Nama : Novi Yuli Astuti

NIM : 42420026

Prodi/Smt : Informatika/4

Matkul : Sistem Proteksi Data

Tugas!!!

Bedah Jurnal

Judul Jurnal

Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher

Keamanan informasi pada sebuah aplikasi sangatlah penting. Sistem keamanan sangat diperlukan pada sebuah aplikasi dan informasi penting yang tidak boleh diakses oleh sembarangan penerima pesan. Kriptografi merupakan salah satu cara yang bisa digunakan untuk mencegah kebocoran data yang bersifat rahasia dan mempermudah pemrosesan data (diperlukan sebuah aplikasi), aplikasi kriptografi berbasis web bisa dibangun dan digunakan untuk mempermudah pemrosesan data, selain itu aplikasi berbasis web dapat diakses dimana saja.

Secara umum ada dua jenis kriptografi, yaitu kriptografi klasik (simetrik) dan kriptografi modern (asimetrik).

- Pembuatan aplikasi berbasis web menggunakan PHP dengan algoritma vigenere cipher. Dalam pembuatan aplikasi ini akan menggunakan kriptografi klasik. Kriptografi klasik (simetrik) adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua Teknik dasar yang biasa dilakukan adalah substitusi dan transposisi. Teknik substitusi dilakukan dengan mengganti salah satu karakter yang ada dalam sebuah teks menggunakan karakter yang lain. Teknik yang termasuk dalam kategori substitusi adalah kriptografi Caesar. Kemudian ada sandi vigenere yang merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf yang lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi vigenere terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel vigenere, tabel vigenere berisi alfabet yang dituliskan dalan 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda sesuai kata kunci yang diulang. Sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan.

- Implementasi dan pengujian system dengan melakukan pengujian aplikasi yang telah dibuat dan membandingkan dengan aplikasi yang sudah ada.
  Dari hasil uji coba menggunakan aplikasi yang dikembangkan dan aplikasi online yang sudah ada dapat diketahui bahwa aplikasi hasil pengembangan memiliki kesesuaian dengan hasil test manual menggunakan tabel vigenere cipher sedangkan pada aplikasi online ditemukan ketidaksesuaian pada perulangan kata kunci dan cipertext.