

**รายงานวิชา Computer Security**

Assignment I

**จัดทำโดย**

นายปณิธาน ดวงขวัญ

รหัส 5735512036 Section 02

**เสนอ**

อาจารย์ฐิตินันท์ เกลี้ยงสุวรรณ

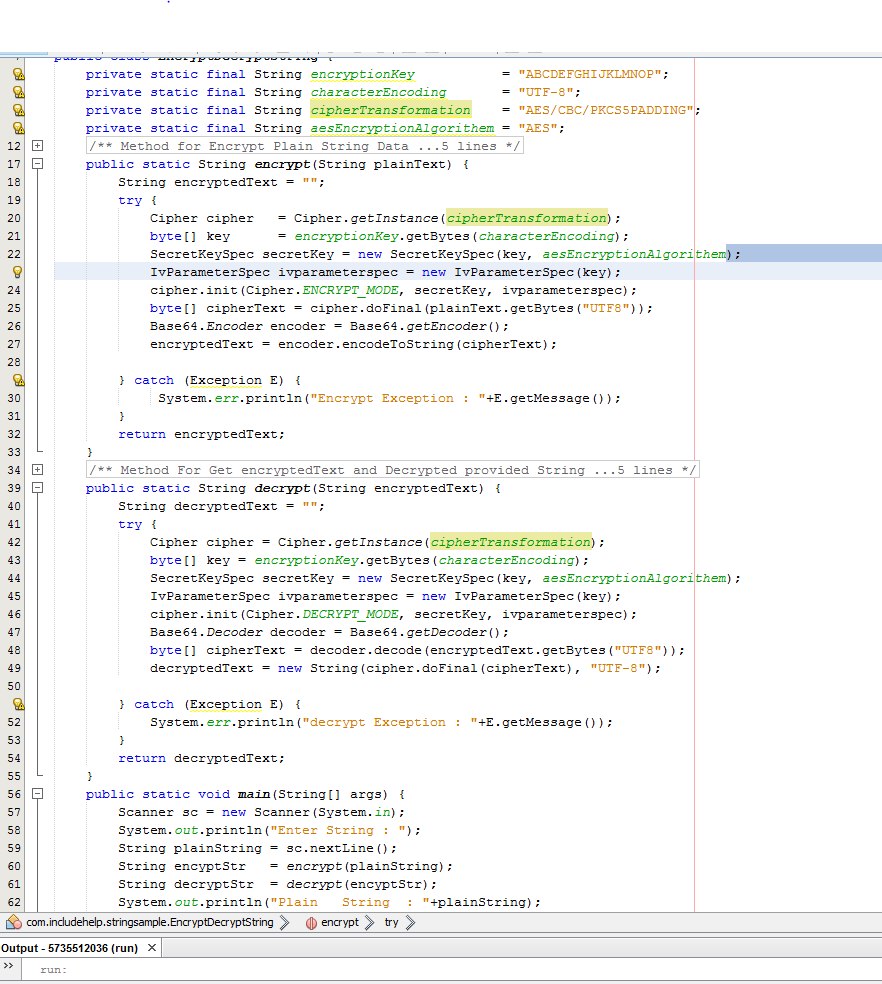
รหัสวิชา 242-312 Computer Security

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

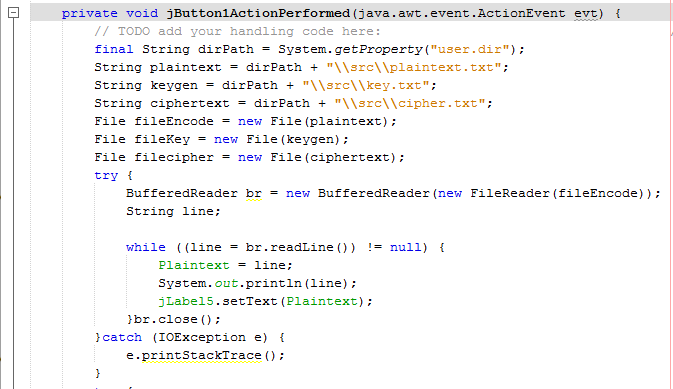
มหาวิทยาลัยสงขลานครินทร์

**Assignment I**

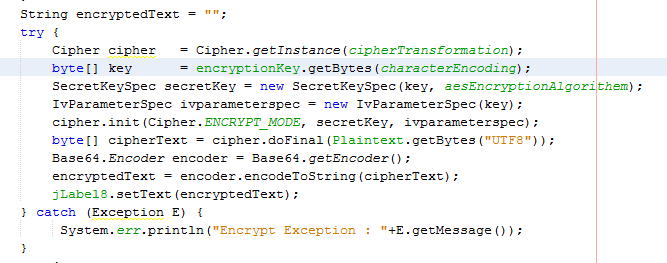
**โจทย์ : จงเขียนโปรแกรมเพื่อใช้ในการเข้ารหัสและถอดรหัส ภายใต้มาตรฐานการเข้ารหัส AES โดยใช้ภาษาโปรแกรมที่ถนัด กำหนดให้โปรแกรมรองรับข้อความต้นฉบับภาษาอังกฤษซึ่งประกอบด้วยตัวอักษร 26 ตัวและตัวเลข 0 ถึง 9 โดยโปรแกรมต้องรอบรับค่ากุญแจผ่านไฟล์ key.txt และข้อความต้นฉบับผ่านไฟล์ plaintext.txt เมื่อโปรแกรมประมวลผลเพื่อเข้ารหัสข้อความต้นฉบับเสร็จสิ้นแล้ว ผลลัพธ์ข้อความไซเฟอร์ต้องบรรจุในไฟล์ cipher.txt และเมื่อโปรแกรมประมวลผลเพื่อถอดรหัสข้อความไซเฟอร์เสร็จสิ้น ผลลัพธ์ข้อความต้นฉบับที่ได้จะบรรจุอยู่ในไฟล์ textout.text**



**คำอธิบายโค้ด:** ในส่วนของตัวโค้ดจะประกอบด้วย ทั้งหมด 2 Method เพื่อทำงานในส่วนของถอดรหัสนั่นเองโดย method แรกนั้นจะเป็น method encrypt หรือเป็นฟังก์ชั่นในการทำงานส่วนของเข้ารหัสข้อมูล และ อีก Metthod ในส่วนของ decrypt นั่นคือส่วนของการถอดรหัส



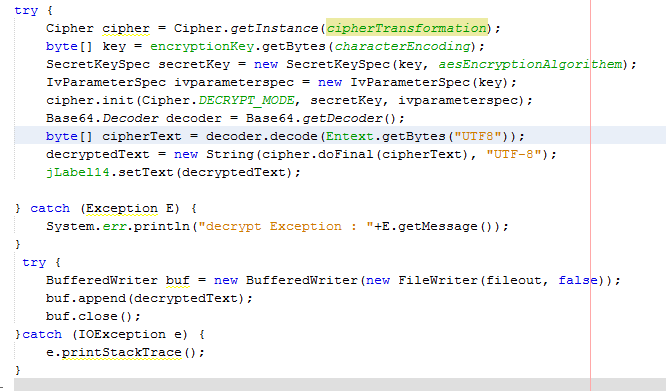
**คำอธิบายโค้ด :** ในส่วนของโค้ดนี้จะมีการประกาศที่อยู่ของไฟล์และมีการประกาศ Object ที่ใช้ในการอ่านไฟล์ หลังจากนั้นในส่วนของการวนลูป จะมีการอ่านค่าของไฟล์ plaintext มาเก็บไว้ในตัวแปร



**คำอธิบายโค้ด :** ในส่วนของหลังจากเก็บค่าไว้ในตัวแปรแล้วมีการเข้ารหัสโดยจะใช้อัลกอลิทึมของการเข้ารหัส โดยจะมีการแปลงเป็น Key เป็นเลข ASCII หลังจากนั้นประกาศ Object โดยนำ Key ไปไว้ในอัลกอริทึม ต่อไปจะนำ text ที่เรามีข้อความไว้มาแปลงเป็น byte เสร็จแล้วจะสร้าง Object การเข้ารหัสขึ้นพอสร้างเสร็จนำ text มาเข้ารหัสและนำตัวที่เข้ารหัสแล้วมาแสดงบน GUI และหลังจากนั้นจะมีการเขียน text mเข้ารหัสลงบนไฟล์โดยจะอยู่ในส่วนของโค้ด BufferedWriter buf นั่นเอง



**คำอธิบายโค้ด :** เริ่มต้นโดยการประกาศที่อยู่ของไฟล์ หลังจากนั้นจะอ่านไฟล์ที่เข้ารหัสโดยในลูปจะอ่านไฟล์ที่เข้าเข้ารหัสเรียบร้อยแล้ว เสร็จแล้วจะแสดง text ที่เข้ารหัสบน GUI



**คำอธิบายโค้ด :** เริ่มต้นจะเป็นโค้ดของส่วนการถอดรหัส และ แปลง key ให้ได้มาตฐาน UTF-8 โดยมีการสร้าง key ลับ ตามมาตรฐาน AES หลังจากนั้น ใช้ base 64 ในการถอดรหัส ในส่วนต่อไปจะเป็นการถอดรหัส และหลังจากถอดรหัสก็จะแสดง text ที่ถอดรหัสเสร็จแล้วบน GUI และสุดท้ายจะนำค่าไฟล์ไปเก็บในไฟล์

**ผลการ RUN**

