Lab 3

Sunday, February 14, 2021 8:42 AM

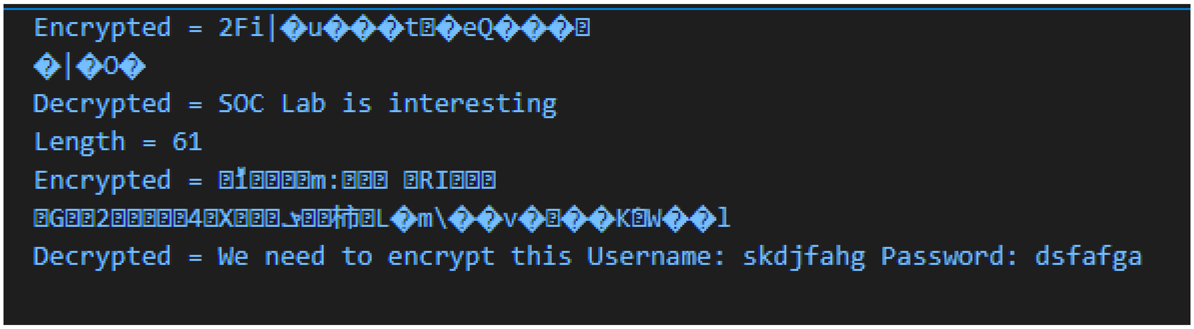
a. Encryption and decryption using **symmetric** key cryptography

- DES
- Size of key
- Raw data -> Cipher object -> encrypted output
- Symmetric key passed to the cipher object
- Key generator object

Check documentation at https://docs.oracle.com/javase/8/docs/api/

```
import java.io.*;
import java.security.Key;
import javax.crypto.*;

public class SymmetricCrypto
{
    public static void main(String[] args)throws Exception
    {
        //create KeyGenerator Object
        //generate a symmetric key from KeyGenerator Object
        //make use of cipher object for encryption
        KeyGenerator KeyGenObj = KeyGenerator.getInstance("DES");
        //static constructor
        SecretKey SymmetricKeyObj = KeyGenObj.generateKey();
        Cipher CipherObj = Cipher.getInstance("DES/ECB/PKCS5Padding");
        CipherObj.init(Cipher.ENCRYPT_MODE, (Key)SymmetricKeyObj);
        String toEncrypt = "SOC Lab is interesting";
        //convert to byte array (for encryption and decryption)
        byte[] toEncryptByte = toEncrypt.getBytes();
        byte[] encryptedBytes = CipherObj.doFinal(toEncryptByte);
        String encrypted = new String(encryptedBytes);
        System.out.println("Encrypted = " + encrypted);

        CipherObj.init(Cipher.DECRYPT_MODE, SymmetricKeyObj);
        byte[] DecryptedBytes = CipherObj.doFinal(encryptedBytes);
        String Decrypted = new String(DecryptedBytes);
        System.out.println("Decrypted = " + Decrypted);
        //reading from a file
        File FileObj = new File("FileForEncrypt.txt");
        int length = (int)FileObj.length();
        System.out.println("Length = " + length);
        FileInputStream inStreamObj = new FileInputStream(FileObj);
        byte[] dataRead = new byte[length];
        inStreamObj.read(dataRead, 0, length-1); //contains data read from file

        Cipher CipherObj2 = Cipher.getInstance("DES/ECB/PKCS5Padding");
        CipherObj2.init(Cipher.ENCRYPT_MODE, (Key)SymmetricKeyObj);
        encryptedBytes = CipherObj2.doFinal(dataRead);
        encrypted = new String(encryptedBytes);
        System.out.println("Encrypted = " + encrypted);
        CipherObj2.init(Cipher.DECRYPT_MODE, (Key)SymmetricKeyObj);
        DecryptedBytes = CipherObj.doFinal(encryptedBytes);
        Decrypted = new String(DecryptedBytes);
        System.out.println("Decrypted = " + Decrypted);
        inStreamObj.close();

    }
}
```

Output:



```
Encrypted = 2Fi|�u���t□�eQ���□
�|�O�
Decrypted = SOC Lab is interesting
Length = 61
Encrypted = □ǐ□□□□m:□□□ □RI□□□
□G□□2□□□□□4□X□□□␣□□□柿□L�m\��v�□���K□W��l
Decrypted = We need to encrypt this Username: skdjfahg Password: dsfafga
```