Qixiang Liu
2856114
Homework 1
EECS 565

Decryption: English prose quotation

Question 1: "fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc";

Step 1: n: 7 j: 7 b: 5 w: 4 x: 3 c: 3 v: 3 u: 3 f: 3 a: 2 h: 2 q: 2
k: 1 d: 1 m: 1 r: 1

Step 2: English high frequency: {e,t,a}

Shift Cipher: $D_K(c)=c-K \bmod 26$ ←-Guess

Step3: fqjcb = whats

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

K=9   14-9 = 5 (E)   Guess N-J = E-A

Answer: whats in a name arose by any other name would smell as sweet – Shakespeare's Romeo and Juliet

Question 2:

"oczmz vmzor jocdi bnojv dhvod igdaz "
"admno ojbzo rcvot jprvi oviyv aozmo "
"cvooj ziejt dojig toczr dnzno jahvi "
"fdiyv xcdzq zoczn zxjiy";

```
o: 18 z: 13 v: 10 d: 9 j: 9 i: 9 c: 7 n: 5 r: 4 a: 4 m: 4 t: 3 y:
3 h: 2 g: 2 x: 2 b: 2 f: 1 p: 1 e: 1 q: 1 u: 0 w: 0 l: 0 k: 0 s: 0
```

English Frequency: {'e','t','a'}
Guess common English diagram : {EN,RE,ER} ➔ there are many mz;zm
So oczmz = there;
O Z V   VWXYZ ABCDEFGH I J KLMNOPQ R STU
15 26 22   AB CDE FGH I J KMLN OPQRSTUVWXY Z

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Answer: K = 21; there are two things to aim at in life first to get what you want and after that to enjoy it only the wisest of mankind achieve the second ---- Logan Pearsall Smith

Question 3: "pbegu uymiq icuuf guuyi qguuy qcuiv fiqgu uyqcu qbeme vp"

```
u: 12 q: 6 i: 5 g: 4 y: 4 e: 3 c: 3 v: 2 b: 2 f: 2 p: 2 m: 2
```

“pbe guuy miqi cuuf guy iq guuy qcuiv fiq guuy qcu qbeme vp”

EE;TT;AA;OO; guess UU = OO; The English start: The {E,T,A,O};

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J

Answer: the cook was a good cook as cooks go and as cooks go she went -----Saki (Reginald on Besetting Sins)

Question 4:
jrgdg idxgq anngz gtgtt sitgj ranmn oeddi omnwj rajvk sexjm dxkmn wjrgm ttgdt gognj ajmzg ovgki nlaqg tjamn xmsmj jrgko jtgnw jrgnj rgvat tmgta wamno jjrgw izgtn sgnji babgu

```
g: 23 j: 17 n: 14 t: 13 m: 11 a: 10 r: 8 o: 6 i: 6 d: 6 w: 5 k: 4 s: 4
x: 4 v: 3 z: 3 e: 2 q: 2 b: 2 l: 1 u: 1
```

Guess: G=E J=T N= N T=R
Tre = The; nezer = Never
R: H; Z:V;

- Answer: The people can never err more than in supposing that by multiplying their representatives beyond a certain limit, they strengthen the barrier against the government of a few. ----- James Madison, No. 58

Question 5:
ejitp spawa qleji taiul rtwll rflrl laoat wsqqj atgac kthls iraoa twlpl qjatw jufrh lhuts qataq itats aittk stqfj cae

```
a: 15 t: 15 l: 11 q: 7 j: 6 s: 6 i: 6 r: 5 w: 5 e: 3 u: 3 f: 3 p: 3 h:
3 k: 2 c: 2 o: 2 g: 1
```

Guess: T=T; A = {E,A}; because there are many it, at;
ej it pspawa qlej it aiul rtwll rflrl laoat wsqqj atgac kthls iraoa twlpl qjatw jufrh lhuts qataq itats aittk stqfj cae

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I		G		C	L	M	B	N	O	H	E			F	R	S	D	A	T	N		W			

Answer:
contrariwise continued tweedledee if it was so it might be and if it were so it would be but as it isnt it aint thats logic

Coding: Calculate times of each letter: Just help to calculate high frequency of letters;

```
/*
Author: Qixiang Liu
Date: 01/31/2018
Log: 1. Substition ciphertext
       2. Sort
         3. Guess shift OR substitution
         4. Search from Internet
*/
#include <iostream>
#include <map>
#include <set>
#include <functional>
#include <algorithm>
#include <utility>
#include <vector>
using namespace std;

std::map<char,int> letters;

typedef pair<char, int> PAIR;

bool cmp_by_value(const PAIR& lhs, const PAIR& rhs) {
  return lhs.second < rhs.second;
}

struct CmpByValue {
  bool operator()(const PAIR& lhs, const PAIR& rhs) {
    return lhs.second > rhs.second;
  }
};


void calculateEachOfLetterNum(std::string ciphertext){
  for(int i=0;i<ciphertext.length();i++){
    char eachOfLetter = 'a';
    while(eachOfLetter<='z'){
      if(ciphertext[i]==eachOfLetter){
        letters[eachOfLetter]+=1;
      }
      eachOfLetter++;
    }
  }
}
```

```
void printLetterNumOfText(std::map<char,int> myletters){
  char letter = 'a';
  while(letter<='z'){
    std::cout << letter<<": "<< letters[letter]<<std::endl;
    letter++;
  }
}


int main(){
  char ruleOfEnglish[9] = {'e','t','a','o','i','n','s','h','r'}; //the first 9 letters -high frequency
  char ruleOfEnglish2[9] = {'t','e','a','o','i','s','n','h','r'};
  char ruleOfEnglish3[9] = {'e','a','s','n','o','t','m','l','w'};
  char ruleOfEnglish4[9] = {'t','a','e','o','i','s','n','h','r'};
  char ruleOfEnglish5[9] = {'a','e','t','o','i','n','s','h','r'};
  char ruleOfEnglish6[3] = {'e','t','a'};
  char ruleOfEnglish7[3] = {'t','e','a'};

  char letter = 'a';
  while(letter<='z'){
    letters[letter] = 0;
    letter++;
  }
  std::string test1= "fqjcbrwjwjvnjaxbnkhjwhxcq"
    "nawjvnfxdumbvnuujbbfnnc";
  std::string test2= "oczmz vmzor jocdi bnojv dhvod igdaz "
                   "admno ojbzo rcvot jprvi oviyv aozmo "
                   "cvooj ziejt dojig toczr dnzno jahvi "
                   "fdiyv xcdzq zoczn zxjiy";
  std::string test3= "pbegu uymiq icuuf guuyi qguuy qcuiv fiqgu uyqcu qbeme vp";
  std::string test4 = "ejitp spawa qleji taiul rtwll rflrl laoat wsqqj "
                    "atgac kthls iraoa twlpl qjatw jufrh lhuts "
                    "qataq itats aittk stqfj cae";
  std::string test5 = "jrgdg idxgq anngz gtgtt sitgj ranmn oeddi omnwj rajvk "
                    "sexjm dxkmn wjrgm ttgdt gognj ajmzg ovgki nlaqg tjamn "
                    "xmsmj jrgko jtgnw jrgnj rgvat tmgta wamno jjrgw izgtn sgnji babgu";
  std::string guess1,guess2,guess3,guess4,guess5;
  guess1 = guess2 = guess3 = guess4 = guess5=test4;


  calculateEachOfLetterNum(test4);
  std::vector<PAIR> letterVector(letters.begin(),letters.end());

  std::sort(letterVector.begin(),letterVector.end(),CmpByValue());

  for (int i = 0; i != letterVector.size(); ++i) {
    cout << letterVector[i].first <<": "<<letterVector[i].second << " ";
  }
  std::cout << std::endl;

  return 0;
}
```