Homework 1

Question 1

- The differences
  - **Operation mode:**

    The substitution cipher replaces the plaintext characters with other characters, numbers and symbols. The common way is to shift the plaintext. After the operation, the relative position of letters didn't change.

    And transposition cipher rearranges the position of the characters of the plaintext, which means the relative position of the words changes.
  - **Minimum operating unit:**

    The substitution cipher operates on each letter and the transformation happens on each letter as well. However, the transposition cipher operates on a group of letters. For example, the demo cipher of transposition cipher on PPT operates on each 4 letters.
  - **Complexity:**

    Some kinds of substitution cipher, like Caesar rotation algorithm, has billions of possibilities. Relatively speaking, the complexity of transposition cipher will be lower.
  - **Results:**

    After the substitution cypher, the identity of the character is changed while its relative position remains unchanged.

    After the transposition cypher, the position of the character is changed in spite of its identity.
  - **Detection:**

    With the help of the low-frequency letter, the plaintext can be easily discerned in the substitution technique. On the contrary, in the transposition technique, the keys near to the right key lead to the detection of the plaintext.

- Examples
  - Substitution Cipher:
    - Caesar rotation cipher: It's introduced during the class.
    - Using the following S-box:

      ```
      plain alphabet : abcdefghijklmnopqrstuvwxyz
      cipher alphabet: phqgiumeaylnofdxjkrcvstzwb
      ```

      eg: input `i love zju`, the output will be `andsibyv`
  - Transposition Cipher:
    - Fence cipher: choose a depth and divided the plaintext by the depth. Output the first letter of each group in turn, then the second... until all letters are output.

      eg: `I love zju` using 2 as the depth. the output will be `Ioejlvzu`

- The algorithm introduced during class.

Question 2

- Programming Environment

  Simply using C compiler under windows.

  Contain the `<stdlib.h>` library if possible.

- Design And Implementation

  The encipher algorithm is improved by the Caesar rotation algorithm. In order to better adapt to production, the algorithm is to encrypt the visible ASCII (95 at all).

  - First, divide the text to many blocks by a fixed number (BLOCK_SIZE)
  - In Group **i**, the first **j** letter's substitution is

    $$X = \begin{cases} X + offset & if\ X + offset < Max \\ X + offset - Num & if\ X + offset > Max \end{cases}$$

    where,

    $$\text{X is the original ASCII of the letter and Num is the number of visible ASCII}$$
    $$\text{and } offset = (i * Blocksize + j)\ mod\ Num$$

  - The pseudo code is:

    ```
    fuc encipher( char* buf, int radix, int times )
    {
        // This is the main encipher algorithm.
        // The information we use is
        //      the block_idx: radix
        //      the letter_idx: i
        // And offset = block_idx * block_size + letter_index
        // If out of range, we make a adjust.
        for(int i = 0; i < times; i++){
            bufInt = buf[i];
            offset = (radix * BLOCK_SIZE + i) % ASC_VISIBLE_NUM;
            if( bufInt + offset > ASC_VISIBLE_MAX )
                bufInt = bufInt + offset - ASC_VISIBLE_NUM;
            else
                bufInt += offset;
            buf[i] = bufInt;
        }
    }
    ```

  - For example, in production, if block size is 16 bit, the in a long text, the first 16 bit is encrypted like

    ```
    original text: I love zju so much
    cipher text:   Y1~#+z62#/:/,=,5$*
    ```

    and in the next group, the encryption rule will be different.

  - The improved algorithm can be implied in all visible ASCII letters' encryption, which is useful in our production. And the encryption rule will be changed between blocks. Also, since we add the position **j** as a factor to encrypt, the probability of each letter

appearing is not fixed. So the frequency analysis will be difficult to apply, which guarantees our codes' security.

- Results (all the test is under Block_size = 16)
  - Sample

```
Please input the plain text:
I love zju, Zhejiang, China very much !!! ^^*@#()&@(*)(@IDU@(I
Please to enter your choice:
0.Esc    1.Encipher      2.Decipher
1
Input:  I love zju, Zhejiang, China very much !!! ^^*@#()&@(*)(@IDU@(I
Encode: Y1~#+z62#/F;v&$**#1+PEi028,KC3AIP?H7=UWXYY9:f}agig#knnn(2.@,t7

Please input the plain text:
Y1~#+z62#/F;v&$**#1+PEi028,KC3AIP?H7=UWXYY9:f}agig#knnn(2.@,t7
Please to enter your choice:
0.Esc    1.Encipher      2.Decipher
2
Input:  Y1~#+z62#/F;v&$**#1+PEi028,KC3AIP?H7=UWXYY9:f}agig#knnn(2.@,t7
Decode: I love zju, Zhejiang, China very much !!! ^^*@#()&@(*)(@IDU@(I
```

  - Check the string with student ID and name

```
Please input the plain text:
Hello, i am liuxuanming, my nick_name is L.Bruyne, and my student number is 318016071 8932f0901ildip10jdj
Please to enter your choice:
0.Esc    1.Encipher      2.Decipher
1
Input:  Hello, i am liuxuanming, my nick_name is L.Bruyne, and my student number is 318016071 8932f0901ildip10jdj
Encode: Xv~ $A6!8z(;)'486#11.4.SH7DK;72;0@4A:U@KX&h}OSXNFmbESJfUbi``bRT^eqaibX\jxcn{0/70283;6&?A<<q<F>@yBv|%FF"|$

Please input the plain text:
Xv~ $A6!8z(;)'486#11.4.SH7DK;72;0@4A:U@KX&h}OSXNFmbESJfUbi``bRT^eqaibX\jxcn{0/70283;6&?A<<q<F>@yBv|%FF"|$
Please to enter your choice:
0.Esc    1.Encipher      2.Decipher
2
Input:  Xv~ $A6!8z(;)'486#11.4.SH7DK;72;0@4A:U@KX&h}OSXNFmbESJfUbi``bRT^eqaibX\jxcn{0/70283;6&?A<<q<F>@yBv|%FF"|$
Decode: Hello, i am liuxuanming, my nick_name is L.Bruyne, and my student number is 318016071 8932f0901ildip10jdj
```

    It can be seen my name is replaced as `)'486#11.4.` and ID is replaced as `0/70283;6`. However the cipher is not fixed because of the position of the letter.

```
Please input the plain text:
i am liuxuanming, my nick_name is L.Bruyne, and my student number is 318016071
Please to enter your choice:
0.Esc    1.Encipher      2.Decipher
1
Input:  i am liuxuanming, my nick_name is L.Bruyne, and my student number is 318016071
Encode: y1s!4" -1/{**'-'LAO=D4O+4)9-:3N9DQ~avHLQG?f[>LC_N[bWY[KMW^jZb[QUcq\gt)(0)+1,4/

Please input the plain text:
```

    from this example we can see the cipher is changed.

  - Big data

```
Input:  Substitution of single letters separately-simple substitution-can be demonstrated by writing out the alphabet in
 some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or
 reversed (creating the Caesar and Atbash ciphers, respectively) or scrambled in a more complex fashion, in which case i
t is called a mixed alphabet or deranged alphabet. Traditionally, mixed alphabets may be created by first writing out a
keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.
Encode: c't')`+--#**<-%?4+1+1+F4.>?1?ANC6B4F6J<DRfNEJNKE`UXFXZP\``T[[zRQ_qUYtZ\ehhnpo_see"e}%}yq}sys-}%%1'{y5w$)"{}"2>)/
A632+F7;.O>LB>OC7CF:I<FMYODB]RUCUWMY[[QXXxkAVXcp[fsi[ie``z]|qtbtvlxzzpww*lx}vprv'A4i^`[8|$,%#1?".3,&(,<H7,ELO4OD:<:I;;WHL
ZNBTDRTGGclIYMJ`TZTmcXVq6UZiXjx[i`|?sbbuk$howpn|`8-!t$"wv)~-|%3C;,O>3$4$1'2,,H39K.M<?C7R7DCGD>RZB>QGIPPncNTf_QSNTlQPcVq\
ht_jw\[ghbb`a!ol|jj'iuzsmos$O!%3xz)x'!  <~+O)#%)9SF{;+/5A7>>2>?M`UDAQ??[>JOHBDHXXeTIbiMQlQaURfXXtXpw_cmoq}vrjvlrl&v}}*l,
xs)(!%w@5)|&)1%+%>2&2(%9++G5/?@2@BO:@R=IaVLA?I[TPHTJPJcFRSg]RPk_S\QZ`\b\uc]mn`np}hn!vki%gsxqkmq".x`l'{y5,+.z';,O#%3O
```

    This is a part of substitution's definition from WIKI.

```
Input:  c't')`+--#**<-%?4+1+1+F4.>?1?ANC6B4F6J<DRfNEJNKE`UXFXZP\``T[[zRQ_qUYtZ\ehhnpo_see"e}%}yq}sys-}%%1'{y5w$)"{}"2>)/
A632+F7;.O>LB>OC7CF:I<FMYODB]RUCUWMY[[QXXxkAVXcp[fsi[ie``z]|qtbtvlxzzpww*lx}vprv'A4i^`[8|$,%#1?".3,&(,<H7,ELO4OD:<:I;;WHL
ZNBTDRTGGclIYMJ`TZTmcXVq6UZiXjx[i`|?sbbuk$howpn|`8-!t$"wv)~-|%3C;,O>3$4$1'2,,H39K.M<?C7R7DCGD>RZB>QGIPPncNTf_QSNTlQPcVq\
ht_jw\[ghbb`a!ol|jj'iuzsmos$O!%3xz)x'!  <~+O)#%)9SF{;+/5A7>>2>?M`UDAQ??[>JOHBDHXXeTIbiMQlQaURfXXtXpw_cmoq}vrjvlrl&v}}*l,
xs)(!%w@5)|&)1%+%>2&2(%9++G5/?@2@BO:@R=IaVLA?I[TPHTJPJcFRSg]RPk_S\QZ`\b\uc]mn`np}hn!vki%gsxqkmq".x`l'{y5,+.z';,O#%3O
Decode: Substitution of single letters separately-simple substitution-can be demonstrated by writing out the alphabet in
 some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or
 reversed (creating the Caesar and Atbash ciphers, respectively) or scrambled in a more complex fashion, in which case i
t is called a mixed alphabet or deranged alphabet. Traditionally, mixed alphabets may be created by first writing out a
keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.
```

    We can see the encryption and decryption can be done perfectly!

  - More examples can be done through the executable file.

- Summary

  I use C to create a program which can encrypt the text in substitution way. This algorithm is safe and dependable which can be applied to all visible ASCII letter. Because of the block operation, the role of frequency analysis becomes very small, which guarantees our security.

  Through this assignment, I have a deeper understanding of the substitution algorithm and the permutation algorithm. I also have a better understanding of how to design and implement an industry-level encryption algorithm. This is a meaningful practice assignment.