Assignment 3

Zehao Ba (B00732676)

1. Note:
    a. Please input uppercase when choose cipher and lowercase when input encrypt or decrypt;

- Caesar cipher
    - Please input secret key between 0 and 25

Here is the sample of encrypt ‘hello’ with secret key = 4:

```
========== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py ==========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
C
Please choose to encrypt(e) or decrypt(d):
e
Enter the message:
hello
Enter the secret key:
4
The encrypted output is: lipps
```

Here is the sample of decrypt ‘lipps’ with secret key = 4:

```
========== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py ==========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
C
Please choose to encrypt(e) or decrypt(d):
d
Enter the message:
lipps
Enter the secret key:
4
The encrypted output is: hello
```

- Vigenere cipher

Here is the sample of encrypt ‘helloworld’ with secret key ‘secret’:

```
========== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py ==========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
V
Please choose to encrypt(e) or decrypt(d):
e
Enter the message:
helloworld
Enter the secret key:
secret
The encrypted output is: zincspgvnu
```

Here is the sample of decrypt ‘zincspgvnu’ with secret key ‘secret’:

```
============== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py =========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
V
Please choose to encrypt(e) or decrypt(d):
d
Enter the message:
zincspgvnu
Enter the secret key:
secret
The encrypted output is: helloworld
```

- Matrix tansposition cipher
  - Note: please input the secret key directly without space.

  Here is the sample of encrypt ‘you guessed it!’ with secret key ‘3412’:

```
============== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py =========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
M
Please choose to encrypt(e) or decrypt(d):
e
Enter the message:
you guessed it!
Enter the secret key:
3412
The encrypted result is: ued!%s%%ygsiouet
```

  Here is the sample of decrypt ‘ued!%s%%ygsiouet’ with secret key ‘3412’:

```
============== RESTART: C:₩Users₩zehao₩Desktop₩6708₩ass3₩q1.py =========
=====
Please choose Caesar(C), Vigenere(V) or Matrix transposition(M) cipher:
M
Please choose to encrypt(e) or decrypt(d):
d
Enter the message:
ued!%s%%ygsiouet
Enter the secret key:
3412
The decrypted result is: you guessed it!
```

2. Advanced encryption standard

- Overview

  The advanced encryption standard is developed by US National Institute of Standards and Technology in 1997 [1]. The overall achievement of AES is to protect sensitive information of government. The institution began to use advanced encryption standard instead of older data encryption standard. The advanced encryption standard is the open selection process, which means everyone can unload the candidate cipher. Rijndael's license is a government standard which represents the certificate of quality. Besides, the International Organization for Standardization, the Internet Engineering Task Force, and the Institute of Electrical and Electronics Engineers are also use AES as a standard.

  The minimum functional requirements build the symmetric block ciphers which can solve 128-bit plaintext and key length between 128, 192 and 256 bits. At the beginning, the requirements were asked to support 192 and 256 bits' plaintext but they dropped them finally. At we talked before, the advanced encryption standard's submitter is worldwide basis, if you want to be one of the advanced encryption standard candidate, there are some requirements you should provide [1]:

  1. A plaintext with a complete written specification algorithm;
  2. An implementation in ANSI C, and the optimization with math method in ANSI C and Java;
  3. Implementation based on this method with series example and Monte Carlo test, including the output;
  4. Estimation including both software and hardware, potential attack, advantages and disadvantages of the cipher application across areas;
  5. The analysis of cipher's advantages to against known cryptanalytic attack.

  This is the first stage of advanced encryption standard, which presented in the first advanced encryption standard candidate conference. It is called the first evaluation round.

- Key generation

  There are four transformations key in the advanced encrypted standard process: 'ByteSub', 'ShiftRow', 'MixColumn' and 'AddRoundKey'.

  1. AddRoundKey

     State and round key are the two inputs of the AddRoundKey. The state is represented as $a_{i,j}$, where $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nb}$; round key is represented as an array of bytes $\mathrm{r}k_{i,j}$, where $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nb}$. The round key is got by expanding the cipher key into an array $k_{i,j}$, where $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nb} \cdot \mathrm{Nr}$, which is called expanded key. Doing the XOR with state key $a_{i,j}$ and round key $\mathrm{r}k_{i,j}$, and get the output of AddRoundKey $b_{i,j}$. The round key is from the expanded key's first Nb column [1].

2. ByteSub
   In this transformation, the invertible function is used on state array. Assuming the state array is $a_{i,j}$, where $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nb}$, the invertible function $\mathrm{S}: \{0,1\}^8 \rightarrow \{0,1\}^8$ to each state byte $a_{i,j}$, where S is non-linear in the advanced encrypted standard encryption process [1]. This figure 1 shows how the S function works:

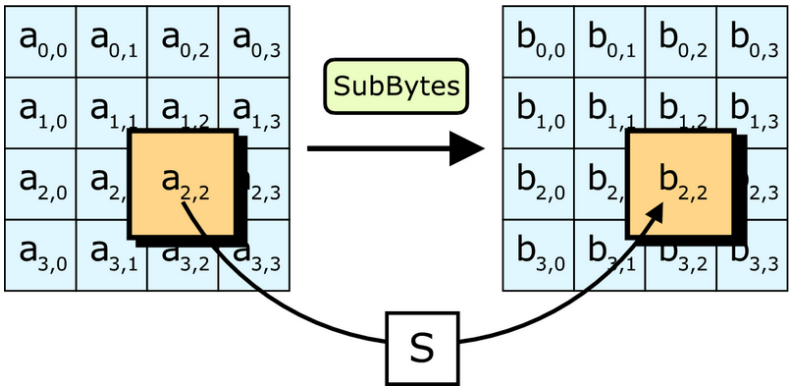

Figure 1. How the function S working in advanced encrypted standard.

3. ShiftRow
   This transformation is shift each row of state $a_{i,j}$ independently to the left. While there is a note that Row 0 will not be shifted. The bytes of shifting are decided by Nb [1].
4. MixColumn
   In this transformation, a fixed linear transformation is applied to each column of the state. Put the elements into the field F_{2^8} and hexadecimal them. For example, interpreting 01 to 0000 0001. Applying the MixColumn to each row of state [1].

- Encryption process.
  Advanced encrypted standard encrypts the plaintext by 1b bytes, 1b = 16, 24 or 32. The plaintext is constructed as $(4 \times \mathrm{Nb})$ array, we represent it as $(a_{i,j})$, which $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nb} - 1, \mathrm{Nb} = 4, 6, 8$. Nb is decided by 1b. Assuming there is n-th plaintext, it is stored in the array $a_{i,j}$ where $\mathrm{i} = \mathrm{n} \bmod 4$, $\mathrm{j} = \left\lfloor \frac{n}{4} \right\rfloor$ [1].
  The secret key in advanced encrypted standard is called cipher key. The cipher key is consisted by 1k bytes, where $\mathrm{k} = 16, 24 \text{ or } 32$. The cipher keys 1k are combined with plaintexts 1b. Similarity, the cipher key is also stored in the $4 \times \mathrm{Nk}$ array $k_{i,j}$, where $0 \leq \mathrm{i} \leq 4, 0 \leq \mathrm{j} \leq \mathrm{Nk} - 1$, $\mathrm{Nk} = 4, 6 \text{ or } 8$, which is depended on the value of 1k. Assuming there is n-th cipher key, it is stored in array $k_{i,j}$ where $\mathrm{i} = \mathrm{n} \bmod 4$, $\mathrm{j} = \left\lfloor \frac{n}{4} \right\rfloor$ [1].

The advanced encrypted standard encryption process is consisted of rounds. In each round, there are four transformations called ‘ByteSub’, ‘ShiftRow’, ‘MixColumn’ and ‘AddRoundKey’ except the last round. The intermediates result in the rounds are called states. The states come from the plaintext information. Usually, the number of round (Nr) will be set as 10, 12 and 14, which depends on the $\max\{\mathrm{Nb}, \mathrm{Nk}\}$. Specially, there is an initial AddRoundKey which is applied before the first round to the plaintext [1].

References

[1] V. R. Joan Daemen, The Design of Rijndael: AES - The Advanced Encryption Standard, German: Springer Science & Business Media, 2013.

[2] A. M. K. a. S. R. Kaminsky, "An overview of cryptanalysis research for the advanced encryption standard," in *MILITARY COMMUNICATIONS CONFERENCE*, MILCOM, 2010.

3.

a) ① $p = 7$, $q = 11$

② $n = p * q = 77$. $(p-1)(q-1) = 6 \times 10 = 60$

③ $e = 7$

④ $d = 43$

$e * d \bmod (p-1)(q-1) = 1$

$7d \bmod 60 = 1$

$7d = 301$ $d = 43$

public key = $(e, n) = (7, 77)$

private key = $(d, n) = (43, 77)$

Encryption is $c = m^e \bmod n = 6^7 \bmod 77$

$= [(6^3 \bmod 77) \cdot (6^3 \bmod 77) \cdot (6^1 \bmod 77)] \bmod 77$

$= (62 \times 62 \times 6) \bmod 77$

$= (62 * 64) \bmod 77$

$= 41$

b) ① $p = 11$, $q = 13$

② $n = p * q = 143$ $(p-1)(q-1) = 120$.

③ $e = 7$

④ $d = 103$

$e * d \bmod (p-1)(q-1) = 1$

$7d \bmod 120 = 1$

$7d = 721$. $d = 103$

public key = $(e, n) = (7, 143)$

private key = $(d, n) = (103, 143)$

Encryption is $C = m^e \bmod n = 9^7 \bmod 143$

$= (9^3 \times 9^3 \times 9^1) \bmod 143$

$= (14 \times 14 \times 9) \bmod 143$

$= (53 \times 9) \bmod 143$

$= 48$

c) ① $p = 17$, $q = 31$

② $p \cdot q = 527 = n$ $(p-1)(q-1) = 480$

③ $e = 7$

④ $d = 343$

* $d \bmod (p-1)(q-1) = 1$

$7d \bmod 480 = 1$

$7d = 2401$ $d = 343$

public key $= (e, n) = (7, 527)$

private key $= (d, n) = (343, 527)$

Encryption is $c = m^e \bmod n = 5^7 \bmod 527$

$= (5^4 \cdot 5^3) \bmod 527$

$= (98 \times 125) \bmod 527$

$= 129$.

4.

```
============== RESTART: C:/Users/zehao/Desktop/6708/ass3/q4.py ==============
=
Please enter the integer message:
9
Please enter integer e in key(e,n):
7
Please enter integer n in key(e,n):
143
Ciphertext is:  48
============== RESTART: C:/Users/zehao/Desktop/6708/ass3/q4.py ==============
=
Please enter the integer message:
5
Please enter integer e in key(e,n):
7
Please enter integer n in key(e,n):
527
Ciphertext is:  129
============== RESTART: C:/Users/zehao/Desktop/6708/ass3/q4.py ==============
=
Please enter the integer message:
6
Please enter integer e in key(e,n):
7
Please enter integer n in key(e,n):
77
Ciphertext is:  41
```