the ciphertext letter ‘Q’, etc. To decrypt a ciphertext made with this substitution, we would want to store the inverse substitution. In the example above, for the inverse substitution, inverse[1] = ‘D’ because the ciphertext letter ‘B’ maps to the plaintext letter D. Complete the function below, so that it takes in a string of length 26 storing a substitution code and returns another string of length 26 storing the corresponding inverse substitution code. Some of the code has been provided (mostly the annoying dynamic memory and NULL char code). **Assume that code stores 26 unique uppercase letters. The string your function returns should also store 26 unique uppercase letters. Note: Code is short for this one.**

```
char* getInverse(char* code) {

    char* inverse = calloc(27, sizeof(char));
    inverse[26] = ‘\0’;

    for (int i=0; i<26; i++)                        // Grading: 2 pts
        inverse[code[i]-'A'] = (char)('A'+i);

    // Grading LHS: 1 pt inverse[], 2 pts code[i], 1 pt –‘A’
    // Grading RHS: 2 pts ‘A’, 2 pts +i
    return inverse;
}
```

5) (10 pts) The ciphertext “MIHOILYYFH” was encrypted with the Vigenere Cipher with the secret key, “HOUSE”. What is the plaintext?

M	I	H	O	I	L	Y	Y	F	H
12	8	7	14	8	11	24	24	5	7
-7	-14	-20	-18	-4	-7	-14	-20	-18	-4 (HOUSE=7,14,20,18,4)

---

5	-6	-13	-4	4	4	10	4	-13	3
5	20	13	22	4	4	10	4	13	3
F	U	N	W	E	E	K	E	N	D

F U N W E E K E N D

Grading: 1 pt per letter, just grade the answer.

6) (6 pts) A set of letters contains 20 As, 10 Bs, 10 Cs and 10 Ds. What is the index of coincidence for this set of letters? Express your answer as a **fraction in lowest terms.**

$$IC = \frac{20 \times 19 + 3(10 \times 9)}{50 \times 49} = \frac{380 + 270}{50 \times 49} = \frac{650}{50 \times 49} = \frac{13}{49}$$

Grading: 2 pts numerator, 1 pt denominator, 1 pt simplify numerator, 2 pts to simplify to lowest terms

7) (1 pt) The United States Open, a major tennis tournament is set to conclude this Sunday. In what country does this tournament take place?

United States (Grading: 1 pt give to all)