

Assignment 1

เรื่อง การเข้ารหัสแบบ AES

รายวิชา 242-312 COMPUTER SECURITY

เสนอ

อาจารย์ รุติพันธ์ เกลี้ยงสุวรรณ

จัดทำโดย

นายณัฐวัตร ทองอร่าม

รหัสนักศึกษา 5735512125

มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตภูเก็ต

ภาคเรียนที่ 1 ปีการศึกษา 2560

ผลการรันโปรแกรม

The screenshot displays the NetBeans IDE 8.2 interface. The main editor window shows the source code of `AES.java`. The code implements an AES encryption and decryption process. It uses `java.nio.file` for file operations and `javax.crypto` for cryptographic functions. The program reads a plaintext file, encrypts it to a ciphertext file, and then decrypts the ciphertext back to the original plaintext.

```
1 import java.nio.file.Files;
2 import java.nio.file.Paths;
3 import javax.crypto.*;
4 public class AES {
5     public static void main(String[] args) throws Exception {
6         String FileName = "plaintext.txt"; // ไฟล์ต้นฉบับ
7         String FileName1 = "cipher.txt"; // ไฟล์ที่ถูกเข้ารหัส
8         String FileName2 = "textout.txt"; // ไฟล์ที่ถูกถอดรหัส
9         String FileName3 = "keytext.txt"; // ไฟล์ secret key
10
11         KeyGenerator KeyGen = KeyGenerator.getInstance("AES"); // สร้าง key แบบ AES
12         KeyGen.init(128); // Key ขนาด 128 Bit
13
14         SecretKey SecKey = KeyGen.generateKey(); // นำ key มาทำเป็น key secret Key
15         byte[] Secretkey = SecKey.getEncoded(); // นำ secret key มาเข้ารหัสเป็น byte
16         Files.write(Paths.get(FileName3), Secretkey); // เขียน Secret Key ลงในไฟล์ keytext.txt
17
18         Cipher AesCipher = Cipher.getInstance("AES"); // เลือกแบบการเข้ารหัสและการถอดรหัส แบบ AES
19
20         byte[] byteText = Files.readAllBytes(Paths.get(FileName)); // อ่านไฟล์ plaintext.txt
21
22         AesCipher.init(Cipher.ENCRYPT_MODE, SecKey); // เข้ารหัสด้วย secret key
23         byte[] byteCipherText = AesCipher.doFinal(byteText); // เก็บข้อความที่ถูกเข้ารหัสไว้ในตัวแปร byteCipherText
24         Files.write(Paths.get(FileName1), byteCipherText); // เขียนไฟล์ที่เข้ารหัสไว้ในไฟล์ cipher.txt
25
26         byte[] cipherText = Files.readAllBytes(Paths.get(FileName1)); // อ่านไฟล์ cipher.txt
27
28         AesCipher.init(Cipher.DECRYPT_MODE, SecKey); // ถอดรหัสด้วย Secret Key
29         byte[] bytePlainText = AesCipher.doFinal(cipherText); // เก็บข้อความที่ถูกเข้ารหัสไว้ในตัวแปร
30         Files.write(Paths.get(FileName2), bytePlainText); // นำข้อความที่ถูกถอดรหัสจากตัวแปรเก็บไว้ใน textout.txt
31     }
32 }
33
```






The left sidebar shows the project structure for 'AES', including folders like 'build', 'classes', 'empty', 'generated-sources', 'dist', 'nbproject', 'src', and files like 'build.xml', 'cipher.txt', 'keytext.txt', 'plaintext.txt', and 'textout.txt'. The bottom status bar indicates the build was successful.

Output - AES (run) ×

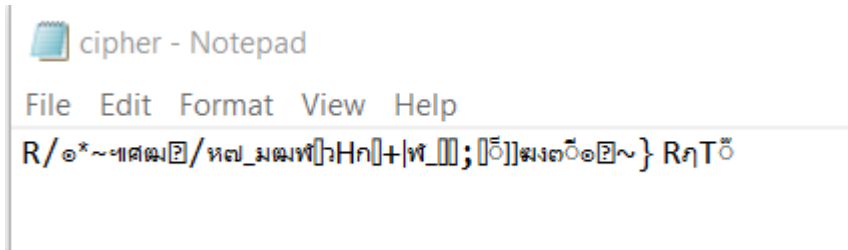
```
run:
BUILD SUCCESSFUL (total time: 0 seconds)
```

33:2 | INS

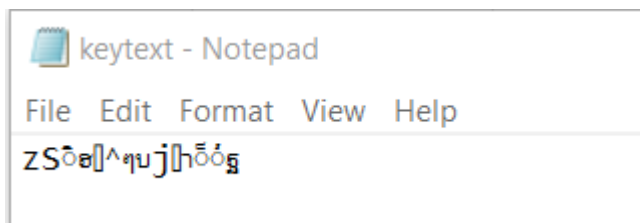
ไฟล์ที่ได้ทั้งหมดจากการรันโปรแกรม

 cipher	7/9/2560 0:21	Text Document	1 KB
 keytext	7/9/2560 0:21	Text Document	1 KB
 manifest.mf	7/9/2560 0:16	MF File	1 KB
 plaintext	7/9/2560 0:20	Text Document	1 KB
 textout	7/9/2560 0:21	Text Document	1 KB

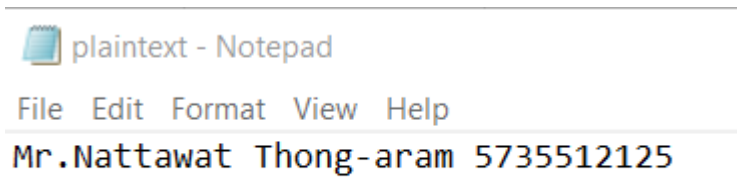
ไฟล์ cipher.txt



ไฟล์ keytext.txt



ไฟล์ plaintext.txt



ไฟล์ textout.txt

