JISAMAR (Journal of Information System, Applied, Management, Accounting and Research

ISSN: 2598-8700 (Printed)
ISSN: 2598-8719 (Online)

Volume 1 Nomor 1 November 2017

PENGAMANAN EMAIL MENGGUNAKAN METODE VIGENERE CIPHER

Dahlan Abdullah[1], Surnihayati[2]
Prodi Teknik Informatika, Fakultas Teknik, Universitas Malikussaleh, Aceh, 24354
e-mail: dahlan@unimal.ac.id

Abstrak

Aktivitas penggunaan internet, pertukaran informasi dan pengiriman pesan sudah banyak mengunakan media internet, salah satunya media *email (electronic mail)*, namun seiring berjalannya waktu permasalahan keamanan pesan dan informasipun muncul,permasalahan keamanan informasi dalam pesan *email* yang sering dijumpai yaitu penyadap aktif, penyadap pasif, penipuan dan pemanipulasi data oleh pihak-pihak yang tidak bersangkutan. Pada penelitian tugas akhir ini penulis ingin membuat suatu aplikasi pengamanan *email* dengan menggunakan metode *vigenere cipher*. Algortima *vigenere cipher* ini, yaitu metode penyandian teks alfabet dengan menggunakan deretan sandi *caesar* berdasarkan huruf-huruf pada kata kunci. Dari permasalahan tersebut akan dilakukan penelitian untuk membuat suatu aplikasi yang berguna untuk mengubah pesan *email* yang memerlukan pengamanan agar terhindar dari penyadapan aktif seorang *cracker*. Pengamanan yang dilakukan yaitu menggunakan kriptografi. Dengan adanya enkripsi dan dekripsi, pesan teks biasa (*plaintext*) akan diubah menjadi suatu pesan yang tidak mudah dibaca (*ciphertext*) dengan menggunakan kunci. Sehingga, pesan akan sampai dengan aman pada penerima tanpa mengalamai perubahan isi sedikitpun dari pihak yang tidak bertanggung jawab.

Kata Kunci : Dekripsi, Enkripsi, Kriptografi, Pesan *Email, Vigenere Cipher*

1. PENDAHULUAN

Perkembangan teknologi khususnya kegunaan alat bantu komputer semakin meningkat. Berbagai kelebihan dari komputer dapat membantu memudahkan beberapa pekerjaan dari pengguna. Aktivitas penggunaan internet semakin meningkat pertukaran informasi pun sudah banyak menggunakan media internet, salah satunya adalah menggunakan media *email* (*electronic mail*). Dengan menggunakan *email*, pesan menjadi lebih cepat tersampaikan bahkan hanya dalam hitungan detik serta tidak memakan banyak biaya. Berbeda dengan pengiriman pesan atau surat menggunakan metode konvensional yang segala sesuatunya harus diurus secara fisik dan tentunya banyak mengeluarkan biaya.

Namun seiring dengan berjalannya waktu, muncul berbagai macam masalah yang kerap dijumpai dalam aplikasi berkirim surat ini terutama dalam hal keamanan informasi atau pesan. Permasalahan keamanan informasi dalam *e-mail* yang sering dijumpai antara lain, penyadapan pasif, penyadapan aktif, penipuan, dan lain-lain. Atas dasar permasalahan tersebut peneliti membuat suatu aplikasi yang berguna untuk mengubah pesan yang memerlukan pengamanan agar terhindar dari penyadapan aktif seorang *cracker*.

Atas dasar permasalahan tersebut akan dilakukan penelitian untuk membuat suatu aplikasi yang berguna untuk mengubah pesan yang memerlukan pengamanan agar terhindar dari penyadapan aktif seorang *cracker*. Pengamanan yang dilakukan yaitu menggunakan kriptografi. Dengan enkripsi, pesan teks biasa (*plaintext*) akan diubah menjadi suatu pesan yang tidak mudah dibaca (*ciphertext*). Sehingga, pesan akan sampai dengan aman tanpa mengalamai perubahan isi sedikitpun dari penyadap.

Aplikasi ini diharapkan bisa membantu pengguna dalam mengamankan pesan atau informasi yang akan dikirim melalui jaringan internet yaitu dengan menggunakan *e-mail*. Metode yang digunakan adalah metode *Vigenere Cipher*. Metode *vigeneri cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci

2. KAJIAN LITERATUR

2.1. Email

Email atau surat elektronik adalah layanan surat-surat melalui media elektronik di internet. Layanan *e-mail*, yaitu layanan yang memungkinkan pengguna mengirim dan menerima pesan dalam bentuk surat elektronik. *Electronic mail* (Surat elektronik), sering disebut *e-mail* atau *email* juga merupakan metode *Store and Forward* dari menulis, mengirim, menerima dan menyimpan surat melalui sebuah system komunikasi elektronik (Jasmadi: 2010).

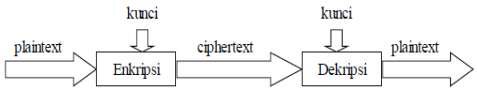
Email terdiri dari dua bagian besar yaitu:

1. *Header*: Terstruktur menjadi beberapa fields seperti *summary*, *sender*, *receiver*, dan *informasi lain* mengenai *e-mail* tersebut.

2. *Body*: isi surat sebagia teks yang tidak berstruktur, juga berisi *signature block* pada akhir. *Header* dipisahkan dari *body* dengan sebuah baris kosong.

2.2. Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik metematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Rifki Sadikin: 2012). Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Proses enkripsi mengubah plaintext menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Untuk melihat ilustrasi dari proses kriptografi dapat dilihat pada gambar mekanisme kriptografi**.**



Gambar 1. Skema Kriptografi

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut yang dilakukan oleh pihak ketiga, berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data, informasi, dan dokumen tersebut.

2.3. Sistem Kriptografi

Menurut Rifki Sadikin (2012) sistem kriptografi terdiri dari 5 bagian yaitu:

1. *Plaintext*: pesan atau data dalam bentuk aslinya yang dapat terbaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Untuk selanjutnya digunakan istilah teks asli sebagai padanan kata *plaintex*t.

2. *Secret Key*: *Secret Key* yang juga merupakan masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap texs asli dan menentukan keluaran algoritma enkripsi. Untuk selanjutnya digunakan istilah kunci rahasia sebagai padanan kata *Secret Key.*

3. C*iphertext*: *ciphertext* adalah keluaran algoritma enkripsi. *Ciphertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *ciphertext*yang terlihat acak. Untuk selanjutnya digunakan istilah teks sandi sebagai padanan *ciphertext*.

4. Algoritma Enkripsi: Algoritma enkripsi memiliki 2 masukan teks asli dan rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.

5. Algoritma Dekripsi: Algoritma dekripsi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma dekripsi.

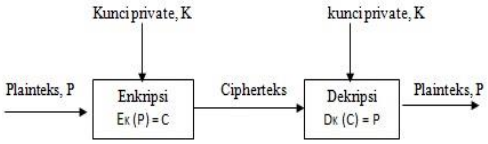
2.4. Algoritma Kriptografi

Algoritma kriptografi disebut juga cipher yaitu aturan untuk *enciphering* dan *deciphering*, atau

fungsi matematik yang digunakan untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yaitu himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi ciphertext. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (key). *Cipher* adalah fungsi matematika yang digunakan untuk mengenskripsi dan mendeskripsi sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenskripsi dan mendekripsi data. Algoritma kriptografi dapat dibedakan atas algoritma simetri dan algoritma asimetri. Pengembangan kedua algoritma tersebut diperlukan *cipher* dan kunci.

a. Kunci Simetrik

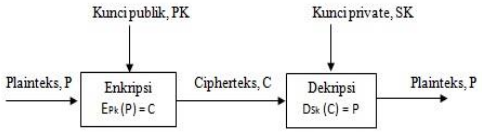
Penyandian dengan kunci simetrik (*Symmetric key encipherment*) adalah penyandian yang kunci enkripsi dan kunci dekripsi bernilai sama. Kunci pada penyandian simetrik diasumsikan bersifat rahasia hanya pihak yang melakukan enkripsi dan dekripsi yang mengetahui nilainya. Oleh karna itu penyandian dengan kunci simetrik disebut juga penyandian dengan kunci rahasia *secret key enchiperment* (Rifki Sadikin: 2012).



Gambar 2. Algoritma Simetrik

b. Kunci Asimetrik

Penyandian dengan kunci asimetrik (*Asymmetric key encipherment*) atau sering juga disebut dengan penyandia kunci public (*public key*) adalah penyandian dengan kunci enkripsi dan dekripsi berbeda nilai. Kunci enkripsi yang juga disebut dengan kunci public (*public key*) bersifat terbuka. Sedangkan kunci dekripsi yang juga disebut kunci privat (*private key*) bersifat tertutup / rahasia (Rifki Sadikin: 2012).



Gambar 3. Algoritma Asimetrik

2.5. Vigenere Cipher

Vigenere Cipher termasuk dalam cipher abjad majemuk (*polyalphabetic substitution Chiper*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586). *Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *caesar* berdasarkan huruf-huruf pada kata kunci. (Putu H. Arjana, dkk : 2012). *Vigenere cipher* merupakan bagian dari algoritma kriptografi klasik yang sangat dikenal karena menggunakan rumus matematika, selain itu *Vigenere cipher* juga dapat menggunakan tabel *Vigenere* untuk melakukan enkripsi plaintext ataupun dekripsi ciphertext. Tabel *Vigenere* ini digunakann untuk memperoleh ciphertext berdasarkan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari plainext maka maka kunci akan diulang penggunaannya secara periodik. Terdapat dua proses dalam penggunaan *Vigenere cipher*, yaitu:

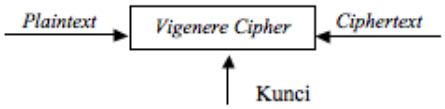
a. Proses Enkripsi *Vigenere cipher*

Proses enkripsi menggunakan *Vigenere cipher* membutuhkan 1 buah kunci untuk dapat menghasilkan ciphertext. Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf. Kemuadian dari kunci yang sudah ditentukan akan dikonversikan menggunakan tabel konversi sehingga menjadi bentuk desimal. Selain mengkonversi kunci yang digunakan, *Vigenere cipher* juga harus mengkonversi Plaintext (Pi) menggunakan table konversi agar menjadi bentuk desimal, kemudian ciphertext (Ci) akan diperoleh dengan mengenkripsi plaintext dengan persamaan :

$$Ci = (Pi + Ki) \bmod 26$$

Ci merupakan ciphertext dari pergeseran karakter yang terdapat pada plaintext. Pi merupakan pergeseran karakter pada plaintext.

Ki merupakan kunci berupa hasil konversi tabel berbentuk bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan.



Gambar 4. Proses Enkripsi *Vigenere*

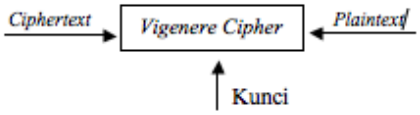
Gambar 4 menjelaskan bahwa untuk merubah plaintext menjadi ciphertext pada *Vigenere cipher* dibutuhkan input berupa plaintext dan sebuah kunci.

b. Proses Dekripsi *Vigenere Cipher*

Proses dekripsi menggunakan *Vigenere cipher* membutuhkan 1 buah kunci untuk dapat menghasilkan plaintext. Kunci yang digunakan merupakan kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Kemuadian dari kunci yang sudah ada akan dikonversikan mengguakan tabel konversi sehingga menjadi bentuk desimal. Selain mengkonversi kunci yang digunakan, *Vigenere cipher* juga harus mengkonversi ciphertext (Ci) menggunakan table konversi yang juga menghasilkan bilanngan desimal, kemudian plaintext (Pi) akan diperoleh dengan mendekripsi plaintext dengan persamaan:

$$Pi = (Ci - Ki+26) \bmod 26$$

Pi merupakan plaintext dari pergeseran karakter yang terdapat pada ciphertext. Ci merupakan pergeseran karakter pada ciphertext. Ki merupakan kunci berupa hasil konversi tabel berupa bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan. Kemudian untuk mendapatkan Pi dapat dilakukan dengan terlebih dahulu mengurangi nilai Ci dengan nilai Ki hasil dari pengurangan yang sudah dilakukan akan dijumlahkan dengan angka 26 untuk kemudian hasil penjumlahan akan di modulo 26. Hasilnya akan berupa bilangan desimal, dari hasil bilangan desimal yang didapat akan dikonversi dengan tabel konfersi sehingga diperoleh karakter plaintext yang diinginkan.



Gambar 5. Proses Dekripsi *Vigenere*

Gambar 5 menjelaskan bahwa untuk merubah ciphertext menjadi plaintext pada *Vigenere cipher* dibutuhkan input berupa ciphertext dan sebuah kunci. *Vigenere cipher* dikenal luas karena cara kerjanya yang mudah dimengerti dan dijalankan serta bagi para pemula akan sulit untuk dipecahkan. Pada saatkejayaannya, *Vigenere cipher* dijuluki sebagai *le chiffre indenchiffrable* (bahasa perancis: “sandi yang tak terpecahkan”). Metode pemecahan Vigenere cipher sendiri baru ditemukan pada abad ke-19 tepatnya ditahun 1854 oleh Charles Babbage.

Menurut Rifki Sadikin (2012) *Vigenere Cipher* merupakan sistem sandi poli-alfabetik mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. Sandi *vigenere* menggunakan substitusi dengan fungsi *shift* seperti pada *Caesar*. Teknik dari substitusi *vigenere cipher* bisa dilakukan dengan dua cara yaitu dengan vigenere cipher angka dan vigenere cipher huruf.

c. *Vigenere Cipher* Angka

Teknik subtitusi *vigenere cipher* menukarkan huruf dengan angka, hal itu hamper sama dengan *shift cipher*.

Tabel 1. *Vigenere Cipher* dengan Angka

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabel 2. Contoh *Vigenere Cipher* Angka

P		S	A	Y	A	H	A	R	I	Y	A	N	T	O
		18	0	24	0	7	0	17	8	24	0	13	19	14
K		7	0	17	8	7	0	17	8	7	0	17	8	7
P+K		25	0	41	8	14	0	34	16	31	0	30	27	21
MOD		25	0	15	8	14	0	8	16	5	0	4	1	21
C-K		18	0	-2	0	7	0	-9	8	-2	0	-13	-7	14
MOD		18	0	24	0	7	0	17	8	24	0	13	19	14

d. *Vigenere Cipher* Huruf

Tabel 2 *Vigenere Cipher* dengan huruf berisi alfabet yang dituliskan dalam 26 baris, masing masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi *Caesar* setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang.

Tabel 3. *Vigenere Cipher* dengan Huruf

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3. METODE PENELITIAN

Metode Penelitian yang digunakan dalam judul tersebut adalah :

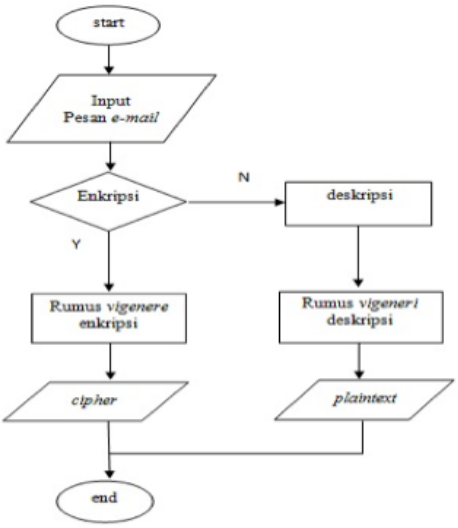
1. Studi kepustakaan

   Sebelum memulai penelitian yang dilakukan terlebih dahulu adalah studi kepustakaan mengenai referensi tentang algoritma *Vigenere Cipher* dan teori pendukung lainnya. Setelah memperoleh referensi tersebut, kemudian merancang sistem untuk pengamanan *e-mail* dengan menerapkan metode *vigenere cipher* berdasarkan dari studi kepustakaan yang dilakukan tersebut.

2. Perancangan aplikasi
   Pada tahap ini penulis melakukan perancangan aplikasi pengamanan *email* menggunakan metode *vigenere cipher* terlebih dahulu sebelum melanjutkan ke tahap selanjutnya. Perancangan dengan menggunakan alat bantu DFD (*Data Flow Diagram*) dengan menggambarkan proses-proses yang ada pada sistem/ aplikasi sehingga akan mempermudah dalam menyelesaikan program tersebut.
3. Pembuatan program
   Pembuatan program menggunakan bahasa pemrograman Delphi dan *database* Microsoft Office Access .

4. Pengujian terhadap aplikasi
   Yaitu melakukan pengujian terhadap program yang telah dibangun dengan melakukan beberapa tes terhadap program terutama pada penerapan algoritma *vigenere cipher* dan menganalisa keluaran yang dihasilkan benar atau salah sehingga jika terdapat kesalahan bisa diperbaiki kembali.

Berikut Skema Sistem Yang dirancang dalam merancang penelitian tersebut adalah :



Gambar Skema Sistem.

4. HASIL DAN PEMBAHASAN

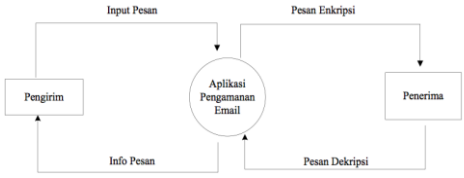
Berikut ini akan diuraikan tentang Hasil dan Pembahasan dalam Penelitian yang telah dilaksanakan, untuk melengkapi Laporan atau Jurnal tersebut.

4.1. Perancangan Sistem

Perancangan sistem merupakan hal yang paling utama sebelum melakukan proses pembuatan program, agar tidak lari dari tujuan penelitian ini.

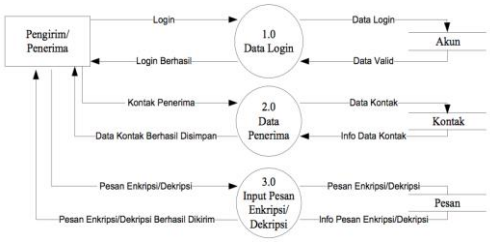
4.2. Konteks Diagram

Konteks diagram berfungsi untuk menggambarkan aktivitas entitas terhadap sistem secara keseluruhan atau umum. Berikut ini adalah konteks diagram dari sistem aplikasi pengamanan pesan Email.



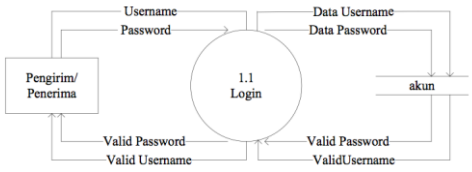
Gambar 6. Konteks Diagram

4.3. Data Flow Diagram Level 0



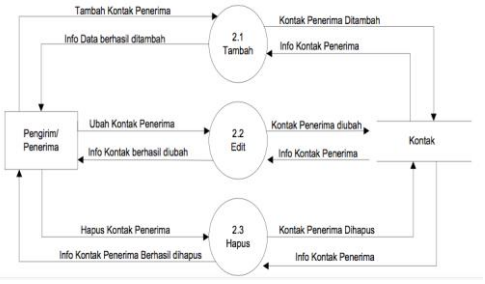
Gambar 7. Data Flow Diagram Level 0

4.4. DFD Level 1 Proses 1.0 Data Login



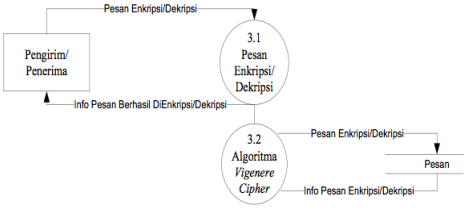
Gambar 8. DFD Level 1 Proses 1.0 Login

4.5. DFD Level 1 Proses 2.0 Data Kontak Penerima



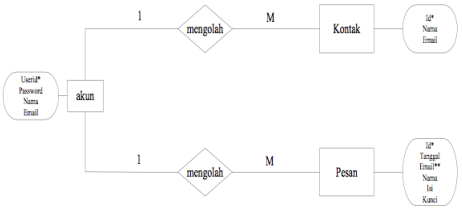
Gambar 9. DFD Level 1 Proses 2.0 Data Kontak Penerima

4.6. DFD Level 1 Proses 3.0 Enkripsi & Denkripsi



Gambar 10. DFD Level 1 Proses 3.0 Enkripsi Atau Dekripsi

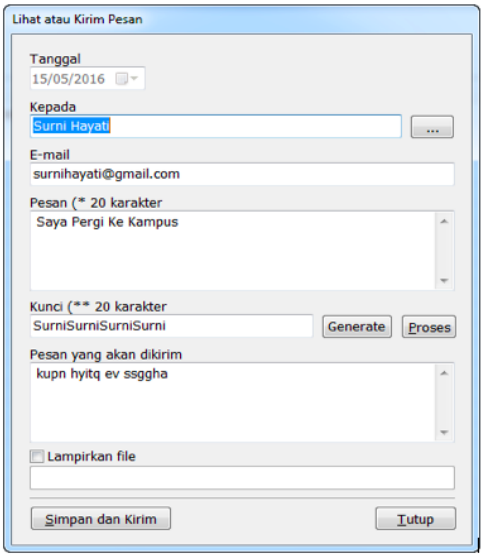
4.7. Entity Relationship Diagram



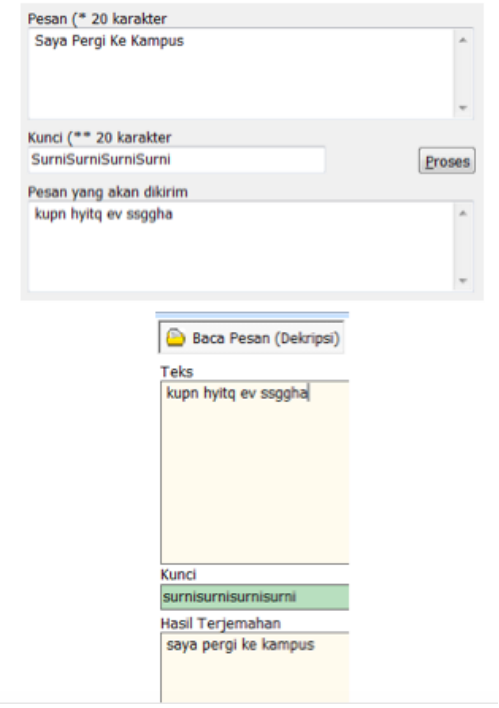
Gambar 11. *Entity Relationship* Diagram

4.8. Implementasi Program

Aplikasi kriptografi ini merupakan sebuah sistem yang akan mengamankan setiap pesan yang akan dikirim kepada pihak penerima agar tidak dapat dibaca oleh pihak yang tidak di beri akses/izin. Sistem ini mengenskripsi setiap Pesan yang telah diinputkan oleh si Pengirim Atau si Penerima, yang dapat dilihat pada gambar 12.



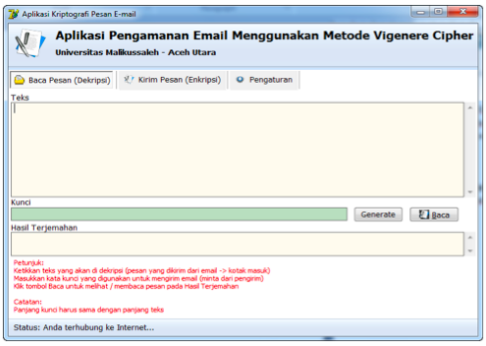
Gambar 12. Lihat atau Kirim Pesan



Gambar 13. Isi Pesan Enkripsi dan Denkripsi

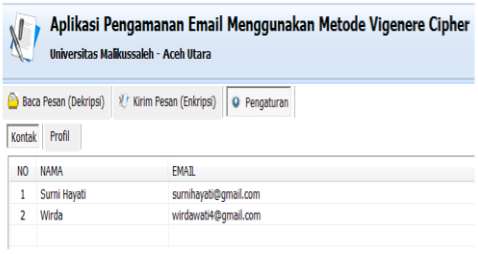
Berikut ini secara detail perancangan tampilan program sesuai dengan penelitian yang telah kami lakukan.

4.8.1. Tampilan Menu Utama



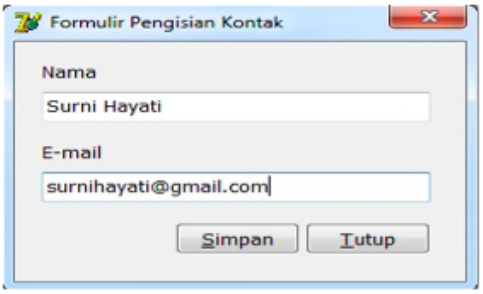
Gambar 14. Tampilan Menu Utama

4.8.2. Menginput Kontak Penerima



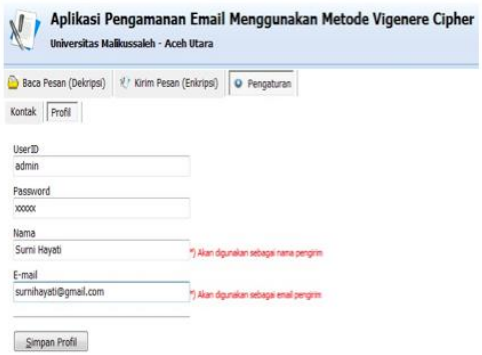
Gambar 15. Input Kontak Penerima

4.8.3. Tampilan Pengisian Kontak Penerima



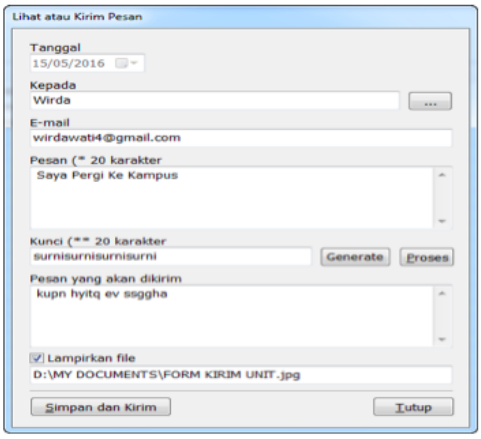
Gambar 16. Tampilan Pengisian Kontak Penerima

4.8.4. Tampilan Menambah Atau Mangubah Profil Admin.



Gambar 17. Tampilan Menambah Atau Mangubah Profil Admin

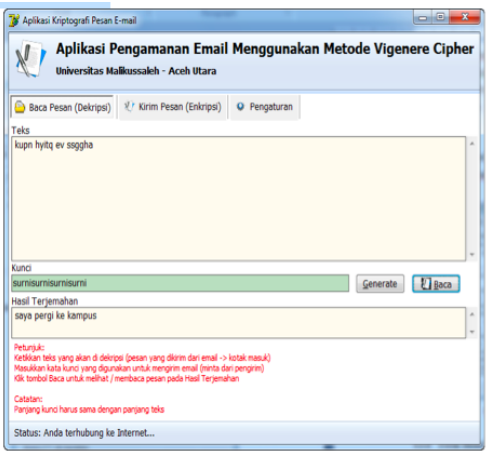
4.8.5. Tampilan Lihat Atau Kirim Pesan



Gambar 18. Tampilan Lihat Atau Kirim Pesan

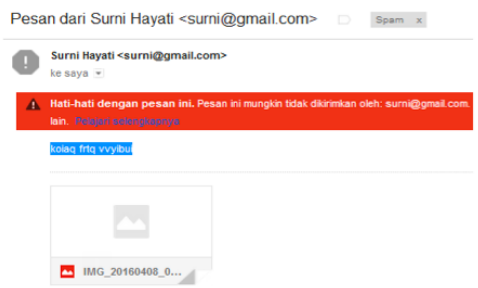
4.8.6. Tampilan Menu Dekripsi.

Tampilan ini berfungsi untuk membaca isi pesan yang telah dienkripsi menggunakan metode *vigenere cipher* dengan menginputkan pesan enkripsi dan kunci yang telah diberikan oleh si pengirim. Tanpa kunci dari si pengirim pesan tidak dapat dibaca.



Gambar 19. Tampilan Menu Dekripsi

4.8.7. Tampilan Hasil Pengiriman Pesan



Gambar 20. Tampilan Hasil Pengiriman Pesan

5. KESIMPULAN

Berdasarkan pembahasan diatas maka dapat disimpulkan beberapa hal, diantaranya:

1. Aplikasi pengamanan *email* ini telah mencapai tujuan utama dari sistem yaitu dapat melakukan pengamanan *email* dengan proses enkripsi dan dekripsi dengan menggunakan metode *Vigenere Cipher*.
2. Metode *vigenere cipher* tidak dapat mengenkripsi atau mendekripsi karakter seperti angka dan simbol-simbol lainnya, metode ini hanya bisa dilakukan pada teks.
3. Dengan adanya kriptografi sistem pengamanan email dilakukan untuk melindungi data yang akan dikirim melalui suatu jaringan komunikasi. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab.

4. Penggunaan algoritma *Vigenere Cipher* merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik abjad majemuk. Kelebihan dari metode *vigenere cipher* adalah tidak begitu rentan terhadap metode pemecahan *cipher* yang disebut analisis frekuensi.

6. REFERENSI

[1] Arjana, Putu H, dkk, 2012, *Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher*, Seminar Nasional Teknologi Informasi Dan Komunikasi, Program Studi Teknik Informatika, STMIK Dharma Putra Tanggerang, Yogyakarta.

[2] Ghofur, A, dkk, 2010, *Membangun Pengontrol Peralatan Keamanan Rumah Dengan Menggunakan AT89C51 Dan Borland Delphi 6*, Vol. 5 No. 2, Jurnal Informatika Murlawan.

[3] Jasmadi, 2010, *Panduan Praktis Menggunakan Fasilitas Internet*, Penerbit Andi, Yogyakarta.

[4] Kustiyaningsih, Yeni., R.A. Devie, 2011, *Pemrograman Basis Data Berbasis Web Mangguanakan PHP & MySQL*, Graha Ilmu, Yogyakarta.

[5] Pabokory, Fresly Nandar, dkk, 2015, *Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen menggunakan Algoritma Advandencryption Standard*, Vol. 10, No. 1, Jurnal Informatika Mulawarma, Universitas Mulawarma.

[6] Raharjo, Budi, 2015, *Belajar Outodidak My SQL Teknik Pembuatan Dan Pengelolaan Database*, Penerbit Informatika Bandung.

[7] Religia, Yoga, 2014, *Implementasi Algoritma Affine Cipher Dan Vigenere Cipher Untuk Keamanan Login sistem Inventori TB Mita Jepara*, Program Studi Teknik Informatika, Universitas Dian Nuswantoro, Semarang.

[8] Sugiantoro, Bambang, 2012, *Aplikasi Keamanan Email Memamfaatkan Spam Dan Algoritma Vigenere*, Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaya, Yogyakarta.

[9] Sadikin, Rifki, 2012, *Kriptografi Untuk Keamanan Jaringan*, Penerbit Andi, Yogyakarta.