

รายงานโครงงาน

วิชา Computer Programming

เรื่อง Rijndael Encryption and Decryption

จัดทำโดย

พรพรหม เขียวจักร์ 59070113

ภาณุเดช สุนทรสุโขติ 59070130

รัตนจักร สุขสัมพันธ์ 59070147

วีรภัทร ทรัพย์สมบูรณ์ 59070162

อภิษฐา คำโพธิ์ 59070186

นำเสนอ

ผศ.ดร.กิตติ์สุชาติ พสุภา

ผศ.ดร.ปานวิทย์ ฐะนุติ

รายงานฉบับนี้เป็นส่วนหนึ่งของรายวิชา 06016206 COMPUTER PROGRAMMING

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง

หัวข้อโครงการ : Rijndael Encryption and Decryption

วิชา : COMPUTER PROGRAMMING 06016206

ผู้จัดทำ :

1. พรพรม เขียวจักร์	59070113
2. ภาณุเดช สุกนธสุขโชติ	59070130
3. รัตนันตร สุขสัมพันธ์	59070147
4. วีรภัทร ทรัพย์สมบูรณ์	59070162
5. อภิษฎา คำโพธิ์	59070186

ปีการศึกษา : พ.ศ. 2559

อาจารย์ที่ปรึกษา : ผศ.ดร.กิตติ์สุชาติ พสุภา

ผศ.ดร.ปานวิทย์ ฐะนุนติ

บทคัดย่อ

ในชีวิตประจำวัน ข้อมูลที่ส่งผ่านในโลก Internet จำเป็นต้องมีการเข้ารหัสเพื่อไม่ให้มีบุคคลที่สามารถเข้ามาล่วงรู้ข้อมูลที่สำคัญได้ เช่น รหัสผ่าน หรือ รหัสบัตรเครดิต เป็นต้น ซึ่งการเข้ารหัสช่วยปกป้องบทสนทนาของเราไม่ว่าจะเป็นวิดีโอเสียงหรือข้อความ ปกป้องความเป็นส่วนตัวของเรา ช่วยปกป้องนักข่าว ผู้พิทักษ์สิทธิมนุษยชน และนักเคลื่อนไหวทางการเมืองในประเทศเผด็จการได้อย่างง่ายดาย

ซึ่งคณะผู้จัดทำได้เล็งเห็นถึงความสำคัญของการเข้ารหัสข้อมูลเป็นอย่างดี คณะผู้จัดทำจึงเลือกการเข้ารหัส Rijndael (อ่านว่า Rhine-Dahl) ซึ่งเป็น Advanced Encryption Standard (AES) เป็นโครงงานในวิชา Computer Programming เพื่อความท้าทาย และเป็นการดึงเอาความรู้ และทักษะที่ได้เรียนรู้มาทั้งหมดมาประยุกต์ใช้ให้เกิดประโยชน์สูงสุด อีกทั้งโครงงานนี้อาจสามารถนำไปประยุกต์กับโปรแกรมอื่นๆได้อีกในอนาคต

สารบัญ

บทที่ 1.....	1
บทนำ.....	1
ที่มาและความสำคัญของโปรแกรม.....	1
วัตถุประสงค์.....	1
ขอบเขตการศึกษา.....	1
ผลที่คาดว่าจะได้รับ.....	1
บทที่ 2.....	2
ทฤษฎีที่เกี่ยวข้อง.....	2
เครื่องมือที่ใช้ในการจัดทำ.....	2
เอกสารที่เกี่ยวข้อง.....	2
พื้นที่เก็บข้อมูล.....	2
กระบวนการเข้ารหัสแบบ Rijndael 128-bit.....	3
AddRoundKey.....	4
SubBytes.....	4
ShiftRows.....	5
MixColumns.....	6
กระบวนการถอดรหัส.....	6
InvShiftRows.....	8
InvMixColumns.....	9
การใช้งานโปรแกรม.....	9
เข้ารหัส-ถอดรหัส File.....	13
การเข้ารหัส.....	13
การถอดรหัส.....	14
เข้ารหัส-ถอดรหัส Text.....	16
การเข้ารหัส.....	16
ถอดรหัส.....	17
บทที่ 3.....	18
สรุปผล.....	18
ผลที่ได้รับ.....	18
ข้อเสนอแนะ.....	18

บทที่ 1

บทนำ

ที่มาและความสำคัญของโปรแกรม

เพื่อการศึกษากระบวนการเข้ารหัสข้อมูลมีมาตรฐานและความนิยมสูงในปัจจุบันอย่าง Advanced Encryption Standard นำมาประยุกต์สร้างโปรแกรมที่สามารถเข้ารหัสได้ทุกอย่าง ตัวอย่างเช่น ข้อความ รูปภาพ เสียง หรือแม้แต่วิดีโอ เพื่อความเป็นส่วนตัวในโลกออนไลน์ ไม่ให้ผู้ไม่หวังดีล่วงรู้ความลับของเราได้

วัตถุประสงค์

1. ศึกษาการเข้ารหัสแบบ Rijndael 128-bit
2. พัฒนาทักษะในการเขียนโปรแกรมในภาษา C
3. ฝึกฝนการพัฒนาซอฟต์แวร์โดยใช้หลักการ System development Life Cycle (SDLC)

ขอบเขตการศึกษา

ศึกษาการเข้ารหัสแบบ Rijndael 128-bit โดยอ่านข้อมูลแบบ Binary และใช้ภาษา C ในการเขียนโปรแกรม

ระยะเวลาในการศึกษา

6 มีนาคม 2560 – 6 เมษายน 2560 ในภาคเรียนที่ 2 ปีการศึกษา 2560

ผลที่คาดว่าจะได้รับ

1. ฝึกการเขียนโปรแกรมด้วยภาษา C จนเป็นผลสำเร็จ
2. มีความสามัคคีภายในกลุ่ม
3. รู้จักการแบ่งหน้าที่
4. รู้จักการเข้ารหัสแบบ Rijndael 128-bit
5. นำความรู้ไปต่อยอดได้ในอนาคต

บทที่ 2

ทฤษฎีที่เกี่ยวข้อง

เครื่องมือที่ใช้ในการจัดทำ

1. Sublime
2. Electron frameworks
3. Apple Base64 Opensource Library
4. Jet Brains IDE
5. Electron API

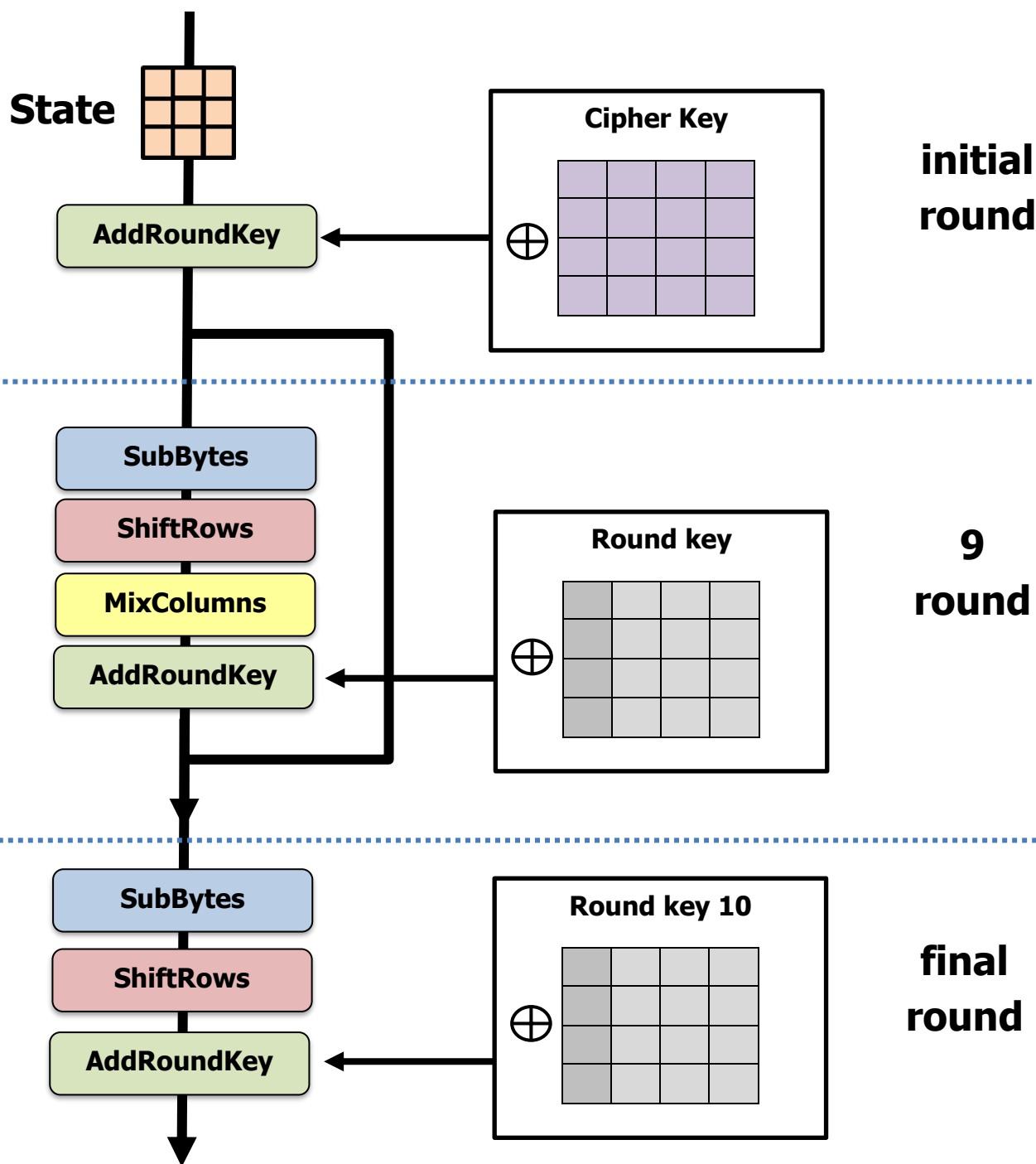
เอกสารที่เกี่ยวข้อง

1. https://www.cp.eng.chula.ac.th/~piak/thesis/supachai_complete_thesis2.pdf
2. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
3. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
4. <http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>
5. https://www.cp.eng.chula.ac.th/~piak/thesis/supachai_complete_thesis2.pdf

พื้นที่เก็บข้อมูล

<https://github.com/XIIKJII/CP59-RijndaelEncryption>

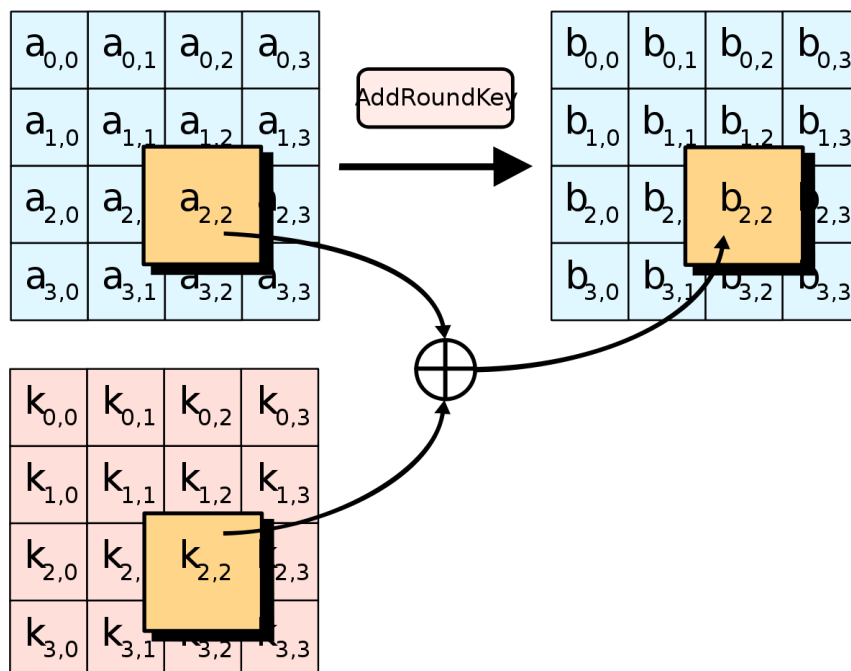
กระบวนการเข้ารหัสแบบ Rijndael



การเข้ารหัสแบบ Rijndael มีกระบวนการสำคัญ 4 อย่างได้แก่ AddRoundKey, SubBytes, ShiftRows, MixColumns โดยการเข้ารหัสจะแบ่งเป็น 3 ช่วง คือ ช่วงเริ่มต้น ช่วงวนรอบซ้ำ และช่วงสุดท้าย โดยช่วงที่วนรอบซ้ำ จำนวนรอบขึ้นอยู่กับขนาดของกุญแจ 128-bit วน 10 รอบ 192-bit วน 12 รอบ 256-bit วน 14 รอบ

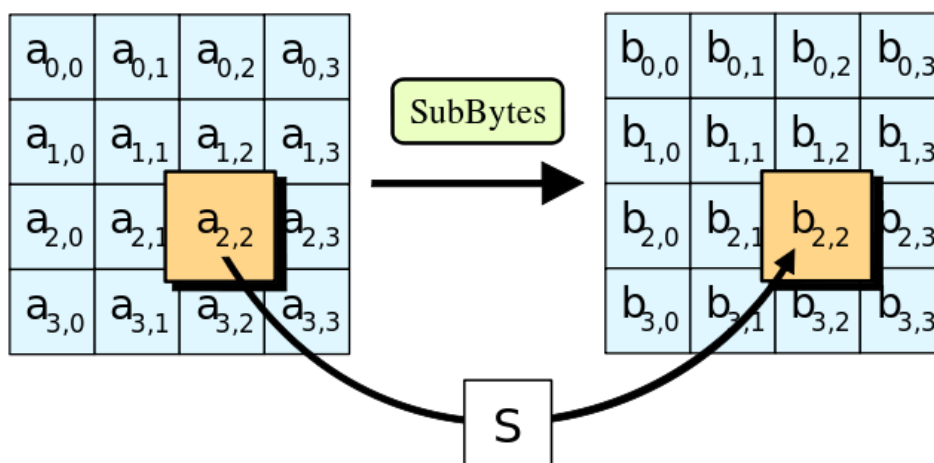
AddRoundKey

เป็นกระบวนการนำชุดข้อมูล XOR กับ RoundKey ที่ได้สร้าง มาก่อนหน้านี้



SubBytes

การแทนค่าแต่ละไบต์ข้อมูลด้วยตารางแทนค่า หรือ S-box

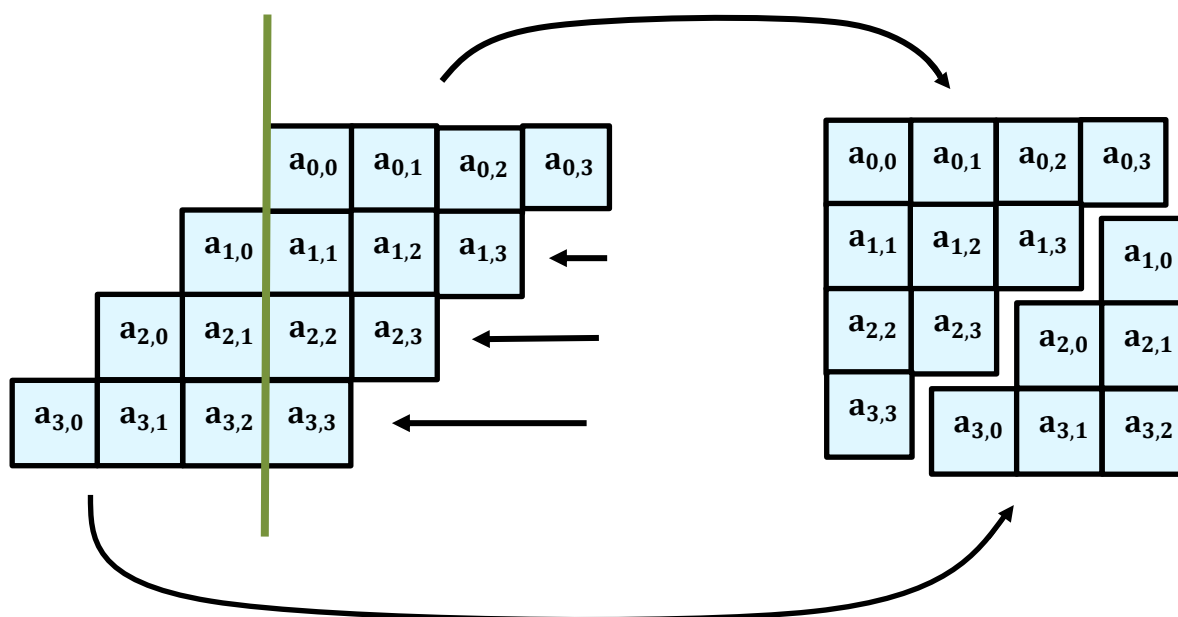


S-box

	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

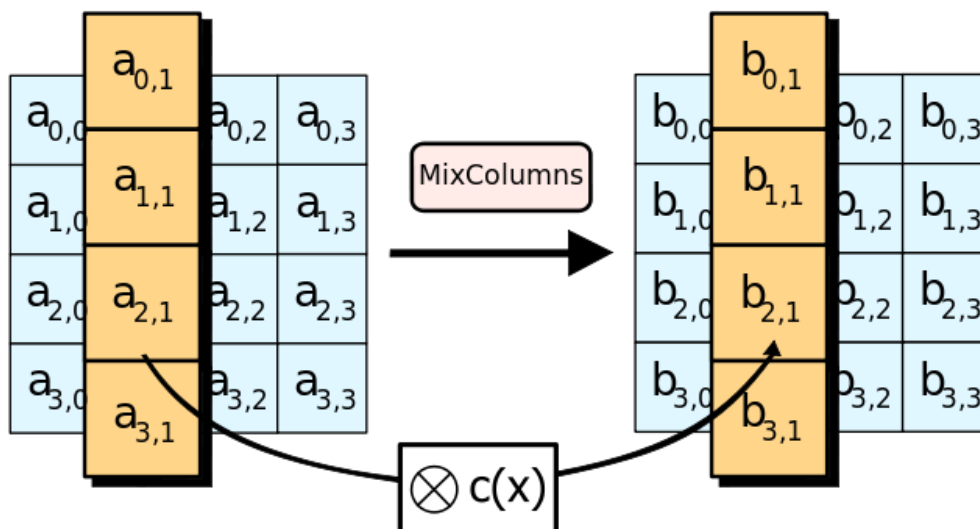
ShiftRows

เลื่อนไบต์ของข้อมูล 3 แถวล่างไปทางซ้าย โดยแถวที่ 2 เลื่อน 1 ตำแหน่ง แถวที่ 3 เลื่อน 2 ตำแหน่ง และแถวที่ 4 เลื่อน 3 ตำแหน่ง ส่วนไบต์ที่เกินออกไปทางด้านซ้ายจะถูกนำกลับมาต่อทางด้านขวาของแถวตามลำดับ



MixColumns

การนำชุดข้อมูลไปคูณกับ Matrix ค่าคงที่

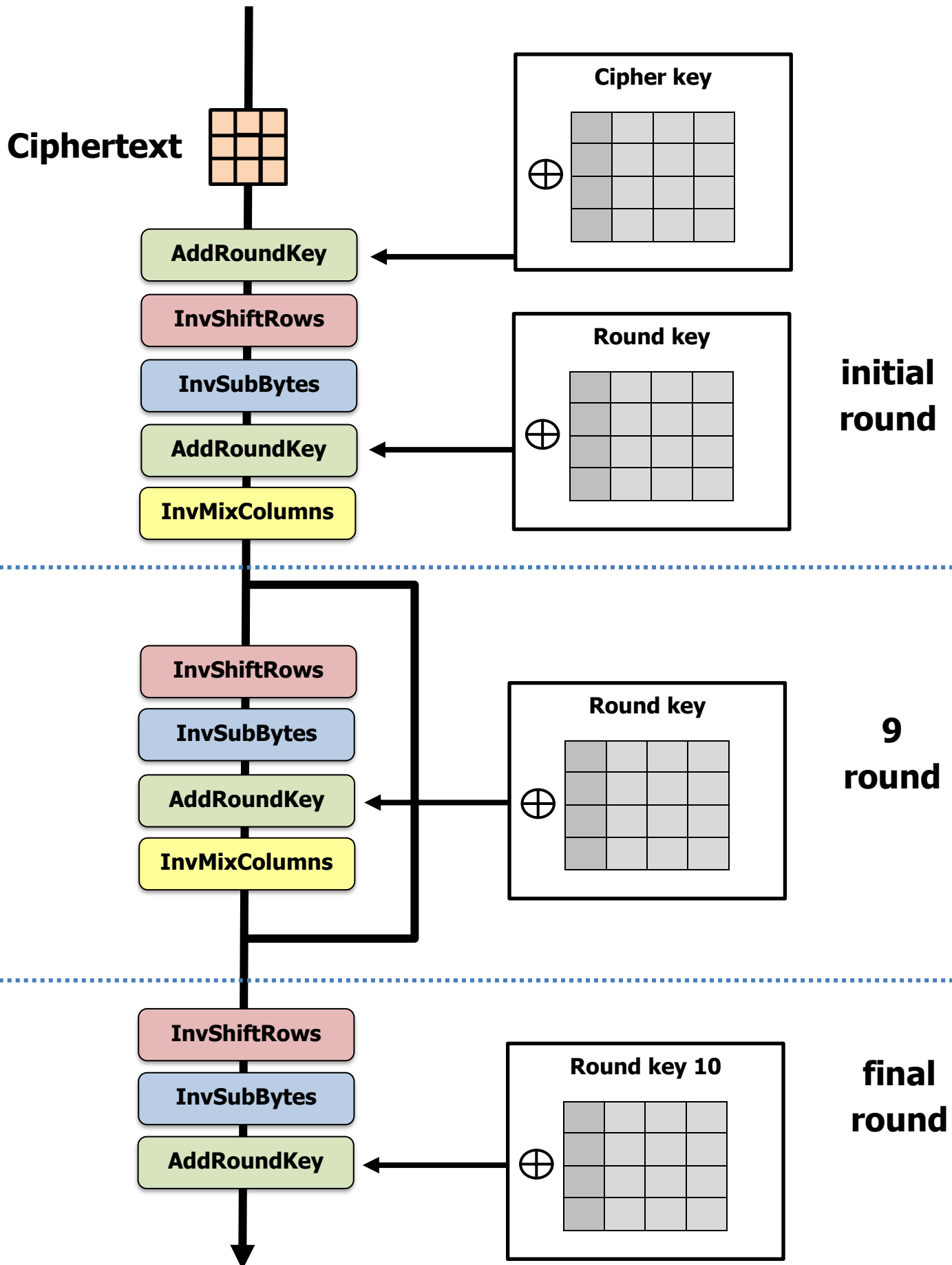


$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Matrix ค่าคงที่

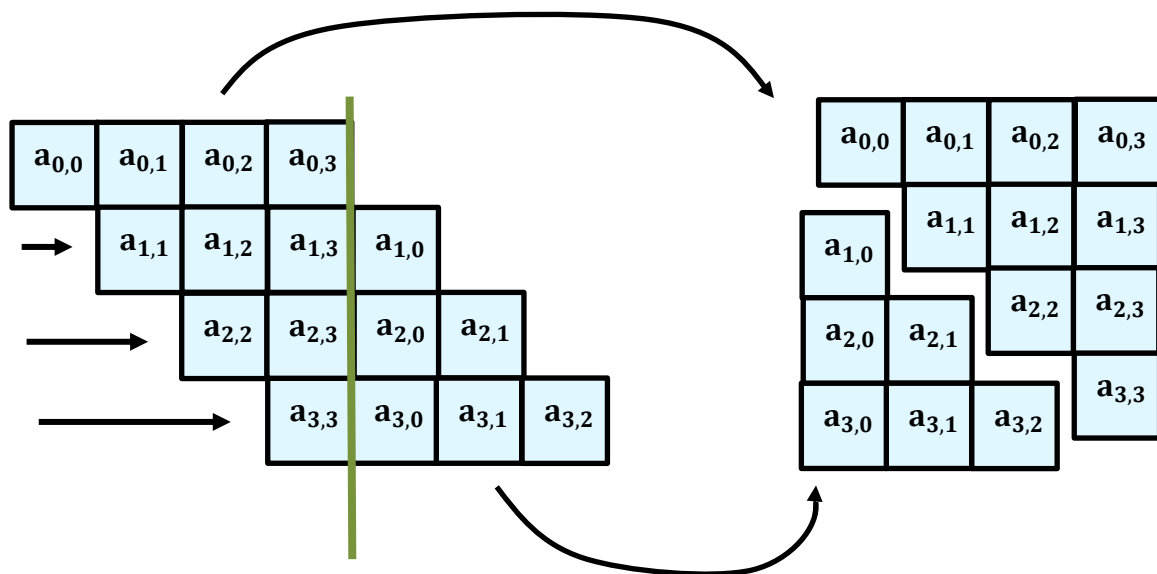
กระบวนการถอดรหัส

คล้ายขั้นตอนการเข้ารหัส เป็นกระบวนการทำย้อนกลับ กระบวนการที่เพิ่มขึ้นมา ได้แก่ InvSubBytes
InvShiftRows และ InvMixColumn



InvShiftRows

คล้ายกับการทำ ShiftRows แต่จะเป็นการเลื่อนขวา



InvSubBytes

คล้ายกับการทำ SubBytes แต่จะเปลี่ยนจากการใช้ตาราง S-box เป็นตาราง Inverse 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

InvMixColumns

คล้ายกับการทำ MixColumns แต่ Maxtrix ค่าคงที่ที่ใช้จะเป็น Inverse ของ Matrix ค่าคงที่นั้น

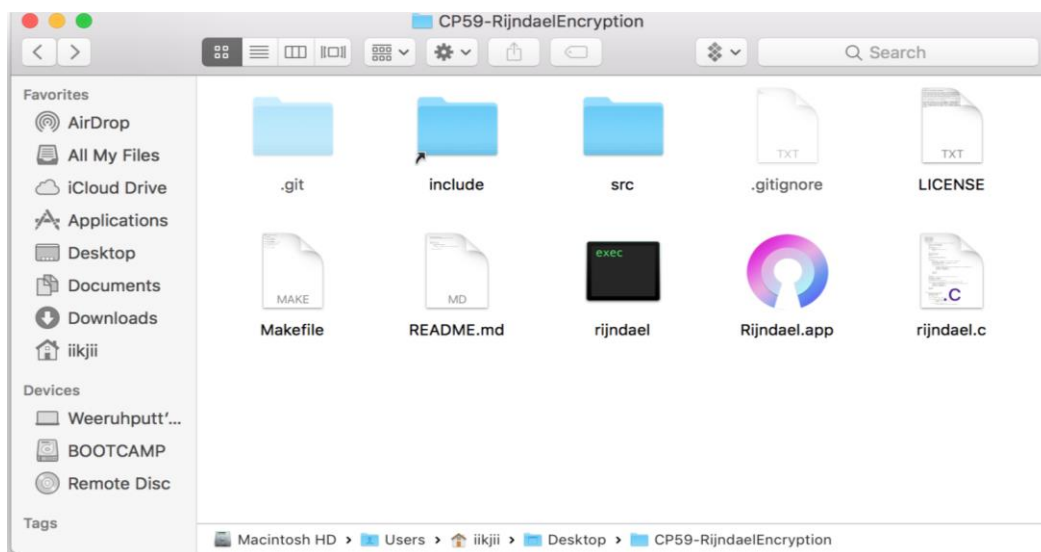
$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Inverse ของ Matrix ค่าคงที่

การใช้งานโปรแกรม

วิธีการใช้งานผ่าน Command Line Interface (ใช้ได้แค่บน MacOS เท่านั้น)

1. เข้าไปที่ Directory ของ Project ชื่อ CP59-RijndaelEncryption



2. เรียกตัว Executable ผ่าน CLI เพื่อดูคู่มือการใช้งาน

```
./rijndael
```

```
~/Desktop/CP59-RijndaelEncryption > master > ./rijndael
Usage (Text Mode): ./rijndael -m [plaintext|base64Encrypted Message] -p [password] [--encrypt|--decrypt]
For special character use \ before. Ex. space use '\ '.
Usage (File Mode): ./rijndael -f [/path/to/file] -p [password] [--encrypt|--decrypt]
The output encrypted file will be named [filename].[type].encrypted
REMARK: MAX length of PASSWORD is 16 characters.
```

โปรแกรมมีวิธีการเข้ารหัส-ถอดรหัส 2 แบบ

1. เข้ารหัส-ถอดรหัส File
2. เข้ารหัส-ถอดรหัส Text

เข้ารหัส-ถอดรหัส File

เข้ารหัส

```
./rijndael -f ไฟล์ที่ต้องการเข้ารหัส -p รหัสเพื่อการเข้ารหัส --encrypt
```

ไฟล์ที่เข้ารหัสแล้วจะมีนามสกุลต่อท้ายเป็น `.encrypted`

ถอดรหัส

```
./rijndael -f ไฟล์ที่ต้องการถอดรหัส -p รหัสเพื่อการถอดรหัส --decrypt
```

นำไฟล์ที่มีนามสกุล มาเพื่อการถอดรหัส `.encrypted`

เข้ารหัส-ถอดรหัส Text

เข้ารหัส

```
./rijndael -m ประโยคที่ต้องการเข้ารหัส -p รหัสลับ --encrypt
```

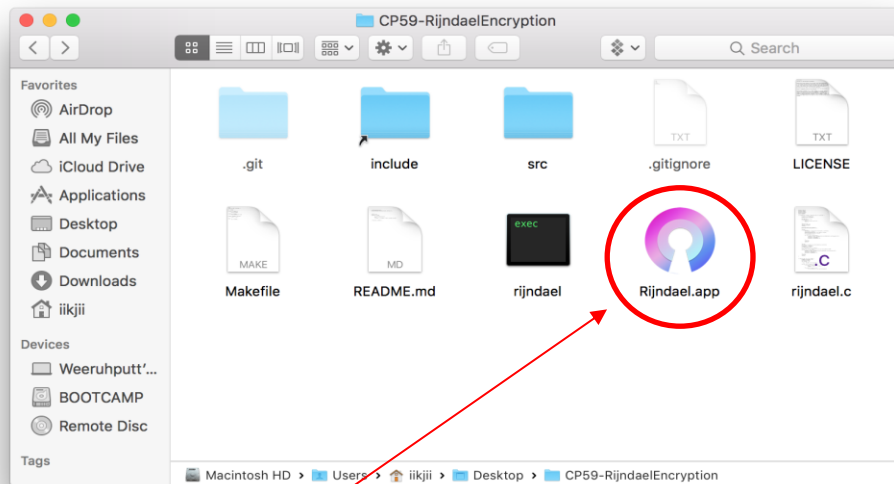
ประโยคที่เข้ารหัสแล้วจะอยู่ในรูปของ Base64

ถอดรหัส

```
./rijndael -m ประโยคที่อยู่ในรูปของ Base64 -p รหัสลับ --decrypt
```

วิธีการใช้งานผ่าน GUI (ใช้ได้แค่บน MacOS เท่านั้น)

1. เข้าไปที่ Directory ของ Project ชื่อ CP59-RijndaelEncryption

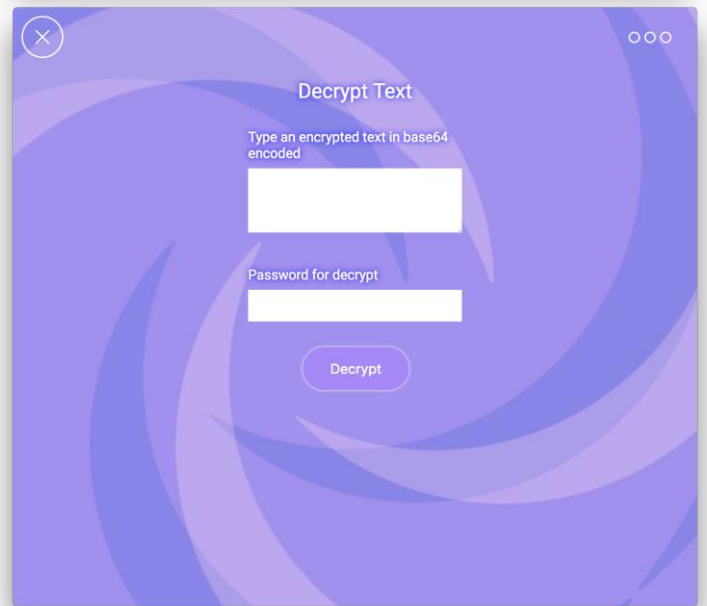
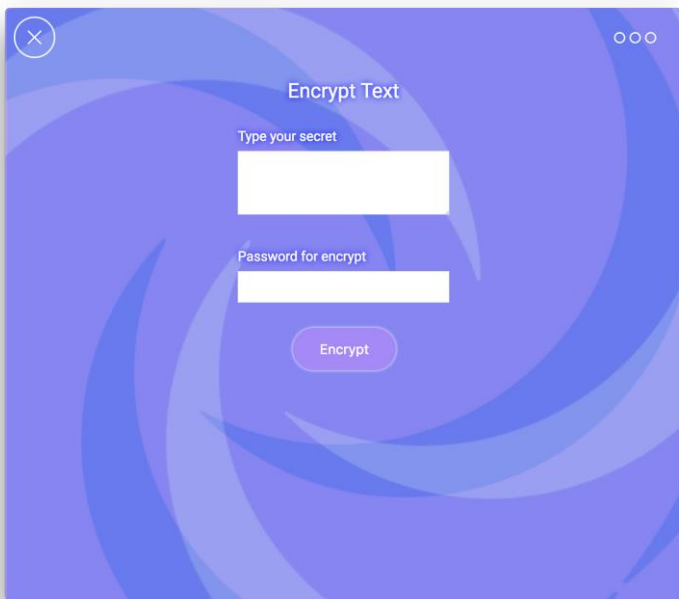
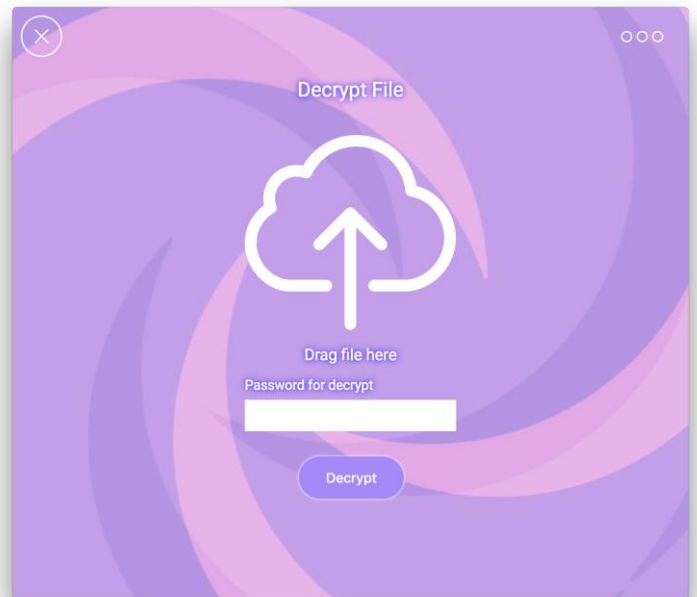
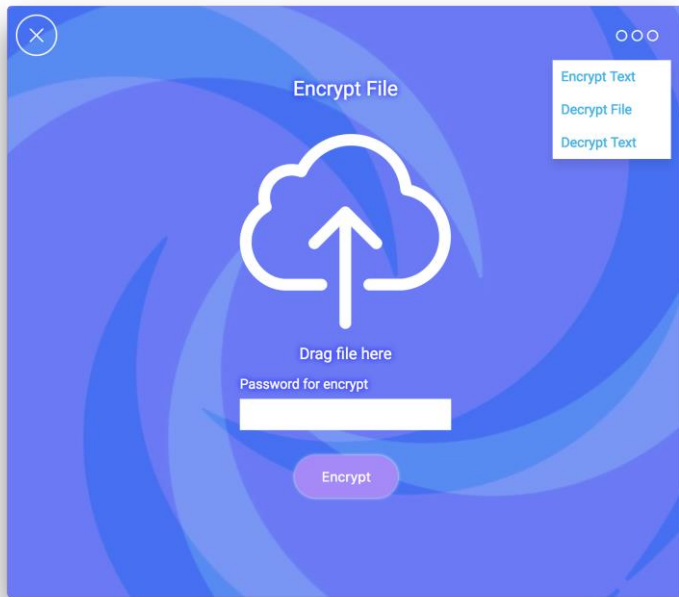


เรียกตัว Rijndael.app ขึ้นมาจะได้หน้าต่างดังรูปด้านล่าง



สามารถกดปุ่ม Start เพื่อเริ่มการใช้งานตัวโปรแกรม

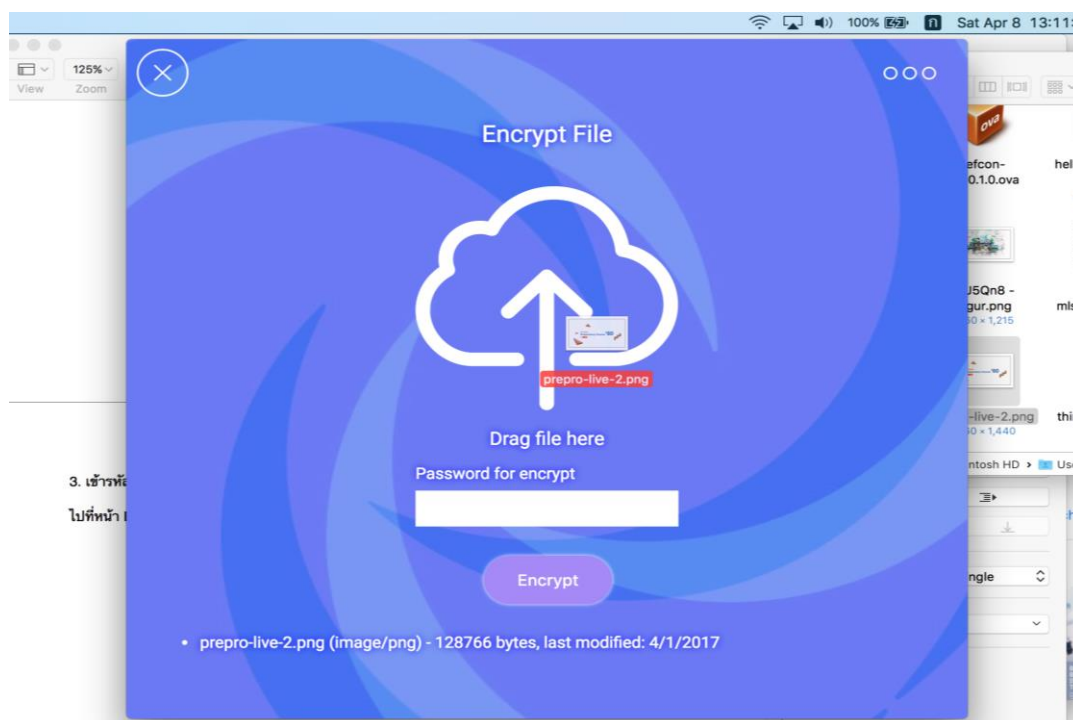
3. หลังจากกดปุ่ม Start ก็จะมาที่หน้าเข้ารหัสไฟล์ โดยที่มุมขวาบนเป็น Navigator Bar เพื่อนำไปหน้าต่างๆ



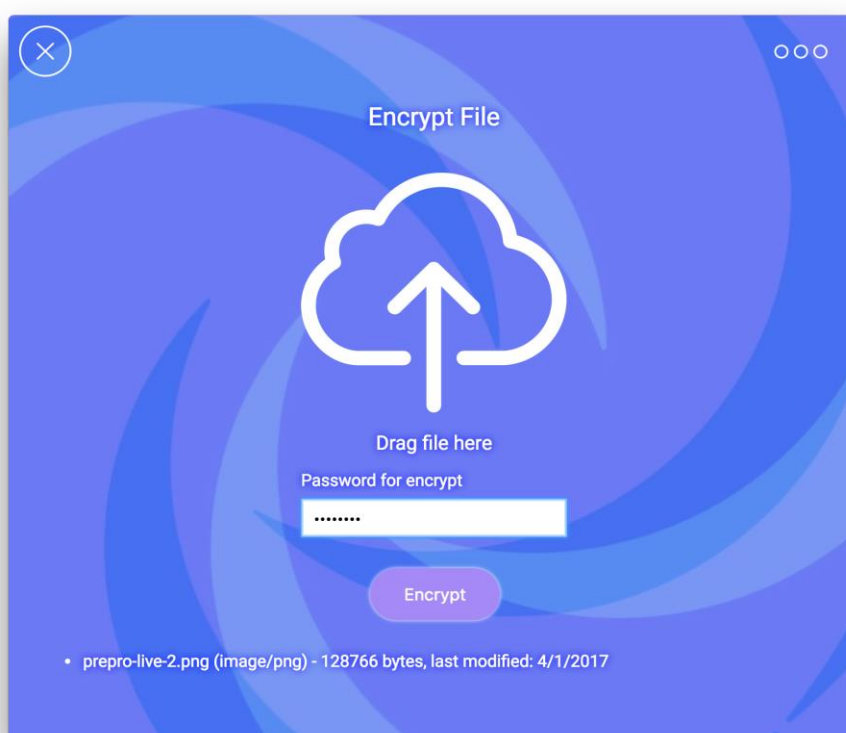
เข้ารหัส-ถอดรหัส File

การเข้ารหัส

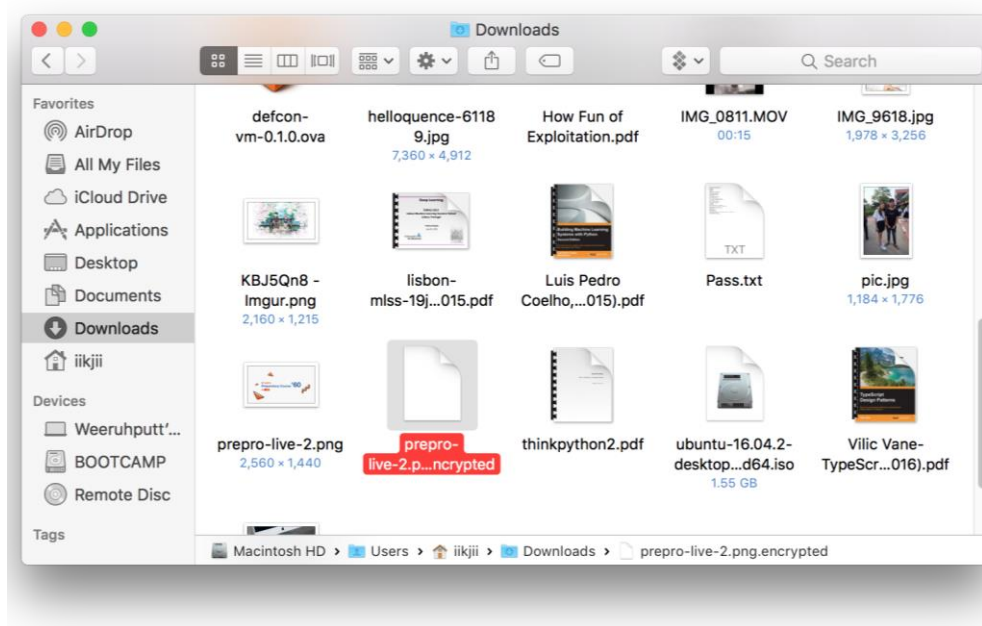
1. ไปที่หน้า Encrypt File พร้อมกับลากไฟล์ที่ต้องการเข้ารหัสมาปล่อยในโปรแกรม



2. ใส่รหัสผ่านที่ต้องการเข้ารหัส พร้อมกด Encrypt

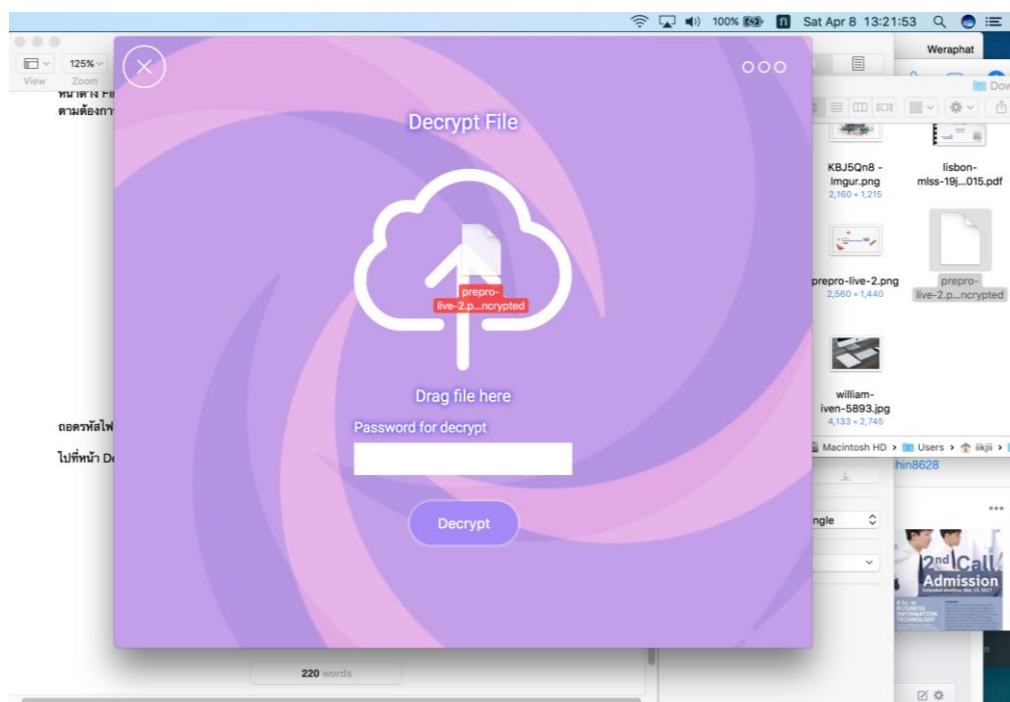


หน้าต่าง Finder จะตั้งขึ้นมาพร้อมกับแสดงให้เห็นถึงไฟล์ที่เข้ารหัสแล้ว สามารถนำไฟล์ที่เข้ารหัสแล้วไปใช้ได้ตามต้องการ

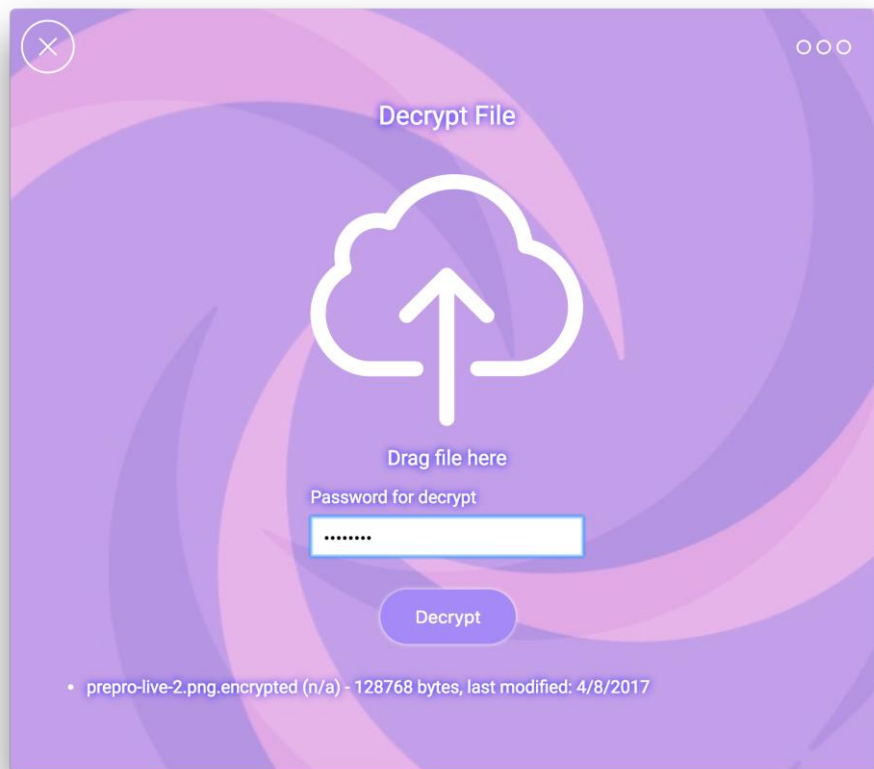


การถอดรหัส

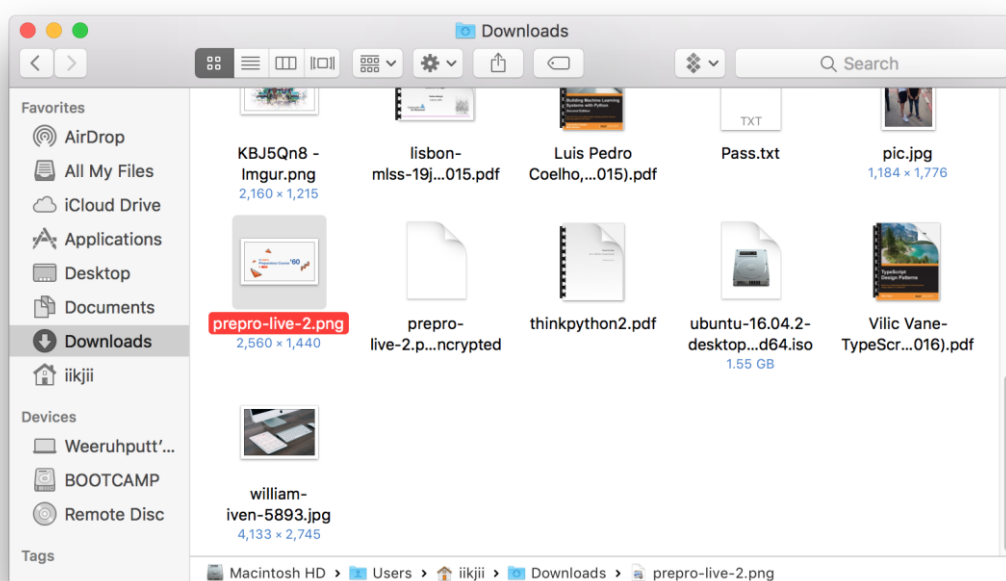
1. ไปที่หน้า Decrypt File พร้อมกับลากไฟล์ที่เข้ารหัสเข้ามาในตัวโปรแกรม



2. ใส่รหัสพร้อมกด Decrypt



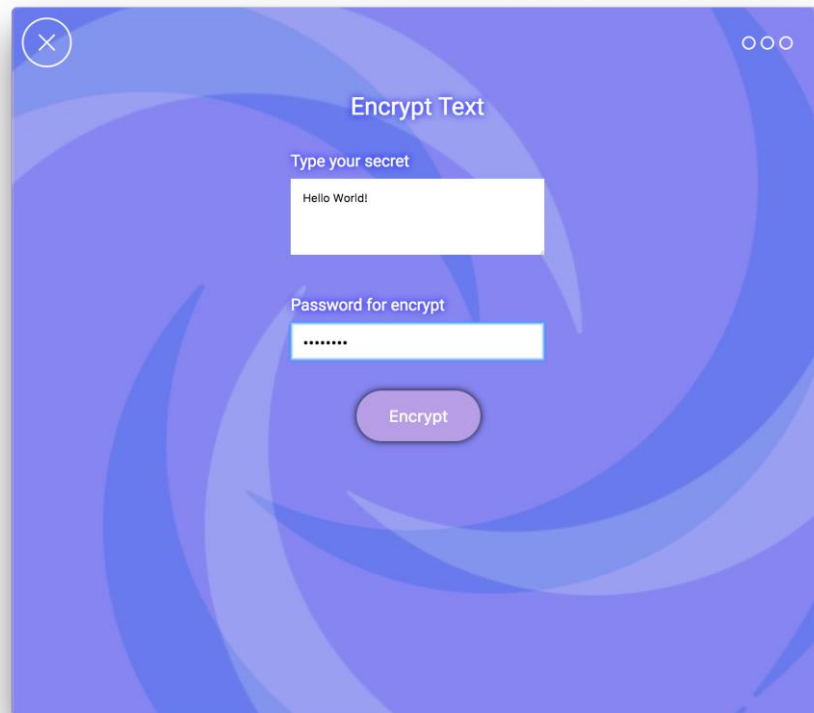
หน้าต่าง Finder จะตั้งขึ้นมาพร้อมกับแสดงให้เห็นถึงไฟล์ที่ถอดรหัสแล้ว



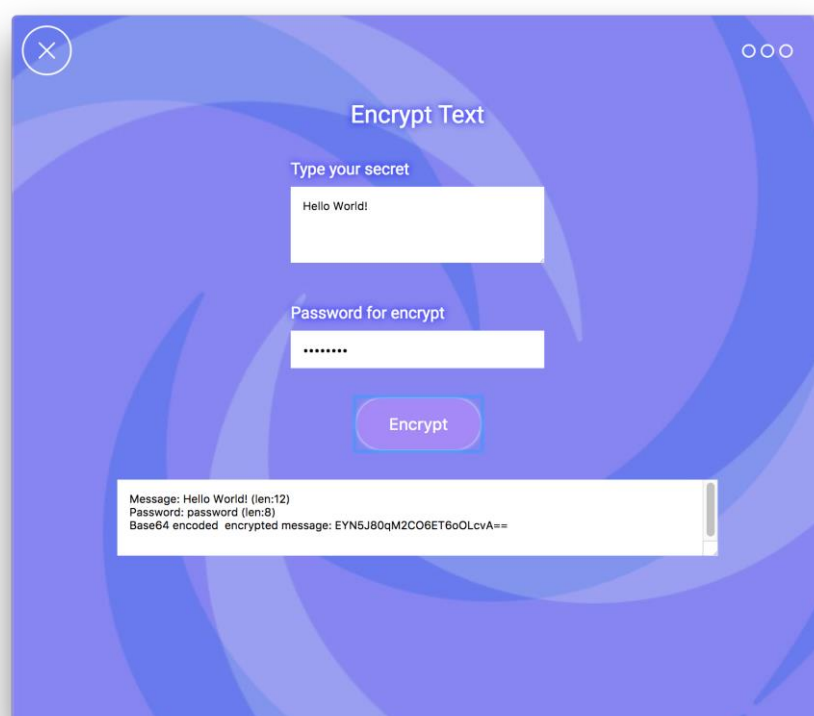
เข้ารหัส-ถอดรหัส Text

การเข้ารหัส

1. ไปที่หน้า Encrypt Text พร้อมใส่ text ที่ต้องการที่จะเข้ารหัสพร้อมทั้งใส่รหัสผ่าน จากนั้นกด Encrypt



เมื่อเข้ารหัสเสร็จจะได้ผลลัพธ์ออกมาดังรูป (ในที่นี้รหัสผ่านคือ password)



ซึ่งข้อความที่เข้ารหัสแล้วจะอยู่ในรูปของ Base64 encode (EYN5J80qM2CO6ET6oOLcvA==)

การถอดรหัส

1. ไปที่หน้า Decrypt Text พร้อมใส่ ข้อความที่เข้ารหัสในรูปของ Base64 พร้อมทั้งใส่รหัสผ่าน จากนั้นกด Decrypt

เมื่อกด Decrypt ก็จะได้ดังรูป

บทที่ 3

สรุปผล

ผลที่ได้รับ

- ได้โปรแกรมที่สามารถเข้ารหัสไฟล์ได้ทุกประเภทตอบสนองต่อความเป็นส่วนตัวของบุคคล
- การฝึกเขียนภาษา C ทำให้สามารถเขียนอัลกอริทึมใหม่ๆได้
- มีพื้นฐานในการเข้ารหัส นำไปประยุกต์ใช้กับการเข้ารหัสแบบอื่นๆได้
- พัฒนาทักษะในการค้นคว้าข้อมูลเพื่อนำมาปฏิบัติกับโครงการ
- พัฒนาทักษะในการแก้ปัญหาเฉพาะหน้าเมื่อทำงานเป็นกลุ่ม

ข้อเสนอแนะ

- การเข้ารหัสแบบ Rijndael นั้น ค่อนข้างซับซ้อน ต้องใช้เวลาทำความเข้าใจให้ดีก่อนจะทำการเขียนโค้ด
- ภาษา C เป็นภาษาที่เก่า มี syntax ที่ง่ายถึงปานกลางจะต้องระวังเรื่องเครื่องหมาย ; (semicolon)
- การถอดรหัสควรทำข้ามระบบปฏิบัติการได้ ถ้าเข้ารหัสในวินโดวส์ก็ต้องถอดในวินโดวส์เท่านั้น
- มีปัญหาเรื่องข้อจำกัดของระบบปฏิบัติการเพราะคณะผู้จัดทำมีการใช้ทั้งระบบปฏิบัติการวินโดวส์ และแมคโอเอส