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

Date: 9/4/2024

1) (5 pts) The ciphertext "ECLTY" was encrypted via the shift cipher with the encryption key = 11. What is the corresponding plaintext?

```
    E  C  L  T  Y
    4  2  11 19 24
-  11 11  11 11 11
-------------------
   -7  -9  0  8 13
  +26 +26
------------------
   19  17  0  8 13
   T   R   A  I  N
```

TRAIN (Grading: 1 pt per letter, no exceptions)

2) (7 pts) Encrypt the plaintext "PACKING" using the Affine Cipher with the keys a = 9, b = 17.

f(15) = 9(15) + 17 = 135 + 17 = 152 ≡ 22 (mod 26) W
f(0) = 9(0) + 17 = 0 + 17 = 17 ≡ 17 (mod 26) R
f(2) = 9(2) + 17 = 18 + 17 = 35 ≡ 9 (mod 26) J
f(10) = 9(10) + 17 = 90 + 17 = 107 ≡ 3 (mod 26) D
f(8) = 9(8) + 17 = 72 + 17 = 89 ≡ 11 (mod 26) L
f(13) = 9(13) + 17 = 117 + 17 = 134 ≡ 4 (mod 26) E
f(6) = 9(6) + 17 = 54 + 17 = 71 ≡ 19 (mod 26) T

W R J D L E T (Grading: 1 pt per letter, no exceptions)

3) (5 pts) Let the encryption keys for an Affine Cipher for an alphabet size of 26 be a = 15, b = 8. What are the corresponding decryption keys? (Note: You may use the formula sheet to look up the appropriate information to greatly reduce the amount of computation necessary for this question.)

First swap x and y in the encryption function:

x = (15y + 8) mod 26
(x – 8) = 15y mod 26, look up $15^{-1} = 7 \pmod{26}$ from the reference sheet **1 pt**
7(x – 8) = y mod 26 **2 pts**
y = 7x – 56 (mod 26), multiply through **1 pt**
y = 7x + 22 (mod 26), map back into range. **1 pt**

a = 7 b = 22

4) (18 pts) Find the ordered pair of integers (x, y) with $0 \leq x, y < 106$ which satisfies the following system of mod equations:

$$(15x + y) \equiv 34 \; mod \; 106$$
$$(88x + y) \equiv 39 \; mod \; 106$$

This question does require a good deal of calculation by hand. One hint to reduce the size of the numbers you work with is that although your final answer has to have integers in between 0 and 105, inclusive, on occasion, for intermediate computations, it may make sense to use a value not in that range that is equivalent under mod. But, at the very end of the question, follow the directions and map the answers back into the desired range.

Subtract the top equation from the bottom equation to yield:

$$73x \equiv 5 \; (mod \; 106)$$

We need to calculate 73^{-1} mod 106 and multiply this equation through with that value to solve for x. Use the Extended Euclidean Algorithm:

106 = 1 x 73 + 33
73 = 2 x 33 + 7
33 = 4 x 7 + 5
7 = 1 x 5 + 2
5 = 2 x 2 + 1, gcd = 1 as required

5 – 2 x 2 = 1
5 – 2(7 – 1 x 5) = 1
5 – 2 x 7 + 2 x 5 = 1
3 x 5 – 2 x 7 = 1
3(33 – 4 x 7) – 2 x 7 = 1
3 x 33 – 12 x 7 – 2 x 7 = 1

3 x 33 – 14 x 7 = 1
3 x 33 – 14(73 – 2 x 33) = 1
3 x 33 – 14 x 73 + 28 x 33 = 1
31 x 33 – 14 x 73 = 1
31(106 – 1 x 73) – 14 x 73 = 1
31 x 106 – 31 x 73 – 14 x 73 = 1
31 x 106 – 45 x 73 = 1

Take this equation mod 106 to yield

$-45 \times 73 \equiv 1 \ (mod \ 106)$

It follows that $73^{-1} \equiv -45 \equiv 61 \ (mod \ 106)$

Going back to the equation we have:

$$(61)73x \equiv (61)5 \ (mod \ 106)$$
$$x \equiv 305 \equiv 93 \ (mod \ 106)$$

Now, we must back substitute to solve for y. Let's use the top equation to do this and also note that $93 \equiv -13 \ (mod \ 106)$.

$$(15x + y) \equiv 34 \ mod \ 106$$
$$(15(-13) + y) \equiv 34 \ mod \ 106$$
$$y \equiv (34 + 195) \equiv 229 \equiv 17 \ mod \ 106$$

It follows that the desired ordered pair is **(93, 17).**

x = 93 y = 17

Grading: Subtracting equations to get to $73x \equiv 5 \ (mod \ 106)$ **– 2 pts**
Euclidean Algorithm – 3 pts
EEA to get to 31 x 106 – 45 x 73 = 1 **– 8 pts**
Extracting Inverse – 1 pt (okay to use -45 also)
Solving for x – 2 pts
Solving for y – 2 pts

5) (8 pts) Let the set X of letters contain 10 As, 15 Bs, 5 Cs, 2 Ds and 8 Es. Let the set Y of letters contain 4 As, 14 Bs, 20 Cs, 30 Ds and 12 Es. What is the mutual index of coincidence between set X and set Y? Express your answer as a **fraction in lowest terms.**

$$MIC = \frac{10 \times 4 + 15 \times 14 + 5 \times 20 + 2 \times 30 + 8 \times 12}{(10 + 15 + 5 + 2 + 8)(4 + 14 + 20 + 30 + 12)}$$

$$MIC = \frac{40 + 210 + 100 + 60 + 96}{40 \times 80} = \frac{350 + 156}{40 \times 80} = \frac{506}{3200} = \mathbf{\frac{253}{1600}}$$

$\frac{253}{1600}$, Grading: 2 pts numerator, 2 pts denominator, 2 pts get to 506/3200, 2 pts to reduce to final answer.

6) (5 pts) Explain in words what the code below does. Some partial comments have been added for students who have not previously used Python.

```
# Pre-condition: s is a string of lowercase letters only.
def whatdoesitdo(s):

    n = len(s)

    # Works like an array but we can index with anything.
    chart = {}
    sz = 0

    for i in range(n-1):

        # Grabs a substring of s starting at index i of length 2.
        tmp = s[i:i+2]

        # Checks if our "array" has an entry for tmp.
        if tmp in chart:
            chart[tmp] += 1
        else:
            chart[tmp] = 1

        sz = max(sz, chart[tmp])

    # Creates sz+1 lists.
    res = []
    for i in range(sz+1):
        res.append([])

    for tmp in chart:
        res[chart[tmp]].append(tmp)

    # Sorts each list in alphabetical order.
    for i in range(sz+1):
        if len(res[i]) > 0:
            res[i].sort()
```

```
    return res

def main():

    inp = input().strip()

    res = whatdoesitdo(inp)

    # Loops from length of res downto 2.
    for i in range(len(res)-1,1,-1):

        print(i)
        print("--------")
        for x in res[i]:
            print(x)
        print()

main()
```

Explanation Below

The code calculates the frequency of each diagram in the inputted string in main, assuming that string has lowercase letters only. Then, it puts each digram in a list according to how many times it appeared. So, for example, if "th" appears 6 times in the inputted string, then the digram "th" would be stored in list #6. Each non-empty list is then sorted in alphabetical order. Finally, the code prints out these sorted lists, in descending order of number of appearances of each digram. Overall, the order of the digrams is sorted by frequency, breaking ties by alphabetical order.

Grading: 1 pt for mentioning digrams
1 pt for describing that the frequency of each digram is calculated.
1 pt for explaining that each digram gets put into a list based on its frequency
1 pt for explaining that each list is then sorted in alphabetical order
1 pt for explaining the order of printing.

7) (2 pts) In 1981, due to a sizeable donation to UCF from a businessman, UCF changed the name of "General Classroom Building" to Howard Phillips Hall. What businessman made the donation?

Howard Phillips (Grading: give to all)