GROUP 05

FILE PROTECTION

342376
INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

วัตถุประสงค์

- เพื่อศึกษา Algorithm RSA
- เพื่อศึกษา Algorithm DES
- เพื่อศึกษา Algorithm AES

หลักการและเหตุผล

ปัจจุบันการรับส่งไฟล์เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น พวกเราจึงมีแนวคิดที่จะทำแอปพลิเคชั่นบนคอมพิวเตอร์ที่มีความสามารถในการรับ-ส่งไฟล์ที่มีความปลอดภัย และมีการเข้ารหัสข้อมูลเพื่อปกป้องความลับของข้อมูลดิจิทัล เนื่องจากข้อมูลที่ส่งโดยใช้อินเทอร์เน็ตหรือเครือข่ายคอมพิวเตอร์อาจถูกขโมยความลับระหว่างการส่งข้อมูลได้

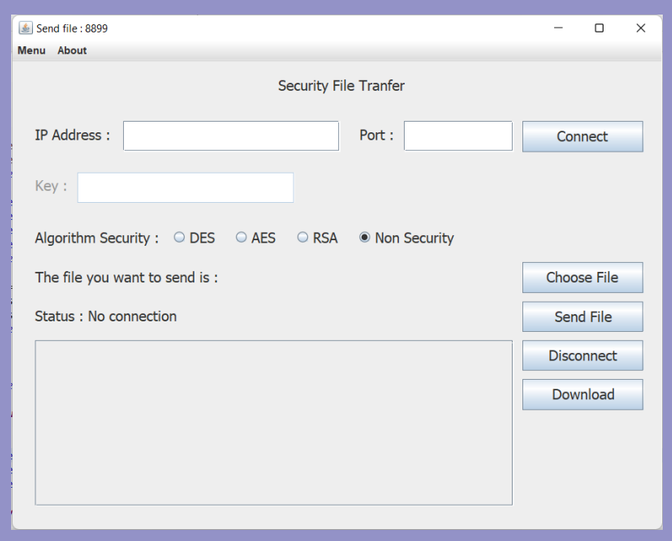
ขอบเขตและฟังก์ชั่น

- สามารถรับ และส่งไฟล์ระหว่างกันได้
- สามารถ เลือก Algorithm ในการเข้ารหัสไฟล์ได้
- สามารถ Download ไฟล์ได้

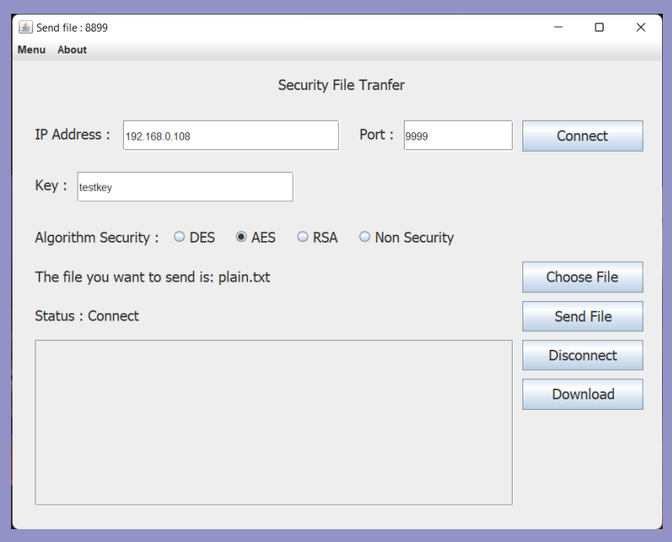
สรุป

-เป็นการใช้ภาษา Java ในการพัฒนาโปรแกรมเพื่อเชื่อมต่อหากันโดยการเชื่อมต่อระหว่าง Sever กับ Client และ สามารถเลือก Algorithm ในการเข้ารหัสไฟล์ได้ เพื่อความปลอดภัยในการส่งไฟล์

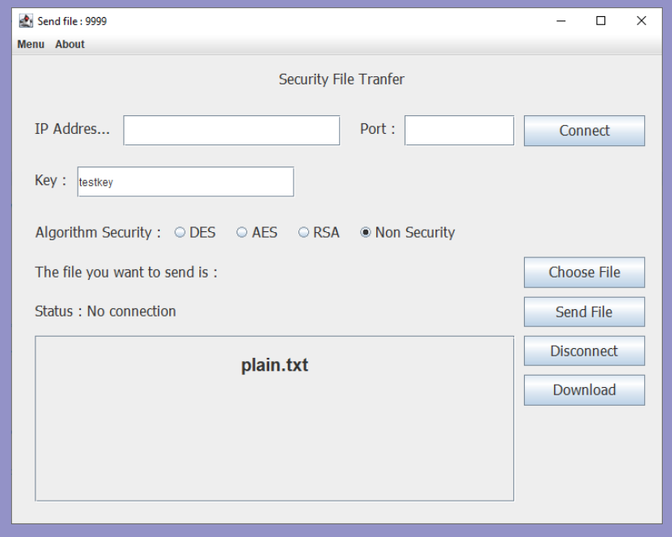
วิธีใช้งาน



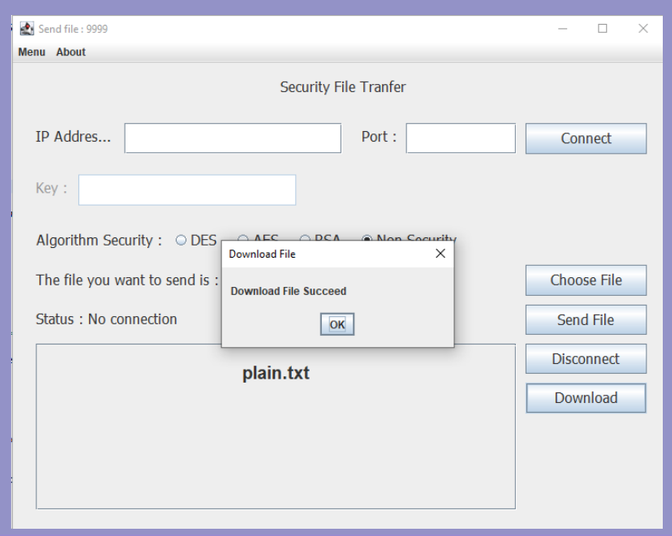
ทำการเชื่อมต่อโดยส่ง ip address และ port ของเครื่องที่เราต่องการส่งไฟล์



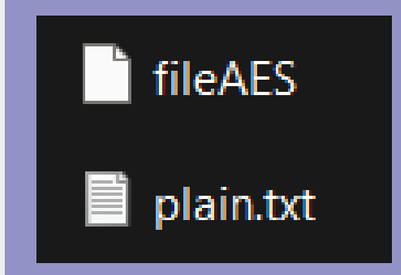
ทำการเลือก Algorithm โดยมี DES AES RSA และ Non Security และ ทำการใส่ key เมื่อเลือก Algorithm DES , AES แล้วทำการกดส่งไฟล์



ฝั่งที่รับไฟล์จะเห็นไฟล์ที่ส่งมา และต้องทำการใส่ key และทำการ Download



เมื่อ Download เสร็จ จะมีแจ้งเตือนเสร็จสิ้น และจะได้ไฟล์ที่ทำการเข้ารหัส และถอรหัสมา



ตัวอย่างไฟล์ เลือก Algorithm AES

รศ.ดร.จักรชัย โสอินทร์
342376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

633020290-2 ฐิติพงศ์ กาญจนดำรงนันท์
633020297-8 ธีรนันท์ หัสจรรย์
633020316-0 พีรกานต์ ภวภูตานนท์
633020333-0 สิรวิชญ์ ลิ่มสุวัฒนาพงษ์
633020452-2 ณัฐพงษ์ ทองยา
633020458-0 ปวิธ อึ้งอารุณยะวี

โปรแกรมที่ใช้พัฒนา eclipse Java

อ้างอิง : https://kku.world/ifruj https://kku.world/1qmdf https://kku.world/1l2m0 https://kku.world/r9f7y