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

Date: 9/4/2024

Name : _____

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

_____

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

__ __ __ __ __ __ __

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.)

a = _____ b = _____

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.

x = _____ y = _____

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.**

---

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()

    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

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?

_____

Scratch Page – Please clearly mark any work on this page you would like graded.