ANALISA DAN PERANCANGAN SISTEM INFORMASI ENKRIPSI DATA DENGAN ALGORITMA VIGENERE CHIPER BERBASIS WEB

Samsul Makin[1], Dodi Rindiansyah[2], Muhammad Arif Kurniawan[3], Angger Styo Yuniarti[4], Andi Rukmana[5]

[1345]Dosen tetap, Universitas Insan Pembangunan Indonesia
Jl. Raya Serang KM. 10 Bitung-Tangerang
samsulmakin25@gmail.com[1] dodirindiansyah90@gmail.com [2] awan.insanpembangunan@gmail.com[3]
anggeryuniarti06@gmail.com [4] andi.rukmana@ipem.ac.id [5]

ABSTRACT

Cryptography is a field of knowledge that uses mathematical equations to perform encryption and decryption processes. This technique is used to convert data into certain codes, with the aim that the stored information cannot be read by anyone except those who have the right. In this study, a cryptography learning application was designed that implements encryption and decryption methods using the Vigenere cipher method. The results of the study are a cryptography learning application using the Vigenere cipher method that can encode secret messages and also help increase the understanding of users who want to learn about cryptography, especially the Vigenere cipher method.

***Keywords**: Cryptography, Encryption, Decryption, Vigenere, Web*

PENDAHULUAN

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting pada sebuah sistem pengiriman informasi. Dalam hal ini, sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi akan tidak berguna lagi apabila di tengah proses pengiriman, informasi itu disadap atau dibajak oleh orang yang tidak berhak.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Ilmu sandi (kriptografi) sendiri telah ada sejak lama. Tercatat dalam sejarah bahwa Julius Caesar, seorang kaisar Romawi menggunakan penyandian untuk menyampaikan pesan rahasia saat perang.

Enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan atau alat khusus. Sedangkan dekripsi merupakan algoritma atau cara yang dapat digunakan untuk membaca informasi yang telah dienkripsi untuk kembali dapat dibaca.

Sandi Vigenere sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf pada teks digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E dan seterusnya. Sandi Vigenere terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda.

Tujuan yang diinginkan dalam penelitian ini adalah memahami penggunaan sandi Vigenere untuk menyandikan pesan rahasia yang hendak dikirimkan tanpa takut dibaca oleh orang yang tidak memiliki hak dengan menggunakan aplikasi ini.

Pengertian Sistem Informasi

Menurut Sutabri (2012) menyatakan "sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang

bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan".

Pengertian Analisa

Menurut Rosa A. S-M.Shalahuddin (2011) mengatakan "kegiatan analisis sistem adalah kegiatan untuk melihat sistem yang sudah berjalan, melihat bagian mana yang bagus dan tidak bagus, dan kemudian mendokumentasikan kebutuhan yang akan dipenuhi dalam sistem yang baru".

Pengertian kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2006: 9).

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Vigenere Chiper

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Pengertian PHP

PHP adalah bahasa pemrograman *script server side* yang didesain untuk pengembangan *web*. Selain itu, PHP juga bisa digunakan sebagai bahasa pemrograman umum (wikipedia). PHP dikembangkan pada tahun 1995 oleh Rasmus Lerdorf dan sekarang dikelola oleh *The PHP Group*.

PHP disebut bahasa pemrograman *server side* karena PHP diproses pada komputer *server*. Hal ini berbeda dibandingkan dengan bahasa pemrograman *client-side* seperti *JavaScript* yang diproses pada *web browser* (*client*). Pada awalnya PHP merupakan singkatan dari *Personal Home Page*. Sesuai dengan namanya, PHP digunakan untuk membuat *website* pribadi. Dalam beberapa tahun perkembangannya, PHP menjelma menjadi bahasa pemrograman *web* yang *powerful* dan tidak hanya digunakan untuk membuat halaman *web* sederhana, tetapi juga *website* populer yang digunakan oleh jutaan orang seperti wikipedia, *wordpress*, joomla, dan lain-lain.PHP dapat digunakan dengan gratis (*free*) dan bersifat *Open Source*. PHP dirilis dalam lisensi PHP *License*, sedikit berbeda dengan lisensi GNU *General Public License* (GPL) yang biasa digunakan untuk proyek *Open Source.*

METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode analisa deskriptif. Metode analisa deskriptif adalah metode yang digunakan dengan cara menganalisa dan menguraikan untuk menggambarkan keadaan obyek yang diteliti yang menjadi pusat perhatian penelitian dalam suatu penelitian. Metode analisisi deskriptif secara hakekatnya adalah data yang telah terkumpul kemudian diseleksi, dikelompokkan, dilakukan pengkajian, interpretasi dan kesimpulan.Dengan menggunakan metode ini penulis dapat dengan mudah menemukan masalah-masalah yang terjadi pada sistem yang digunakan saat ini dan memecahkan masalah yang ditemukan.

Sumber data yang digunakan oleh penulis
Pada langkah ini, dilakukan pengumpulan data dan informasi dengan melakukan studi pustaka. Melalui teknik ini, dilakukan kegiatan penghimpunan data, keterangan, dan informasi dengan memahami secara cermat atas berbagai buku ilmiah, dan bahan-bahan tertulis maupun dari media internet lainnya yang relevan dengan sistem yang akan dirancang.

ANALISA DAN PEMBAHASAN

Analisa sistem

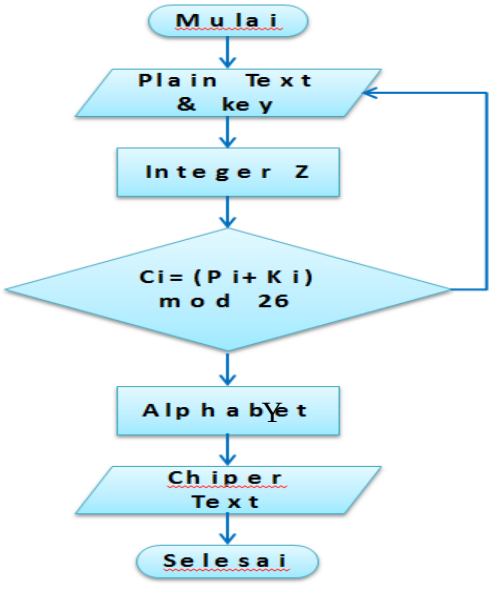
Aplikasi ini dibuat sesuai dengan harapan penulis untuk meningkatkan pemahaman pengguna yang ingin belajar kriptografi tentang metode sandi Vigenere. Kriptografi saat ini sangat diperlukan agar informasi yang dikirimkan tidak bisa dibaca ataupun disadap oleh orang yang tidak berhak. Dengan adanya aplikasi ini, pengguna dapat menambah pemahaman tentang sandi Vigenere dan juga dapat menggunakannya untuk mengamankan pesan dari orang yang tidak memiliki hak untuk membacanya.

Rancangan Sistem

Proses perancangan yang akan digunakan merupakan proses perancangan yang berorientasi pada prosedural, sehingga diperlukan flowchart serta perancangan tampilan. Untuk aplikasi ini, dirancang sistem yang dapat memproses karakter American Standard Code for Information Interchange (ASCII).

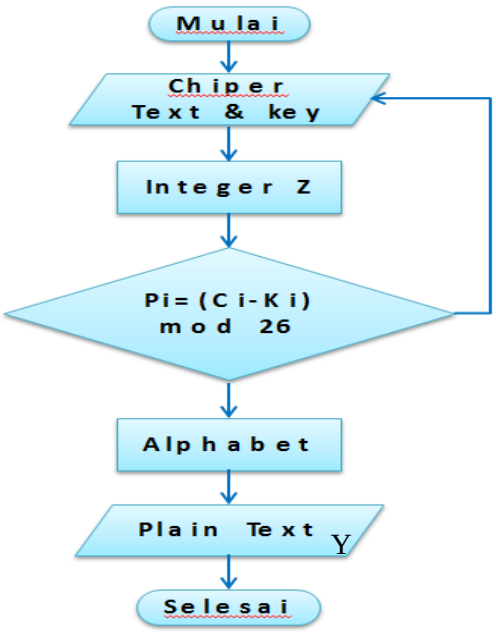
Flowchart Sistem Usulan

Flowchart untuk proses enkripsi dapat dilihat pada gambar 4.1 berikut:



Gambar 1 Flowchart Proses Enkripsi

Flowchart untuk proses dekripsi dapat dilihat pada gambar 4.2 berikut:



Gambar 2 Flowchart Proses Dekripsi

Hasil dan Pembahasan

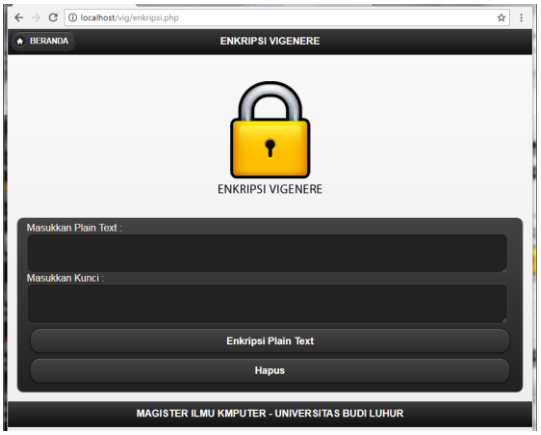
Untuk memulai aplikasi ini, pengguna dapat menghidupkan xampp terlebih dahulu. Kemudian buka browser dan kemudian ketik http://localhost/vig/index.php. Setelah itu akan muncul tampilan utama yang terlihat seperti gambar berikut:

Gambar 3 Menu Utama

Pada tampilan utama ini, terdapat tiga *menu* yaitu Enkripsi *Vigenere*, Dekripsi *Vigenere* dan sekilas tentang *Vigenere*.

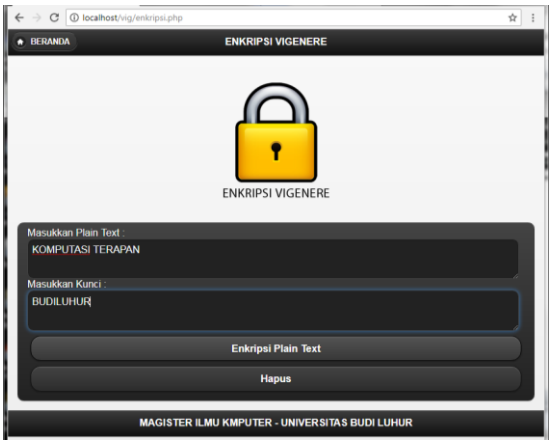
Proses Enkripsi

Jika pengguna akan melakukan enkripsi pesan, maka pilih menu enkrpsi Vigenere. Form tampilan enkripsi bisa dilihat pada gambar beikut:



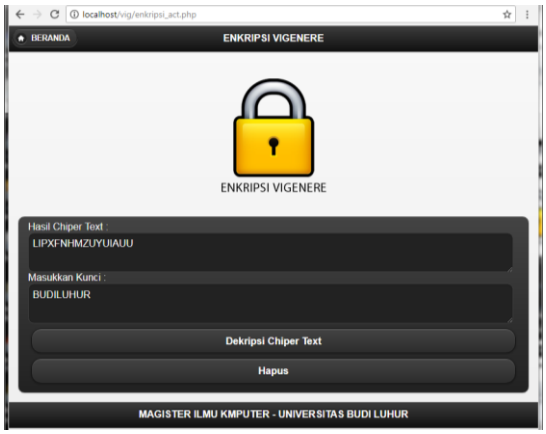
Gambar 4. Menu Enkripsi

Masukkan pesan yang akan dienkripsi, contoh "KOMPUTASI TERAPAN" dan maukkan kunci yang akan menjadi kunci rahasia, contoh "BUDILUHUR".



Gambar 5 Menu Proses Enkripsi

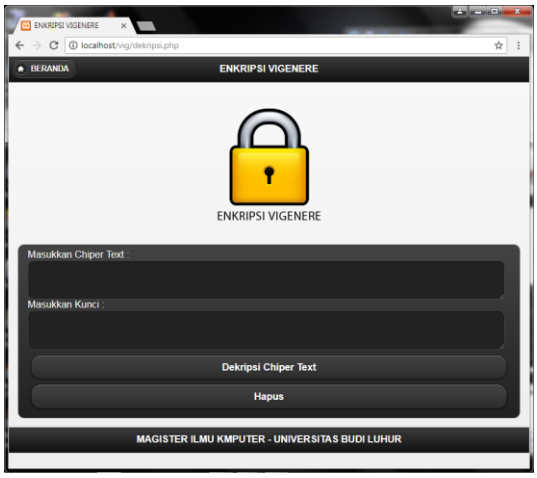
Kemudian tekan tombol "Enkripsi Plain Text", maka pesan tersebut berubah menjadi chipper text "LIPXFNHMZUYUIAUU". Berikut screenshoot gambar aplikasinya :



Gambar 6 Halaman Setelah Enkripsi

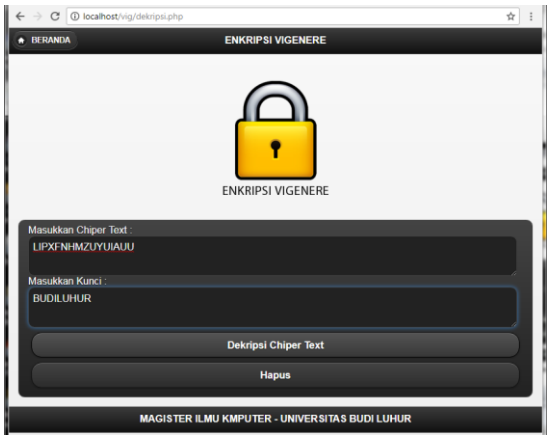
Proses Dekripsi

Jika pengguna akan melakukan dekripsi pesan rahasia, maka pilih menu Dekripsi Vigenere. Form tampilan Dekripsi bisa dilihat pada gambar beikut :



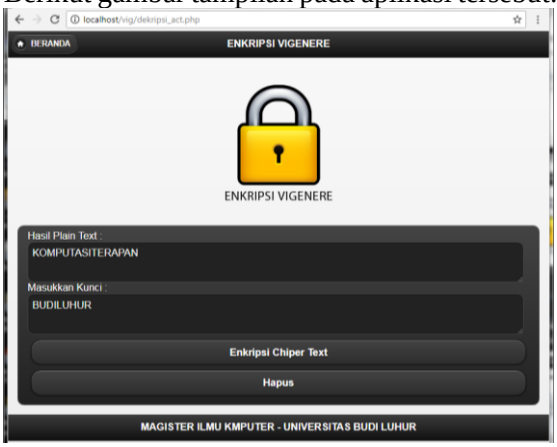
Gambar 7 Halaman Proses Dekripsi

Masukkan pesan rahasia yang sudah diterima yaitu "LIPXFNHMZUYUIAUU". Masukkan kunci rahasia yaitu "BUDILUHUR". "Kemudian tekan tombol Dekripsi Chiper Text"



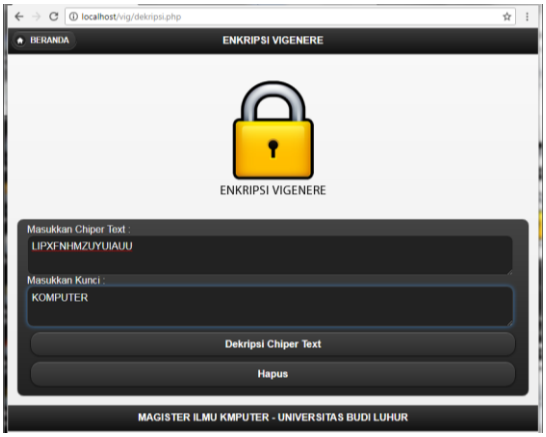
Gambar 8 Halaman setelah Dekripsi

Maka pesan rahasia tersebut akan berrubah menjadi pesan "KOMPUTASITERAPAN". Berikut gambar tampilan pada aplikasi tersebut:



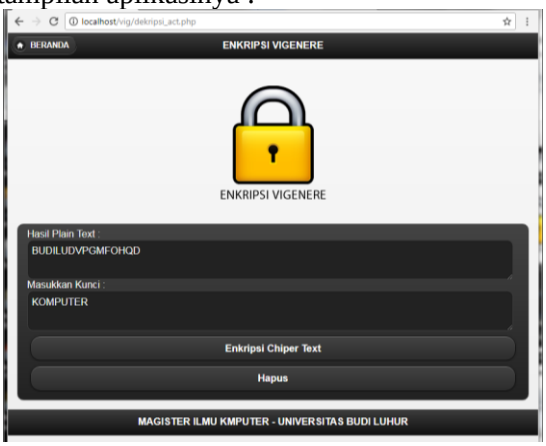
Gambar 9 Halaman setelah Dekripsi (Kunci Salah)

Jika kunci yang diberikan salah, makan pesan rahasia tidak bisa dibaca. Contoh pesan rahasia "LIPXFNHMZUYUIAUU", kunci "KOMPUTER".



Gambar 10 Halaman Proses Dekripsi (Kunci Salah)

Maka pesan yang ditampilkan yaitu "BUDILUDVPGMFOHQD", dan pesan tersebut tidak mempunyai arti. Berikut gambar tampilan aplikasinya :



Gambar 4.11Halaman setelah Dekripsi (Kunci Salah)

KESIMPULAN

Setelah penulis melakukan penelitian pada manual *service control board* di PT. XYZ, penulis dapat mengambil kesimpulan sebagai berikut:

a. Aplikasi pembelajaran kriptografi metode sandi Vigenere ini dapat menghasilkan pesan yang bersifat rahasia dimana informasi atau isi dari pesan tersebut tidak akan mudah diketahui oleh pihak yang tidak memiliki hak akses dan juga dapat menambah pemahaman pengguna mengenai kriptografi dengan metode sandi Vigenere.
b. Dalam menggunakan kriptografi, kunci harus tetap dijaga kerahasiaannya. Sedangkan algoritmanya dapat diketahui oleh siapapun tanpa mempengaruhi keamanannya. Kunci yang digunakan untuk mengenkripsi plain text sama dengan kunci yang digunakan untuk mendekripsi cipher text. Apabila kunci yang digunakan untuk mendekripsikan tidak sama dengan kunci yang digunakan untuk mengenkripsikan, maka hasil pendekripsian tidak akan sama dengan plain text semula sebelum dienkripsi.

c. Hasil dekripsi dari cipher text dengan menggunakan kunci yang sama saat melakukan enkripsi, akan menghasilkan plain text yang sama dengan plain text sebelum dienkripsi.

DAFTAR PUSTAKA

Ariyus, D., (2010). Kriptografi. Yogyakarta: Graha Ilmu.

Munir, R., (2011), Kriptografi. Bandung: Informatika.

Raharjo, Budi. (2011). Belajar Otodidak Membuat Data Menggunakan MYSQL. Bandung: Informatika.

S, Rosa, A Dan Shalahuddin, M. (2013). Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek). Bandung: Informatika.

Http://berbagi-ilmu-mifa309.blogspot.com/2012/05/pengertian-aplikasi.html, tanggal akses 2 Mei 2018.

Http://bwahyudi.staff.gunadarma.ac.id/Downloads/files/13543/kriptografi-01.doc, tanggal akses 2 Mei 2018.

Http://id.wikipedia.org/wiki/Aplikasi, tanggal akses 4 Mei 2018.

Http://id.wikipedia.org/wiki/Sandi_Vigenere, tanggal akses 4 Mei 2018.

Http://mzivara.blogspot.com/2011/04/desain-dan-analisis-keamanan-jaringan.html, tanggal akses 9 Me1 2018.

Http://sun-coolin.blogspot.com/2012/07/algoritma-kriptografi-klasik-vigenere-cipher.html, tanggal akses 9 Mei 2018.

Http://www.erdisusanto.com/2012/10/konsep-dasar-kriptografi-simetris-dan.html, tanggal akses 11 Mei 2018.