Assignment 3

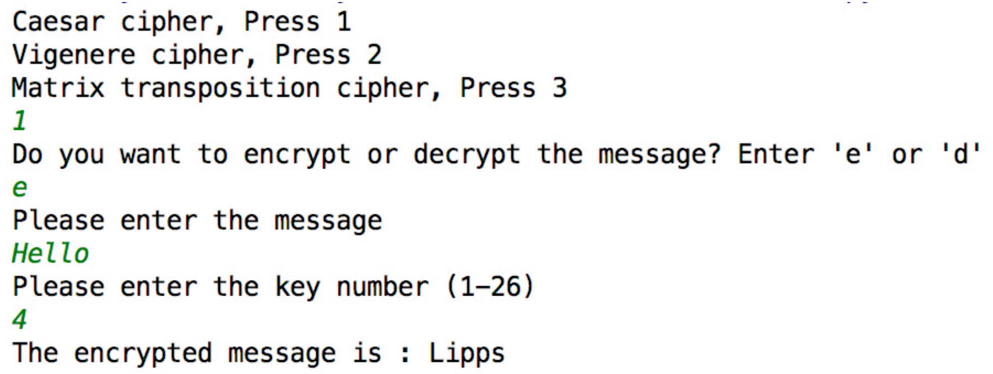
Name: Zewen Wang B#: B00756586

For program questions, I use python3 to code.

Q1 Program (Source codes can be seen in this finder)

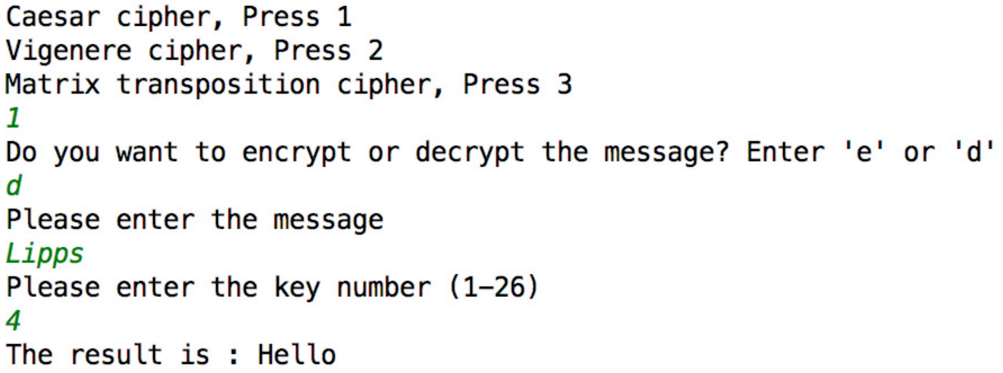
1. Caesar Cipher

(1) Sample for encryption by using Caesar cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
1
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
e
Please enter the message
Hello
Please enter the key number (1-26)
4
The encrypted message is : Lipps
```

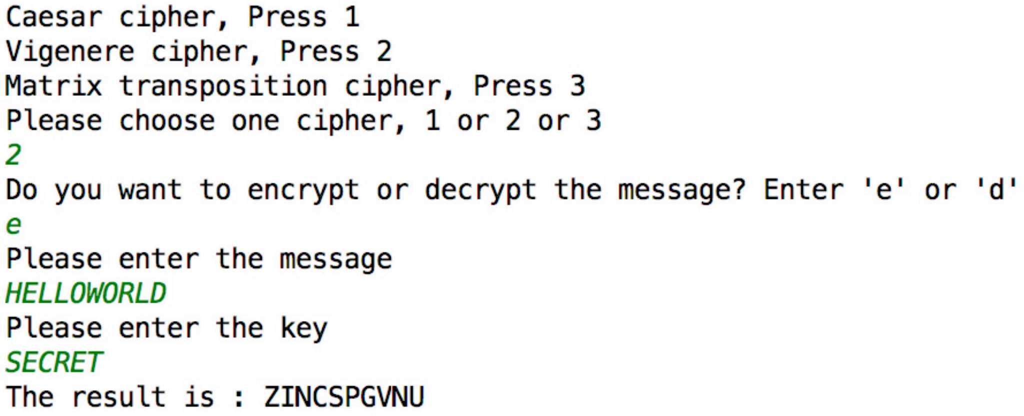
(2) Sample for decryption by using Caesar cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
1
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
d
Please enter the message
Lipps
Please enter the key number (1-26)
4
The result is : Hello
```

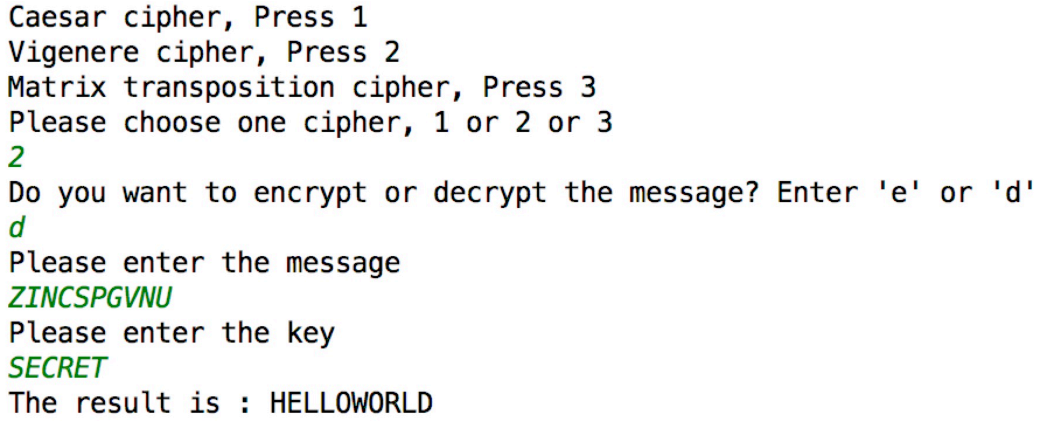
2. Vigenere Cipher

(1) Sample for encryption by using Vigenere Cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
Please choose one cipher, 1 or 2 or 3
2
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
e
Please enter the message
HELLOWORLD
Please enter the key
SECRET
The result is : ZINCSPGVNU
```

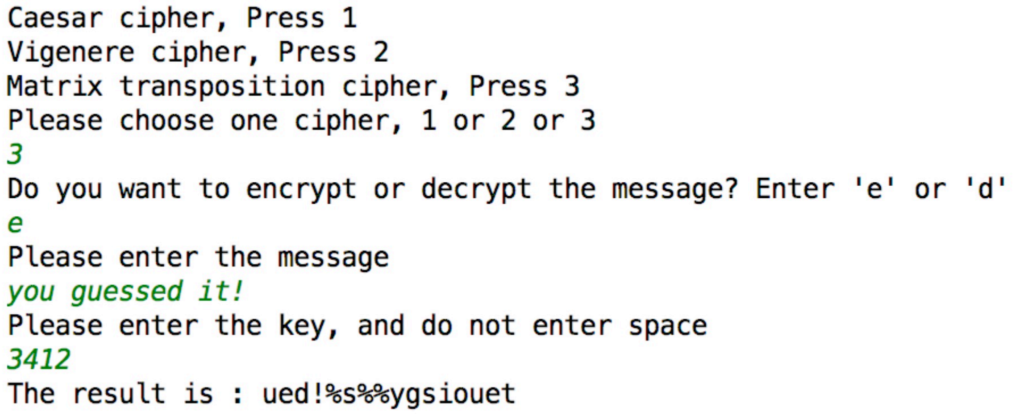
(2) Sample for decryption by using Vigenere Cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
Please choose one cipher, 1 or 2 or 3
2
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
d
Please enter the message
ZINCSPGVNU
Please enter the key
SECRET
The result is : HELLOWORLD
```

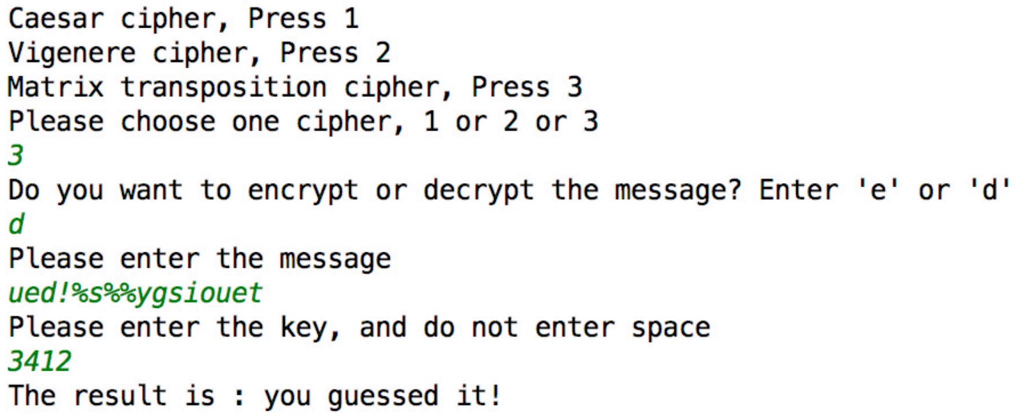
3. Matrix Transposition Cipher

(1) Sample for encryption by using Matrix Transposition Cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
Please choose one cipher, 1 or 2 or 3
3
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
e
Please enter the message
you guessed it!
Please enter the key, and do not enter space
3412
The result is : ued!%s%%ygsiouet
```

(2) Sample for decryption by using Matrix Transposition Cipher:



```
Caesar cipher, Press 1
Vigenere cipher, Press 2
Matrix transposition cipher, Press 3
Please choose one cipher, 1 or 2 or 3
3
Do you want to encrypt or decrypt the message? Enter 'e' or 'd'
d
Please enter the message
ued!%s%%ygsiouet
Please enter the key, and do not enter space
3412
The result is : you guessed it!
```

Q2. AES

(1) Overview [1]

Advanced Encryption Standard(AES), whose original name is Rijindael, is an electronic data encryption specification. This specification is a subset of the Rijindael algorithm which developed by Joan Daemen and Vincent Rijmen. Rijndael algorithm is a family of ciphers with different block sizes and key sizes. The block size of Rijindael can be specified and the key size can be any multiple of 32 bits with a minimum of 128 bits and a maximum of 256 bits, while the block size of AES is restricted to 128 bits and the key size of AES can only be 128, 192 and 256 bits.

(2) Key generation

The key size used for an AES cipher specifies the number of rounds of transformation that convert the plaintext into cipher text. The number of [2] cycles of repetition are as follows:

- 10 rounds of processing for 128-bit keys.
- 12 rounds of processing for 192-bit keys.
- 14 rounds of processing for 256-bit keys.

Last round of each case is different from the previous rounds.

The process of generating key is as follows [3]**:**

Assuming a 128-bit key

1. Firstly, the 128-bit key is converted into 16 bytes.
2. The 128-bit key is arranged in the form of a matrix of 4*4 bytes. The first four bytes from the key fill the first column of the matrix, the second four bytes from the key fill the second column of the matrix, and so on.
3. This key matrix is expanded into 44 words through AES Key Expansion algorithm. The logic of the key expansion algorithm is designed to ensure that changing one bit of the encryption key should affect the round keys for several rounds. This step can be seen from Fig.1.

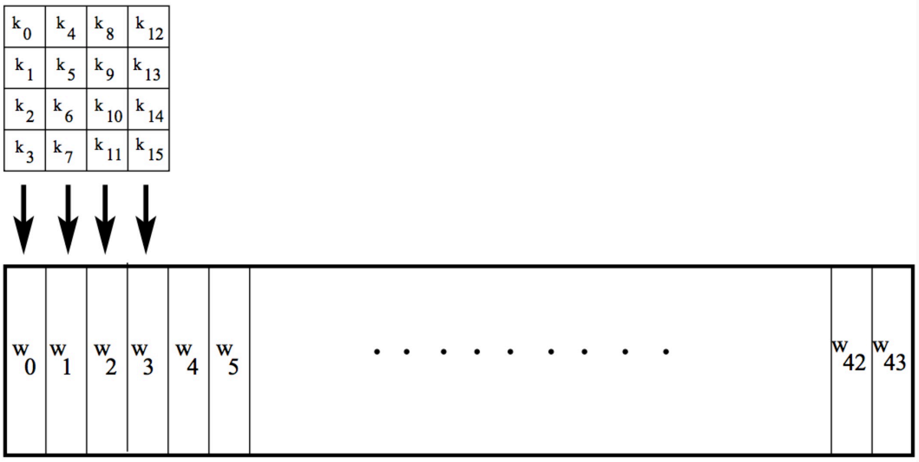

k_0 k_4 k_8 k_{12}
k_1 k_5 k_9 k_{13}
k_2 k_6 k_{10} k_{14}
k_3 k_7 k_{11} k_{15}
w_0 w_1 w_2 w_3 w_4 w_5 . . . . w_{42} w_{43}

Fig.1 Key matrix is expanded into 44 words. [3]

The details of the process of expansion are as follows [4]:

- The first four bytes of the encryption key constitute the word w0, the second four bytes constitute the word w1, and so on. The words w0, w1, w2, w3 are bitwise XOR'ed with the input block before the round process.

- The remaining 40 words of the key are used four words at a time in each of the 10 rounds.
- Subsequently, each of the four words in the remaining 40 words of the key schedule are used in each of the ten rounds of processing, which can be seen from Fig.2 below:

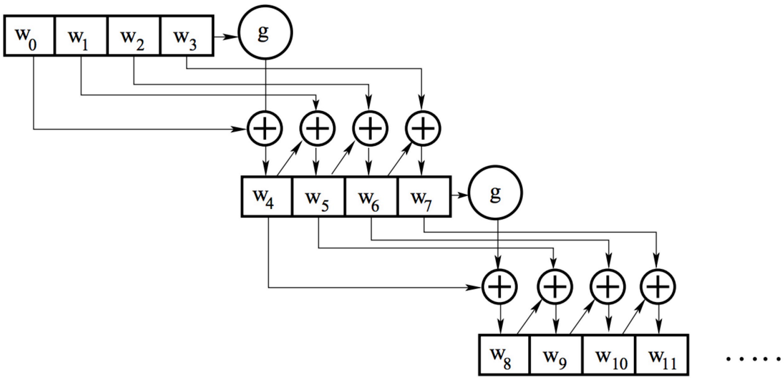


Fig.2 The words are bitwise. [3]

(3) Encryption process [5]

Assuming a 128-bit key, the process of encryption by using AES are as following: [参考]

Step1: Key Expansions—This step has been mentioned above.

Step2: Initialize the state array with the block data

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise XOR.

Step3: Perform nine rounds of state manipulation.

Why performing nine rounds not ten is because the tenth round uses a slightly different manipulation from the others. There are four operations in the first nine rounds.

- SubBytes: a non-linear substitution step where each byte is replaced with another based on a lookup table.
- ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

Step4: Perform the final Round of state manipulation (no MixColumns).

- SubBytes
- ShiftRows
- AddRoundKey

Step5: Copy the final state array out as the encrypted data which is ciphertext.

(4) Decryption process [6]

During decryption, the process is like the encryption process, but there are some differences between encryption and decryption. Assuming a 128-bit key,

1. XOR with ciphertext matrix with the last four words of the key schedule.
2. The four operations in each round are as follows:
    - Inverse shift rows
    - Inverse substitute bytes

- Add round key
- Inverse mix columns

The last round of decryption does not include the “Inverse mix columns” operation. The process of encryption and decryption can be seen from the Fig.3.

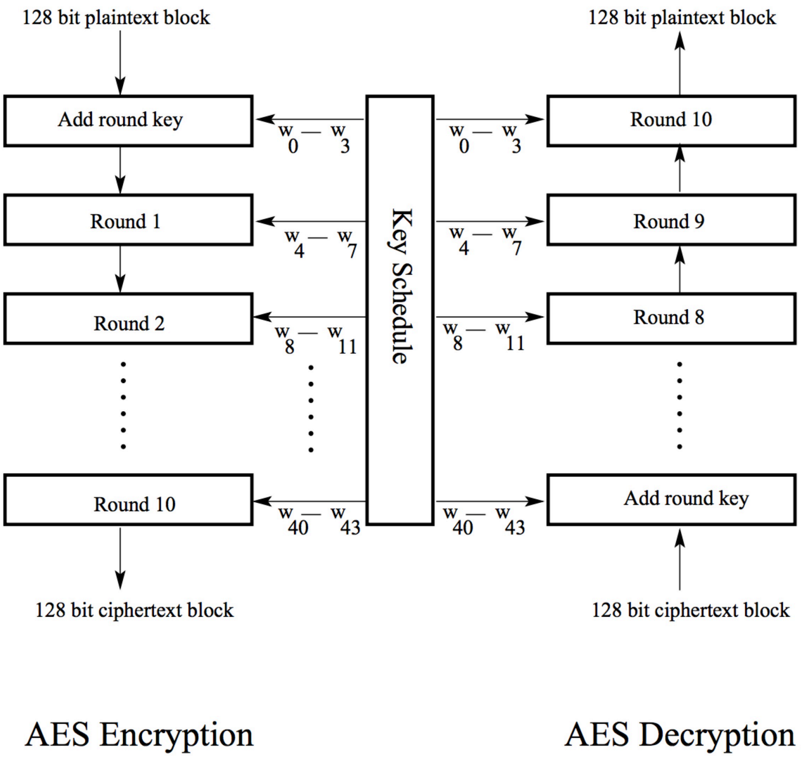


Fig.3 The process of encryption and decryption [6]

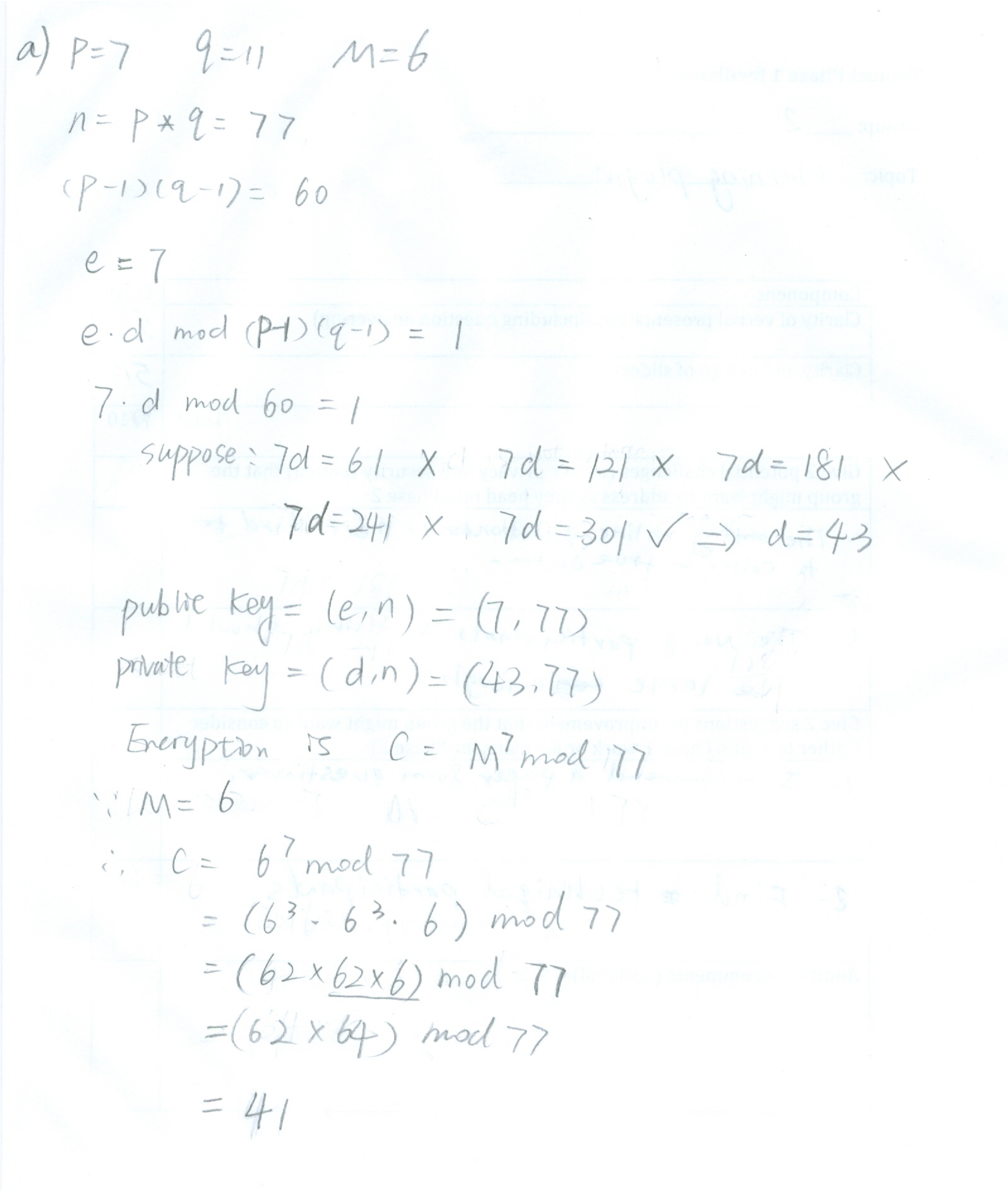
Reference:

[1] Advanced Encryption Standard. (2017, March 15). Retrieved March 20, 2017, from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] T. (n.d.). Advanced Encryption Standard. Retrieved March 20, 2017, from https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
[3] https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf
[4] http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf
[5] Steps in the AES Encryption Process. (n.d.). Retrieved March 20, 2017, from http://etutorials.org/Networking/802.11 security. wi-fi protected access and 802.11i/Appendixes/Appendix A. Overview of the AES Block Cipher/Steps in the AES Encryption Process/
[6] http://www.cse.wustl.edu/~jain/cse571-11/ftp/l_05aes.pdf

Q3

The process of each question can be seen from the pictures below:

a)



a) $P=7 \quad q=11 \quad M=6$

$n = P * q = 77$

$(P-1)(q-1) = 60$

$e = 7$

$e \cdot d \bmod (P-1)(q-1) = 1$

$7 \cdot d \bmod 60 = 1$

suppose: $7d = 61$ × $7d = 121$ × $7d = 181$ ×

$7d = 241$ × $7d = 301$ ✓ $\Rightarrow d = 43$

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

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

Encryption is $C = M^7 \bmod 77$

$\because M = 6$

$\therefore C = 6^7 \bmod 77$

$= (6^3 \cdot 6^3 \cdot 6) \bmod 77$

$= (62 \times \underline{62 \times 6}) \bmod 77$

$= (62 \times 64) \bmod 77$

$= 41$

b)

b) $p=11 \quad q=13 \qquad M=9$

$n=p*q=143$

$(p-1)(q-1)=120$

$e=7$

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

$7d \bmod 120 = 1$

suppose $7d=121$ × $7d=241$ × $7d=361$ ×

$7d=481$ × $7d=601$ × $7d=721 \Rightarrow d=103$

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

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

$\because M=9$

$\therefore$ Encryption $c = M^e \bmod n$

$= 9^7 \bmod 143$

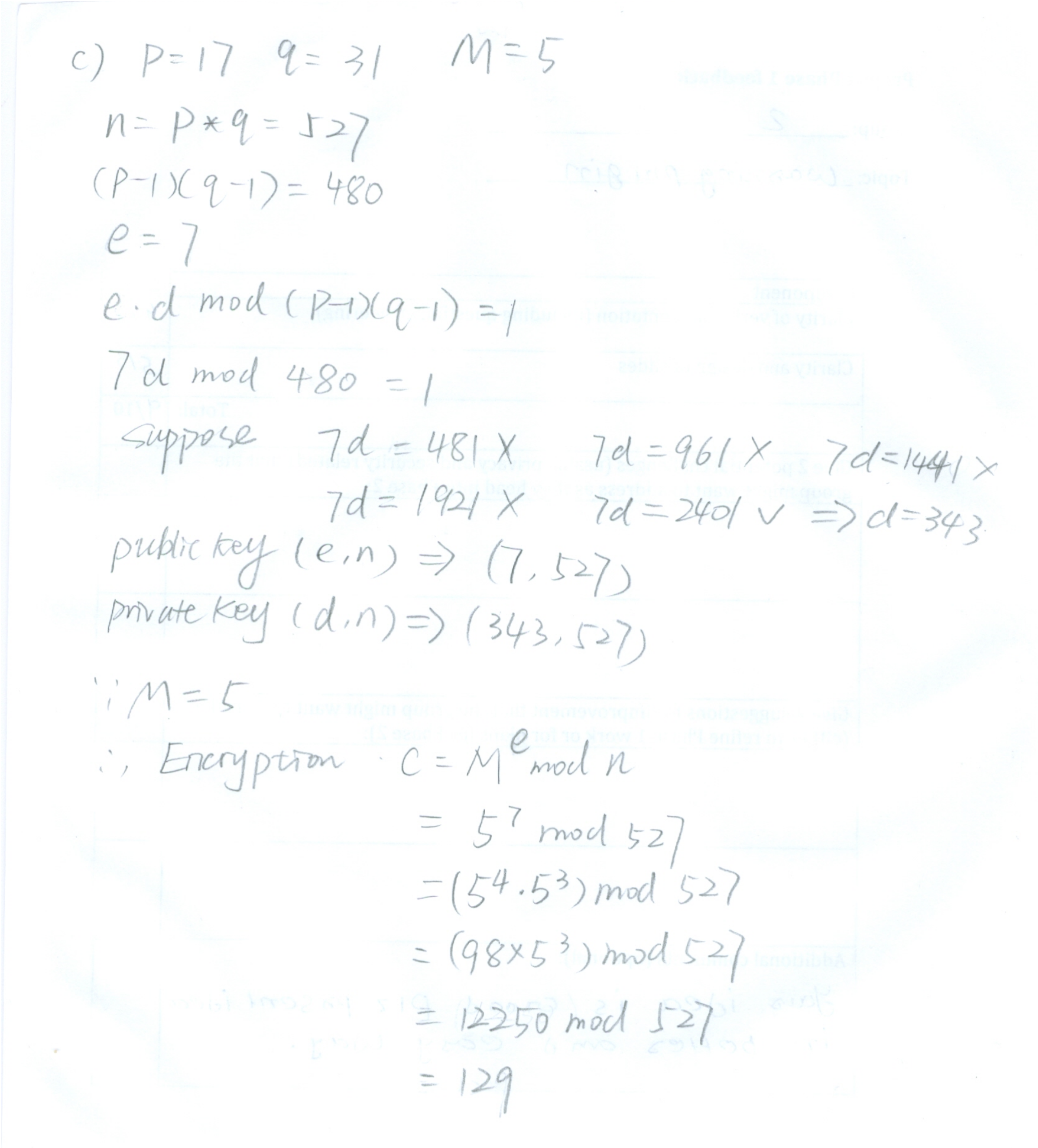
$= (9^3 \cdot 9^3 \cdot 9) \bmod 143$

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

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

$= 48$

c)



c) $P=17$ $q=31$ $M=5$

$n = P * q = 527$

$(P-1)(q-1) = 480$

$e = 7$

$e \cdot d \bmod (P-1)(q-1) = 1$

$7d \bmod 480 = 1$

suppose $7d = 481$ × $7d = 961$ × $7d = 1441$ ×

$7d = 1921$ × $7d = 2401$ ✓ $\Rightarrow d = 343$

public key $(e,n) \Rightarrow (7, 527)$

private key $(d,n) \Rightarrow (343, 527)$

$\because M = 5$

$\therefore$ Encryption $C = M^e \bmod n$

$= 5^7 \bmod 527$

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

$= (98 \times 5^3) \bmod 527$

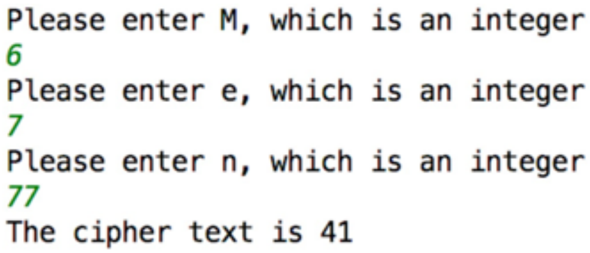
$= 12250 \bmod 527$

$= 129$

Q4.

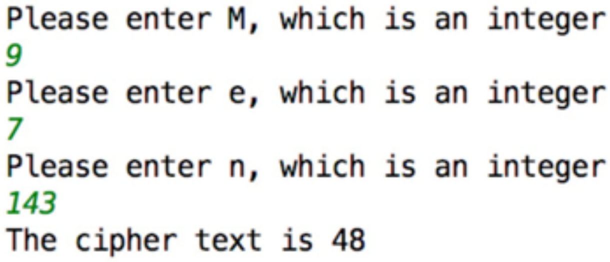
There are three samples which are corresponded to Question 3 respectively.

(1) M = 6, e = 7, n = 77



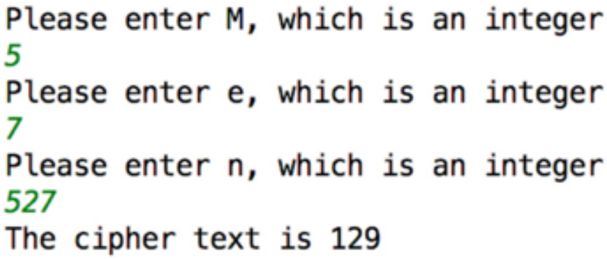
```
Please enter M, which is an integer
6
Please enter e, which is an integer
7
Please enter n, which is an integer
77
The cipher text is 41
```

(2) M = 9, e = 7, n = 143



```
Please enter M, which is an integer
9
Please enter e, which is an integer
7
Please enter n, which is an integer
143
The cipher text is 48
```

(3) M = 5, e = 7, n = 527



```
Please enter M, which is an integer
5
Please enter e, which is an integer
7
Please enter n, which is an integer
527
The cipher text is 129
```