RESUME

UAS KEAMANAN INFORMASI KELAS TI-PAGI

oleh :

LUKMAN EFENDI
111 065 1073

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2015

SOAL

1. 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. Hasil resume tidak boleh sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.
2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

JAWABAN 1 :

1. Resume Kriptografi

Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

2. Jenis-Jenis Kriptografi

Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

- ✓ **Algoritma simetris**
  - Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama
- ✓ **Algoritma asimetris**
  - Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

3. Serangan Terhadap Kriptografi

Serangan terhadap kriptografi pada dasarnya adalah memecahkan (membongkar keamanan) algoritma kriptografi, yang selanjutnya digunakan untuk usaha mengupas data tersandi tanpa mengetahui/menggunakan kunci. Kegiatan ini (memecahkan algoritma kriptografi) adalah bagian dari kriptanalisis, yaitu ilmu/seni memecahkan data tersandi. Kripanalisis dan kriptografi merupakan sebuah cabang ilmu pengetahuan yang disebut kriptologi.

- ✓ **Enkripsi Simetris**

  adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok).

- ✓ **Enkripsi Asimetris**

  Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua

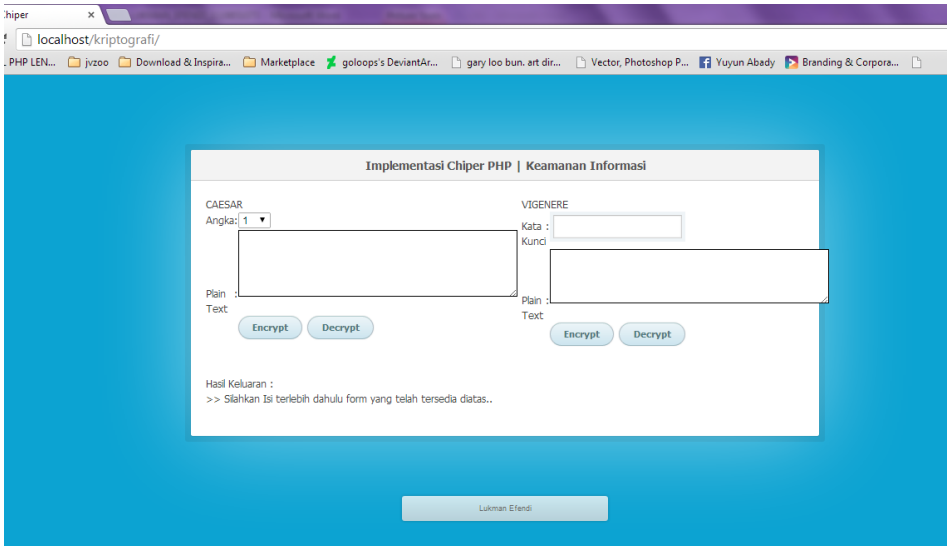
orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu – dalam hal ini kunci privat – untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

JAWABAN 2 :

2. Tools Kriptografi

Dalam menangani kasus pencurian data, maka dibuatlah tools yang bisa menangi pencurian data menggunakan kriptografi. Dalam kasus ini terdapat beberapa parameter yaitu tools ini berfungsi untuk mengirim sebuah pesan rahasia *(berisi teks ter-enkripsi)* kepada calon penerima kemudian memecahkan pesan tersebut oleh calon penerima agar pihak dari luar tidak bisa mengetahui peesan yang dikirimkan oleh pembuat pesan rahasia.

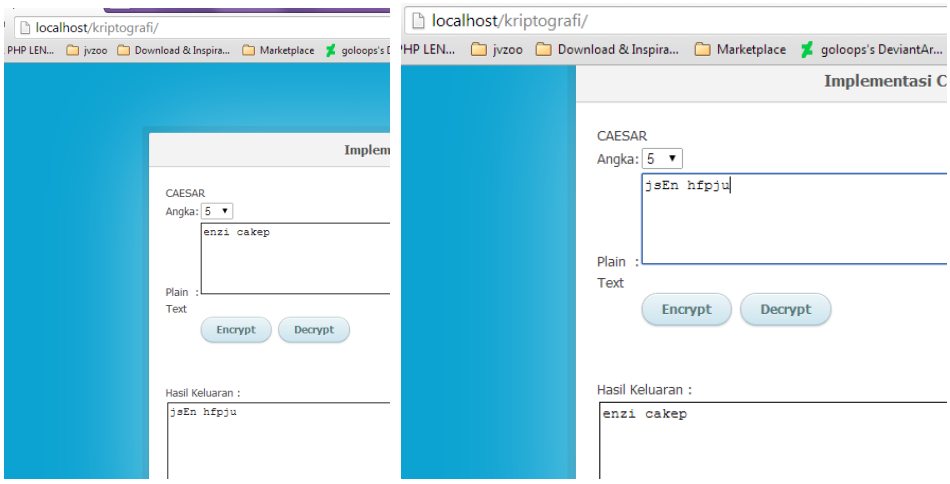
Contoh kasusnya dan penerapannya bisa dilihat bawah ini :



Terdapat beberapa metode yang pertama enkripsi menggunakan caesar dan yang kedua menggunakan vigenere.

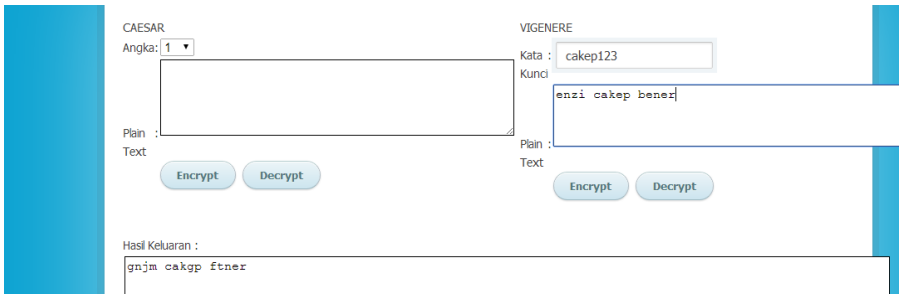
✓ **Pada Kasus Caesar**

terdapat kata kunci menggunakan angka, jadi urutannya akan disesuaikan oleh angka, dan untuk membuka pesan angka yang digunakan adalah harus sama terhadap encript dan decript.

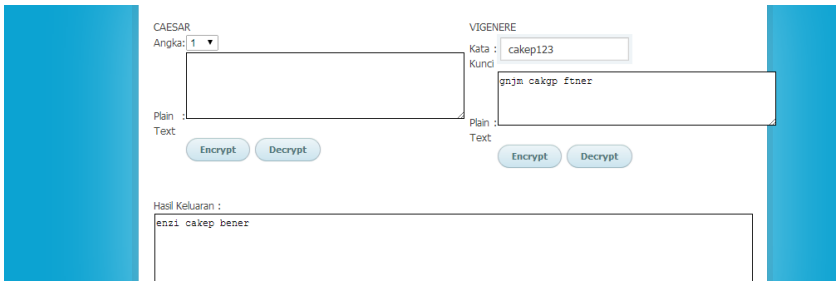


Pada keterangan gambar diatas digunakan pergerakan 5 angka dan meng encript sebuah kata dengan hasil keluaran seperti digambar. Dan gambar ke dua adalah hasi decript yang dilakukan dengan pergeseran angka yang sama, maka hasil yang di decipt akan sama.

✓ **Pada Kasus Vigenere**



Pada kasus vigenere kata kunci bisa berupa teks dan angka.



Pada gambar diatas merupakan enkripsi menggunakan vigenere. Hasil dan langkah-langkahnya sama dengan caesar namum di vigenere bisa juga menggunakan pergerakan dengan angka dan kombinasi huruf, dan terdapat perbedaan hasil dari keduanya.