



รายงาน

เว็บแอปพลิเคชันแจกจ่ายงานให้สายลับ

จัดทำโดย

นายเอกนรินทร์ เลิศนันทวัฒน์ 6110490023

นายชนกนันท์ ชูศักดิ์ศิลป์ 6110612998

นายสุธิชัย ชูแก้ว 6110613038

นายธีรรัช ประสิทธิ์เวช 6110613178

นายณัฐพร วิมลอนุพงษ์ 6110613319

นายธาม เขียวระวิบูลย์ 6110680565

เสนอ

ผศ.ดร.ปิยะ เตชะธีราวัฒน์

รายงานนี้เป็นส่วนหนึ่งของรายวิชา CN322 Network Security

ปีการศึกษา 2564 ภาคการศึกษาที่

## คำนำ

รายงานนี้เป็นส่วนหนึ่งของรายวิชา CN322 Network Security มีจุดประสงค์คือ เพื่อสร้างเว็บแอปพลิเคชันสำหรับแจกจ่ายงานให้สายลับ ตัวเว็บมีฟีเจอร์ที่ช่วยอำนวยความสะดวกให้กับหัวหน้าสายลับที่มีหน้าที่แจกจ่ายงาน และตัวสายลับที่มีหน้าที่รับงานมาทำ โดยมีการเข้ารหัสข้อมูลสำคัญเพื่อป้องกันการโจมตี และรักษาความปลอดภัยให้กับผู้ใช้

## สารบัญ

	หน้า
คำนำ	1
บทที่ 1 บทนำ	3
บทที่ 2 ขั้นตอนการพัฒนา	10
บทที่ 3 ผลการดำเนินงาน	13

## บทที่ 1 บทนำ

### RSA

ภายใต้การเข้ารหัส RSA ข้อความจะถูกเข้ารหัสด้วยรหัสที่เรียกว่า กุญแจสาธารณะ ซึ่งสามารถเปิดเผยต่อสาธารณะได้ เนื่องจากคุณสมบัติทางคณิตศาสตร์ที่แตกต่างกันของอัลกอริทึม RSA เมื่อข้อความได้รับการเข้ารหัสด้วยกุญแจสาธารณะ ข้อความจะสามารถถอดรหัสได้ด้วยกุญแจอื่นหรือที่รู้จักกันในชื่อไพรเวตคีย์เท่านั้น ผู้ใช้ RSA แต่ละคนมีคู่ของคีย์ซึ่งประกอบด้วยกุญแจสาธารณะและกุญแจส่วนตัว คีย์ส่วนตัวจะต้องถูกเก็บเป็นความลับ รูปแบบการเข้ารหัสคีย์สาธารณะแตกต่างจากการเข้ารหัสคีย์สมมาตร ซึ่งทั้งกระบวนการเข้ารหัสและถอดรหัสใช้ไพรเวตคีย์เดียวกัน ความแตกต่างเหล่านี้ทำให้การเข้ารหัสพับลิคคีย์ เช่น RSA มีประโยชน์สำหรับการสื่อสารในสถานการณ์ที่ไม่มีโอกาสแจกจ่ายคีย์อย่างปลอดภัยไว้ล่วงหน้า

การเข้ารหัส RSA มักใช้ร่วมกับแผนการเข้ารหัสอื่นๆ หรือสำหรับลายเซ็นดิจิทัล ซึ่งสามารถพิสูจน์ความถูกต้องและความสมบูรณ์ของข้อความ โดยทั่วไปจะไม่ใช้ในการเข้ารหัสข้อความหรือไฟล์ทั้งหมดเนื่องจากมีประสิทธิภาพน้อยกว่าและใช้ทรัพยากรมากกว่าการเข้ารหัสแบบ symmetric-key เพื่อให้สิ่งต่างๆ มีประสิทธิภาพมากขึ้น โดยทั่วไปไฟล์จะถูกเข้ารหัสด้วยอัลกอริทึมแบบ symmetric-key จากนั้นคีย์ symmetric จะถูกเข้ารหัสด้วยการเข้ารหัส RSA ภายใต้กระบวนการนี้เฉพาะเอนทิตีที่สามารถเข้าถึงคีย์ส่วนตัวของ RSA เท่านั้นที่จะสามารถถอดรหัสคีย์สมมาตรได้

### ตัวอย่างการทำงานของ RSA

1. สร้าง Private Key และ Public Key

กำหนด  $p, q$  คือจำนวนเฉพาะโดย  $p = 3, q = 5$

#### 1.1 ทำการหาค่า $n$ (modulus)

$$n = p \times q$$

$$n = 3 \times 5 = 15$$

1.2 ทำการหาค่า  $\phi(n)$  (phi)

$$\phi(n) = (p - 1) \times (q - 1)$$

$$\phi(n) = (3 - 1) \times (5 - 1) = 8$$

1.3 เลือกค่า e โดย  $1 < e < \phi$

$$\gcd(e, \phi) = 1$$

$$\gcd(e, 8) = 1 \text{ ดังนั้นเลือก } e = 5$$

1.4 หาค่า d โดย  $1 < d < \phi$

$$ed = 1 \bmod \phi$$

$$5 \times d = 1 \bmod 8 \text{ ดังนั้น } d = 5$$

ดังนั้น ได้ private key(n, d) = (15, 5) และ public key(n, e) = (15, 5)

2. การแปลง Plaintext เป็น Ciphertext

$$\text{กำหนด Plaintext} = 3$$

$$c = m^e \bmod n$$

$$c = 3^5 \bmod 15$$

$$c = 3$$

3. การแปลง Ciphertext เป็น Plaintext

$$m = c^d \bmod n$$

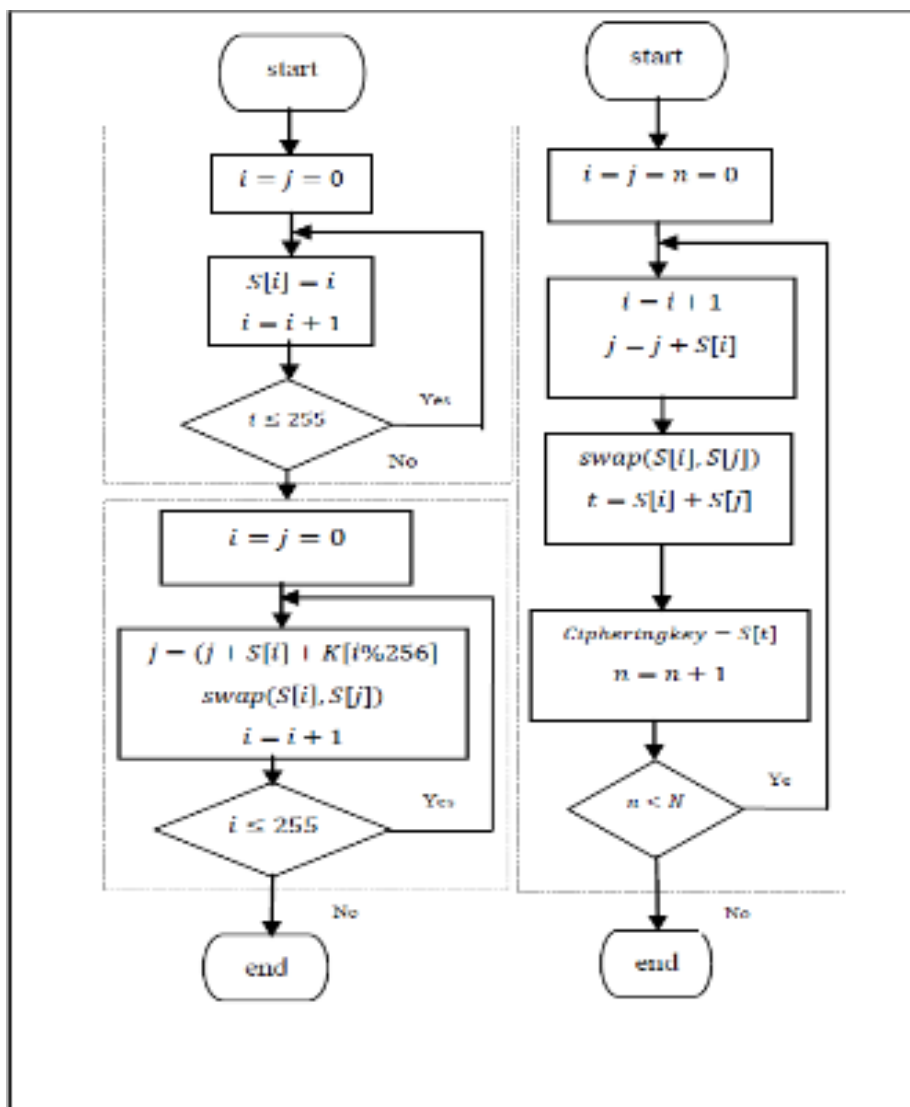
$$m = 3^5 \bmod 15$$

$$m = 3$$

## ขั้นตอนการเข้ารหัส RSA

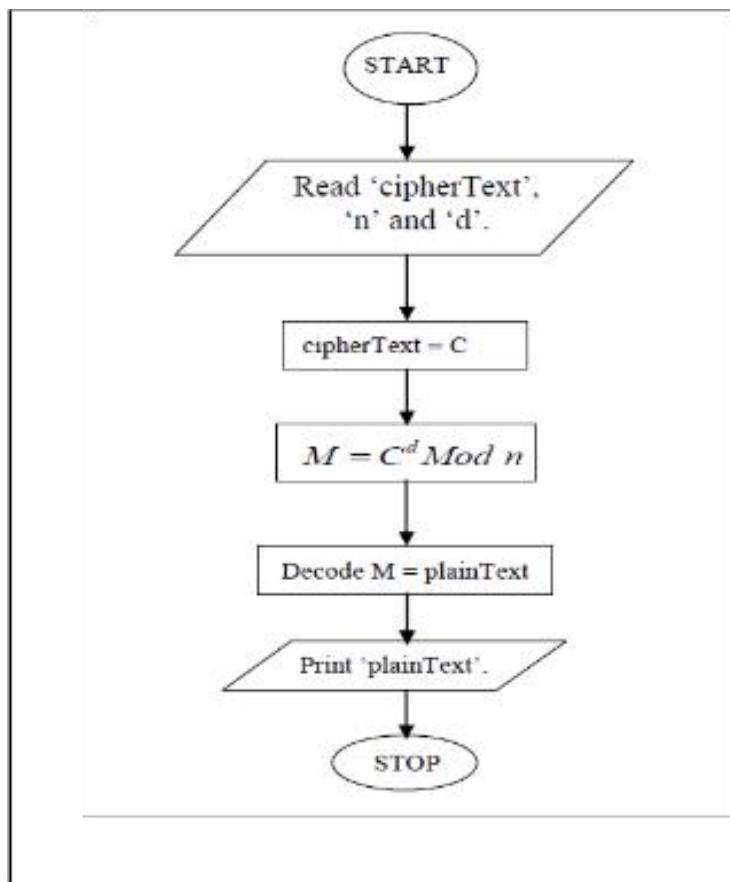
### 1. ส่วนของการเก็บข้อมูลลงฐานข้อมูล

Encryption = นำข้อมูลของคนที่ต้องการจะเก็บลงฐานข้อมูลไปทำการเข้ารหัสด้วย RSA โดยใช้ public key ของผู้รับ



## 2. ส่วนของการแสดงข้อมูลที่หน้าเว็บแอปพลิเคชัน

Decryption = นำข้อมูลของคนที่ต้องการจะแสดงที่หน้าเว็บ มาถอดรหัส โดยใช้ private key ของผู้รับ



## Python

Python เป็นภาษาการเขียนโปรแกรมระดับสูง โดยนำข้อดีของภาษาต่างๆ รวมเข้าด้วยกัน เรียนรู้ได้ง่าย และมีไวยากรณ์ที่ช่วยให้เขียนโค้ดสั้นกว่าภาษาอื่นๆ มีความสามารถใช้ชนิดข้อมูลแบบไดนามิก จัดการหน่วยความจำอัตโนมัติ สนับสนุนการเขียนโปรแกรมเชิงวัตถุ (OOP) การเขียนโปรแกรมเชิงคำสั่ง (Imperative Programming) การเขียนโปรแกรมเชิงฟังก์ชัน (Functional) และมีลักษณะเป็นภาษาสคริปต์ที่ทำงานร่วมกับภาษาอื่นได้ มีไลบรารีมาตรฐานมากมาย และใช้อินเตอร์พรีเตอร์แปลภาษาโปรแกรมให้ทำงานบนระบบปฏิบัติการได้หลากหลาย ทั้งบน Windows, MAC, Linux และ Unix นอกจากนั้นยังเป็นโปรแกรมแบบ Open source ที่นำใช้ได้ฟรี เหมาะสำหรับโปรแกรมทั้งขนาดเล็กและขนาดใหญ่ เช่น การสร้างเกม เฟรมเวิร์กพัฒนาเว็บ โปรแกรมที่ใช้กราฟฟิคติดต่อกับผู้ใช้งาน (GUI)

## Django

Django Framework เป็น open-source web framework ที่พัฒนาขึ้นมาสำหรับการใช้งาน ภาษา python โดย pattern ที่ใช้คือ Model-Template-Views (MTV) ซึ่ง Django Framework นั้นจะช่วยในการอำนวยความสะดวกต่าง ๆ ในการเขียน web application ดังนี้

### 1. การจัดการในด้าน frontend

ในส่วนของ templates ทำให้สะดวกในการทำหน้าเว็บซึ่งสามารถแบ่งส่วนของ templates ออกเป็นหลาย ๆ ส่วนได้ เพื่อใช้ในการแบ่งการทำงานอย่างชัดเจน หรือการใส่เงื่อนไขต่าง ๆ เช่น if-else , for-loop ใน view เป็นต้น

### 2. การจัดการในด้าน backend

ในส่วนของ backend นั้น Django Framework ก็มีระบบช่วยในการอำนวยความสะดวกต่าง ๆ เช่น ระบบ admin ซึ่งมี admin site มาให้สำหรับการจัดการฐานข้อมูล การสร้าง Model สำหรับข้อมูลต่างๆ รวมถึงระบบ security สำหรับ Web application ที่ Django Framework นั้นได้ทำการป้องกันไว้ให้แล้ว เป็นต้น

### 3. Model-Template-Views (MTV)

ใน Django Framework นั้นใช้ pattern คือ Model-Template-Views (MTV) ซึ่งหลักการทำงานของ MTV นั้นจะทำการแบ่งแยกการทำงาน ดังนี้



### 3.1 Model (M) มีหน้าที่ในการติดต่อกับ Database และใช้ในการสร้างตารางข้อมูลในฐานข้อมูล

Model คือส่วนที่ใช้ติดต่อกับ Database เช่นเมื่อเราได้ทำการสร้างตารางขึ้นมา การสร้างตารางเพื่อที่จะ Migrate ไปที่ Database นั้น จะมีการใช้ Class ซึ่งเป็น Object เหมือนใน Python ซึ่งเรียกกันว่า ORM (Object Relational Mapper) ซึ่งเป็นการติดต่อกับ Database โดยที่ไม่ต้องเขียนภาษา SQL แม้แต่คำสั่งเดียว ซึ่ง ORM คือการ Map ข้อมูลในตารางข้อมูลบนฐานข้อมูลให้อยู่ในรูปแบบของ Object-Oriented Language ทำให้การสร้าง Database นั้นเสมือนกับการ Language Programming ทำให้ไม่ต้องไปยุ่งกับคำสั่ง SQL ต่าง ๆ โดยใช้คำสั่ง Migrate เพื่อให้สร้าง Table

### 3.2 Templates (T) มีหน้าที่ในการจัดการหน้าตาของข้อมูลที่จะแสดงให้ผู้ใช้งาน

Template คือส่วนที่เป็นส่วนหนึ่งของหน้าบ้าน (Front end) หรือฝั่งที่เอาไว้มองแสดงผลโดยจะรองรับฟังก์ชันต่าง ๆ จาก View ซึ่งจะถูกส่งไปในรูปแบบ Context โดย Context นั้นจะเป็นตัวแปรที่เก็บผลลัพธ์จากคำสั่งต่าง ๆ ใน View หลังจากนั้น Template จะเอา Context ออกไปแสดงผล โดยการเขียนตัวแปรเพื่อแสดงผลในหน้า HTML ฝั่ง Template นั้นจะเรียกผ่าน {{ }} ซึ่งเรียกว่า Django Template Variable และสามารถเรียกใช้ For loop ผ่าน {% %} เรียกว่า Django Template Tag

### 3.3 Views(V) มีหน้าที่ในการทำ Business Logic และทำการส่งข้อมูลที่ต้องการแสดงผล ไปให้ template ใช้งาน

เป็นส่วนที่ใช้สำหรับเขียนฟังก์ชันต่าง ๆ เพื่อจัดการกับข้อมูลใน Model เช่นการ Query ข้อมูลมาคำนวณ แล้วหลังจากนั้นนำไป Create, Read, Update, Delete ได้ตามต้องการ View นั้นยังสามารถรับ Input จาก User ผ่าน Template ได้และยังสามารถ Return ข้อมูลออกไปแสดงผลที่ฝั่ง Template ก็ได้เช่น การรับ Input จาก HTTP Request ซึ่งเป็นการติดต่อกันระหว่าง Client และ Server ผ่าน HTTP Protocol แล้วนำผลลัพธ์ที่ได้จากการคำนวณหรือตรวจสอบส่งกลับไปเพื่อแสดงผลที่ Template ผ่าน HTTP Response

## 4. โครงสร้างการทำงานของ Django Framework

ในโครงสร้างของ Django Framework ถูกแยกออกเป็น 2 ส่วนหลักคือ ส่วนของ project และส่วนของ application โดยในส่วนของ project จะมีโครงสร้างการทำงานของไฟล์ ดังนี้

### 4.1 \_\_init\_\_.py ไฟล์นี้มีหน้าที่ในการบอกตัวแปลภาษา python ทราบว่าภายในโฟลเดอร์นี้เป็นจุดเริ่มต้นของการทำงานภายใน Project

4.2 setting.py เป็นไฟล์ที่ใช้ในการกำหนด config ต่างๆของ Django Project เช่น การกำหนดข้อมูลของ Database และการเพิ่ม application ที่ทำการสร้างขึ้นมาในโปรเจค

4.3 urls.py ไฟล์นี้มีหน้าที่ในการกำหนด path ของการเรียกใช้ Website

4.4 wsgi.py ไฟล์นี้มีหน้าที่ในการส่งต่อ request ต่อไปยัง Django Application Project

## 5. asgi.py

ไฟล์นี้มีหน้าที่การทำงานเหมือนกับไฟล์ wsgi.py แต่จะมีความสามารถในการรองรับ Sync และ Async ข้อมูลและในส่วนของ application จะมีโครงสร้างการทำงานของไฟล์ ดังนี้

5.1. \_\_init.py\_\_ ไฟล์นี้มีหน้าที่การบอกตัวแปลงภาษา python ทราบว่าภายในไฟล์เดอรั้นี้เป็นจุดเริ่มต้นของการทำงานภายใน Application

5.2. admin.py ไฟล์นี้มีหน้าที่ในการจัดการ model ที่ต้องการส่งไปที่ Django Administration

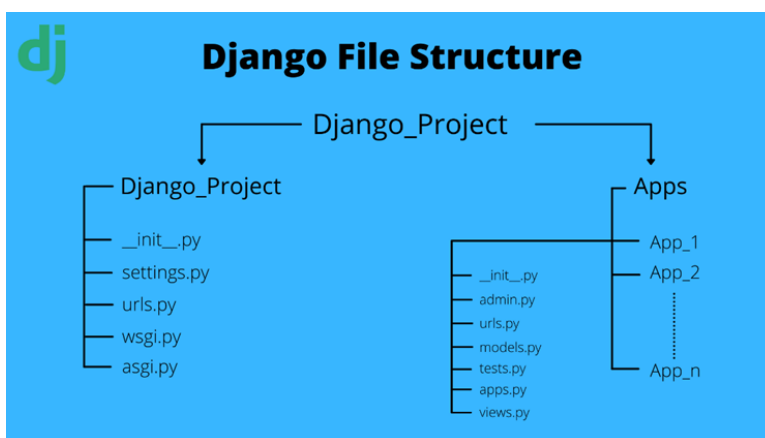
5.3. apps.py ไฟล์นี้มีหน้าที่ในการจัดการ config ภายใน Django Application

5.4. models.py ไฟล์นี้มีหน้าที่ในการจัดการโครงสร้างของ Database

5.5. views.py ไฟล์นี้มีหน้าที่ในการจัดการข้อมูลที่ต้องใช้ในการแสดง Web Application

5.6. urls.py ไฟล์นี้มีหน้าที่ในการกำหนด path ของการเรียกใช้ Website(จำเป็นต้องสร้างขึ้นมาเองทุกครั้งที่ทำ การสร้าง application)

5.7. test.py ไฟล์นี้มีหน้าที่ในการเขียนโค้ดเพื่อทำการ test Web Application



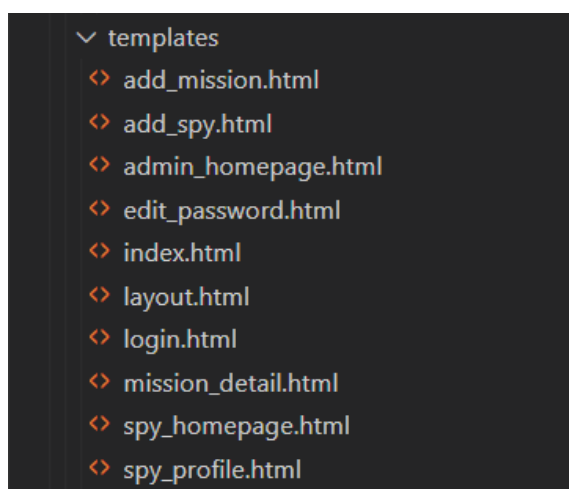
## บทที่ 2 ขั้นตอนการพัฒนา

### ออกแบบการทำงานของเว็บแอปพลิเคชัน

1. แบ่งส่วนของพีเจอร้อออกเป็น 2 ส่วน คือส่วนของหัวหน้า spy และส่วนของ spy โดยเมื่อเริ่มต้นการทำงานเว็บไซต์จะต้องทำการ login ก่อน หาก login ด้วย id ของหัวหน้า spy จะแสดงหน้าเว็บไซต์ในรูปแบบของหัวหน้า spy คนนั้น หาก login ด้วย id ของ spy จะแสดงหน้าเว็บไซต์ในรูปแบบของ spy
2. พีเจอร้อของหัวหน้า spy ประกอบด้วย
  - 2.1 สามารถดูรายละเอียดของ id ตัวเอง ประกอบด้วย code name, ภารกิจทั้งหมด, ภารกิจที่รอการอนุมัติ และภารกิจที่อนุมัติแล้ว
  - 2.2 สามารถดูรายชื่อและรายละเอียดภารกิจของ spy ที่อยู่ในสังกัดได้
  - 2.3 สามารถเพิ่มบัญชีของ spy คนใหม่ได้
  - 2.4 สามารถลบบัญชีของ spy ในสังกัดได้
  - 2.5 สามารถเพิ่มภารกิจใหม่และระบุ id spy ที่รับผิดชอบภารกิจนั้นได้
  - 2.6 เมื่อ spy ยื่นขอการอนุมัติภารกิจมา จะสามารถเลือกอนุมัติเพื่อให้ภารกิจ เพื่อเปลี่ยนสถานะภารกิจจาก รอการอนุมัติ ให้อยู่ในสถานะ เสร็จสิ้น หรือปฏิเสธเพื่อให้ภารกิจกลับไปอยู่ในสถานะยังไม่สำเร็จ ได้ (ภารกิจจะมีด้วยกัน 3 สถานะคือ ยังไม่สำเร็จ, รอการอนุมัติ และเสร็จสิ้นแล้ว)
3. พีเจอร้อของ spy ประกอบด้วย
  - 3.1 สามารถดูรายละเอียดของ id ตัวเอง ประกอบด้วย code name, ภารกิจทั้งหมด, ภารกิจที่รอการอนุมัติ และภารกิจที่อนุมัติแล้ว
  - 3.2 สามารถดูรายชื่อและรายละเอียดภารกิจของบัญชีตัวเองได้
  - 3.3 สามารถยื่นขอการอนุมัติภารกิจไปที่หัวหน้า spy เพื่อเปลี่ยนสถานะภารกิจจาก ยังไม่สำเร็จ ให้อยู่ในสถานะ รอการอนุมัติ
4. ใช้ RSA ในการเก็บรักษาความปลอดภัยชื่อภารกิจและรายละเอียดภารกิจไม่ให้บัญชีของ spy ผู้อื่น นอกจากบัญชีของผู้รับผิดชอบภารกิจนั้นและหัวหน้า spy สามารถอ่านได้

## การพัฒนาเว็บแอปพลิเคชัน

1. ศึกษาการใช้งาน library RSA
2. ศึกษาการใช้งาน Django Framework
3. เริ่มต้นการพัฒนาเว็บแอปพลิเคชันตามที่ได้ออกแบบไว้
  - 3.1 สร้างส่วน front-end เป็นไฟล์ html ทั้งหมด 10 ไฟล์ สำหรับแสดงผลหน้าต่างๆของเว็บไซต์ ดังรูป



- 3.2 พัฒนาฟังก์ชันในการทำงานต่างๆในเว็บแอปพลิเคชันเพื่อใช้งานในหน้าเว็บไซต์ที่ได้สร้างไว้

ประกอบด้วย

- login/logout
- เพิ่ม/ลบ spy
- เพิ่มภารกิจสำหรับ spy
- เปลี่ยนรหัสผ่าน
- เปลี่ยนสถานะภารกิจ
- ดูรายละเอียดและสถานะภารกิจของ spy
- RSA สำหรับป้องกันข้อมูล ชื่อภารกิจ และรายละเอียดภารกิจ

ตัวอย่างโค้ด encryption ด้วย RSA

นำข้อมูลของคนที่ต้องการจะเก็บลงฐานข้อมูลไปทำการเข้ารหัสด้วย RSA โดยใช้ public key ของเจ้าของภารกิจ

```

195 def AddMission(request):
196     if request.user.is_authenticated and request.user.userprofile.role == 'Admin':
197         if request.method == 'POST':
198             missionName = request.POST['mission_title']
199             missionDescriptions = request.POST['mission_detail']
200             date = request.POST['dateMission']
201             status = "on going"
202             spyID = request.POST['spy_mission_owner']
203             userProfile = UserProfile.objects.filter(id = spyID) #Object UserProfile
204             rsa_key = userProfile[0].rsa_key.getValueInt()
205             publicKey_spy = rsa.PublicKey(n=rsa_key["n"],e=rsa_key["e"])
206             encMissionNameSpy = rsa.encrypt(missionName.encode(),publicKey_spy)
207             encMissionDesSpy = rsa.encrypt(missionDescriptions.encode(),publicKey_spy)
208             user = userProfile[0].user #Object User
209             mission = Mission(mission_name=encMissionNameSpy,mission_descriptions=encMissionDesSpy,date_start=date,status=status,spy=user)
210             mission.save()
211             userProfile.update(ongoing_mission = userProfile[0].ongoing_mission + 1)
212         else:
213             all_spy = UserProfile.objects.filter(role='Spy')
214             return render(request,"add_mission.html",{ 'all_spy': all_spy})
215     return redirect('/')
216

```

ตัวอย่างโค้ด decryption ด้วย RSA

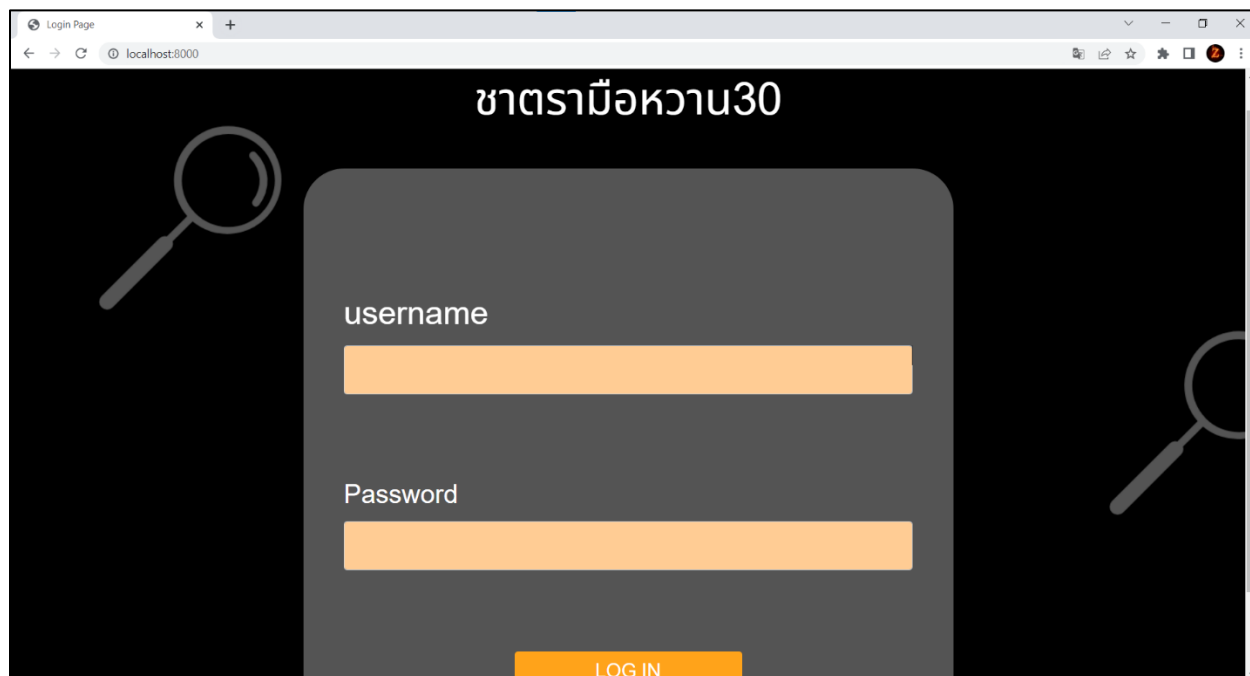
นำข้อมูลของคนที่ต้องการจะแสดงที่หน้าเว็บ มาถอดรหัส โดยใช้ private key ของเจ้าของภารกิจ

```

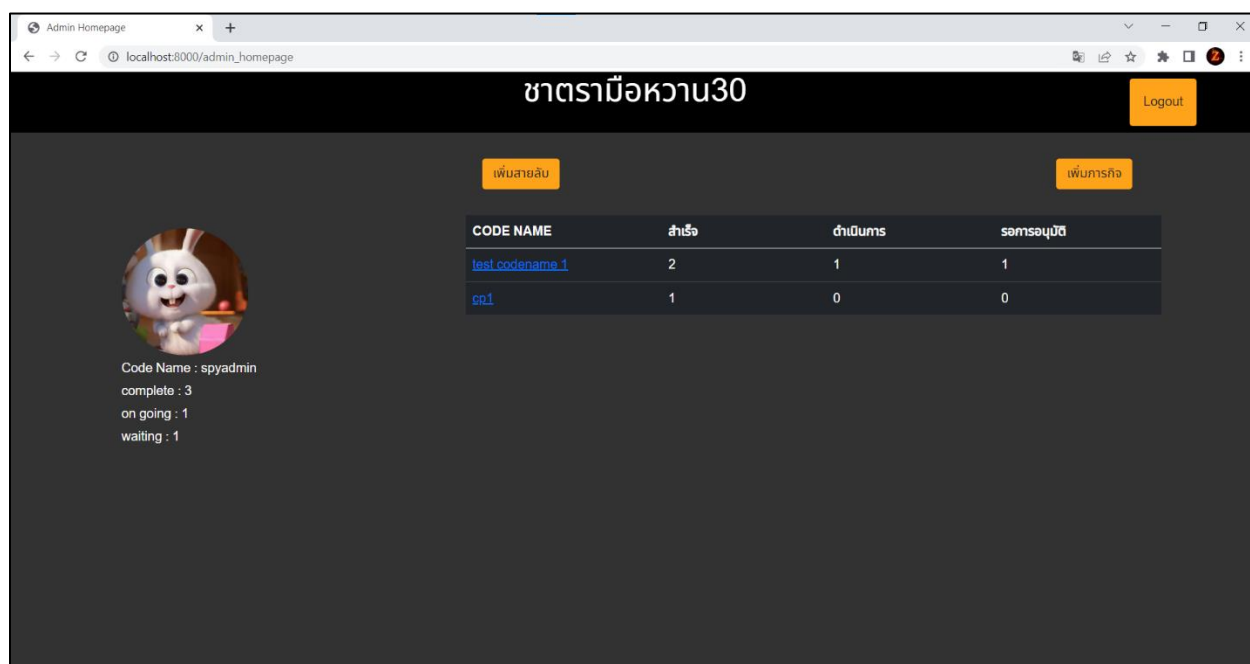
54 def MissionDetail(request , mission_id):
55     if request.user.is_authenticated:
56         mission = Mission.objects.get(id=mission_id)
57         if request.user.userprofile.role == "Admin":
58             userprofile = mission.spy.userprofile
59         else:
60             if request.user.userprofile != mission.spy.userprofile:
61                 return HttpResponseRedirect(reverse('LoginPage'))
62             userprofile = request.user.userprofile
63     rsa_key = userprofile.rsa_key.getValueInt()
64     privateKey = rsa.PrivateKey(n=rsa_key["n"],e=rsa_key["e"],d=rsa_key["d"],p = rsa_key["p"],q= rsa_key["q"])
65
66     name_decrypt = rsa.decrypt(mission.mission_name, privateKey).decode()
67     descriptions_decrypt = rsa.decrypt(mission.mission_descriptions, privateKey).decode()
68     date = mission.date_start
69     status = mission.status
70
71     if request.method == "POST":
72         status = request.POST['status']
73         mission.status = status
74         mission.save()
75
76         on_going = Mission.objects.filter(spy_userprofile=userprofile , status='on going').count()
77         userprofile.ongoing_mission = on_going
78         waiting = Mission.objects.filter(spy_userprofile=userprofile , status='waiting').count()
79         userprofile.waiting_mission = waiting
80         complete = Mission.objects.filter(spy_userprofile=userprofile , status='complete').count()
81         userprofile.complete_mission = complete
82         userprofile.save()
83
84     return render(request , "mission_detail.html" , { "id": mission.id,
85         "mission_name": name_decrypt,
86         "mission_descriptions" : descriptions_decrypt,
87         "date_start": date,
88         "status": status
89     })
90

```

### บทที่ 3 ผลการดำเนินงาน




### ส่วนของหัวหน้า spy



Spy Profile    localhost:8000/spy\_profile/14

## ชาตรามือหวาน30

Logout



code name : test codename 1

ปลด spy

ภารกิจที่สำเร็จ	ภารกิจที่ยังไม่สำเร็จ	ภารกิจที่กำลังรออนุมัติ
2	1	1

ชื่อภารกิจ	วันที่ปฏิบัติการ	สถานะ
<a href="#">ลลล</a>	May 3, 2022	complete
<a href="#">ดลลล</a>	May 3, 2022	on going
<a href="#">ลลล</a>	May 6, 2022	complete
<a href="#">test_mission_1</a>	May 10, 2022	waiting

Mission Detail    localhost:8000/mission\_detail/11

## ชาตรามือหวาน30

Logout

ชื่อภารกิจ : test\_mission\_1

วันที่ปฏิบัติการ : May 10, 2022

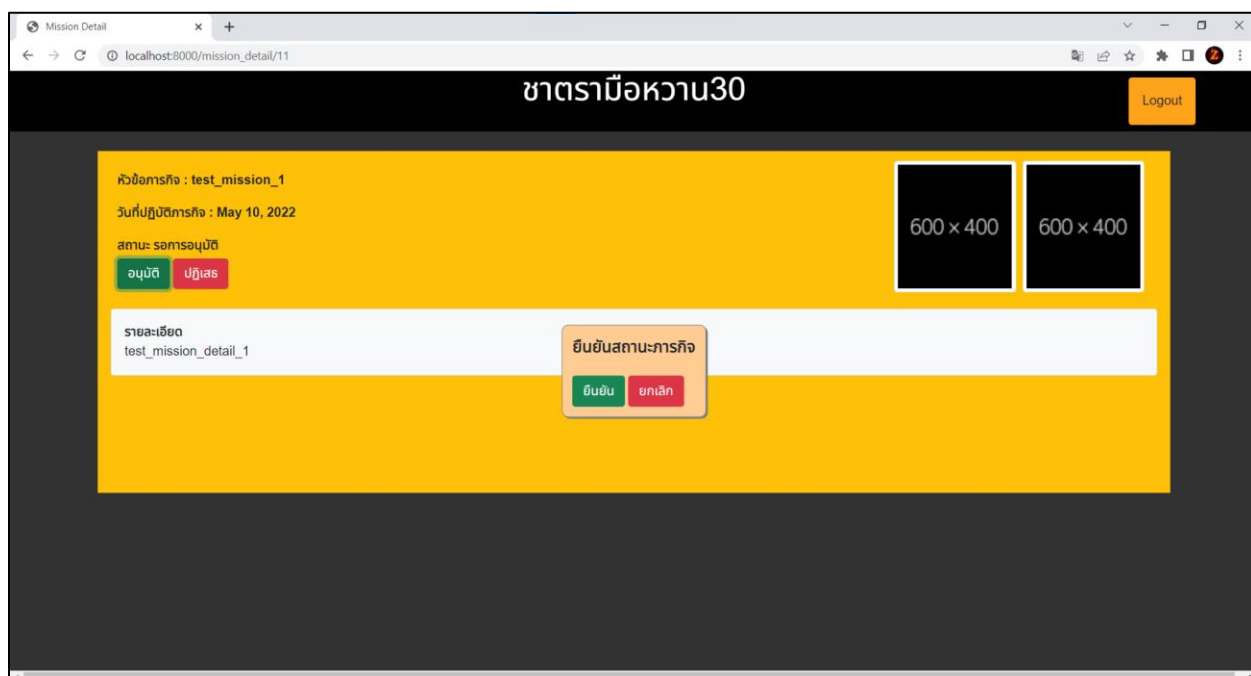
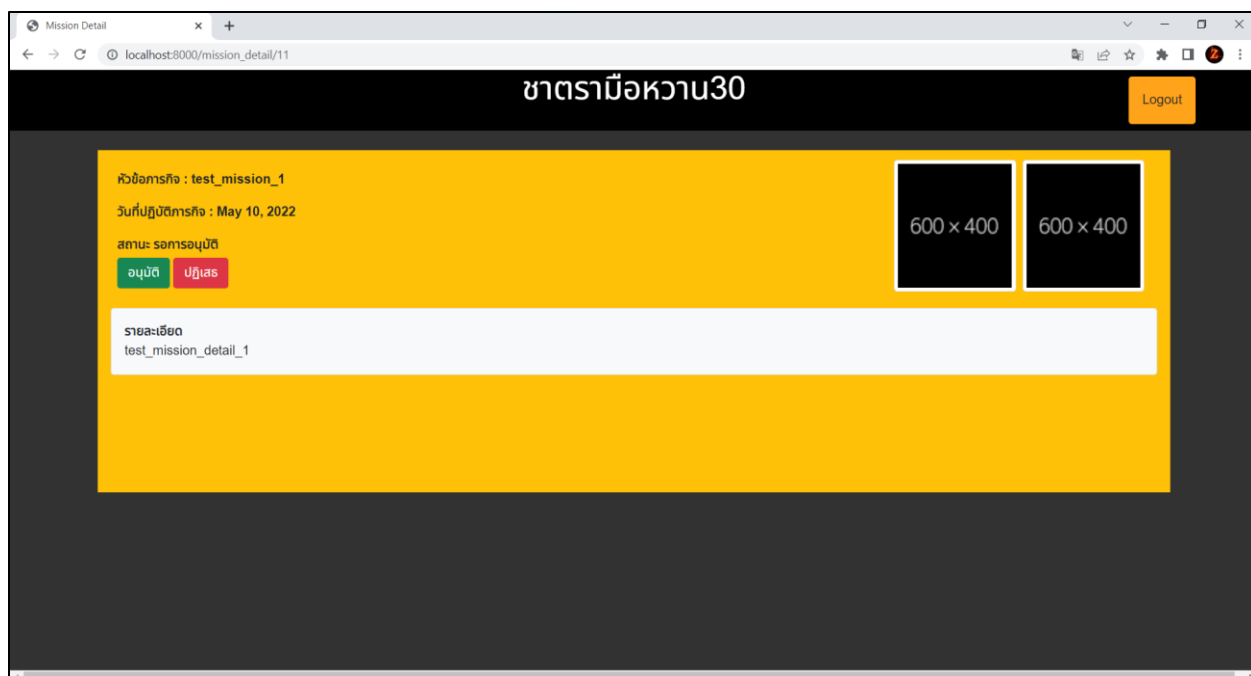
สถานะ : ยังไม่สำเร็จ

รายละเอียด

test\_mission\_detail\_1

600 × 400

600 × 400





Add Spy Page x +

localhost:8000/add\_spy

## ชาตรามือหวาน30

Logout

### เพิ่มสายลับ

600 × 400

เลือกรูปภาพ

CODE NAME

USERNAME

เพิ่มสายลับ

Add Mission Page x +

localhost:8000/add\_mission

## ชาตรามือหวาน30

Logout

หัวข้อภารกิจ

Spy ผู้ทำภารกิจ

วันที่ทำภารกิจ :

รายละเอียดภารกิจ

600 × 400

เลือกรูปภาพ

test codename 1

mm/dd/yyyy

เพิ่มภารกิจ

ส่วนของ spy

