Nama : Novianto Hadi Raharjo

NIM : 1410652015

Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut.

ACCESS CONTROL

Access control memproteksi data terhadap unauthorize access atau akses yang dilakukan oleh orang yang memang tidak memiliki hak akses terhadap reource tersebut. Akses di sini bisa berupa melihat data (view) ataupun melakukan perubahan terhadapt suatu data (modify).

Dengan demikian Access Control mendukung terwujudnya

1. Confidentiality

Memastikan data hanya bisa dilihat oleh orang yang memiliki hak akses untuk melihat data tersebut atau dikenal dengan istilah No Unauthorized Read.

2. Integrity

Memastikan data hanya bisa ditulisi dan diubah oleh orang yang memiliki hak akses untuk melakukan penulisan ataupun pengubahan terhadap data tersebut atau dikenal dengan istilah No Unauthorized Write.

3. Available

Memastikan bahwa informasi tersedia bila diperlukan. Sistem harus tersedia untuk penggunaan s normal. Contoh dari serangan terhadap Available adalah Denial-of-Service (DoS) serangan, yang berusaha untuk menghentikan layanan (atau availability) dari suatu sistem.

Access Control Model terdiri dari

a. Discretionary access controls
   Discretionary access controls adalah memberikan subject control penuh terhadap object yang dimiliki untuk diakses, termasuk berbagi object dengan subject lain.
b. Mandatory access control
   Mandatory access controls adalah system yang memberikan control access terhadap object berdasarkan ijin dari subject. Seorang subject dapat mengakses object hanya jika subject memiliki ijin yang sama dengan atau lebih besar dari label object.
c. Nondiscretionary access control
   Role-Based Access Control(RBAC) mendefinisikan bagaimana informasi diakses pada system berdasarkan peran dari subject. RBAC adalah tipe nondiscretionary access control karena pengguna tidak mempunyai keleluasaan terhadap object yang mereka miliki untuk di akses dan tidak diijinkan untuk mentransfer object ke subject lain.

d. Rule-based access controls
   rule-based access control system menggunakan serangkaian aturan yang telah ditetapkan, pembatasan dan filter untuk mengakses object dalam suatu system. Aturan tersebut dibentuk dalam pernyataan “if/then”. Contoh dari perangkat rule-based access control adalah proxy firewall yang memungkinkan untuk mencari informasi di web dengan konten yang disetujui.

e. Centralized access control
   Access control yang berkonsentrasi pada satu titik logic system atau organisasi. Centralized access control dapat digunakan untuk menyediakan Single Sign-On dimana subjek hanya dapat melakukan sekali otentifikasi dan kemudian mengakses beberapa system.

TUGAS

Buatlah atau cari juga boleh, kode program yang membahas tentang keamanan data (enkripsi) menggunakan algoritma tertentu, kemudian dokumentasikan penggunaan program tersebut, beserta output dari programnya.

Algoritma yang digunakan pada enkripsi ini adalah aes-128 dengan Bahasa pemrograman JAVA, berikut kode programnya:

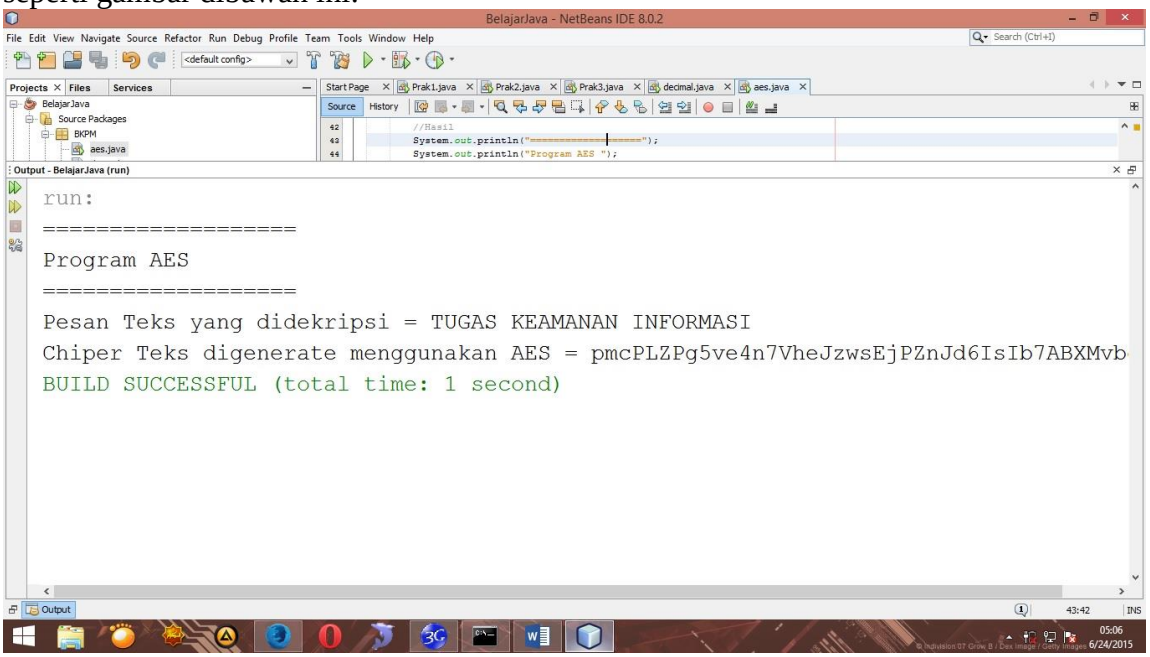
```
package BKPM;

import java.io.*;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.Cipher;
import java.security.NoSuchAlgorithmException;
import java.security.InvalidKeyException;
import java.security.InvalidAlgorithmParameterException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.BadPaddingException;
import javax.crypto.IllegalBlockSizeException;
import java.security.SecureRandom;
import sun.misc.BASE64Encoder;
class aes
{
 public static void main(String[] args)
 {
   DataInputStream dis=new DataInputStream(System.in);
   String strDataToEncrypt = new String();
   String strCipherText = new String();
   String strDecryptedText = new String();
   try
   {
     KeyGenerator keyGen = KeyGenerator.getInstance("AES");
     keyGen.init(128);
     SecretKey secretKey = keyGen.generateKey();
     Cipher aesCipher = Cipher.getInstance("AES");
     aesCipher.init(Cipher.ENCRYPT_MODE,secretKey);
     strDataToEncrypt = "TUGAS KEAMANAN INFORMASI";
     byte[] byteDataToEncrypt = strDataToEncrypt.getBytes();
     byte[] byteCipherText = aesCipher.doFinal(byteDataToEncrypt);
     strCipherText = new BASE64Encoder().encode(byteCipherText);
    aesCipher.init(Cipher.DECRYPT_MODE,secretKey,aesCipher.getParameters());
     byte[] byteDecryptedText = aesCipher.doFinal(byteCipherText);
     strDecryptedText = new String(byteDecryptedText);
     //Hasil
     System.out.println("====================");
     System.out.println("Program AES ");
     System.out.println("====================");
     System.out.println("Pesan Teks yang didekripsi = "+strDecryptedText);
     System.out.println("Chiper Teks digenerate menggunakan AES = "+strCipherText);
```

```
        }
        catch (NoSuchAlgorithmException noSuchAlgo)
        {
System.out.println(" No Such Algorithm exists " + noSuchAlgo);
        }
       catch (NoSuchPaddingException noSuchPad)
       {
          System.out.println(" No Such Padding exists " + noSuchPad);
        }
        catch (InvalidKeyException invalidKey)
        {
          System.out.println(" Invalid Key " + invalidKey);
        }
        catch (BadPaddingException badPadding)
        {
          System.out.println(" Bad Padding " + badPadding);
        }
        catch (IllegalBlockSizeException illegalBlockSize)
        {
          System.out.println(" Illegal Block Size " + illegalBlockSize);
        }
        catch (InvalidAlgorithmParameterException invalidParam)
        {
          System.out.println(" Invalid Parameter " + invalidParam);
        }
    }
}
```

Untuk dapat menjalankan file ini, terlebih dulu harus membuat nama package BKPM dan nama file aes.java, kemudian silahkan klik kanan pada file => run file, hasil dari run file

seperti gambar dibawah ini:



Plaintext dari program diatas ada di dalam kode program pada baris yang tercetak tebal(*bold*), untuk menggantinya cukup dengan mengganti tulisan yang tercetak tebal dan miring dengan kata yang di kehendaki. Pada contoh diatas plaintextnya adalah *TUGAS KEAMANAN INFORMASI* dan chipernya adalah *pmcPLZPg5ve4n7VheJzwsEjPZnJd6IsIb7ABXMvbq9Q=*