DES 加密實作 [張家成]

小組分工
A10615003 張家成 二資工四 —> 加密
A10615001 趙梓丞 二資工四 —> 解密

Data Encrypt Standard 實作 [Java]

- 建置環境

- MacOS Mojave 10.14.1
- Eclipse IDE for Java Developers [Version: Oxygen]
- Java SE 9.0.1

- 執行結果截圖

- **註釋 —output test— 後的結果**

```
< Data Encrypt Standard >
1.Please input the Plaintext [Please input 16 Hexadecimal eg.ABCDEF0123456789]
ABCDEF0123456789
2.Please input the Key [Please input 16 Hexadecimal eg.AFAFAFAFAFAFAFAF]
AFAFAFAFAFAFAFAF
Ciphertext:
4C30FC30FB2B0BFF
```

- 關於註釋

- 將代碼中 output test 的註釋取消，即可的到加密的過程中，數據在每一步的變化

```
//      plaintext(16) to binary
        String ptBinary = hex2binary(plaintext);
//      ---output test---
//      System.out.println("ptBinary:" + ptBinary);

        Scanner getKey = new Scanner(System.in);
        System.out.println("2.Please input the Key [Please input 16 Hexadecimal eg.AFAFAFAFAFAFAFAF]");
        String key = getKey.next();
//      key(16) to binary
        String keyBinary = hex2binary(key);
//      ---output test---
//      System.out.println("keyBinary:" + keyBinary);
```

- 困難與心得

- 當binary的String要轉換成int時會遇到 int無法存儲超過2^32次方的數
  - 解決方案：使用 Biginteger來存儲
- 當一個0開頭的String，轉成Biginteger時，開頭的0會被吞掉，直到最左邊是1
  - 解決方法：在每一個String轉Biginteger前加一個1，這樣就會比原來多一位，但是後續的操作是xor[異或]操作，兩個1會變成0，這樣就防止了兩個biginteger進行xor操作時，因為位數不同而造成不正確的結果。
- 如果得到的biginteger開頭的幾位都是0，那麼得到的位數將小於原本的位數。
  - 寫一個 getBit方法，設定位數，這樣就可以在biginteger轉String的時候還原真實的位數了。
  - ```
    public static int getBit(BigInteger b,int n) {
        return b.testBit(n)?1:0;
    }
    ```
  - ```
    //      防止biginteger類型的第一位是0
            for (int i = 0; i < 48; i++) {
                beforeSboxStr += getBit(beforSbox, 47-i);
            }
    //      ---output test---
    //      System.out.println("beforeSboxStr:"+beforeSboxStr);
    ```