STUDI DAN IMPLEMENTASI ALGORITMA *CAESAR CIPHER* UNTUK KEAMANAN PESAN *EMAIL* YANG BERSIFAT RAHASIA

Cytra Nakasohsie [1], Diana [2] , Vivi Sahfitri [3]
Dosen Universitas Bina Darma [1], Mahasiswa Universitas Bina Darma [2]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : cytranakashoshie@yahoo.co.id [1], cytra.dinata@yahoo.co.id [2], cytra_astaga@yahoo.com [3]

Abstract : *The development of internet technology so rapidly has been a huge benefit. One result of internet technology that is very popular is the email. With email facilities that users can exchange information in the form of text messages with other users. In General, the email does not guarantee the confidentiality and integrity of messages sent by the user. Because text messages sent are sometimes secret messages and personal, so that the confidentiality of the message becomes very important. So the necessary of a system of security in the message conveyed. In this case the message is presented by way of application security encryption algorithms caesar cipher in an e-mail message by using the PHP programming language, so that the confidentiality of the message becoming more awake.*

Keywords: *email, encryption, decryption, caesar, cipher, php*

Abstrak *: Perkembangan teknologi internet begitu pesat telah menjadi manfaat besar. Salah satu hasil dari teknologi internet yang sangat terkenal adalah email. Dengan fasilitas email bahwa pengguna dapat bertukar informasi dalam bentuk pesan teks dengan pengguna lain. Secara umum, email tidak menjamin kerahasiaan dan integritas dari pesan yang dikirim oleh pengguna. Karena teks pesan yang dikirim kadang-kadang adalah pesan rahasia dan pribadi, sehingga kerahasiaan pesan menjadi sangat penting. Sehingga diperlukan suatu sistem keamanan dalam pesan menyampaikan. Dalam hal ini pesan akan disajikan dengan cara aplikasi keamanan algoritma enkripsi caesar cipher pada pesan email dengan menggunakan bahasa pemrograman PHP, sehingga kerahasiaan pesan menjadi lebih terjaga.*

Kata kunci*: email, enkripsi, dekripsi, caesar, cipher, php*

1. PENDAHULUAN

Dunia internet pada era sekarang ini sangatlah luas penggunaan dan perkembangannya, salah satu fasilitas dan layanan yang sangat vital dalam dunia internet adalah pesan *email*. *Email* pada dasarnya hanyalah sebuah pesan elektronik yang dikirimkan melalui media jaringan internet. Dengan adanya *email*, proses pengolahan, penyimpanan serta pendistribusian data dan informasi sangatlah mudah dilakukan dan digunakan oleh semua kalangan lapisan masyarakat. Aspek kemudahan yang di dapat tersebut ternyata berbanding berbalik dengan faktor *confidentiality* (kerahasiaan), *integrity* dan *availability* (ketersediaan).

Proses pengiriman *email* melalui media internet pada dasarnya hanyalah melakukan data tanpa melakukan pengamanan terhadap konten dari data yang dikirim, sehingga ketika dilakukan penyadapan pada jalur pengirimannya maka data yang disadap dapat langsung dibaca oleh penyadap, maka data yang dikirim diacak dengan menggunakan metode penyandian

tertentu sehingga pesan yang terkandung dalam data yang dikirim tersebut menjadi lebih aman.

Banyak sekali cara-cara yang ditempuh untuk memperkuat pengamanan seperti penggunaan auntentikasi *user* dan password berlapis pada *email*, namun tetap saja kerahasiaan dari isi data dan informasinya belumlah bisa dikatakan aman dan terlindungi apabila jatuh kepada orang yang tidak bertanggung jawab. Adapun usaha yang dapat dilakukan untuk mengurangi kejahatan *cyber* dalam hal pencurian pesan *email* yaitu dengan memperkuat sistem keamanan komputer, dengan cara membuat algoritma penyandian yang lebih kuat terhadap serangan. Ukuran dari kekuatan algoritma penyandian tersebut adalah banyaknya usaha yang diperlukan dalam melakukan pemecahan dari kunci sandi tersebut.

Pengiriman data dan penyimpanan data melalui *email* memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan ditujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan. Enkripsi dilakukan saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui dan dibaca oleh penerima setelah data tersebut telah diterjemahkan dengan menggunakan kunci rahasia.

Berawal dari latar belakang masalah tersebut, maka penulis mangambil judul "Studi dan Implementasi Algoritma *Caesar Cipher* Untuk Keamanan Pesan *Email* yang Bersifat Rahasia".

Berdasarkan latar belakang yang telah dijelaskan, maka penulis merumuskan permasalahan yaitu "Bagaimana mengimplementasikan algoritma *caesar cipher* dalam menjaga keamanan pesan *email* agar pihak yang tidak berwenang tidak dapat memecahkan informasi yang terdapat dalam data yang telah disadap sehingga keamanan dan kerahasiaan data tetap terjaga".

Untuk mengidentifikasi masalah dan pembahasan supaya lebih terarah dan tidak menyimpang, penulis akan memberikan beberapa batasan masalah, sebagai berikut :

1. Mengimplementasikan algoritma *caesar cipher* dengan menggunakan bahasa pemrograman *PHP*.
2. Dalam mengimplementasikan algoritma *caesar cipher*, tahapan yang dilakukan dimulai dari desain tampilan , generasi kode, dan pengujian sistem.
3. Aplikasi *caesar cipher* ini nanti memiliki beberapa kebutuhan yang meliputi :
    a. Memiliki kemampuan mengirimkan pesan ke *email.*
    b. Memiliki kemampuan untuk menenkripsi pesan.
    c. Memiliki kemampuan untuk mendekripsi pesan.

d. Dalam pengamanan data hanya sebatas integritas data.

Sesuai dengan konsep yang ada, untuk menyelesaikan hasil penelitian maka tujuan penelitian yang hendak dicapai yaitu mengimplementasikan algoritma *caesar cipher* dalam bentuk system yang dapat menjaga kerahasiaan dan keamanan pesan *email*.

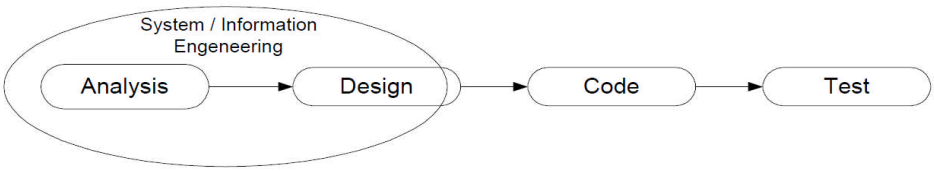
2. METODOLOGI PENELITIAN

Dalam pengerjaan penelitian ini, digunakan metode penelitian dengan tahapan-tahapan sebagai berikut :

Dalam teknik ini, penulis mengumpulkan dan mencari referensi materi yang penulis bahas dari buku-buku dan mengutip dari sumber-sumber yang berhubungan dengan penulisan ini.

2.1 Metode Pengembangan Sistem

Metode yang digunakan untuk mengimplementasikan algoritma *caesar cipher* kedalam bentuk aplikasi adalah *Sequential Linier Model Process* atau juga dikenal dengan nama Model Linier Sekuensial yang memiliki tahapan-tahapan yaitu : rekayasa pemodelan sistem atau informasi, analisis kebutuhan, desain, generasi kode, pengujian serta pemeliharaan.



Rekayasa dan pemodelan sistem/informasi. Karena perangkat lunak selalu merupakan bagian dari sebuah sistem yang lebih besar, kerja dimulai dengan membangun syarat dari semua elemen sistem dan mengalokasikan beberapa subset dari kebutuhan ke perangkat lunak tersebut.

Analisis kebutuhan perangkat lunak. Proses pengumpulan kebutuhan diintensifkan dan difokuskan, khususnya pada perangkat lunak. Untuk memahami sifat program yang dibangun, perekayasa perangkat lunak (analis) harus memahami domain informasi, tingkah laku, unjuk kerja, dan antar muka (interface) yang diperlukan. Kebutuhan baik untuk sistem maupun perangkat lunak didokumentasikan dan dilihat lagi dengan pelanggan.

Desain. Desain perangkat lunak sebenarnya adalah proses multi langkah yang berfokus pada empat atribut sebuah program yang berbeda; struktur data, arsitektur perangkat lunak, representasi *interface*, dan detail (algoritma) prosedural. Proses desain menerjemahkan syarat/kebutuhan ke dalam sebuah representasi perangkat lunak yang dapat diperkirakan demi kualitas sebelum dimulai pemunculan kode. Sebagaimana persyaratan,

desain didokumentasikan dan menjadi bagian dari konfigurasi perangkat lunak.

Generasi Kode. Desain harus diterjemahkan ke dalam bentuk mesin yang bisa dibaca. Langkah pembuatan kode melakukan tugas ini. Jika desain dilakukan dengan cara yang lengkap, pembuatan kode dapat diselesaikan secara mekanis.

Pengujian. Sekali kode dibuat, pengujian program dimulai. Proses pengujian berfokus pada logika internal perangkat lunak, memastikan bahwa semua pernyataan sudah diuji, dan pada eksternal fungsional – yaitu mengarahkan pengujian untuk menemukan kesalahan-kesalahan dan memastikan bahwa input yang dibatasi akan memberikan hasil aktual yang sesuai dengan hasil yang dibutuhkan.

Pemeliharaan. Perangkat lunak akan mengalami perubahan setelah disampaikan kepada pelanggan. Perubahan akan terjadi karena kesalahan-kesalahan ditentukan, karena perangkat lunak harus disesuaikan untuk mengakomodasi perubahan-perubahan di dalam lingkungan eksternalnya, atau karena pelanggan membutuhkan perkembangan fungsional atau unjuk kerja. Pemeliharaan perangkat lunak mengaplikasikan lagi setiap fase program sebelumnya dan tidak membuat yang baru lagi

Model sekuensial linier adalah paradigma rekayasa perangkat lunak yang paling luas dipakai dan paling tua. Masalah-masalah yang kadang-kadang terjadi ketika model sekuensial linier diaplikasikan adalah :

1. Jarang sekali proyek nyata mengikuti aliran sekuensial yang dianjurkan oleh model ini. Meskipun model linier bisa mengakomodasi iterasi, model itu melakukannya dengan cara tidak langsung.
2. Kadang-kadang sulit bagi pelanggan untuk menyatakan semua kebutuhannya secara eksplisit.
3. Pelanggan harus bersikap sabar. Sebuah versi kerja dari program-program itu tidak akan diperoleh sampai akhir waktu proyek dilalui.
4. Pengembang sering melakukan penundaan yang tidak perlu. Bradac mendapatkan bahwa pada model ini banyak anggota tim proyek haus menunggu tim yang lain untuk melengkapi tugas yang saling memiliki ketergantungan.

Masing-masing dari masalah tersebut bersifat riil. Tetapi paradigma siklus kehidupan klasik memiliki tempat yang terbatas namun penting di dalam kerja rekayasa perangkat lunak. Paradigma itu memberikan template di mana metode analisis, desain, pengkodean, pengujian dan pemeliharaan bisa dilakukan. Siklus kehidupan klasik tetap menjadi model bagi rekayasa perangkat lunak yang paling luas dipakai.

2.2 Perencanaan atau Rekayasa Pemodelan Sistem

Pada fase ini dilakukan identifikasi sistem, studi kebutuhan pengguna, dan studi kelayakan sistem baik secara teknis maupun teknologi serta penjadwalan pengembangan sistem.

2.3 Identifikasi Sistem

Berdasarkan hasil studi yang dilakukan oleh penulis mengenai algoritma *caesar cipher*,

maka penulis mengidentifikasi aplikasi yang akan dibuat merupakan aplikasi yang nantinya berupa representasi dari logika algoritma *caesar cipher* dimana aplikasi ini memiliki kemampuan melakukan proses enkrip dan dekrip sebuah teks atau pesan tertulis, yang nantinya akan dilakukan proses langkah demi langkah dalam pergeseran pesan atau teks asli dengan kunci yang ditentukan yang menghasilkan sebuah *cipher* teks. Begitu juga dalam penterjemahan *cipher* teks nantinya akan dilakukan langkah demi langkah dalam penterjemahan kedalam teks asli. Selain itu, aplikasi ini nanti akan ditambahkan sebuah teknologi dimana pesan yang terenkrip dapat dikirimkan kesebuah *email* yang dituju, sehingga dapat disimpulkan aplikasi *caesar cipher* ini nanti merupakan aplikasi berbasis *web*.

Adapun studi yang dilakukan oleh penulis mengenai kebutuhan sistem yang harus dipenuhi adalah pengguna harus memiliki akun untuk mengakses aplikasi ini nanti, akun dapat diperoleh dengan melakukan registrasi pada halaman *web* yang disediakan. Kemudian pengguna harus memiliki *email* tujuan, dikarenakan kembalike fungsi aplikasi yang dapat mengirimkan teks pesan ke *email* yang diinginkan. Untuk kebutuhan sistem sendiri kan lebih dibahas pada bagian analisis kebutuhan.

Dari segi teknologi yang digunakan, aplikasi ini nanti akan menggunakan bahasa pemrograman berbasis *web* yaitu *PHP* dan didukung dengan teknologi basis data berupa *MySQL*. Dalam penggunaannya, aplikasi ini melibatkan teknologi *email* dan *web server*.

2.4 Studi Kebutuhan dan Kelayakan Sistem

No	Uraian Kegiatan	Oktober 2010		November 2010				Desember 2010				Januari 2011				Februari	
		Minggu		Minggu				Minggu				Minggu				Minggu	
		3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
1	Tahap perencanaan sistem																
2	Tahap analisis																
3	Tahap desain																
4	Tahap generasi kode																
5	Tahap pengujian																

Tabel 2.1 Jadwal Pengembangan

2.5 Analisis Sistem

Dalam merancang sebuah sistem, analisis mutlak harus dilakukan. Dengan melakukan analisis yang baik terhadap sistem yang akan dikerjakan, akan memudahkan kita dalam melakukan perancangan sistem, dan apabila di kemudian hari sistem kita ingin dilengkapi maka akan mudah dalam menyelesaikannya.

Salah satu unsur terpenting yang harus dipertimbangkan dalam tahapan analisis sistem

ini yaitu masalah aplikasi, karena nantinya aplikasi yang digunakan haruslah sesuai dengan masalah yang akan diselesaikan. Untuk itu, analisis yang dilakukan terhadap aplikasi algoritma *caesar cipher* ini akan dibagi kedalam beberapa aspek, yaitu analisis kebutuhan perangkat lunak *caesar cipher*, analisis proses enkripsi dan dekripsi algoritma *caesar cipher* serta analisis fungsi perangkat lunak algoritma *caesar cipher*.

2.5.1 Analisis Kebutuhan

Faktor yang mendasari dibentuknya aplikasi dengan algoritma *caesar cipher* adalah keamanan data. Keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah sistem informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangatlah penting untuk mencegahnya agar tidak jatuh kepada pihak-pihak yang tidak berhak. Untuk keperluan tersebut, maka diperlukan sebuah teknik kriptografi dengan menggunakan metode enkripsi dan dekripsi pesan. Aplikasi ini nantinya untuk mengirim pesan *email*. Aplikasi ini akan mengenkripsi pesan yang akan dikirimkan menjadi *ciphertext* dan mendekripsikan menjadi *plaintext*. Dalam membangun aplikasi nanti, diperlukan batasan yang jelas sebagai tujuan agar tidak keluar dari rencana yang telah ditetapkan. Beberapa kebutuhan sistem yang akan didefinisikan antara lain :

1. Memiliki kemampuan mengirimkan pesan.
2. Memiliki kemampuan mengenkripsi pesan.
3. Memiliki kemampuan mendekripsi pesan.

2.5.2 Analisis Algoritma *Caesar Cipher*

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis, (Munir, 2002). Kata *logis* merupakan kata kunci dalam algoritma. Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar. Dalam beberapa konteks, algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu.

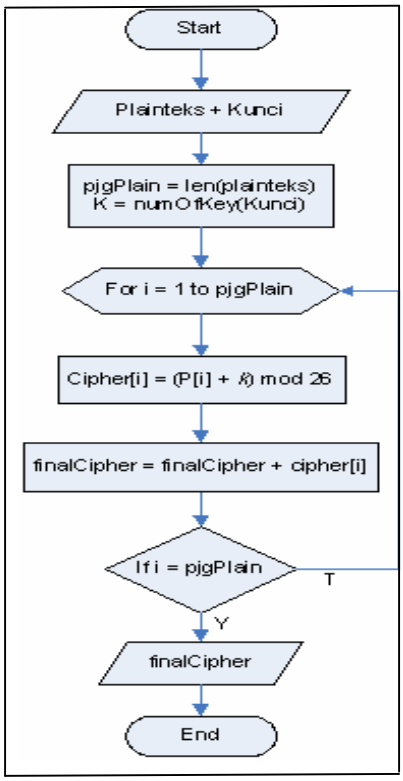
Algoritma *caesar cipher* merupakan algoritma klasik yang memiliki langkah-langkah logis sebagai berikut :

1. Menghitung panjang karakter / huruf yang diinputkan dalam plaintext.
2. Tiap-tiap huruf diubah menjadi kode ASCII menggunakan proses looping.
3. Untuk melakukan pergeseran / proses enkripsi maka kode ASCII tersebut digeser dengan cara ditambah sebanyak pergeseran. Misalnya pergeseran 3 huruf maka kode ASCII ditambah dengan 3.
4. Jika ditemukan spasi (ASCII=32), maka tidak usah dilakukan penambahan.
5. Hasil pergeseran / penambahan bilangan ASCII dikembalikan lagi menjadi huruf / karakter.

2.5.2.1 Proses Enkripsi

Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Adapun proses

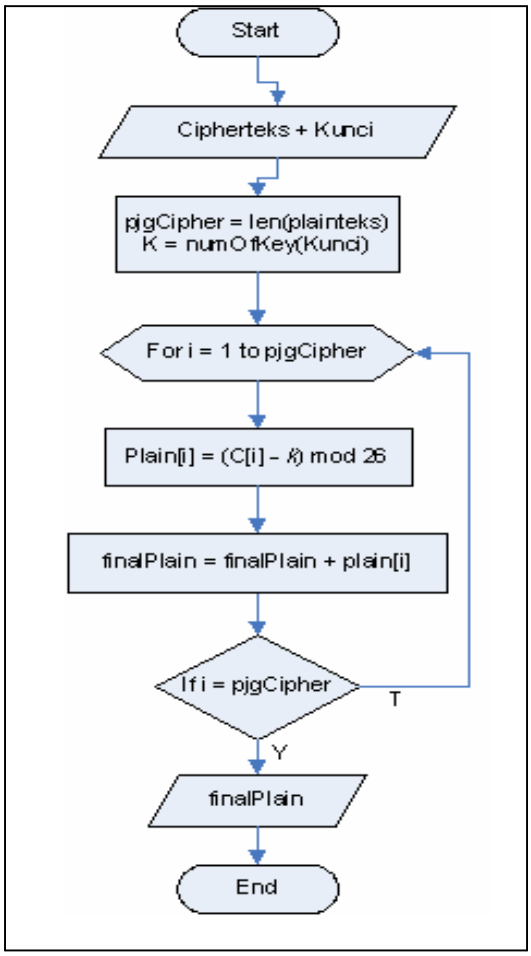
enkripsi dalam algoritma *caesar cipher* dapat dilihat pada gambar ini.



Gambar 2.1 Sistem Kerja Enkripsi

2.5.2.2 Proses Dekripsi

Dekripsi merupakan suatu proses penterjemahan sebuah karakter dengan kunci dan aturan tertentu menjadi sebuah karakter atau kalimat asli yang dapat dibaca dan diketahui informasi didalamnya. Adapun proses dekripsi pada algoritma *caesar cipher* dapat dilihat pada gambar ini.



Gambar 2.2 Sistem Kerja Dekripsi

3. HASIL

Adapun hasil dari pengimlementasian algoritma *caesar cipher* dalam bahasa pemrograman *PHP*, menghasilkan sebuah aplikasi berbasiskan *web*. Beberapa tampilan *web* yang dihasilkan akan dibahas lebih lanjut.

3.1 Halaman Utama

Halaman utama atau lebih dikenal dengan *homepage*, menampilkan tampilan pertamakali ketika mengakses aplikasi *caesar cipher* melalui browser baik menggunakan *Mozilla Firefox, Internet Explorer, Opera,*

maupun browser lain. Adapun tampilannya dapat dilihat pada gambar berikut ini.

Gambar 3.1 Halaman Utama

3.2 Halaman Registrasi

Halaman registrasi merupakan halaman kedua yang didapat ketika memilih menu 'Registrasi' pada *web*. Pada halaman ini, setiap pengguna harus melakukan penginputan beberapa data penting seperti *username*, *password*, dan lain-lain yang akan dicatat kedalam *database* sebagai autentikasi apabila pengguna ingin menikmati fasilitas pengenkripan dalam *web* aplikasi tersebut. Jadi dapat disimpulkan, pengguna harus registrasi terlebih dahulu sebelum dapat menggunakan fasilitas service pada *web* aplikasi. Adapun tampilannya dapat dilihat pada gambar berikut.

Gambar 3.2 Halaman Registrasi

3.3 Halaman Login

Setelah pengguna berhasil mengisikan form registrasi dengan benar, maka pengguna akan diajak untuk masuk kehalaman login yang digunakan sebagai jendela pembuka untuk menikmati fasilitas enkripsi pada aplikasi *caesar cipher* tersebut. Pengguna tinggal menginputkan *username* dan *password* yang telah didaftarkan. Adapun tampilan dari halaman login, dapat dilihat pada gambar berikut ini.

Gambar 3.3 Halaman Login

3.4 Proses Enkripsi dan Dekripsi

Proses enkripsi pesan akan dilakukan setelah pengguna berhasil login kedalam sistem *web* aplikasi *caesar cipher*. Lalu pengguna memasukkan key yang akan dijadikan sebagai angka penentu pergeseran setiap abjad dalam pesan tersebut, kecuali karakter-karakter tertentu. Proses enkripsi dilakukan ketika key dan pesan telah selesai diinputkan, lalu pengguna menekan tombol 'encript' pada *web* aplikasi *caesar cipher* tersebut. Proses enkripsi dapat dilihat pada gambar berikut.

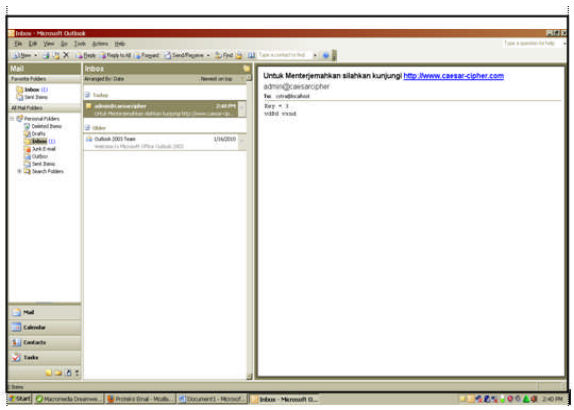
Gambar 3.4 Input Key dan Pesan

Gambar 3.5 Proses Enkripsi

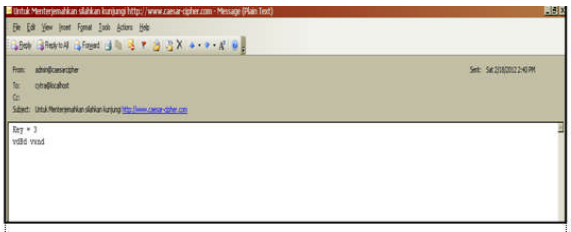
Pada proses gambar diatas, maka proses algoritma *caesar cipher* untuk enkripsi pesan sudah berjalan, prosesnya dapat dibaca lebih detil pada bab tiga dalam penulisan ini. Dalam sebuah proses algoritmanya, tahapan yang dilakukan yaitu sebagai berikut.

1. Pertama, melihat apakah angka yang menjadi keynya lebih besar atau lebih kecil dari 52. Dipembahasan sebelumnya telah dijelaskan angka tolak ukur sebuah key pergeseran dilihat dari rentang dari huruf a-z dan A-Z yang bila kedua rentang tersebut digabungkan 26+26 menjadi total 52.
2. Langkah kedua, menghitung panjang karakter dari plainteks yang diinputkan, nantinya akan digunakan untuk berapa kali perulangan karakter atau berapa banyak karakter yang harus digeser.
3. Langkah ketiga, setiap karakter dalam plainteks diterjemahkan kedalam bentuk desimal dan kemudian diubah kedalam bentuk ASCII.
4. Langkah keempat, setiap karakter baru dijumlahkan dengan angka pergeseran yang didapat dari key yang diinputkan.
5. Langkah kelima, setelah didapat hasil pergeseran dalam bentuk ASCII, maka barulah diubah kembali kedalam bentuk angka desimal dan hasil akhirnya dikonversikan kedalam bentuk abjad.

Kemudian, untuk melihat bahwa pesan telah terkirim pada *email* dengan akun *cytra@localhost* maka kita dapat melihat pada kotak masuk akun *email* tersebut. Adapun hasil pengiriman, dapat dilihat pada gambar berikut.



Gambar 5.0 Kotak Masuk Email



Gambar 5.1 *Email* Detail

4. SIMPULAN

Berdasarkan hasil dari penelitian ini, dapat disimpulkan bahwa :

1. Penelitian ini menghasilkan sebuah *web* aplikasi *caesar cipher*.
2. Dengan adanya *web* aplikasi ini, dapat meningkatkan keamanan pesan sebuah *email* dimana pesan yang dikirimkan sudah terenkripsi.
3. Dalam *web* aplikasi *caesar cipher* ini telah ditambahkan suatu fungsi yang dapat mengirimkan pesan ke *email* tertentu yang dituju, walaupun dalam penulisan ini pembuktian hanya dilakukan dengan *email server local*.

DAFTAR RUJUKAN

Ariyus, Dony. 2008. *Computer Security*. Yogyakarta : Andi Offset.

Hadi, Mulya, 2006, *Dreamweaver 8 Untuk Orang Awam,* Maxikom: Palembang.

Febrian, Jack, 2007, *Menggunakan Internet*, Informatika: Bandung.

Menguasai XHTML, CSS, PHP, & MySQL melalui Dreamweaver, 2009, Andi: Yogyakarta.

Munir, Rinaldi, 2006, *Kriptografi*, Informatika Bandung: Bandung.

_____, 2002, *Algoritma dan pemrograman*, Informatika Bandung: Bandung.

Nugroho, Bunafit, 2008, *Latihan membuat aplikasi web PHP dan MySQL dengan*

Dreamweaver MX (6,7,2004) dan 8, Gava Media: Yogyakarta.

Peranginangin, Kasiman, 2006, *Aplikasi Web dengan PHP dan MySQL*, Andi: Yogyakarta.

Pressman, Roger.S. 2002. *Rekayasa Perangkat Lunak*. Yogyakarta: Andi and McGraw-Hill Book Co.