IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE CAESAR CIPHER DAN VIGENERE CIPHER UNTUK MENGAMANKAN EMAIL PADA EXO DIGITAL AGENCY

Rifky Aditia Hamdan[1)], Painem[2)]
Program Studi Anda, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : rifkyaditia7@gmail.com, painem@budiluhur.ac.id

ABSTRAK

Pesatnya perkembangan teknologi dan komunikasi di era global saat ini membawa pengaruh bebas terutama pada bagian keamanan data dan informasi penting dan rahasia yang di alami di berbagai belahan dunia. Keamanan data dalam pertukaran informasi melalui *email* merupakan hal yang sangat penting di zaman *modern* ini. Informasi menjadi sangat rentan untuk dicuri, dirusak dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Hal ini membuat para pimpinan dan karyawan Exo Digital Agency khawatir jika akan menggunakan media *email* untuk bertukar informasi, karena data dan informasi yang bersifat penting dan rahasia masih rentan terhadap pencurian serta penyalahgunaan oleh pihak tertentu yang dapat menimbulkan kerugian yang sangat besar. Dari fenomena tersebut maka dibutuhkan suatu metode yang dapat menjaga kerahasian informasi. Oleh karena itu, dibuatlah suatu aplikasi pengiriman *email* yang dapat menjaga dan mengamankan kerahasiaan informasi. Dalam perancangan aplikasi ini, penulis membuat suatu metode dengan cara proses enkripsi. Algoritma yang akan digunakan 2(dua) algoritma kriptografi yaitu *Caesar Cipher*, kriptografi klasik dengan teknik substitusi *cipher* dimana setiap huruf pada teks (*plaintext)* digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alphabet geseran 3, dan *Vigenere Cipher* dengan teknik substitusi *cipher* dimana setiap huruf pesan akan dikodekan sebanyak nilai tertentu yang berdasarkan kata kunci dan table yang sudah disebutkan sebelumnya, dan menghasilkan sesuatu yang tampaknya berupa teks acak. Aplikasi ini dibuat dengan menggunakan bahasa pemprograman *PHP*. Dengan aplikasi kriptografi ini, diharapkan informasi pesan yang beredar dikantor akan aman dan tidak bocor kepada penyadap atau pihak yang tidak bertanggung jawab. Pada aplikasi ini, informasi yang dienkripsi hanya berupa teks dan lampiran file dan hanya pengguna akun gmail Exo Digital Agency yang dapat menggunakan aplikasi ini. Berdasarkan implementasi dan pengujian program, penulis dapat menyimpulkan bahwa aplikasi ini mudah digunakan, pesan yang dikirim dan diterima melalui aplikasi ini aman karena sudah melalui proses enkripsi terlebih dahulu serta waktu untuk mengenkripsi dan mendekripsi pesan dengan kecepatan 0.004 *second*s dan 0.568741 *seconds*, dan mampu menjaga dan melindungi kerahasiaan data dan informasi. Serta dapat memberikan manfaat bagi pimpinan dan staff karyawan Exo Digital Agency dalam menjalankan tugas pokok, fungsi, dan peran dalam perusahaan.

Kata kunci : Kriptografi, Keamanan Data Email, Enkripsi Pesan Email, Dekripsi Pesan Email, Algoritma Caesar Cipher, Algoritma Vigenere Cipher

1. PENDAHULUAN

Di era keterbukaan informasi dan perkembangan teknologi seperti sekarang ini, seseorang dengan mudah menyimpan, mengunggah, dan mengakses informasi baik berupa data atau apapun dengan bantuan internet. Akses internet pun kini semakin mudah, tidak hanya komputer atau laptop saja, *smartphone* dan *gadget* pun dapat mengakses internet.

Exo Digital Agency merupakan sebuah agensi media digital yang melayani kegiatan pemasaran berbagai merek lokal maupun internasional bagi perusahaan skala menengah hingga multinational dari berbagai lini industry. Exo Digital Agency beralamat di Jalan Panglima Raya 98 C Ruko Indah Bangunan, Kebayoran Baru, Jakarta Selatan. Exo Digital Agency merupakan agensi dengan layanan yang lengkap yang sangat berpengalaman pada kegiatan pemasaran digital, jejaring sosial, optimalisasi *search engine*, game interaktif, serta pembuatan *website* dan *software*.

Berdasarkan kenyataan di atas, perlu ada suatu sistem pengamanan informasi baik saat pengiriman maupun penerimaan *email*. Pengamanan data akan menggunakan kriptografi, dimana data dirubah menjadi sandi-sandi yang tidak di mengerti oleh sembarang orang serta mengembalikannya kebentuk semula, proses ini disebut enkripsi dan dekripsi. Algoritma enkripsi ternyata sudah cukup beragam. Dalam laporan tugas akhir ini, akan menggunakan metode *Caesar Cipher* dan *Vigenere Cipher* untuk proses enkripsi dan dekripsi teks dan lampiran pada *email*.

Berdasarkan uraian latar belakang di atas, permasalahan yang akan diangkat dalam menyelesaikan tugas akhir ini adalah :

a. Bagaimana cara yang dapat dilakukan untuk memproteksi / melindungi data dan informasi yang dikirim atau diterima melalui media email?
b. Bagaimana cara yang dapat dipilih untuk memproteksi / melindungi data dan informasi dari pencurian dan kerusakan?
c. Bagaimana cara yang dapat untuk memproteksi / melindungi data dan informasi dari pencurian dan kerusakan ?
d. Bagaimana cara menempatkan algoritma *caesar cipher* dan algoritma *vigenere cipher* sebagai metode pada aplikasi?

Maksud dan tujuan penulis dalam melakukan kegiatan penulisan Tugas Akhir ini adalah untuk memberikan solusi terhadap masalah keamanan data pada Exo Digital Agency dengan teknik kriptografi yang menggunakan metode algoritma *Caesar Cipher* dan Vigenere Cipher yaitu meng*enkripsi* data saat mengirim email berupa teks dan lampiran *file* ke dalam dokumen yang sudah dienkripsi atau disandikan. Sehingga data tersebut tidak terbaca dan tidak menimbulkan kecurigaan dari pihak-pihak yang tidak bertanggung jawab.

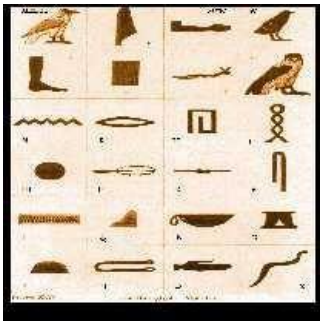
2. TINJAUAN PUSTAKA

2.1 Keamanan Komputer

Keamanan Komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab (*John D. Howard*). Bagi para perancang dan pengelola system informasi, masalah kemanan sering berada di urutan setelah tampilan, atau bahkan di urutan paling terakhir dalam daftar hal-hal yang dianggap penting. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern saja tidak berurusan hanya dengan penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Sadikin, 2012).

2.2 Sejarah Kriptografi

Sejak 300 SM yang lalu kriptografi sudah diperkenalkan orang Mesir lewat *hieroglyph* (gambar 2.2) walaupun bukan dalam bentuk tulisan standard. *Hieroglyohcs* diturunkan dari bahasa Yunani *hieroglyphcs* yang berarti ukiran. rahasia. *Hieroglyohcs* berevolusi menjadi *hieratic*, yaitu *stylized script* yang lebih mudah untuk digunakan



Gambar 1: Hieroglyph

2.3 Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi (sehingga dinamakan algoritma kriptografi klasik), namun sekarang algoritma tersebut sudah usang karena ia sangat mudah dipecahkan. Algoritma kriptografi klasik terdiri dari dua bagian yaitu: *Cipher* Substitusi (*Substitution Ciphers*) dan *Cipher* Transposisi (*Transposition Ciphers*) (Munir, 2009).

Gambar 2: Caesar Wheel

2.4 Kriptografi Modern

Kriptografi modern dipicu oleh perkembangan peralatan komputer. Kriptografi modern menggunakan gagasan dasar yang sama seperti kriptografi klasik (permutasi dan transposisi) tetapi penekanannya berbeda. Pada kriptografi klasik, kriptografer menggunakan algoritma yang sederhana, yang memungkinkan cipherteks dapat dipecahkan dengan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya).

Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit memecahkan cipherteks tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter (seperti yang dilakukan pada *cipher* substitusi atau *cipher* transposisi dari algoritma kriptografi klasik).

2.5 Algoritma Kriptografi

Algoritma dalam kriptografi merupakan sekumpulan aturan (fungsi matematis yang digunakan) untuk proses enkripsi dan dekripsi. Dalam beberapa metode kriptografi terdapat beberapa perbedaan antara fungsi enkripsi dan fungsi dekripsi.

Konsep matematis yang mendasari algoritma adalah relasi antara himpunan, yaitu relasi antara himpunan yang berisi elemen-elemen *chipertext.* Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tesebut. Misalkan himpunan elemen *plaintext* dinotasikan *P* dan himpunan elemen *chipertext* dinotasikan *C*, maka fungsi enkripsi *E* memetakan himpunan *P* ke himpunan *C*.

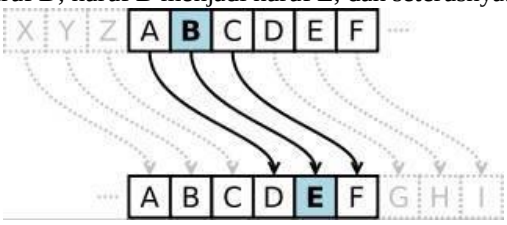
$$E(P) = C$$

Dan fungsi dekripsi memetakan himpunan *C* ke himpunan *P*,

$$D(C) = P$$

2.6 Caesar Cipher

Metode penyandian ini dinamakan *caesar cipher*, setelah digunakan Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi, *caesar cipher* dikenal dengan beberapa nama seperti: *shift cipher, caesar's code* atau *caesar shift*. *Caesar cipher* merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. *Cipher* ini berjenis *cipher* substitusi, dimana setiap huruf pada *plaintext*nya digantikan dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.



Gambar 3: Tabel Subsitusi Caesar Cipher

2.7 Vigenere Cipher

Vigenere Cipher merupakan salah satu algoritma klasik dengan teknik substitusi. Nama vigenere diambil dari seorang yang bernama blaise de vigenere.

Vigenere cipher menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bisa lebih pendek ataupun sama dengan panjang plainteks. Jika panjang kunci kurang dari panjang plainteks, maka kunci yang tersebut akan diulang secara periodic hingga panjang kunci tersebut sama dengan panjang plainteksnya.

3. METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode atau pendekatan umum yang digunakan dalam pengembangan aplikasi pada laporan ini adalah *Waterfall*, dengan tahapan sebagai berikut:

a. Analisa Masalah
   Setelah data-data dikumpulkan, maka selanjutnya akan dilakukan analisa terhadap masalah dan analisis kebutuhan sistem, yang nantinya akan dilakukan pengambilan keputusan terhadap masalah yang akan dikaji.
b. Desain
   Pada tahap ini bertujuan untuk menentukan spesifikasi detil dari komponen-komponen program (manusia, perangkat lunak, perangkat keras, jaringan dan data) dan membuat rancangan tampilan berupa *input* dan *output*.
c. Implementasi
   Pada tahap ini sistem sudah dikembangkan menjadi suatu perangkat lunak yang siap dipakai, kemudian dilakukan proses pengujian. Perangkat lunak yang telah diuji dan diterima pengguna siap untuk digunakan.
d. Perawatan
   Perangkat lunak yang telah dioperasikan akan dilakukan proses perawatan yaitu berupa monitoring, evaluasi dan perubahan bila diperlukan agar sesuai dengan yang diharapkan.

3.2 Analisa Masalah

Teknologi informasi dan komunikasi saat ini selain memiliki potensi dalam menyaring data dan mengolah menjadi informasi, teknologi informasi mampu menyimpannya dalam bentuk yang tidak dimengerti orang tidak berkepentingan. Hal ini dilakukan demi menjaga informasi agar tetap aman dan terjaga dari pencurian isi informasi. Pengiriman email saat belum ada sistem keamanannya, sehingga memungkinkan orang lain bisa menyadap email. Dengan belum adanya sistem keamanan maka pengiriman email saat ini dianggap belum aman.

3.3 Penyelesaian Masalah

Berdasarkan analisa masalah diatas maka, diperlukan adanya sebuah aplikasi yang dapat menjaga kerahasiaan data dari sebuah *text* dan lampiran *email* sehingga isi dari data tersebut tidak bisa dibaca atau tidak bisa diketahui oleh pihak lain yang tidak berhak atas *text* dan lampiran *email* tersebut. Aplikasi tersebut nantinya akan mengubah sebuah *text* dan lampiran *email* asli menjadi *text* dan lampiran *email* yang isinya tidak bisa dibaca dan tidak bisa diketahui, agar isi dari data tersebut terjaga kerahasiaannya. Kemudian mengembalikan *email*

text dan *attachment* tersebut menjadi seperti semula tanpa mengalami perubahan sedikitpun.

3.4 Perancangan Basis Data

3.4.1 Database Pengguna

Pada Database Pengguna, *administrator* dapat menambahkan *user* baru pada aplikasi kriptografi dan setiap data *user* memiliki *email* dan *password* untuk melakukan login ke halaman aplikasi tersebut, berikut ini merupakan spesifikasi basis data dari menu tersebut :

Nama Field	Type	Ukuran	Keterangan
pengguna_id	Int	11	ID Pengguna
pengguna_fullname	Varchar	100	Nama Lengkap Pengguna
pengguna_photo	Varchar	100	Foto Pengguna
pengguna_email	Varchar	100	Email Pengguna
Password	Varchar	100	Password
pengguna_phone	Varchar	25	No. Handphone
pengguna_address	Text	65. 535	Alamat Pengguna
status	Tinyint	5	Status
create_at	Datetime	11	Tanggal Daftar
update_at	Datetime	11	Ubah Data

Gambar 4: Database Pengguna

3.4.2 Database Email

Pada *Database Email*, pengguna dapat melihat data hasil *email* yang dikirimkan ke pengguna lain di aplikasi kriptografi *email text*, data tersebut akan masuk ke menu kotak masuk dan kotak keluar, berikut ini merupakan spesifikasi basis data dari *Database Email :*

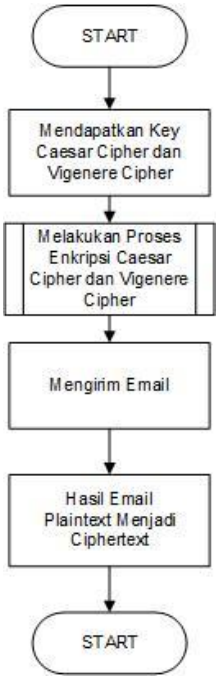
Nama Field	Type	Ukuran	Keterangan
email_id	Int	11	ID Email
email_keys_caesar	Int	5	*Keys Caesar Cipher*
email_keys_vigenere	Varchar	50	*Keys Vigenere Cipher*
email_dari_id	Int	11	Pengirim Email
email_kepada_id	Int	11	Penerima Email
email_cc_id	Int	11	Penerima Email Pasif (Carbon Copy)
email_bcc_id	Int	11	Penerima Email yg tidak diketahui penerima lain (Blank Carbon Copy)
subject	Varchar	255	Subject Email
message_textasli	Text	65. 535	Pesan Asli (*Plaintext*)
message_textenkripsi	Text	65. 535	Pesan Enkripsi (*Chipertext*)
document_filename	Varchar	150	Nama dokumen *enkripsi*
document_size	Varchar	150	Ukuran Dokumen
Document_fileasli	Varchar	150	Nama Dokumen Asli
created_at	Datetime	11	Tangga Kirim Email
status_decrypt	Int	10	Status Decrypt
status_algo	Varchar	50	Status Algoritma
status	Tinyint	4	Status Email

Gambar 5: Database Email

3.5 Flowchart

3.5.1 Flowchart Proses Enkripsi

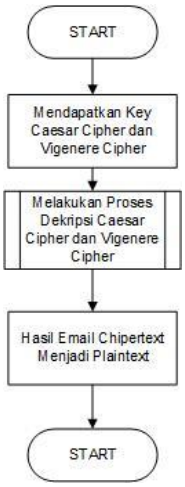
Flowchart ini menggambarkan alur atau jalannya proses enkripsi *text* dan lampiran *email*. *Flowchart* proses *enkripsi* dimulai dari mengirimkan pesan ke *email* penerima, mendapatkan *key Caesar Cipher* dan *Vigenere Cipher* sehingga menjadi *chipertext*



Gambar 6: Flowchart Proses Enkripsi

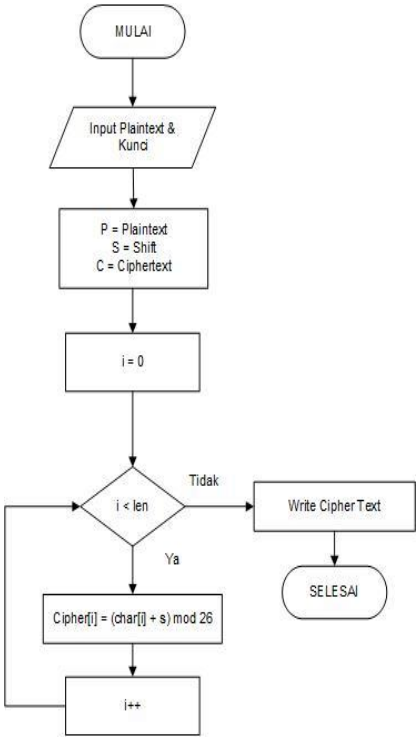
3.5.2 Flowchart Proses Dekripsi

Flowchart ini menjelaskan bagaimana proses pengembalian data terjadi, dari *email text* yang telah terenkripsi (*chipertext*) menjadi *email text* asli (*plaintext*). Proses Dekripsi dimulai dari mendapatkan panjang *key Caesar Cipher* dan *Vigenere Cipher*.



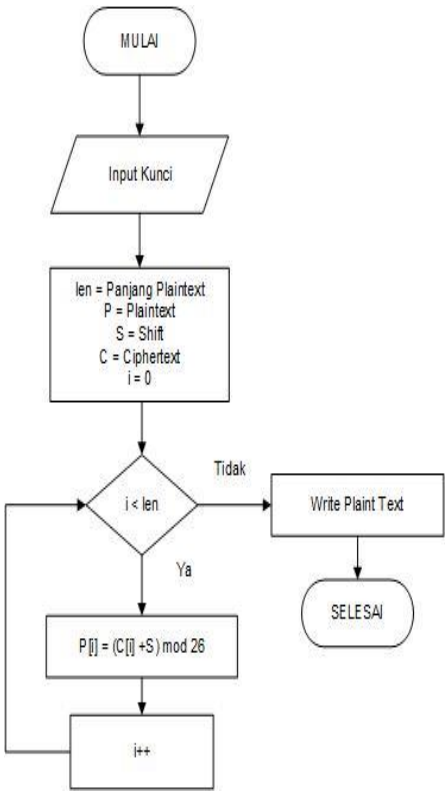
Gambar 7: Flowchart Proses Dekripsi

3.5.3 Flowchart Proses Enkripsi Caesar Cipher



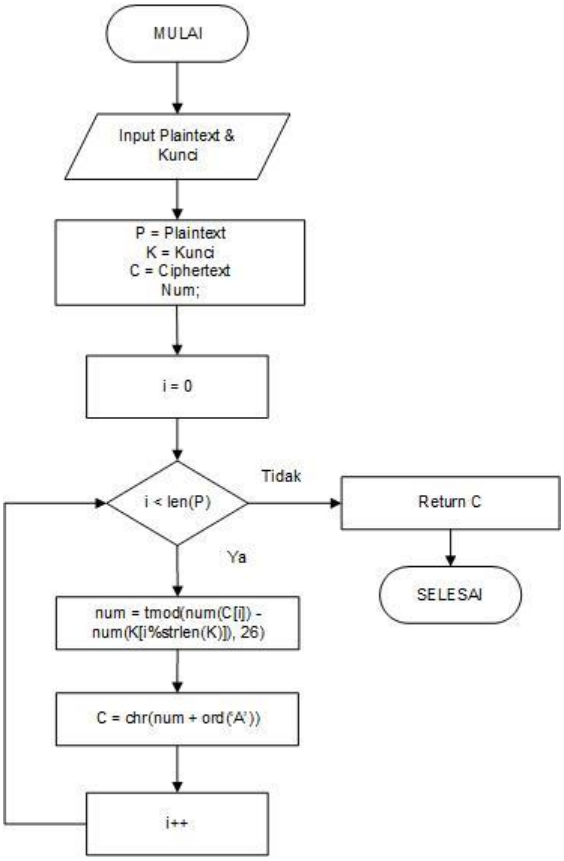
Gambar 8: Flowchart Proses Enkripsi Caesar Cipher

3.5.4 Flowchart Proses Dekripsi Caesar Cipher



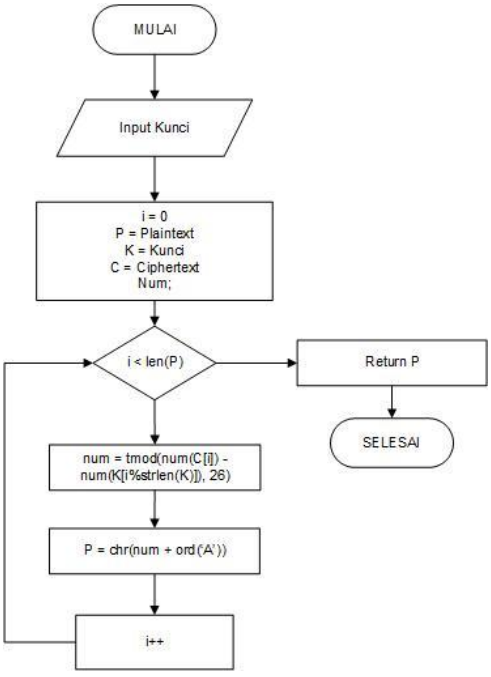
Gambar 8: Flowchart Proses Dekripsi Caesar Cipher

3.5.5 Flowchart Enkripsi Vigenere Cipher



Gambar 9: Flowchart Proses Enkripsi Vigenere Cipher

3.5.6 Flowchart Dekripsi Vigenere Cipher



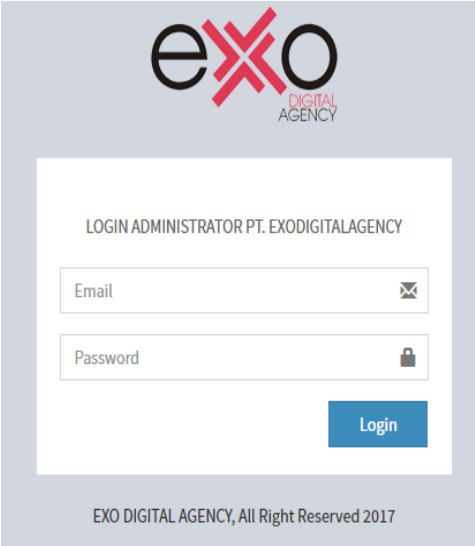
Gambar 10: Flowchart Proses Dekripsi Vigenere Cipher

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

4.1.1 Tampilan Layar *Form* Login

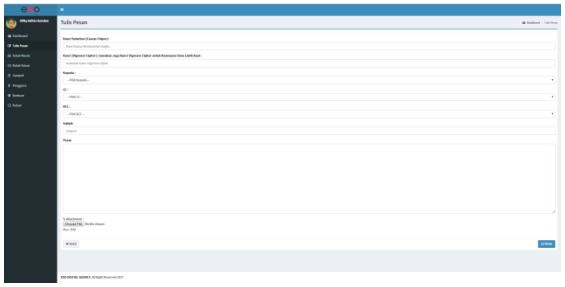
Form login akan tampil ketika aplikasi pertama kali di jalankan. Karyawan harus memasukan *username* dan *password* untuk masuk ke *form* menu utama.



Gambar 11: Tampilan Layar Form Login

4.1.2 Tampilan Layar *Form* Tulis Pesan

Pada *form* ini Untuk melakukan proses enkripsi *email text* dan lampiran *email*, *user* terlebih dahulu memilih menu "Tulis Pesan", setelah itu isi *form* "*Key*", isi *form* "subjek", dan isi *form* "Kepada". Sedangkan jika *user* pengirim ingin menambahkan tujuan alamat pengiriman ke beberapa *user* penerima lebih dari satu alamat *email*, maka *user* pengirim diharuskan untuk memasukan alamat *email user* penerima baru yang terdaftar pada *form* "CC" dan "BCC", setelah itu *user* bisa menuliskan *email text* pada *form* "Pesan" dan *user* dapat melampirkan dokumen. Setelah itu *user* pengirim bisa langsung mengirimkan *email text* dan lampiran *email* yang terenkripsi pada *user* penerima.



Gambar 12: Tampilan Layar Form Tulis Pesan

4.2 Tabel Pengujian

Dalam pengujian kali ini, akan dibahas perbandingan antara proses enkripsi dan dekripsi *email* yang diuji yaitu *email text*. Pengujiannya yaitu mengukur lamanya waktu proses enkripsi dan dekripsi, berikut yang akan kami jelaskan dalam tabel-tabel dibawah ini :

4.2.1 Tabel Pengujian Enkripsi

mahasiswa saya sedang tugas akhir	5	kunci	0.016001	bzzhfxrohbhzqh bhdvhavnlbtprg hxwhj
saya sedang tugas akhir	12	kunci	0.004	ogxobokcohcnsi awygoedoq
selamat pagi bapak	7	kunci	0.004	jffjbrugypxjgkp gbe
selamat siang	20	kunci	0.004	wsswoehgokeb
bapak				nvdedhg
sidang tugas akhir	15	kunci	0.004	rrfrkfnvldzbgrh grtvbdnnzbdng vbdngvbdngvb dngvbdngvb
universitas budi luhur	18	kunci	0.005	wznpetennaun godknqohwd
cerdas berbudi luhur	1	kunci	0.004	gfxvmaxpvdqoi mxsngvbkrgvbd ngvbdngvbdng vbdngvbdngvb
uji coba testing	2	kunci	0.004	eblndvnjzrnpgf vufhvbdnnzbdn gvbdngvbdngv bdngvbdngvb
revisi tugas akhir	3	kunci	0.004	yzvdnankpqpm y
jadwal sidang	5	kunci	0.004001	tolmbdpxupym uqbw
dosen pembimbing	6	kunci	0.004	upmncdqyvvlk cvbdnnzbdngvb dngvbdngvbdn gvbdngvbdn
dosen penguji	7	kunci	0.004	tqcrfmdgoflhjvg xqcfabngvbkrgv bdngvbdngvbd ngvbdngvb
anggota dosen penguji	9	kunci	0.004001	cgoeqdfjcufnko dywesbdngcfdn gvbdngvbdngv bdngvbdngvb
ketua dosen penguji	8	kunci	0.004	mndxrdfbvmdf guthiyabdngcfd ngvbdngvbdng vbdngvbdngvb

Gambar 13: Tabel Pengujian Enkripsi

4.2.2 Tabel Pengujian Dekripsi

Dalam pengujian ini, akan dibahas proses dekripsi. Pengujiannya yaitu antara lain *email text* dan lampiran *email* setelah dilakukan enkripsi yang nantinya akan dilakukan dekripsi, *subject*, *key*, waktu enkripsi*(second)*, *email text* dan lampiran *email* enkripsi setelah dilakukan dekripsi dan bentuk *email text* dan lampiran *email* asli setelah dilakukan dekripsi.

rrfrkfnvldzbgrhgrtvbdnnzbdngvbdngvbdngvbdngvbdngvb	20	kunci	0.549432	selamat siang bapak
wznpetennaungodknqohwd	15	Kunci	0.722043	sidang tugas akhir
gfxvmaxpvdqoimxsngvbkrgvbdngvbdngvbdngvbdngvbdngvb	18	kunci	0.566684	universitas budi luhur
eblndvnjzmpgfvufhvbdnnzbdngvbdngvbdngvbdngvbdngvb	1	Kunci	0.608144	cerdas berbudi luhur
yzvdnankpqpmy	2	Kunci	0.627859	uji coba testing
tolmbdpxupymuqbw	3	Kunci	0.004001	revisi tugas akhir
upmncdqywvlkcvbdnnzbdngvbdngvbdngvbdngvbdngvbdn	5	Kunci	0.070488	jadwal sidang
tqcrfmdgoflhjvgxqcfabngvbkrgvbdngvbdngvbdngvbdngvb	6	kunci	0.567321	dosen pembimbing
cgoeqdfjcufnkodywesbdngcfdngvbdngvbdngvbdngvbdngvb	7	Kunci	0.216629	dosen penguji

Gambar 14: Tabel Pengujian Dekripsi

4.3 Kelebihan dan Kekurangan

Setelah dilakukan analisa dari hasil implementasi aplikasi, maka didapatkan sebagai berikut :

1) Kelebihan

a) Teks dan lampiran *email* yang dikirim melalui aplikasi langsung dapat terenkripsi dan tidak dapat dibaca apabila tidak menggunakan aplikasi ini
b) Adanya pemberitahuan pesan masuk via akun *email* yang terdaftar pada aplikasi.
c) Pengguna aplikasi ini bisa mendaftar dengan menggunakan akun penyedia layanan *email*, seperti : akun *Gmail*.

2) Kekurangan

a) Belum adanya fitur *Reply*, *Forward*, *Draft*, *Forgot Password* dan *Restore* pada menu *trash*..
b) Belum bisa meng-*upload* gambar *profile* dengan ukuran di atas 2 MB.
c) Belum bisa mengirimkan *email* lebih dari tiga penerima secara langsung.

5. KESIMPULAN

Berdasarkan analisis yang dilakukan dimulai dari pengumpulan informasi, pemecahan masalah hingga pengembangan aplikasi ini, maka dapat ditarik beberapa kesimpulan dan saran yang perlu diperhatikan demi kelancaran sistem yang dibangun ini.

1. Kesimpulan

Berdasarkan dari uraian permasalahan dan penyelesaian masalah pada bab-bab sebelumnya, maka dapat disimpulkan bahwa program aplikasi pengamanan *email text* dan lampiran *email* berbasis *Web* menggunakan metode algoritma *Caesar Cipher* dan *Vigenere Cipher* sangat diperlukan karena:

a. Aplikasi yang telah di implementasikan dapat dimengerti oleh pengguna.
b. Aplikasi ini dapat menjadi sebuah solusi dari kekhawatiran banyak orang terhadap pentingnya keamanan data yang terdapat di akun *email.*
c. Aplikasi ini telah diatur oleh sistem sehingga isi pesan atau data yang terkandung di dalam akun-akun *email* yang terdaftar tersebut otomatis telah dienkripsi dengan baik.
d. Dengan adanya aplikasi ini maka *email* yang dianggap penting dapat terjaga kerahasiaanya dari pihak yang tidak berkepentingan dan tidak berhak untuk mengetahui isi dari *email text* dan lampiran *email* tersebut.

DAFTAR PUSTAKA

[1] (n.d.). Retrieved from http://www.history-world.org/hieroglyphics.htm [Diakses Desember 28, 2017].

[2] Alim Zikrul A., C. Y. (2016). Meningkatkan Keamanan Data Cloud Computing Menggunakan Algoritma Vigenere Cipher Modifikasi. Jurnal TIMES, Vol. V No 1 : 22-27, 2016. ISSN : 2337 - 3601.

[3] Ariyus D., 2008. "Pengantar Ilmu Kriptografi, Teori, Analisis, dan Implementasi", Yogyakarta.

[4] Jauhari, A. (2014, Juni 13). Retrieved from http://adibjauhari.blogspot.co.id/2014/06/sejarah-kriptografi.html [Diakses Desember 28, 2017].

[5] Kromodimeljo, S. (n.d.). *Teori dan Aplikasi Kriptografi, Jakarta SPK IT.*

[6] Maizarti. (2011, April 12). Retrieved from https://maizarti.wordpress.com/2011/04/12/kriptografi-asimetris/ [Diakses Desember 28, 2017].

[7] Puspita K., R. W. (2015). Analisa Kombinasi Metode Caesar Cipher, Vernam Cipher dan Hill Cipher dalam proses Kriptografi. Seminar Nasional Teknologi Informasi dan Multimedia. ISSN : 2302 - 3805.

[8] Said, F. (2010, Agustus 6). Retrieved from https://fairuzelsaid.wordpress.com/2010/08/06/keamanan-sistem-informasi-caesar-chipher/ [Diakses Desember 28 2017].

[9] Silalahi, D. (2015, April). Retrieved from http://desijugul.blogspot.co.id/2015/04/algoritma/2015/04/algoritma-kriptografi-klasik.html

[10] Sugiantoro B. (2012). Aplikasi Keamanan Email Memanfaatkan Spam dan Algoritma Vigenere. Simposium Nasional RAP I XI FT UMS - 2012. *ISSN : 1412 - 9612*.

[11] Triyuswoyo Y., F. F. (2014). Implementasi Algoritma Caesar, Cipher Disk, dan Sctytale

Pada Aplikasi Enkripsi dan Dekripsi Pesan Singkat, Luma SMS. Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014), Vol. 8 Oktober 2014. ISSN : 2302 - 3740.

[12] Zuli F., I. A. (2014). Penerapan Kombinasi Sandi Caesar Cipher dan Vigenere Untuk Pengamanan Data Pesan Surat Elektronik. Studi Informatika: Jurnal Sistem Informasi, 7(2), 2014, 1-11. ISSN : 1479 - 0767.