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

Date: 9/6/2023

1) (9 pts) The ciphertext "MYCQBIJTG" was encrypted with the Shift Cipher, with a key of 8. What is the corresponding plaintext?

M	Y	C	Q	B	I	J	T	G
12	24	2	16	1	8	9	19	6
-8	-8	-8	-8	-8	-8	-8	-8	-8
4	16	-6	8	-7	0	1	11	-2 →
4	16	20	8	19	0	1	11	24
E	Q	U	I	T	A	B	L	Y

EQUITABLY (Grading: 1 pt per letter), -2 for not showing appropriate work

2) (5 pts) Consider an Affine cipher for an alphabet with 35 symbols. How many possible encryption keys would there be for the Affine cipher for an alphabet of this size?

The integers from 1 to 35 that share a common factor with 35 are: 5, 10, 15, 20, 25, 30, 35, 7, 14, 21, and 28. (There are 11 numbers listed.) Thus, the number of integers from 1 to 35 that do NOT share a common factor with 35 is 35 – 11 = 24. Thus, there are 24 possible values for a and 35 possible values for b.

It follows that the total number of possible keys for an Affine cipher on an alphabet of size 35 is 35 x 24 = 70 x 12 = **840.**

Grading: 1 pt for # choices for b
1 pt to multiply
3 pts for # of choices for a

3) (5 pts) The encryption function for an Affine Cipher (in English) is f(x) = (15x + 19) mod 26. What is the corresponding decryption function, $f^{-1}(x)$? (Please make use of the reference sheet to speed up your work.)

Switch x and y and solve for y:

x = (15y + 19) mod 26
(x – 19) = 15y (mod 26)

Look up that $15^{-1} \equiv 7 \pmod{26}$ on the reference sheet:

7(x – 19) = 7(15y) (mod 26)
y = 7x – 133 (mod 26)
y = 7x + 23 (mod 26)

$f^{-1}(x) = 7x + 23 \pmod{26}$

Grading: 1 pt subtract 19, 2 pts look up and mult by 7, 1 pt distribute 7, 1 pt map -133.
1/5 for answer 7x + 11, 3/5 for answer 7(x – 19).

4) (10 pts) Encrypt the plaintext "SEMIFINALS" using the Vigenere cipher with the keyword "HOME".

H = 7, O = 14, M = 12, E = 4

S	E	M	I	F	I	N	A	L	S
18	4	12	8	5	8	13	0	11	18
7	14	12	4	7	14	12	4	7	14
25	18	24	12	12	22	25	4	18	32 → 6
Z	S	Y	M	M	W	Z	E	S	G

ZSYMMWZESG

Grading: 1 pt per letter in most cases
-2 pts if appropriate work isn't shown
0/10 automatic if wrong system is used (ie sub instead of add, or any other systemic issue)

5) (10 pts) Determine 59^{-1} mod 203.

203 = 3 x 59 + 26
59 = 2 x 26 + 7
26 = 3 x 7 + 5
7 = 1 x 5 + 2
5 = 2 x 2 + 1

5 – 2 x 2 = 1
5 – 2(7 – 5) = 1
5 – 2 x 7 + 2 x 5 = 1
3 x 5 – 2 x 7 = 1
3(26 – 3 x 7) – 2 x 7 = 1
3 x 26 – 9 x 7 – 2 x 7 = 1
3 x 26 – 11 x 7 = 1
3 x 26 – 11(59 – 2 x 26) = 1
3 x 26 – 11 x 59 + 22 x 26 = 1
25 x 26 – 11 x 59 = 1
25(203 – 3 x 59) – 11 x 59 = 1
25 x 203 – 75 x 59 – 11 x 59 = 1
25 x 203 – 86 x 59 = 1

Take this equation mod 203 to get

-86 x 59 ≡ 1 (mod 203) → 59^{-1} ≡ -86 ≡ 203 – 86 ≡ **117 (mod 203).**

Grading: 3 pts Euclidean
5 pts Extended
1 pt to get -86
1 pt to map to 117.

6) (10 pts) A store has 100 types of candy, labeled 0 through 99. Complete the function in C below that takes in an integer array, `numcandy`, of size 100, where `numcandy[i]` represents the number of candy i that the store has and returns the probability that 2 randomly chosen candies from the store are of the same type. (Note: Please pay careful attention to the difference between integer division and floating point division.)

```
double probsame(int numcandy[]) {

    int n = 0;
    int num = 0;
    for (int i=0; i<100; i++) {
        n += numcandy[i];
        num += (numcandy[i]*(numcandy[i]-1));
    }

    return 1.0*num/n/(n-1);
}
```

Grading: 3 pts for calculating total number of letters
5 pts for calculating numerator of formula
1 pt for dividing numerator by n*(n-1)
1 pt for doing floating pt division

7) (1 pt) Air Canada is the largest airline of which country? **Canada (Give to all)**