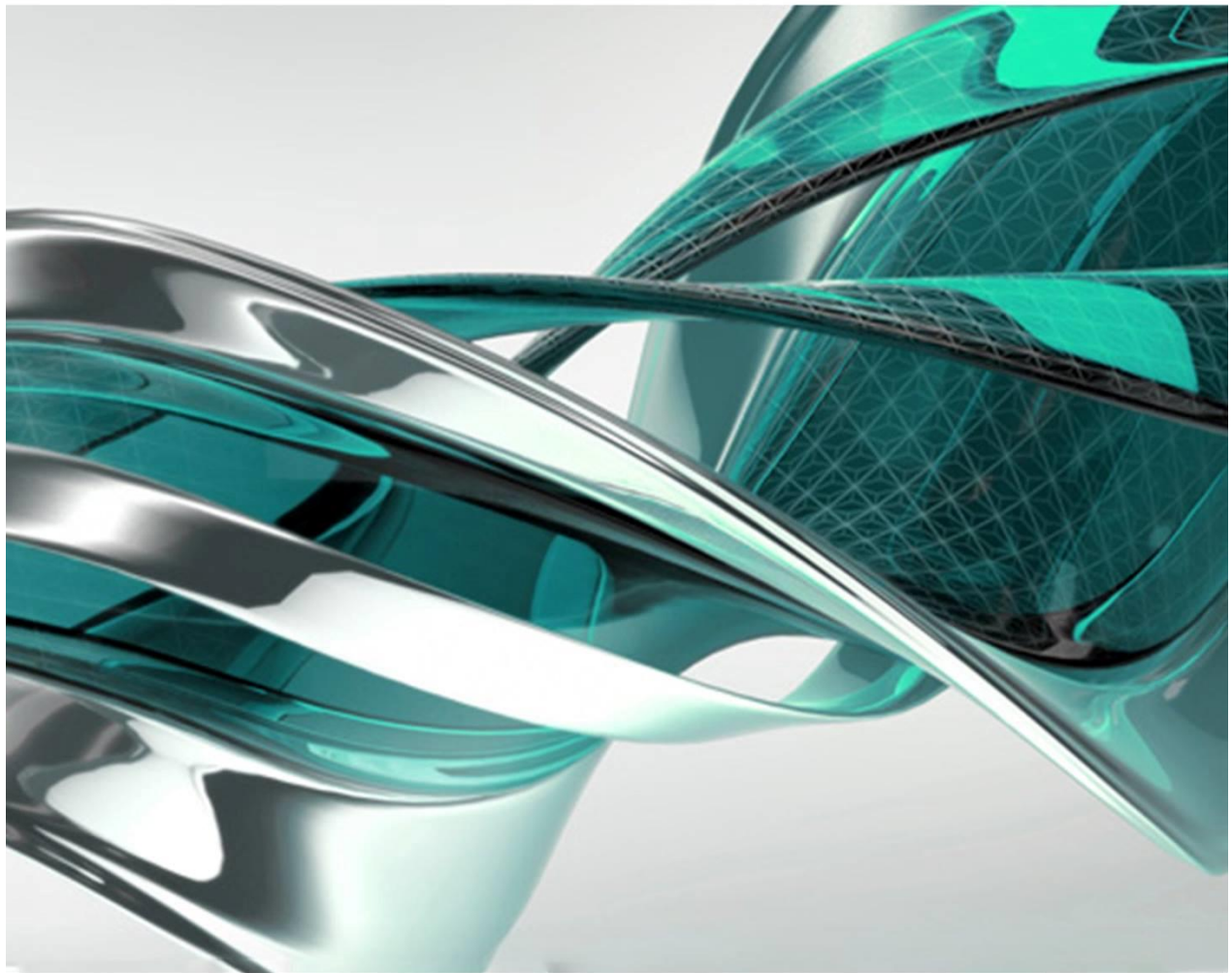


# Advanced Encryption Standard

Computer Programming Project



# ENCRYPT DECRYPT

128 bits  
Keys

Can Encrypt  
or Decrypt  
from text files

Can Continue to  
192 or 256 bits  
Keys

## Advisors

Asst. Prof. Dr. Kitsuchart Pasupa  
Asst. Prof. Dr. Natapon Pantuwong  
Mr. Anuntapat Anuntachai

## Production Teams

Mr. Thitikorn Lomlai  
Mr. Nuttapol Phomthon  
Mr. Taweewong Tocharoen  
Mr. Pongsakorn Khemanitthathai  
Mr. Mathas Anchaleekorane

**รายงานโครงงาน**  
**วิชา Computer Programming**  
**เรื่อง AES Encryption and Decryption**

**จัดทำโดย**

นายจิติกกร ล้อมลาย 58070031

นายณัฐพนธ์ พุ่มเถื่อน 58070037

นายทวิวงศ์ โตเจริญ 58070045

นายพงศกร เขมานิษฐาไท 58070087

นายเมธัส อัญชลีกรณีย์ 58070117

**นำเสนอ**

ผศ.ดร. กิติ์สุชาติ พสุภา

ผศ.ดร. ณัฐพล พันธุ์วงศ์

อาจารย์ อนันตพัฒน์ อนันตชัย

รายงานฉบับนี้เป็นส่วนหนึ่งของรายวิชา 06016206 COMPUTER PROGRAMMING

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง

หัวข้อโครงการ : AES Encryption and Decryption

วิชา : COMPUTER PROGRAMMING 06016206

ผู้จัดทำ :

|                          |          |             |
|--------------------------|----------|-------------|
| 1. นายจิติกกร ล้อมลาย    | 58070031 | Section : 2 |
| 2. นายณัฐพนธ์ พุ่มเถื่อน | 58070037 | Section : 2 |
| 3. นายทวิวงศ์ ไตเจริญ    | 58070045 | Section : 2 |
| 4. นายพงศกร เขมานิภูงาไท | 58070087 | Section : 2 |
| 5. นายเมธัส อัญชลีกรณีย์ | 58070117 | Section : 2 |

ปีการศึกษา : พ.ศ. 2558

อาจารย์ที่ปรึกษา :

1. ผศ.ดร. กิตติสุชาติ พสุภา
2. ผศ.ดร. ณัฐพล พันธุวงศ์
3. อาจารย์ อนันตพัฒน์ อนันตชัย

## บทคัดย่อ

เนื่องจากในชีวิตประจำวันของเรา บางข้อมูลที่เราส่งหากันในโลก Internet จำเป็นต้องมีการเข้ารหัส เพื่อเพิ่มความปลอดภัยในตัวข้อมูล ป้องกันการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต หรือแม้แต่นำไปสร้างความเสียหายจากข้อมูลที่ได้ไป เช่น การกรอกข้อมูล Username Password ในเว็บไซต์ ถ้าไม่มีการเข้ารหัส ผู้ใดที่ได้ข้อมูลไป ก็สามารถนำข้อมูลไปใช้ได้ทันที ซึ่งอาจจะนำไปก่อความเสียหายได้

ซึ่งทำให้กลุ่มของเรา ต้องการรู้เกี่ยวกับโครงสร้างของการเข้ารหัสและถอดรหัสของ AES ซึ่งมีความซับซ้อน หลากหลาย สามารถนำไปต่อยอดการเข้ารหัสแบบอื่น ๆ ได้ เป็น algorithm พื้นฐานในการเข้ารหัสที่มีความปลอดภัยสูง และสามารถมาเพิ่มความปลอดภัยให้กับข้อมูลเราได้ อีกทั้งอาจจะนำไปประยุกต์กับโปรแกรมอื่น ๆ ที่เราใช้งานในปัจจุบัน เพื่อป้องกันข้อมูลส่วนตัวของเราได้

## สารบัญ

|  |    |
|--|----|
| บทที่ 1 .....                          | 5  |
| บทนำ .....                             | 5  |
| ที่มาและความสำคัญของโปรแกรม .....      | 5  |
| วัตถุประสงค์.....                      | 5  |
| ขอบเขตการศึกษา .....                   | 5  |
| ระยะเวลาในการศึกษา.....                | 5  |
| ผลที่คาดว่าจะได้รับ .....              | 5  |
| บทที่ 2 .....                          | 6  |
| ทฤษฎีที่เกี่ยวข้อง.....                | 6  |
| เครื่องมือที่ใช้ในการจัดทำ.....        | 6  |
| เอกสารที่เกี่ยวข้อง.....               | 6  |
| Flowchart อธิบายโปรแกรม .....          | 7  |
| หลักการการเข้ารหัส .....               | 8  |
| หลักการเข้ารหัส (2) .....              | 8  |
| หลักการถอดรหัส .....                   | 10 |
| หน้าต่างของโปรแกรม .....               | 12 |
| วิธีใช้งานโปรแกรม .....                | 12 |
| ถ้าผู้ใช้เลือกการเข้ารหัสโดย Text..... | 13 |
| ถ้าผู้ใช้เลือกการเข้ารหัสโดย File..... | 16 |
| บทที่ 3 .....                          | 19 |
| สรุปผล .....                           | 19 |
| ผลที่ได้รับ .....                      | 19 |
| ข้อเสนอแนะ .....                       | 19 |

## บทที่ 1

### บทนำ

#### ที่มาและความสำคัญของโปรแกรม

ต้องการศึกษาเกี่ยวกับโครงสร้างของการเข้ารหัสและถอดรหัสของ AES ซึ่งมีความซับซ้อน มี algorithm ที่เป็นเอกลักษณ์ และสามารถนำไปประยุกต์สู่การเขียนโปรแกรมอื่น ๆ ในอนาคต อีกทั้งยังเพิ่มความปลอดภัยให้กับข้อมูลในปัจจุบันที่พึ่งพาระบบคอมพิวเตอร์มากขึ้นด้วย

#### วัตถุประสงค์

1. ต้องการศึกษาระบบการเข้ารหัสในปัจจุบัน
2. ฝึกการเขียนโปรแกรม ให้สามารถเขียนได้จริง
3. เพิ่มประสบการณ์การทำงานเป็นกลุ่ม

#### ขอบเขตการศึกษา

ศึกษาเฉพาะการเข้ารหัสแบบ AES เท่านั้น โดยใช้การเขียนโปรแกรมด้วยภาษา C เพียงอย่างเดียวในการประยุกต์การเขียนโปรแกรม

#### ระยะเวลาในการศึกษา

26 มีนาคม 2559 – 16 เมษายน 2559 ในภาคเรียนที่ 2 ปีการศึกษา 2558

#### ผลที่คาดว่าจะได้รับ

1. ฝึกการเขียนโปรแกรมด้วยภาษา C จนเป็นผลสำเร็จ
2. มีความสามัคคีภายในกลุ่ม
3. รู้จักการแบ่งหน้าที่
4. รู้จักการเข้ารหัสด้วย AES
5. นำความรู้ไปต่อยอดได้ในอนาคต

## บทที่ 2

### ทฤษฎีที่เกี่ยวข้อง

#### เครื่องมือที่ใช้ในการจัดทำ

1. Code :: blocks 16.01
2. Sublime Text 3
3. Dev-C++
4. Atom

#### เอกสารที่เกี่ยวข้อง

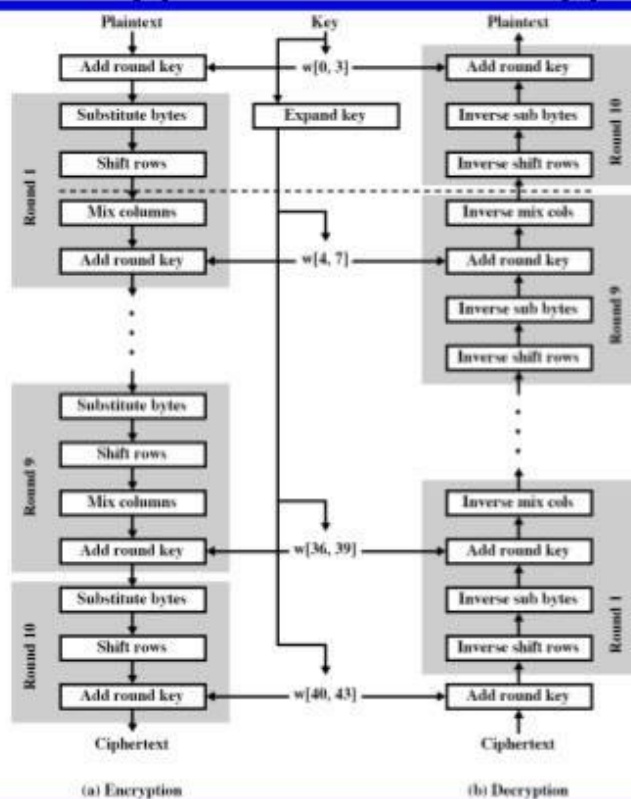
1. <https://books.google.co.th/books?isbn=6169022426>
2. [http://www.tnetsecurity.com/content\\_attack/crypt\\_basicknowledge.php](http://www.tnetsecurity.com/content_attack/crypt_basicknowledge.php)
3. [http://www.cp.eng.chula.ac.th/~piak/thesis/supachai\\_complete\\_thesis2.pdf](http://www.cp.eng.chula.ac.th/~piak/thesis/supachai_complete_thesis2.pdf)
4. <https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf>
5. <http://www.cs.columbia.edu/~sedwards/classes/2008/4840/reports/AES.pdf>
6. [http://www.infosecwriters.com/text\\_resources/pdf/AESbyExample.pdf](http://www.infosecwriters.com/text_resources/pdf/AESbyExample.pdf)
7. <http://www.kaagaard.dk/service/convert.htm>
8. <http://aesencryption.net/>

#### พื้นที่เก็บข้อมูล

<https://github.com/GunTH13/AES-Project-CP58->

Flowchart อธิบายโปรแกรม

## AES Encryption & Decryption



การเข้ารหัสแบบ AES จะประกอบไปด้วยการรับ Input แบบข้อความ 128 บิต และคีย์ที่จะใช้ในการเข้ารหัส

ขนาด 128 192 หรือ 256 บิต

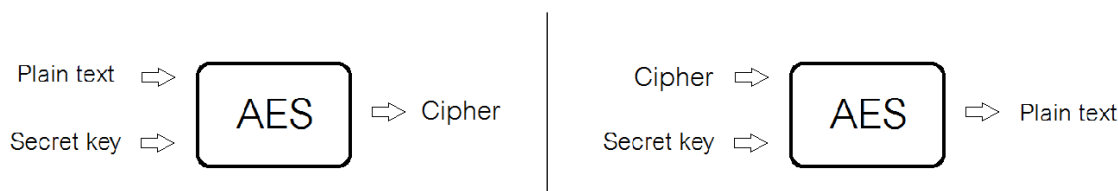


## หลักการเข้ารหัส

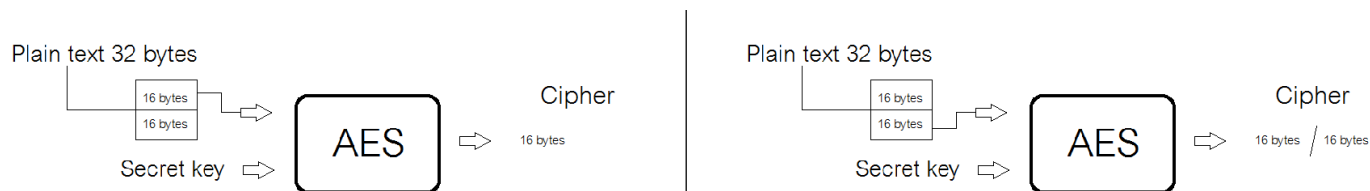
ในการเข้ารหัสนั้นมีความซับซ้อนในกระบวนการเปลี่ยนค่า ascii ของตัวอักษรเพื่อที่จะใช้อัลกอริทึมในการเข้ารหัส ปรับค่าให้ค่าตัวอักษรเปลี่ยนไปจากเดิมในส่วนของ algorithm มีความหลากหลายไม่แน่นอนขึ้นอยู่กับตัวเลือกที่จะใช้ โดยต้องคำนึงถึงค่าที่รับเข้ามาและออกไป

## หลักการเข้ารหัส (2)

การเข้ารหัส AES หรือที่รู้จักกันในชื่อ Rijndael เป็นหลักการเข้ารหัสแบบสมมาตร (Symmetric key algorithms) อัลกอริทึมนี้จะมี รหัสลับ (Secret key) เพื่อใช้เข้ารหัสและถอดรหัส โดยการเข้ารหัส AES ที่จะกล่าวถึงต่อไปนี้จะเป็นการเข้ารหัสโดยใช้ key ที่มีขนาด 128 bit



โปรแกรมจะดึงข้อความที่ผู้ใช้ใส่เข้าไปทีละ 16 bytes และออกมาทีละ 16 bytes



## ในอัลกอริทึม AES จะมีขั้นตอนดังนี้

1. นำข้อความที่รับเข้ามา มาทำการ Add round key ก่อน 1 รอบ
2. นำผลลัพธ์ที่ได้จากข้อ 1. ไปทำการ วนลูปขั้นตอนต่อไปนี้ 10 รอบ (key 192 bit 12 รอบ, 256 bit 14 รอบ)

- SubBytes

เป็นการดึงข้อมูลมาทีละ byte แล้วมาเทียบกับตำแหน่งในตาราง s-box (s-box เป็นข้อมูลที่ถูกระบุมาแล้ว) แล้วนำข้อมูลใน s-box มาแทนที่ เช่น Byte ที่ดึงมาคือ '19' (เป็นข้อความที่แปลงเป็นเลขฐาน 16 แล้ว) ให้นำไปเทียบในตาราง s-box ตำแหน่งที่ 1, 9 แล้วนำข้อมูลในช่อง 1, 9 ซึ่งก็คือ d4 มาแทนที่ 19 ไปเลย

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

(S-Box)

- Shift Rows

ข้อมูล 16 bytes ที่ดึงมาจะเรียงเป็น matrix 4x4 ในขั้นตอนนี้จะทำการเลื่อนตำแหน่งของ matrix ในแถวที่ 2 ไป ทางซ้าย 1 ครั้ง, แถวที่ 3 เลื่อนไปทางซ้าย 2 ครั้ง, แถวที่ 4 เลื่อนไปทางซ้าย 3 ครั้ง ส่วนแถวแรกนั้นไม่มีการเลื่อน

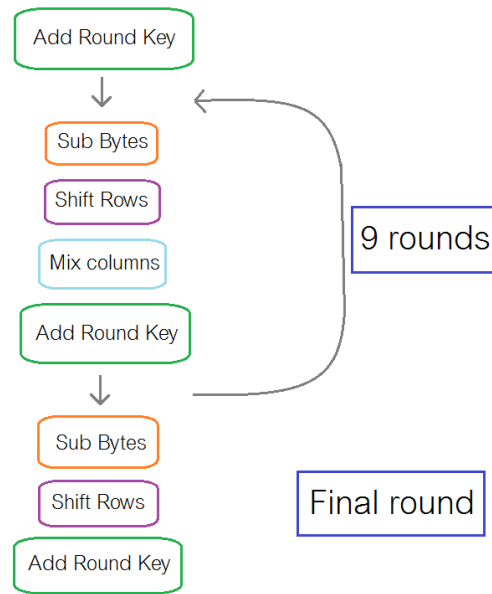
- Mix Columns (ยกเว้นรอบสุดท้าย [รอบที่ 10] จะไม่มีขั้นตอนนี้)

นำ column แต่ละ column มาคูณกับ matrix ----- >

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

- Add round key

นำ column แต่ละ column มา XOR กับ Key



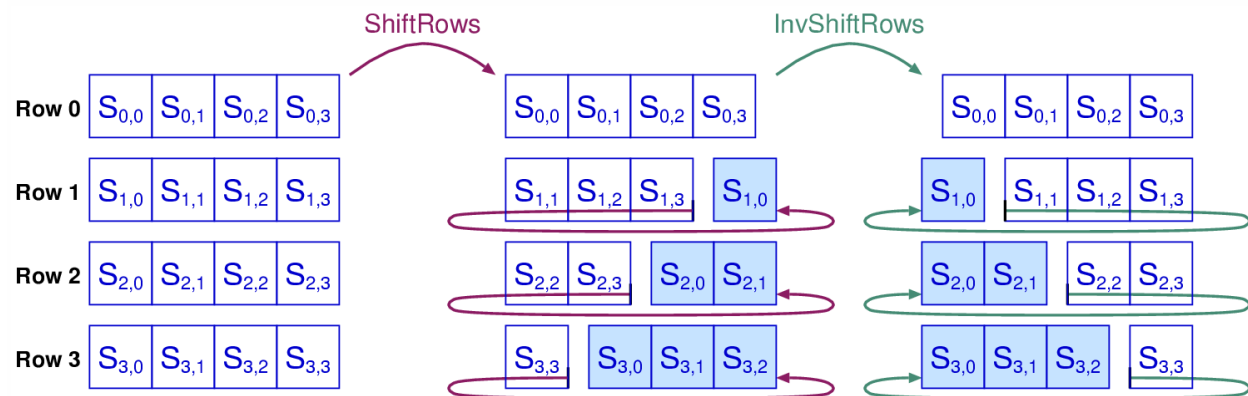
### หลักการถอดรหัส

ลักษณะขั้นตอนการทำงานคล้ายกับการเข้ารหัส โดยมีขั้นตอนการทำงานคือ

Inverse Shift rows > inverse sub byte > Add round Key > inverse mix column

ความแตกต่างระหว่าง inverse shiftrow กับ shiftrow คือ

shift row เลื่อนซ้าย inv เลื่อนขวา



ความแตกต่างระหว่าง inverse sub byte กับ sub byte คือ

sub byte เรียกจาก s box inv เรียก inv s box

|   |   | y  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|   |   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | a  | b  | c  | d  | e  | f  |
| x | 0 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
|   | 1 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
|   | 2 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
|   | 3 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
|   | 4 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
|   | 5 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
|   | 6 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
|   | 7 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
|   | 8 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
|   | 9 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
|   | a | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
|   | b | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
|   | c | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
|   | d | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
|   | e | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
|   | f | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

ความแตกต่างระหว่าง add round key ใน encrypt และ decrypt คือ

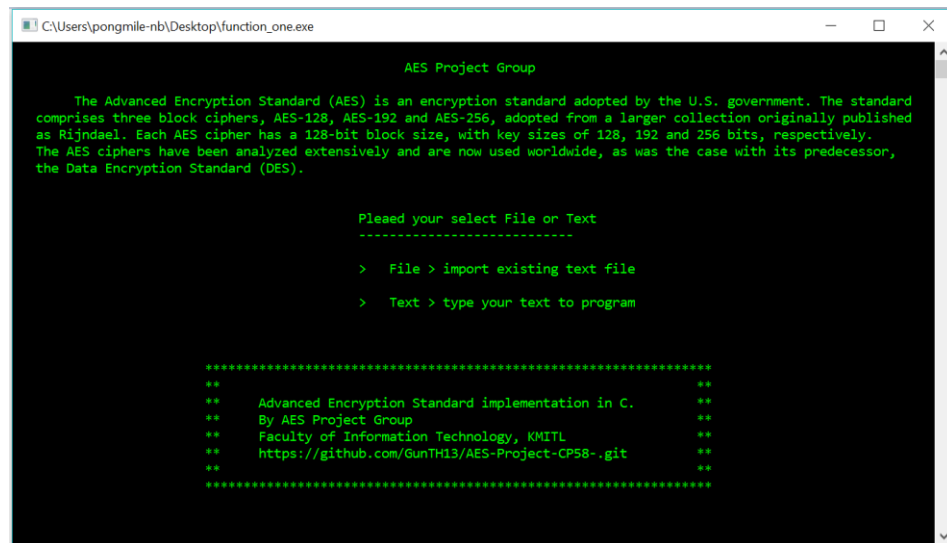
ใน encrypt เริ่มใช้จากชุดที่ 0-10 decrypt ใช้ 10-0

ความแตกต่างระหว่าง inverse mix column กับ mix column คือ

matrix ที่ใช้ในการ xor ของ inv mix column คือ inverse ของ matrix ที่ใช้ในขั้นตอน mix column

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

## หน้าตาของโปรแกรม



```
C:\Users\pongml-nb\Desktop\function_one.exe

AES Project Group

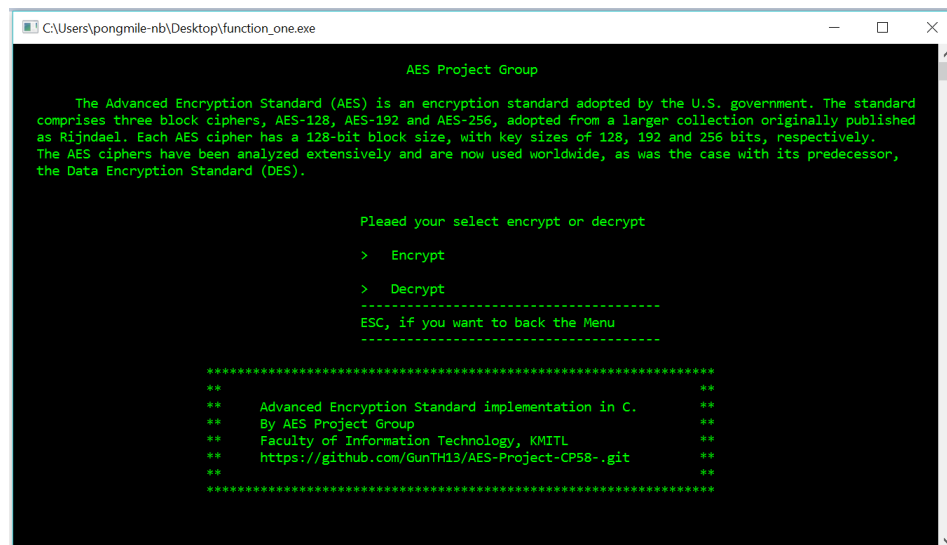
The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard
comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published
as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor,
the Data Encryption Standard (DES).

Pleaed your select File or Text
-----
> File > import existing text file
> Text > type your text to program

*****
** Advanced Encryption Standard implementation in C. **
** By AES Project Group **
** Faculty of Information Technology, KMITL **
** https://github.com/GunTH13/AES-Project-CP58-.git **
*****
```

## วิธีใช้งานโปรแกรม

1. โปรแกรมจะแบ่งออกเป็น 2 เมนูหลักๆ ได้แก่เมนู File และเมนู Text โดยผู้ใช้งานสามารถเข้ารหัสได้ทั้งไฟล์ที่มีข้อความอยู่ด้านในไฟล์ หรือนำข้อความมาใส่โดยตรงก็ย่อมได้



```
C:\Users\pongml-nb\Desktop\function_one.exe

AES Project Group

The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard
comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published
as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor,
the Data Encryption Standard (DES).

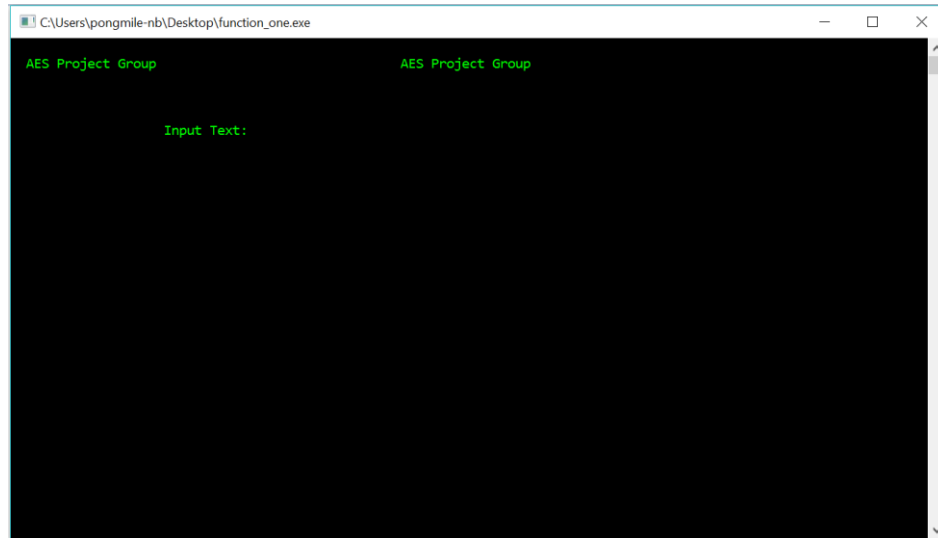
Pleaed your select encrypt or decrypt
-----
> Encrypt
> Decrypt
-----
ESC, if you want to back the Menu
-----

*****
** Advanced Encryption Standard implementation in C. **
** By AES Project Group **
** Faculty of Information Technology, KMITL **
** https://github.com/GunTH13/AES-Project-CP58-.git **
*****
```

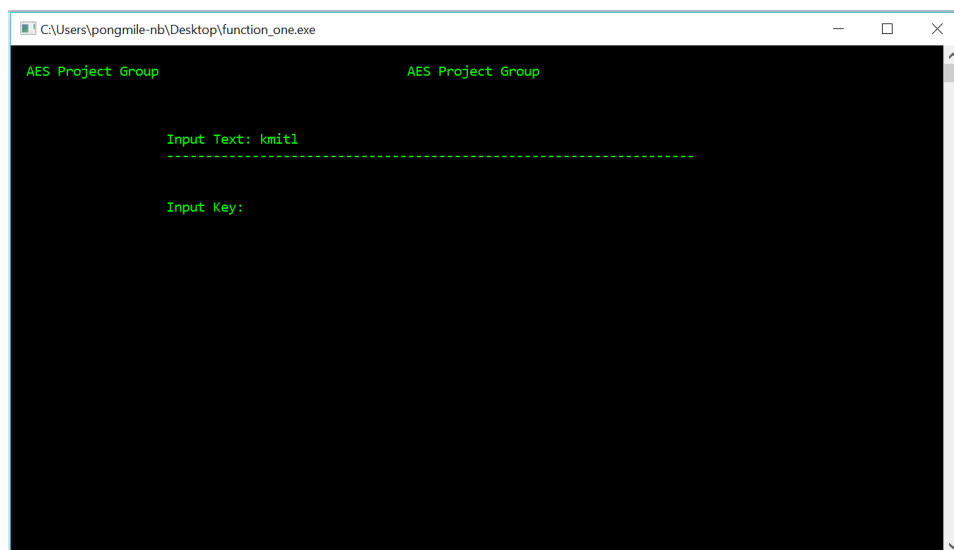
2. เมื่อผู้ใช้เลือกจากเมนูที่แล้ว ในหน้านี้ ผู้ใช้จำเป็นต้องเลือกระหว่างการ Encrypt ซึ่งคือการเข้ารหัส หรือเมนูที่ 2 คือ Decrypt ซึ่งคือการถอดรหัส ซึ่งผู้ใช้งานจำเป็นต้องการเข้ารหัสมาก่อนหน้านี้

ถ้าผู้ใช้เลือกการเข้ารหัสโดย Text

การเข้ารหัส



พิมพ์ข้อความที่ต้องการเข้ารหัส



พิมพ์ Key เพื่อเป็นกุญแจในการเข้ารหัส

```
C:\Users\pongmile-nb\Desktop\function_one.exe

AES Project Group                                AES Project Group

Input Text: kmitl
-----

Input Key: it
-----

This is you Encryption
*****
26 17 5f e8 02 c8 36 d1 da 22 8d 08 5f 2a 7c d3 EN
```

เมื่อทำการกรอกข้อความแล้ว key แล้ว ก็จะมีข้อความที่เข้ารหัสแสดงผลออกมา ซึ่งสามารถทำการคัดลอกได้  
โดยการลากข้อความที่ถอดรหัส แล้วกดปุ่ม Ctrl – C หรือคลิกขวาก็ได้เช่นกัน

## การถอดรหัส

```
function_one

AES Project Group

Enter the CipherText:
26 17 5f e8 02 c8 36 d1 da 22 8d 08 5f 2a 7c d3 EN
-----

Enter the Key:
```

ใส่ข้อความที่ถอดรหัสเข้าไปในช่อง Cipher Text

```
function_one
AES Project Group

Enter the CipherText:
26 17 5f e8 02 c8 36 d1 da 22 8d 08 5f 2a 7c d3 EN
-----

Enter the Key: it
```

ใส่ key ที่สัมพันธ์กับข้อความที่เข้ารหัสแล้ว

```
function_one
AES Project Group

Enter the CipherText:
26 17 5f e8 02 c8 36 d1 da 22 8d 08 5f 2a 7c d3 EN
-----

Enter the Key: it

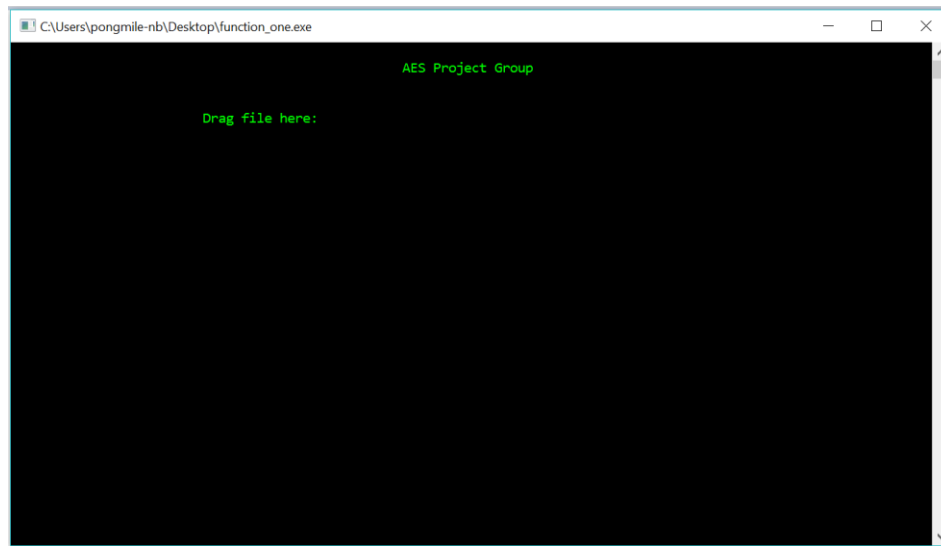
This is you Text: --> kmitl
```

ข้อความที่ถูกเข้ารหัสก็จะถูกถอดรหัสออกมาเป็นข้อความธรรมดา

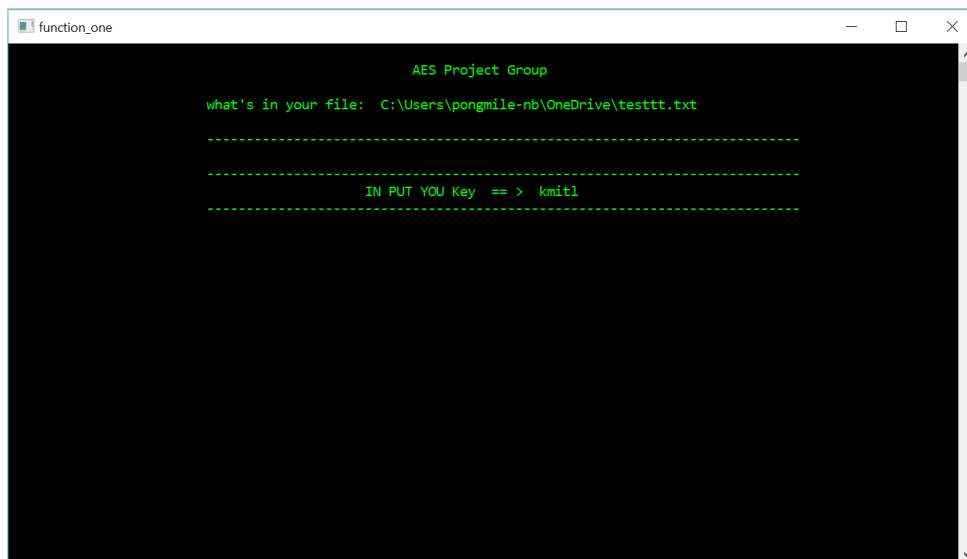


ถ้าผู้ใช้เลือกการเข้ารหัสโดย File

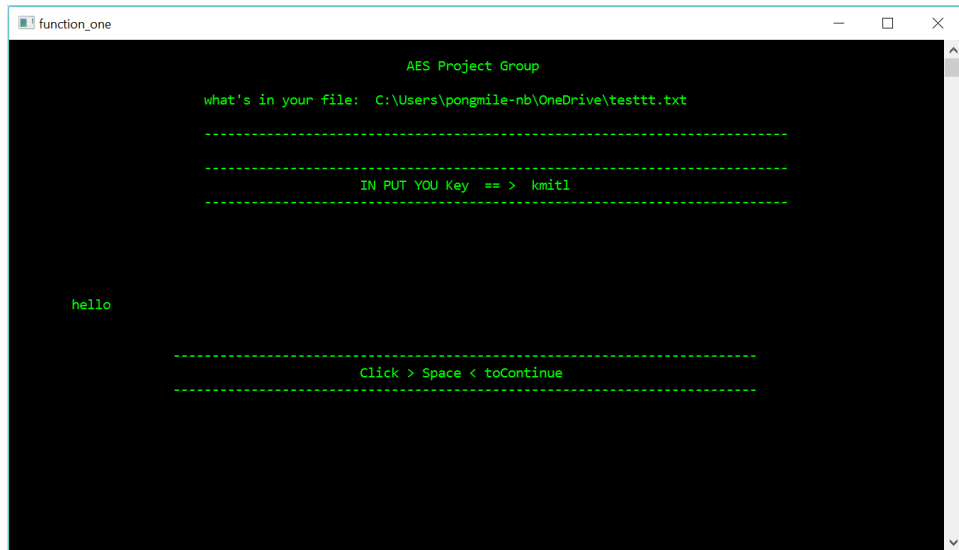
### การเข้ารหัส



ลากไฟล์เข้ามายังในตัวโปรแกรม ไฟล์ที่รองรับคือ .txt .int .bin .dat



จากนั้น ใส่ key ที่ต้องการเป็นกุญแจในการเข้ารหัส

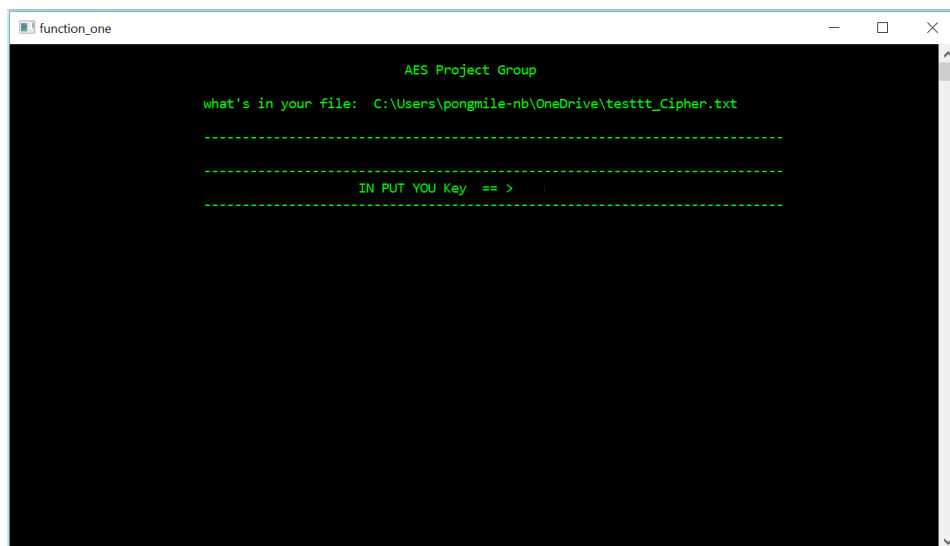


```
function_one
AES Project Group
what's in your file: C:\Users\pongmile-nb\OneDrive\testtt.txt
-----
IN PUT YOU Key == > kmit1
-----
hello
-----
Click > Space < toContinue
-----
```

จะได้ข้อความที่ได้รับการเข้ารหัสมาแล้ว

และตัวไฟล์ที่ได้รับการเข้ารหัสจะมีนามสกุลไฟล์ลงท้ายด้วย “\_Cipher”

## การถอดรหัส



```
function_one
AES Project Group
what's in your file: C:\Users\pongmile-nb\OneDrive\testtt_Cipher.txt
-----
IN PUT YOU Key == > kmit1
-----
-----
Click > Space < toContinue
-----
```

หากไฟล์ที่ถูกเข้ารหัสมา จะมีนามสกุลไฟล์ลงท้ายด้วย “\_Cipher”

```
function_one
AES Project Group

what's in your file: C:\Users\pongmile-nb\OneDrive\testtt_Cipher.txt
-----
IN PUT YOU Key == > kmitl
-----

de ab 38 18 b7 82 5a f9 29 2c e1 a0 e1 5f c9 c0 EN

-----
Click > Space < toContinue
-----
```

ใส่ key ที่เป็นกุญแจในการเข้ารหัสให้สัมพันธ์กับไฟล์ที่ต้องการถอดรหัส

```
function_one
AES Project Group

This is you Encryption
-----
ESC, if you want to back Main function
-----

hello
```

ข้อความใน File ที่ถูกเข้ารหัสจะแสดงขึ้นมา และจะมีไฟล์ที่ถูกถอดรหัสบันทึกอยู่ที่เดียวกันกับไฟล์ต้นฉบับ โดยจะมีชื่อไฟล์ต่อท้ายว่า “\_Cipher\_Des”

## บทที่ 3

### สรุปผล

#### ผลที่ได้รับ

1. ฝึกการค้นหารู้แบบการเข้ารหัสต่าง ๆ ของระบบคอมพิวเตอร์
2. สามารถอธิบายการเข้ารหัสแบบ AES ได้อย่างคร่าวๆ
3. ฝึกการเขียนภาษา C ให้สามารถประยุกต์นำมาเขียนเป็นโปรแกรมได้อย่างแท้จริง
4. สร้างความสามัคคี และเข้าใจกันในกลุ่มของตนเอง
5. มีทักษะในการแก้ปัญหาเฉพาะหน้า และการแก้ปัญหาที่ต้องใช้การทำงานเป็นกลุ่มมาร่วมด้วย
6. เพิ่มทักษะในการค้นคว้าหาข้อมูลเพื่อนำมาเขียนเป็นโปรแกรม และสืบค้นข้อมูลการเขียนโปรแกรมเพิ่มเติมได้ดียิ่งขึ้น
7. มีความรู้ในการเข้ารหัสข้อมูล เพื่อนำไปศึกษาต่อในอนาคตได้

#### ข้อเสนอแนะ

1. การเขียนค่อนข้างมีความซับซ้อน และมีความยากลำบากในการเขียนมากกว่าภาษาอื่นๆ เช่น Python เพียงมีฟังก์ชันที่สามารถใช้ได้น้อยกว่า เลยจำเป็นต้องเขียนให้ครอบคลุม จึงอาจจะใช้เวลาเขียนมากกว่า
2. การเข้ารหัสแบบ AES มีอัลกอริทึมที่หลากหลาย ทำให้ทางผู้จัดทำต้องใช้ระยะเวลาที่มากกว่า และจำเป็นต้องลองเขียนในรูปแบบต่าง ๆ ด้วย จึงทำให้พบความผิดพลาดในการเลือกใช้วิธีการคิดต่าง ๆ แต่สุดท้ายก็สามารถค้นหาวิธีคิดที่มีปัญหาและข้อผิดพลาดที่น้อยที่สุดได้
3. ในตอนแรก ทางทีมผู้จัดทำยังไม่มีแบ่งหน้าที่ที่ชัดเจน จึงทำให้ในตอนแรกมีความล่าช้า และมีความทับซ้อนในการเขียนโปรแกรม ในตอนหลังจึงมีการแบ่งงานทำงาน ทำให้มีประสิทธิภาพในการทำงาน และมีความรวดเร็วมากขึ้น