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

Date: 9/8/2021

1) (8 pts) What is the index of coincidence of the following set of letters: 10 As, 50 Bs, 50 Cs,and 40 Ds? For full credit, please express your answer as a **fraction in lowest terms.**

$$IC = \frac{10\times9+50\times49+50\times49+40\times39}{150\times149} = \frac{10(9+5\times49+5\times49+4\times39)}{10\times15\times149} = \frac{9+490+156}{15\times149} = \frac{655}{15\times149} = \frac{131}{3\times149} = \mathbf{\frac{131}{447}}$$

Grading: 4 pts numerator, 1 pt denominator, 3 pts simplification

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

```
K E L S X B E Y M F
S K Y S K Y S K Y S

10 - 18 = -8 = 18 (mod 26)  S
4 - 10 = -6 = 20 (mod 26)   U
11 - 24 = -13 = 13 (mod 26) N
18 - 18 = 0                 A
23 - 10 = 13                N
1 - 24 = -23 = 3 (mod 26)   D
4 - 18 = -14 = 12 (mod 26)  M
24 - 10 = 14                O
12 - 24 = -12 = 14 (mod 26) O
5 - 18 = -13 = 13 (mod 26)  N
```

SUNANDMOON (Grading: 1 pt per letter)

3) (5 pts) Encrypt "SEPTEMBER" using the shift cipher with an encryption key of 21.

Note that 21 ≡ -5 (mod 26), so we can equivalently add -5 to each numeric value for encryption.

```
S   E   P   T    E  M   B   E   R
18  4   15  19   4 12   1   4  17
-5 -5   -5  -5  -5 -5  -5  -5  -5
--------------------------------
13,-1,  10, 14, -1, 7, -4, -1, 12 (calculate mod 25)
13, 25, 10, 14, 25, 7, 22, 25, 12
N   Z   K   O   Z   H  W   Z   M
```

Ciphertext is NZKOZHWZM. **(Grading: 1/2 pt per letter, round score up to next integer if ends in 1/2)**

4) (15 pts) Using the Extended Euclidean Algorithm determine 108^{-1} mod 239. Please answer with an integer in between 0 and 238, inclusive. **Note: most of the credit will be for the steps of the algorithm and not the final answer.**

239 = 2 x 108 + 23
108 = 4 x 23 + 16
23 = 1 x 16 + 7
16 = 2 x 7 + 2
7 = 3 x 2 + 1 **(Grading: 5 pts)**

7 - 3 x 2 = 1
7 - 3(16 - 2 x 7) = 1
7 - 3 x 16 + 6x7 = 1
7 x 7 - 3 x 16 = 1
7(23 - 16) - 3 x 16 = 1
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
7 x 23 - 10 x 108 + 40 x 23 = 1
47 x 23 - 10 x 108 = 1
47(239 - 2 x 108) - 10 x 108 = 1
47 x 239 - 94 x 108 - 10 x 108 = 1
47 x 239 - 104 x 108 = 1 **(Grading: 8 pts)**

Take this equation mod 239 to yield

$-104 \times 108 \equiv 1 \pmod{239}$ **(Grading: 1 pt to get -104)**

It follows that $108^{-1} \equiv -104 \equiv$ **<u>135 (mod 239)</u>** **(Grading: 1 pt to convert to 135)**

5) (10 pts) Consider an affine cipher with the encryption function f(x) = (19x + 12) mod 35. What is the corresponding decryption function?

Switch x and y and solve for y:

$x = (19y + 12) \bmod 35$
$(x - 12) = 19y \pmod{35}$ **(Grading: 2 pts)**

We must find $19^{-1} \bmod 35$:

$35 = 1 \times 19 + 16$
$19 = 1 \times 16 + 3$
$16 = 5 \times 3 + 1$ **(Grading: 2 pts)**

$16 - 5 \times 3 = 1$
$16 - 5(19 - 16) = 1$
$16 - 5 \times 19 + 5 \times 16 = 1$
$6 \times 16 - 5 \times 19 = 1$
$6(35 - 19) - 5 \times 19 = 1$
$6 \times 35 - 6 \times 19 - 5 \times 19 = 1$
$6 \times 35 - 11 \times 19 = 1$ **(Grading: 3 pts)**
Take this equation mod 35 to yield
$-11 \times 19 \equiv 1 \pmod{35}$. It follows that $19^{-1} \equiv -11 \equiv 24 \pmod{25}$

$24(x - 12) = 24(19y) \bmod 35$ **(Grading: 1 pt)**
$y \equiv 24(x - 12) \bmod 35$
$y \equiv (24x - 288) \bmod 35$ **(Grading: 1 pt)**
$y \equiv (24x + 27) \bmod 35$ **(Grading: 1 pt)**

It follows that the decryption function is $\mathbf{f^{-1}(x) = (24x + 27) \bmod 35}$

6) (2 pts) The world's busiest airport, Hartsfield-Jackson Atlanta International Airport is named after which two former mayors of Atlanta?

Hartsfield and Jackson (**Give to All)**