
# 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**

```
    private static final String encryptionKey           = "ABCDEFGHIJKLMNOP";
    private static final String characterEncoding       = "UTF-8";
    private static final String cipherTransformation    = "AES/CBC/PKCS5PADDING";
    private static final String aesEncryptionAlgorithem = "AES";
    /** Method for Encrypt Plain String Data ...5 lines */
    public static String encrypt(String plainText) {
        String encryptedText = "";
        try {
            Cipher cipher    = Cipher.getInstance(cipherTransformation);
            byte[] key       = encryptionKey.getBytes(characterEncoding);
            SecretKeySpec secretKey = new SecretKeySpec(key, aesEncryptionAlgorithem);
            IvParameterSpec ivparameterspec = new IvParameterSpec(key);
            cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivparameterspec);
            byte[] cipherText = cipher.doFinal(plainText.getBytes("UTF8"));
            Base64.Encoder encoder = Base64.getEncoder();
            encryptedText = encoder.encodeToString(cipherText);

        } catch (Exception E) {
            System.err.println("Encrypt Exception : "+E.getMessage());
        }
        return encryptedText;
    }
    /** Method For Get encryptedText and Decrypted provided String ...5 lines */
    public static String decrypt(String encryptedText) {
        String decryptedText = "";
        try {
            Cipher cipher = Cipher.getInstance(cipherTransformation);
            byte[] key = encryptionKey.getBytes(characterEncoding);
            SecretKeySpec secretKey = new SecretKeySpec(key, aesEncryptionAlgorithem);
            IvParameterSpec ivparameterspec = new IvParameterSpec(key);
            cipher.init(Cipher.DECRYPT_MODE, secretKey, ivparameterspec);
            Base64.Decoder decoder = Base64.getDecoder();
            byte[] cipherText = decoder.decode(encryptedText.getBytes("UTF8"));
            decryptedText = new String(cipher.doFinal(cipherText), "UTF-8");

        } catch (Exception E) {
            System.err.println("decrypt Exception : "+E.getMessage());
        }
        return decryptedText;
    }
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);
        System.out.println("Enter String : ");
        String plainString = sc.nextLine();
        String encyptStr   = encrypt(plainString);
        String decryptStr  = decrypt(encyptStr);
        System.out.println("Plain   String  : "+plainString);
com.includehelp.stringsample.EncryptDecryptString > encrypt > try >
Output - 5735512036 (run)
run:
```

**คำอธิบายโค้ด:** ในส่วนของตัวโค้ดจะประกอบด้วย ทั้งหมด 2 Method เพื่อทำงานในส่วนของถอดรหัสนั่นเอง โดย method แรกนั้นจะเป็น method encrypt หรือเป็นฟังก์ชั่นในการทำงานส่วนของเข้ารหัสข้อมูล และอีก Metthod ในส่วนของ decrypt นั่นคือส่วนของการถอดรหัส

```
    private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
        // TODO add your handling code here:
        final String dirPath = System.getProperty("user.dir");
        String plaintext = dirPath + "\\src\\plaintext.txt";
        String keygen = dirPath + "\\src\\key.txt";
        String ciphertext = dirPath + "\\src\\cipher.txt";
        File fileEncode = new File(plaintext);
        File fileKey = new File(keygen);
        File filecipher = new File(ciphertext);
        try {
            BufferedReader br = new BufferedReader(new FileReader(fileEncode));
            String line;

            while ((line = br.readLine()) != null) {
                Plaintext = line;
                System.out.println(line);
                jLabel5.setText(Plaintext);
            }br.close();
        }catch (IOException e) {
            e.printStackTrace();
        }
```

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

```
String encryptedText = "";
try {
    Cipher cipher    = Cipher.getInstance(cipherTransformation);
    byte[] key       = encryptionKey.getBytes(characterEncoding);
    SecretKeySpec secretKey = new SecretKeySpec(key, aesEncryptionAlgorithem);
    IvParameterSpec ivparameterspec = new IvParameterSpec(key);
    cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivparameterspec);
    byte[] cipherText = cipher.doFinal(Plaintext.getBytes("UTF8"));
    Base64.Encoder encoder = Base64.getEncoder();
    encryptedText = encoder.encodeToString(cipherText);
    jLabel8.setText(encryptedText);
} catch (Exception E) {
     System.err.println("Encrypt Exception : "+E.getMessage());
}
```

**คำอธิบายโค้ด :** ในส่วนของหลังจากเก็บค่าไว้ในตัวแปรแล้วมีการเข้ารหัสโดยจะใช้อัลกอลิทึมของการเข้ารหัสโดยจะมีการแปลงเป็น Key เป็นเลข ASCII หลังจากนั้นประกาศ Object โดยนำ Key ไปไว้ในอัลกอริทึม ต่อไปจะนำ text ที่เรามีข้อความไว้มาแปลงเป็น byte เสร็จแล้วจะสร้าง Object การเข้ารหัสขึ้นพอสร้างเสร็จ

นำ text มาเข้ารหัสและนำตัวที่เข้ารหัสแล้วมาแสดงบน GUI และหลังจากนั้นจะมีการเขียน text mเข้ารหัสลงบนไฟล์โดยจะอยู่ในส่วนของโค้ด BufferedWriter buf นั่นเอง

```
private void jButton2ActionPerformed(java.awt.event.ActionEvent evt) {
    // TODO add your handling code here:
    final String dirPath = System.getProperty("user.dir");
    String textout = dirPath + "\\src\\textout.txt";
    String keygen = dirPath + "\\src\\key.txt";
    String ciphertext = dirPath + "\\src\\cipher.txt";
    File fileout = new File(textout);
    File fileKey = new File(keygen);
    File filecipher = new File(ciphertext);
    try {
        BufferedReader br = new BufferedReader(new FileReader(filecipher));
        String line;

        while ((line = br.readLine()) != null) {
            Entext = line;
            System.out.println(line);
            jLabel12.setText(Entext);
        }br.close();
    }catch (IOException e) {
        e.printStackTrace();
    }
    try {
        BufferedReader br = new BufferedReader(new FileReader(fileKey));
        String line;

        while ((line = br.readLine()) != null) {
            encryptionKey = line;
            System.out.println(line);
            jLabel13.setText(encryptionKey);
        }br.close();
    }catch (IOException e) {
        e.printStackTrace();
    }
```

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

```
try {
    Cipher cipher = Cipher.getInstance(cipherTransformation);
    byte[] key = encryptionKey.getBytes(characterEncoding);
    SecretKeySpec secretKey = new SecretKeySpec(key, aesEncryptionAlgorithem);
    IvParameterSpec ivparameterspec = new IvParameterSpec(key);
    cipher.init(Cipher.DECRYPT_MODE, secretKey, ivparameterspec);
    Base64.Decoder decoder = Base64.getDecoder();
    byte[] cipherText = decoder.decode(Entext.getBytes("UTF8"));
    decryptedText = new String(cipher.doFinal(cipherText), "UTF-8");
    jLabel14.setText(decryptedText);

} catch (Exception E) {
    System.err.println("decrypt Exception : "+E.getMessage());
}
 try {
    BufferedWriter buf = new BufferedWriter(new FileWriter(fileout, false));
    buf.append(decryptedText);
    buf.close();
}catch (IOException e) {
    e.printStackTrace();
}
```

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

## ผลการ RUN