Cryptography Assignment - 7
Pramod Aravind Byakod

1: Show that the following procedure defines a cryptosystem. Let w be a string over {A,B, . . . , Z} . Choose two Caesar cipher keys k1, and k2. Encrypt the symbols of w having odd index using k1 and those having even index using k2. Then reverse the order of the encrypted string. Determine the plaintext space, the cipher text space, and the key space.

A cryptosystem is defined as a tuple {P,C,K,E,D} , where in

- P is plaintext space. Its elements are plaintexts.
- C is cipher text space. Its elements are cipher texts.
- K is key space. Its elements are keys.
- E is a set of family of functions which converts plaintext to cipher text.
- D is a set of family of functions which converts cipher text to plaintext.

Let's consider w = "OKLAHOMA"
Symbols of w having even indexes, w_e={O,L,H,M}
Symbols of w having odd indexes, w_o={K,A,O,A}
According to the question statement we encrypt w_o using key k1 and encrypt w_e using k2.

Let's consider k1 = 2 and k2 = 4
Encrypted w_e = {S,P,L,Q}
Encrypted w_o = {M,C,Q,C}
Our encrypted text before reversing is "SMPCLQQC".
Our cipher text becomes (reversed above text) "CQQLCPMS"

Plaintext space is **Σ = {A,B,C……Z}**
Cipher text space is **Σ = {A,B,C……Z}**

To find the key space, we will have to look at the combinations possible. Since there are 26 letters are present in both plaintext and cipher text spaces, we will have 26*26 possibilities for selecting keys. Therefore, key space for the above cryptosystem is **26*26**, that is, $\mathbf{\Sigma^2}$.

2: What is the maximum number of different encryption functions of a block cipher over the alphabet {O, I} with block length n?

The encryption functions of a block cipher are permutations. Therefore, the maximum number of encryption function is $(|\Sigma|^n)! = 2^n!$

4: Suppose that we use Caesar cipher with multiplication over Z/26Z (i.e. affine cipher): \[c = 11 p + 5. \] Can you find the formula for decryption? What is the cipher text for "TEXAS"? What is the plaintext for "OKLAHOMA" if we treat it as cipher text?

A=0 B=1 C=2 D=3 E=4 F=5 G=6 H=7 I=8 J=9 K=10 L=11 M=12 N=13 O=14 P=15 Q=16 R=17 S=18 T=19 U=20 V=21 W=22 X=23 Y=24 Z=25

“TEXAS”
T=19, E=4, X=23, A=0, S=18
For T, 11(19)+5 mod 26 => 6. Which is “G”
For E, 11(4)+5 mod 26 => 23. Which is “X”
For X, 11(23)+5 mod 26 => 24. Which is “Y”
For A, 11(0)+5 mod 26 => 5. Which is “F”
For S, 11(18)+5 mod 26=> 21. Which is “V”

Hence, Cipher text for “TEXAS” is “**GXYFV**”

“OKLAHOMA”
O=14,K=10,L=11,A=0,H=7,O=14,M=12,A=0

Assuming 11x = 1 mod 26, we will solve for x using Euclidian Algorithm

26=2*11+4
11=2*4+3
4=1*3+1
So, 1=4-1*3=4-1*(11-2*4)=3*4-1*11=3(26-2*11)-1*11=3*26-7*11
Thus, x=-7 mod 26 = 19
We can write, 19*11*p = 19(c-5)
19*11*p mod 26 =p mod 26 = 19(c-5) mod 26

Therefore, the formula for decryption is **19(c-5) mod 26**

For O, 19(14-5) mod 26 => 15. Which is “P”
For K, 19(10-5) mod 26 => 17. Which is “R”
For L, 19(11-5) mod 26 => 10. Which is “K”
For A, 19(0-5) mod 26 => 9. Which is “J”
For H, 19(7-5) mod 26 => 12. Which is “M”
For O, 19(14-5) mod 26 => 15. Which is “P”
For M, 19(12-5) mod 26 => 3. Which is “D”
For A, 19(0-5) mod 26 => 9. Which is “J”

Hence, Plaintext for “OKLAHOMA” is “**PRKJMPDJ**”

3: Read the page
https://en.wikipedia.org/wiki/Frequency_analysis
and write a program to calculate the frequencies of English letters (case-insensitive) in the section ``History and usage'' (not including the title of the section and the text in the figures).

Below is the Python program which takes “frequency.txt” as input and gives frequencies of every letter in the file. “frequency.txt” holds history and usage content from the Wikipedia page mentioned above.

In [1]:
```
from string import ascii_lowercase
with open("frequency.txt") as f:
    text = f.read().strip().lower()
    dic = {}
    for x in ascii_lowercase:
        dic[x] = text.count(x)
    for k,v in dic.items():
        print("Frequency of letter "+"'"+ k+ "'" +" is",v)
```

```
Frequency of letter 'a' is 207
Frequency of letter 'b' is 45
Frequency of letter 'c' is 104
Frequency of letter 'd' is 82
Frequency of letter 'e' is 312
Frequency of letter 'f' is 65
Frequency of letter 'g' is 36
Frequency of letter 'h' is 110
Frequency of letter 'i' is 183
Frequency of letter 'j' is 3
Frequency of letter 'k' is 16
Frequency of letter 'l' is 107
Frequency of letter 'm' is 54
Frequency of letter 'n' is 170
Frequency of letter 'o' is 156
Frequency of letter 'p' is 68
Frequency of letter 'q' is 12
Frequency of letter 'r' is 166
Frequency of letter 's' is 205
Frequency of letter 't' is 223
Frequency of letter 'u' is 73
Frequency of letter 'v' is 20
Frequency of letter 'w' is 34
Frequency of letter 'x' is 14
Frequency of letter 'y' is 67
Frequency of letter 'z' is 2
```