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

1) (5 pts) Decrypt the following cipher text, which was encrypted via the shift cipher with an encryption key of 11: AFXAVTYWLEEP.

```
   A    F    X    A    V    T    Y    W    L    E    E    P
   0    5   23    0   21   19   24   22   11    4    4   15
 -11   11   11   11   11   11   11   11   11   11   11   11
-------------------------------------------------------------
 -11   -6   12  -11   10    8   13   11    0   -7   -7    4 mod 26

  15   20   12   15   10    8   13   11    0   19   19    4 convert letters

   P    U    M    P    K    I    N    L    A    T    T    E
```

Grading: ½ pt per unique letter, round down.

Pumpkin Latte

2) (6 pts) Consider an Affine cipher for an alphabet with 49 symbols. How many possible encryption keys could there be? **Please leave your answer in prime factorized form.**

b could be any of 49 values.
a could be any value in the list 1, 2, 3, …, 48 that does not share a common factor with 49. Note that 49 has only one prime factor, 7. Thus, from the list above, a CAN NOT be 7, 14, 21, 28, 35, or 42, the multiples of 7 on the list. It follows that a could be one of 48 – 6 = 42 values.

The total number of possible keys equals 49 x 42 = 7^2 x 2 x 3 x 7 = **$2 \times 3 \times 7^3$**

Grading: 1 pt for # of b's, 3 pts for # of a's, 1 pt to multiply, 1 pt to prime factorize.

3) (10 pts) You believe that the ciphertext of 'W' maps to the plaintext letter 'I' and the ciphertext letter 'H' maps to the plaintext letter 'R' for a ciphertext that you know to be encrypted via the Affine Cipher. What is the only **encryption** function that is consistent with this information? (Note: you may use the formula sheet to speed up your work. If you solve for the decryption function correctly instead, 2 pts will be deducted.)

Your answer should be of the form $f(x) = (ax+b) \bmod 26$, where $\gcd(a, 26) = 1$ and $0 \leq a, b < 26$.

Using the given information 'I' encrypts to 'W', which means $f(8) = 22$, and 'R' encrypts to 'H', which means $f(17) = 7$. Set up the system of equations:

$22 = 8a + b \bmod 26$
$7 = 17a + b \bmod 26$

Subtracting the top equation from the bottom, we get:

$-15 = 9a \bmod 26$, since $9^{-1} \bmod 26 = 3$ we have:

$3(-15) = a \bmod 26$
$a = -45 = 7 \bmod 26$ (note we added 52, a multiple of 26 to get the value of a in range.)

Substitute this value into the top equation to get b:

$22 = 8(7) + b \bmod 26$
$b = 22 - 56 = -34 = 18 \bmod 26$ (note we added 52, a multiple of 26 to get the value of b in range.)

It follows that the **encryption function was $f(x) = (7x + 18) \pmod{26}$.**

Note: The corresponding decryption function is $f^{-1}(x) = (15x + 16) \pmod{26}$.

Grading: 4 pts for setting up equations, give 2 pts if equations are flipped.
1 pt subtracting to isolate 9a or -9a
1 pt mult by multiplicative inverse
1 pt to get mapped value of a in range.
1 pt substitute a value into one equation.
1 pt to solve for b.
1 pt to map b into range.

4) (5 pts) Encrypt the plaintext "BERRYWATER" using the Vigenere Cipher with the keyword "CUBE".

In numbers, CUBE is 2, 20, 1, 4.

B	E	R	R	Y	W	A	T	E	R	
1	4	17	17	24	22	0	19	4	17	
2	20	1	4	2	20	1	4	2	20	
3	24	18	21	26	42	1	23	6	37	mod 26 →
3	24	18	21	0	16	1	23	6	11	letters →
D	Y	S	V	A	Q	B	X	G	L	

DYSVASBXGL

Grading: ½ pt per unique letter, round down.

5) (10 pts) Determine 23^{-1} mod 108.

108 = 4 x 23 + 16 (a)
23 = 1 x 16 + 7 (b)
16 = 2 x 7 + 2 (c)
7 = 3 x 2 + 1 (d)

7 – 3 x 2 = 1 equation (d) written backwards
7 – 3(16 – 2 x 7) = 1, substitute from (c) backwards
7 – 3 x 16 + 6 x 7 = 1
7 x 7 – 3 x 16 = 1
7(23 – 1 x 16) – 3 x 16 = 1 substitute from (b) backwards
7 x 23 – 7 x 16 – 3 x 16 = 1
7 x 23 – 10 x 16 = 1
7 x 23 – 10(108 – 4 x 23) = 1 substitute from (a) backwards
7 x 23 – 10 x 108 + 40 x 23 = 1
47 x 23 – 10 x 108 = 1

Take this equation mod 108 to yield

47 x 23 = 1 (mod 108)

It follows that 23^{-1} = **47 (mod 108).**

Grading: 3 pts Euclidean, 5 pts Extended, 2 pts to extract answer

6) (6 pts) What is the index of coincidence of the following set of letters?

```
10 As, 40 Bs, 20 Cs, 80 Ds
```

Leave your answer as a fraction, in reduced form (so p/q, where p and q are positive integers such that gcd(p, q) = 1.)

$$IofC = \frac{10 \times 9 + 40 \times 39 + 20 \times 19 + 80 \times 79}{150 \times 149}$$

$$= \frac{10(9 + 4 \times 39 + 2 \times 19 + 8 \times 79)}{150 \times 149}$$

$$= \frac{(9 + 156 + 38 + 632)}{15 \times 149}$$

$$= \frac{835}{15 \times 149} = \frac{5 \times 167}{3 \times 5 \times 149} = \frac{167}{447}$$

Grading: 1 pt denominator, 3 pts numerator,
2 pts simplifying to reduced fraction
(give 1 pt out of 2 if fraction isn't fully reduced but is correct)

7) (6 pts) What is the error with the code below which is supposed to decrypt its input string via the shift cipher? Provide the fix to the error.

```
void decrypt(char* cipher, int key) {
    int len = strlen(cipher), i;
    for (i=0; i<len; i++)
        printf("%c", (cipher[i]-'a'-key)%26+'a');
    printf("\n");
}
```

The expression in the inner parentheses of the printf might be negative, leading to a character being printed that isn't a lowercase letter. To make sure the mod is calculated properly, before executing it, the number must be mapped to an equivalent mod value that is non-negative. Since the key is guaranteed to be no bigger than 25, adding a single multiple of 26 fixes the problem:

```
printf("%c", (cipher[i]-'a'-key+26)%26+'a');
```

Grading: 3 pts for pointing out where the error is, 3 pts for the fix, use your discretion.

8) (2 pts) The United States Open, a major tennis tournament, is currently being played. In which country are the matches for the tournament played?

United States (Grading: give to all, even if it's blank.)