e-ISSN : 2722-4368

Penerapan Metode Vigenere Chiper untuk Mengamankan Data Text

Dicky Arfandy[1)], Magdalena Simanjuntak[2)], Tio Pasaribu[3)]
[123]STMIK Kaputama
Jl.Veteran No. 4A-9A, Binjai, Sumatera Utara
e-mail: dickyarfandy@gmail.com

Abstract- *The development of technology in security systems to ensure the confidentiality of data information has grown rapidly. In maintaining the confidentiality of data information, there are sciences in development such as steganography and cryptography. Data and information security is very important in the current reform era. Generally, every institution has important and confidential documents that can only be accessed by certain people. The issue of data security and confidentiality is one of the important aspects of an information delivery system. In this case, it is closely related to how important the information is sent and received by interested people. Information will no longer be useful if in the middle of the delivery process, the information is intercepted or hijacked by unauthorized people. Computer crime is the illegal act of using knowledge of computer technology to commit a crime. Theft of hardware and software (hardware and software), manipulation of data, illegal access to computer systems by telephone, and changing programs.*

Keywords*: Cryptography, PHP, Text, Vigenere Chiper.*

Abstrak- Perkembangan teknologi dalam sistem pengaman untuk menjamin kerahasiaan informasi data sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti *steganografi* dan *kriptopgrafi*. Keamanan data dan informasi merupakan hal sangat penting di era reformasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. 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. Kejahatan komputer adalah tindakan ilegal dengan menggunakan pengetahuan teknologi komputer untuk melakukan tindak kejahatan. Pencurian perangkat keras dan perangkat lunak *(hardware* dan *software*), manipulasi data, pengaksesan sistem komputer secara ilegal dengan telepon, dan mengubah program.

Kata Kunci : Kriptogafi, PHP, Text, *Vigenere Chiper*.

PENDAHULUAN

Perkembangan teknologi dalam sistem pengaman untuk menjamin kerahasiaan informasi data sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti *steganografi* dan *kriptopgrafi*. Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi algoritma(Ginting, 2020). Kejahatan komputer adalah tindakan ilegal dengan menggunakan pengetahuan teknologi komputer untuk melakukan tindak kejahatan. Pencurian perangkat keras dan perangkat lunak *(hardware* dan *software*), manipulasi data, pengaksesan sistem komputer secara ilegal dengan telepon, dan mengubah program.

Keamanan data dan informasi merupakan hal sangat penting di era reformasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan seringkali dapat disadap oleh pihak lain (PATRICIA, 2015). 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(Irawan, 2017). Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi, disertai dengan menggunakan kunci yang benar.

Olehkarena itu peneliti merekomendasikan algoritma *Vigenere Chiper* untuk dapat memberikan keamanan pada Data text. Pada bidang *kriptografi*, Sandi *Vigenère Chiper* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi *Vigenère* merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi.

METODOLOGI

2.1 Penelitian Terdahulu

Penelitian ini didasari dari beberapa acuan untuk dijadikan sumber referensi sebagai berikut "Teknik Keamanan Data Menggunakan Kriptografi Dengan Algoritma *Vigenere Cipher* Dan *Steganografi* Dengan Metode End Of File (EOF)". Metodologi yang digunakan dalam melakukan penelitian ini menggunakan pengumpulan dokumen, studi pustaka dan eksperimen. Pengumpulan dokumen selayaknya guna mendapatkan dokumen input untuk diproses menghasilkan output serta dokumen untuk kelancaran penelitian. Dokumen yang digunakan pada penelitian ini seperti dokumen proses analisa sistem, desain proses, pembuatan kode program dan aplikasi sampai dengan pengujian aplikasi menggunakan Metode *Vigenere Chiper*. Studi pustaka bermanfaat mendapatkan referensi penelitian yang telah dilakukan sebelumnya yang berhubungan dengan penelitian saat ini dilaksanakan untuk diterapkan metode tersebut dalam penelitian. Eksperimen dilakukan dengan memasukan plaintext secara acak (random) dan disimpan ke dalam File Teks (TXT) untuk diproses dengan Metode *Vigenere Chiper* baik saat enkripsi maupun dekripsi serta membandingkan hasil dekripsi dengan isi dokumen asal plaintex(PATRICIA, 2015:2-3).

"Implementasi Kriptografi *Vigenere Chiper* Dengan PHP", Penelitian ini dilakukan untuk membuat implementasi kriptografi *vigenere Chiper*. Sistem ini dirancang dengan melakukan analisa dengan metode deskriptif, dan metode komperatif. Setelah dilakukan analisa, maka dilakukan pemodelan dengan UML (*Unified Modelling Language)* dan dilakukan perancangan sistem kriptografi *vigenere cipher* dengan bentuk enkripsi dan dekripsi text yang dapat diprogram dengan menggunakan software PHP. Hasil penelitian ini adalah sebuah implementasi sistem kriptografi *vigenere cipher* dengan PHP.(Irawan, 2017:11-12)

"Penerapan Algoritma *Vigenere Cipher* Dan *Hill Cipher*", Menggunakan Satuan Massa Penelitian ini dilakukan untuk menerapkan algoritma *vigenere chipper* untuk satuan masa, Sistem ini dirancang untuk pengaman data untuk menjamin kerahasiaan informasi data sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti *steganografi* dan *kriptopgrafi.* Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi *algoritma*. Penelitian ini bertujuan untuk membuat sistem keamanan data dengan melakukan penerapan modifikasi *algoritma vigenere cipher* dan *hill cipher*. Hasil dari penelitian ini sendiri berupa Proses *Enkripsi* dengan menggunakan metode gabungan seperti *Algoritma Vigenere Cipher* dan *Algoritma Hill Cipher* dapat dilakukan dan Menggabungkan dua metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. hal ini dapat memudahkan bagi pengirim pesan untuk menyampaikan pesan yang bersifat rahasia ke penerima(Ginting, 2020:241-242).

"Aplikasi Kriptografi Pesan Menggunakan Algoritma *Vigenere Cipher*", Penelitian ini dilakukan untuk menerapkan algoritma *vigenere chipper* mengaman kan pesan, Salah satu hal yang paling penting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, atau informasi dalam pertukaran data, sehingga menjadisalah satu

pendorong munculnya teknologi kriptografi. Algoritma kriptografi berdasarkan data pengkodean informasi yang mendukung kebutuhan dua aspek keamanan informasi, yaitu kerahasiaan (perlindungan kerahasiaan data informasi) dan keaslian (Perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan.) Penerapan teori - teori yang diperoleh di perguruan tinggi dalam pembuatan aplikasi ini untuk melaksanakan pesan terenkripsi lebih aman. Dalam pembuatan aplikasi kriptografi ini, metode yang digunakan adalah *Vigenere Cipher*, salah satu bentuk lain dari enkripsi jenis poly abjad. Aplikasi dibuat dengan perangkat lunak Visual Basic 6.0 dan pembuatan aplikasi dengan enkripsi diharapkan untuk mengatasi permasalahan tersebut(Studi et al., 2014:120-121).

"Kriptografi Simetris Menggunakan Algoritma *Vigenere Cipher*", Penelitian ini dilakukan untuk menerapkan algoritma *vigenere chipper* untuk mengamankan pesan text, Keamanan informasi pada sebuah aplikasi sangatlah penting, sistem keamanan sangat diperlukan pada sebuah aplikasi karena di sebagian perusahaan atau bahkan di suatu negara membutuhkan keamanan informasi , dan informasi penting yang tidak boleh di akses oleh sembarangan penerima pesan harus di amankan. Untuk megamankan informasi tersebut dibutuhkan suatu algoritma yang dapat menyamarkan pesan penting agar tidak bisa dibaca oleh pihak yang tidak memiliki hak untuk menerima informasi tersebut. Kriptografi merupakan salah satu cara yang bisa digunakan untuk memproteksi pengiriman data, data yang dikirim akan dirubah menjadi kode tertentu dan hanya bisa dibuka oleh penerima yang memiliki kunci untuk merubah kode itu kembali sehingga kerahasian pesan atau informasi tetap dapat dijaga, dan untuk mempermudah pemrosesan data diperlukan sebuah aplikasi, aplikasi kriptografi berbasis web bisa dibangun dan digunakan untuk mempermudah pemrosesan data, selain itu aplikasi berbasis web dapat di akses dari mana saja.(Amrulloh & Ujianto, 2019:71-72).

2.2 Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem *kriptografi*. Sistem *Kriptografi* (Cryptosystem) adalah kumpulan dari fungsi *enkripsi* dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi[3]. Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi. (Gunawan, 2018 : 125).

2.3 Keamanan

Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap seorang teroris, keamanan komputer terhadap hacker, keamanan rumah terhadap maling dan penyusup lainnya, keamanan financial terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. Host Komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada host yang tidak berhubungan kemana-mana. Dengan mengendalikan network security resiko tersebut dapat dikurangi. (Santoso dan Fakhriza, 2018 : 48).

2.4 Algoritma Vigenere Cipher

Algoritma *Vigenere Cipher* ini menggunakan bujursangkar *Vigenere* untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf *cipher*text yang diperoleh dengan Caesar *cipher*. Pada proses enkripsi *Vigenere Cipher* ini selain menggunakan Tabula Recta untuk mendapatkan *cipher*text juga dapat menggunakan rumus berikut:

Ci = (Pi + Ki) mod 26

Sedangkan untuk rumus dekripsi *Vigenere Cipher*:

Pi = (Ci – Ki) mod 26

Dimana : Ci= *cipher* teks
Pi = plainteks
Ki = kunci

e-ISSN : 2722-4368

HASIL DAN PEMBAHASAN

3.1 Perhitungan

Diketahui Plaintext " This Plaintext" dengan kunci "sony". Maka untuk melakukan proses enskripsi menggunakan perhitungan seperti dibawah ini :

Langkah Pertama membuat tabel konversi *vigenere* :

Ciphertext : THIS PLAINTEXT

Kunci : SONY

Penerima memilih kata THIS PLAINTEXT yang akan digunakan untuk melakukan proses enkripsi menggunakan algoritma *vigenere cipher*, sehingga pada prosesnya kata SONY akan mengikuti banyak karakter chipertext 1 yang didapat.

Ciphertext : THIS PLAINTEXT

Kunci : SONY

Selajutnya akan dienkripsi dengan algoritma *vigenere cipher* yaitu :

C = P + K mod 26

Dalam hal ini plaintext adalah ciphertext 1 yang didapat :

C1 = T + S mod 26
= 84 + 83 mod 26
= 89 = Y

C2 = H + O mod 26
= 72 + 79 mod 26
= 73 = I

C3 = I + N mod 26
= 73 + 78 mod 26
= 73 = I

C4 = S + Y mod 26
= 83 + 89 mod 26
= 94 = ^

C5 = P + S mod 26
= 80 + 83 mod 26
= 85 = U

C6 = L + O mod 26
= 76 + 79 mod 26
= 77 = M

C7 = A + N mod 26
= 65 + 78 mod 26
= 65 = A

C8 = I + Y mod 26
= 73 + 89 mod 26
= 84 = T

C9 = N + S mod 26
= 78 + 83 mod 26
= 83 = S

C10 = T + O mod 26
= 84 + 79 mod 26
= 85 = U

C11 = E + N mod 26
= 69 + 78 mod 26
= 69 = E

C12 = X + Y mod 26
= 88 + 89 mod 26
= 99 = c

C13 = T + S mod 26

e-ISSN : 2722-4368

= 84 + 83 mod 26
= 89 = Y

Maka didapatlah hasil enkripsi menjadi : YII^UMATSUEcY

Kemudian dilanjutkan dengan mendeskripsikan kembali hasil enkripsi tersebut dengan rumus sebagai berikut :

P = C - K mod 26

Dalam hal ini plaintext adalah ciphertext 1 yang didapat :

P1 = Y - S mod 26
= 89 – 83 mod 26
= 84 = T

P2 = I - O mod 26
= 73 – 79 mod 26
= 72 = H

P3 = I - N mod 26
= 73 – 78 mod 26
= 73 = I

P4 = ^ - Y mod 26
= 94 – 89 mod 26
= 83 = S

P5 = U - S mod 26
= 85 – 83 mod 26
= 80 = P

P6 = M - O mod 26
= 77 – 79 mod 26
= 76 = L

P7 = A - N mod 26
= 65 – 78 mod 26
= 65 = A

P8 = T - Y mod 26
= 84 – 89 mod 26
= 73 = I

P9 = S - S mod 26
= 83 – 83 mod 26
= 78 = N

P10 = U - O mod 26
= 85 – 79 mod 26
= 84 = T

P11 = E - N mod 26
= 69 – 78 mod 26
= 69 = E

P12 = c - Y mod 26
= 99 – 89 mod 26
= 88 = X

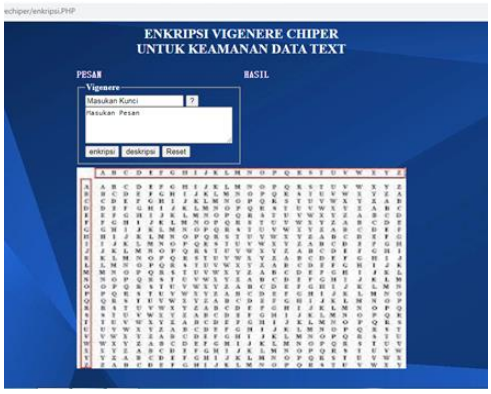
P13 = Y - S mod 26
= 89 – 83 mod 26
= 84 = T

Maka didapatlah hasil deskripsi menjadi : THIS PLAINTEXT

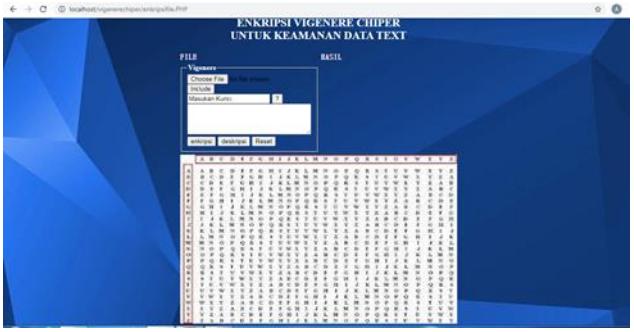
e-ISSN : 2722-4368

Gambar 1. Tampilan Halaman Login

Gambar 2. Tampilan Halaman Utama Sistem



Gambar 3. Tampilan Menu Proses Vigenere Cipher



Gambar 4. Tampilan Menu Proses Upload Text

KESIMPULAN

Setelah penulis melakukan analisis, perancangan, implementasi dan pengujian system pada penelitian yang berjudul Penerapan Metode *Vigenere Chiper* Untuk Mengamankan Data Text, dapat ditarik kesimpulan sebagai berikut:

1. Dengan adanya aplikasi keamanan data text maka data text dapat diamankan dengan baik.
2. Sistem yg dirancang ini dapat mengamankan data text dengan baik dikarenakan menggunakan metode *vigenere Chiper*.

e-ISSN : 2722-4368

3. Sistem ini dapat mengamankan data text dengan metode *vigenere Chiper*

DAFTAR PUSTAKA

[1] Arif Amrulloh, Kriptografi Simetris Menggunakan Algoritma *Vigenere Cipher*, Jurnal CoreIT, Vol.5, No.2, Desember 2019

[2] Efrandi, Aplikasi Kriptografi Pesan Menggunakan Algoritma *Vigenere Cipher*, Jurnal Media Infotama Vol. 10 No. 2, September 2014

[3] Muhammad Dedi Irawan**,** Implementasi Kriptografi *Vigenere Cipher* Dengan Php, JURNAL TEKNOLOGI INFORMASI (JurTI)Volume 1, Nomor 1, Juli 2017

[4] Patricia Handoko, Teknik Keamanan Data Menggunakan Kriptografi Dengan Algoritma *Vigenere Cipher* Dan Steganografi Dengan Metode End Of File (Eof), Fakultas Ilmu Komputer, Universitas Dian Nuswantoro,2015

[5] Victor Saputra Ginting, Penerapan Algoritma *Vigenere Cipher* Dan Hill *Cipher* Menggunakan Satuan Massa, (Jurnal Teknologi Informasi) Vol.4, No.2, Desember 2020