Aplikasi Keamanan Google Mail Berbasis Web Menggunakan Algoritma Vigenere Dan RC4 Pada Kotakpensil.com

Dani Seftian[1)], Mufti[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
1211510423@student.budiluhur.ac.id[1)], mufti@budiluhur.ac.id[2)]

ABSTRAK

Masalah dalam keamanan menjaga data informasi web yang dikirim atau diterima melalui email yang memungkinkan terjadinya pencurian data informasi pada email kotakpensil.com.Untuk menjamin keamanan dan keutuhan data informasi yg berupa web,webtraffice,dan penjualan web,Dibutuhkan suatu metode yang agar bisa menjaga kerahasian informasi tersebut dari pihak-pihak yang tidak diinginkan.Maka diimplementasikan algoritma enkripsi dan dekripsi RC4 dan Vigenere pada email untuk melindungi pesan penting perusahaan pada kotakpensil.com dari pihak-pihak yang tidak bertanggung jawab,Maka dibuatlah aplikasi keamanan email ini yang berbasis web menggunakan bahasa pemgroman PHP.Dari hasil Tugas Akhir ini dapat disimpulkan bahwa rata-rata ukuran email yang di enkripsi 9488,6 *byte* dengan waktu rata-rata 4,44 detik dan rata-rata ukuran email yang di dekripsi 5666,8 *byte* dengan waktu rata-rata 6,7 detik.Maka dengan implementasi menggunakan algoritma RC4 dan Vigenere isi email tidak dapat dibaca oleh pengguna tanpa masuk kedalam aplikasi,sehingga keamanan informasi lebih terjaga.

Kata kunci :Kriptografi, *RC4, Vigenere*, Email, Enkripsi, Dekripsi

I. PENDAHULUAN

1.1 Latar Belakang

Dengan dimilikinya perkembangan dunia informatika bagi para pengguna yang memakai media komunikasi tersebut untuk pertukaran informasi data yang penting.Media yang sering dipakai harus yang dapat diraih dan digunakan oleh masyarakat banyak.Seperti media komunikasi yang sering dipakai seperti internet,layanan email,dan telepon Media teknologi informasi yang digunakan untuk mengirim pesan dan menerima pesan sebuah data informasi,karena mudahnya masyarakat mengakses media penyimpanan data informasi dalam jaringan internet ataupun email berdampak dengan maraknya terjadi pencurian data informasi perusahaan atau pribadi.Saat pertumbuhan dunia teknologi digital informasi suatu media komunikasi menjadi wadah untuk media penyimpanan data informasi dan pengiriman ketempat lainnya. Informasi menjadi sangat rentan untuk diketahui, dicuri dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab.

Di perusahaan yang bergerak di bidang pelayanan webstore seperti Kotakpensil.com,Data informasi *website*,webtraffice dan penjualan *website* yang akan dikirim atau diterima melalui *email* adalah sebuah data informasi yang rahasia. Oleh sebab itu maka dibutuhkan suatu metode yang dapat

menjaga kerahasian informasi tersebut dari pihak –pihak yang tidak di inginkan.Metode yang dimaksud adalah kriptografi informasi atau pesan dengan tujuan menjaga keamanannya agar tidak dapat digunakan oleh sesorang yang tidak berwenang.Metode penyandian yang dibutuhkan pada saat ini tetap harus beradaptasi melalui berkembangnya penggunaan komputer digital pada masa kini.Berdasarkan pernyataan di atas, perlu ada suatu system keamanan data informasi baik saat pengiriman maupun penerimaan email. Untuk mengerjakan bagian ini ada suatu teknik yang bisa di sebut informasi tersandi. Dalam penilitian ini akan mencoba menerapkan suatu akar ilmu matematika yang disebut dengan kriptografi. Dengan kriptografi, , proses ini disebut Enkripsi dan Deskripsi data informasisebuah data informasi dapat diubah menjadi sandi-sandi yang tidak dapat dibaca oleh yang tidak memiliki akses serta mengembalikannya ke bentuk aslinya.Pada laporan Tugas Akhir ini menjelaskan, akan memakai metode enkripsi dan deskripsi yang berupa algoritma RC4(rivest cipher4) dan Vigenere.

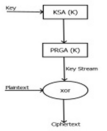
II. LANDASAN TEORI

2.1. Algoritma Rivest Code 4 (RC4)

Pada pertama kalinya di rancang oleh Ron Rivest yang berada dari tempat penelitian RSA pada tahun 1987. RC sendiri memiliki nama lain yang resmi ialah "*Rivest Chiper*", tapi juga di ingat "*Ron's Code*". RC4 sebenarnya disembunyikan dan tidak dipublikasikan kepada masyarakat banyak, akan tetapi diketahui pada september 1994, kode tersebut dikirim oleh sesseorang yang diketahui dan terebar ke banyak situs internet. Kode yang bocor tersebut akhirnya diterima sebagai RC4 karena memiliki keluaran yang sama pada perangkat lunak dengan di dalam lisensi RC4. Karena algoritma sudah diketahui, RC4 tidak lagi dapat menjadi sangat rahasia. Nama RC4 di hak ciptakan, sehingga selalu dikatakan menjadi "ARCFOUR" atau "ARC4" (Alleged RC4) untuk menjauhi pengakuan hak cipta. RSA Security tidak penah secara resmi terbitnya algoritma ini atau yang selalu disebut RC4, namun Rivest secara perseorangan yang merilisnya dengan menggabungkan wikipedia Inggris ke tulisan-tulisan yang ia miliki. RC4 telah menjadi sebuah bagian dari perintah enkripsi yang standart dan selalu digunakan. Faktor utama yang menjadi keberhasilan RC4 adalah efesiensinya dan kecepatannya dalam mengolah banyak aplikasi, sehingga dapat mudah untuk digembangkan implementasi yang efisien ke software dan hardware. RC4 dikategorikan dalam algoritma kriptografi simetris.Atau bias juga disebut dengan algoritma kriptogarfi simetris karena memiliki kunci yang sama untuk mengenkripsi atau mendekripsi suatu pesan, data, ataupun informasi.

2.2. Algoritma Enkripsi Rivest Code 4 (RC4)

RC4 adalah jenis stream cipher yang mempunyai sebuah kotak array S-Box, S0,S1,S2....,S225, yang memiliki perpindahan dari bilangan 0 hingga 225, dan perpindahan sebagai kegunaan dari key dengan ukuran variable. Dalam algoritma enkripsi metode ini akan menciptakan psedo random byte pada key yang akan dijumlahkan oleh operasi XOR terhadap teks asli untuk mendapatkan ciphertext. Untuk memberikan terjadinya enkripsi pada algoritma RC4, berikut bisa melihat pada gambar di bawah ini :



Gambar 2.1. Stream Cipher Enkripsi RC4

Dalam garis besar diketahui algoritama dari metode RC4 stream *cipher* ini dibagi menjadi dua bagian, berupa : *key setup* dan *key schedulling Algoritma* (KSA) dan *system generation* atau *Pseudo Random Generation Algoritma* (PRGA) dan proses XOR dengan *stream* data. Setelah ini dapat dijelaskan bagaimana proses dari algoritma RC4 *stream cipher* tersebut.

1) *key setup* atau *key schedulling Algoritma* (KSA)

Pada bagian ini terdapat tiga tahapan proses didalamnya yaitu :

a) inisialisai S-Box

Pada tahap ini, S-Box akan diisi dengan nilai sesuai indeks untuk mendapatkan S-Box awal. Algoritmanya sebagai berikut:

(1). Untuk i=0 sehingga i=255 lakukan
(2). Mengisi s dengan nilai i
(3). Menambahkan I dengan 1, kembali ke 2

b) Disimpannya kunci dalam *Key Byte Array*

untuk tahap ini kunci (*key*) yang akan digunakan untuk menyandikan atau mengembalikan akan diinput dalam *array* berjumlah 256 secara berulang sampai seluruh *array* terisi. Algoritmanya adalah sebagai berikut:

(1).Mulai dengan 1
(2).Untuk i=0 sehingga i=255 lakukan
(3). Jika j > panjang kunci maka
(4). j diisi dengan nilai 1
(5). Akhir jika
(6). Input K dengan I nilai ASCII karakter kunci ke j
(7). Nilai j diubah menjadi 1
(8). Menambahkan I dengan 1 kembali ke 2

c) Perpindahan pada S-Box

Pada proses ini, akan dibedakan sebuah nilai yang akan menjadi hukum dasar untuk perubahan pada S-Box. Pertama isi secara berurutan s(0)=0, s(1)=1,…,s(255)=255. Kemudian isi array k(0), K(1),…,<K(255) terisi semuanya.Sesudah indeks j dengan 0. Algoritmanya adalah sebagai berikut:

(1). Bila nilai j dengan 0

(2). Maka i=0 sehingga i=panjang *plaintext*

(3). Input nilai j dengan jumlah operasi (j+s(i)+k(i)) mod2356

(4). Pindah nilai s(i) dan s(j)

(5). Menambahkan I dengan 1, kembali ke 2

2) *Stream Generation* atau *pseudo Random Generation Algoritma* (PGRA)

Pada proses ini akan didapatkan *pseudo Random* yang akan diketahui oleh operasi XOR untuk mendapatkan *ciphertext* ataupun kebalikannya yaitu untuk mendapatkan teks asli. Algoritmanya adalah sebagai berikut:

(1). Input indeks I dan J dengan nilai 0

(2). Maka i=0 sehingga i=panjang *plaintext*

(3). input bilangan I dengan jumlah yang didapatkan operasi (i+1) mod 256

(4). Input bilangan j dengan hasil yang didaptkan (j+s(i)+k(i)) mod 256

(5). Pindahkan nilai S(i) dan S(j)

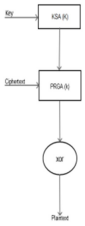
(6). Input bilangan t dengan hasil operasi (S(i)+(S(j) mod 256)) mod 256

(7). Isi nilai y dengan nilai S(t)

(8). Nilai y yang dikenakan operasi XOR terhadap *plaintext*

(9). Tambahkan I dengan 1, mulai kembali pada baris ke 2

2.3. Algoritma Dekripsi Rivest Code 4(RC4)



Gambar 2.2. Stream Cipher Dekripsi RC4

Alogaritma dekripsi RC4 hampir sama dengan algoritma enkripsinya, perbedaanya hanya ketika *stream generation,* yaitu untuk mendapatkan teks asli semula maka *ciphertext* nya akan dikenakan operasi XOR terhadap *pseudo random byte* nya. Algoritma pembuatan kunci pada proses dekripsi sama dengan algoritma enkripsinya yang diperoleh dari inisialisasi S-Box, penyimpanan kunci kedalam *key byte array* hingga proses dekripsi dan enkripsi akan menghasilkan *key stream* yang sama. Perbedaannya hanya ketika *stream generation* nya, yaitu yang dioperasikan bersama *key stream* adalah *ciphertext* untuk mendpatkan kembali teks asli. Algoritmanya adalah sebagi berikut:

1) Isi indeks I dan j dengan nilai 0
2) Pada i=0 sampai i=ukuran *ciphertext*(ukuran*ciphertext*=ukuran *plaintext)*
3) Input nilai I pada hasil operasi (i+1) mod 256
4) Input nilai j dengan hasil yang di dapat dari operasi (j+S(i)) mod 256
5) Menukar nilai S(i) dan S(j)
6) Isi nilai t dengan hasil operasi (S(i)+(S(j) mod 256)) mod 256
7) Isi nilai y dengan nilai S(t)
8) Nilai y dijumlahkan oleh operasi XOR pada *ciphertext*
9) Menambahkan i dengan 1, kembali ke 2

2.4. Algoritma Vigenere Cipher

Pada tahun 1533 seperti dicatat dalam buku *La Cifra del Sig* kode *vigènere* adalah bagian kode dari abjad-majemuk (*polyalphabetic substitution cipher*). Dikatakan oleh seseorang diplomat (sekaligus seorang kriptologis) Blaise de, Perancis,Vigènere pada saat tahun 1586,abad 16. Sesungguhnya Giovan Batista Belaso telah membuat gambar untuk pertama kali. Algoritma ini baru terkenal pada 200 tahun setelahnya dan diberikan nama dengan sebuah sebutan *vigènere kode. Vigènere* merupakan penyebab perang warga di Amerika dan *vigenere kode* digunakan oleh Tentara Aliansi (*Confederate Army*) pada perang warga Amerika (*American Civil War*). Kode *vigènere* berhasil

diselesaikan oleh seseorang yang bernama Babbage dan Kasiski pada abad menengah 19.pada algoritma enkripsi tipe ini sangat diingat karena mudah dipelajari dan diimplementasikan. Teknik untuk mendapatkan *ciphertext* bisa dilakukan menggunakan pergeseran angka maupun bujur sangkar *vigènere*. Teknik susbtitusi menggunakan algoritma *vigènere* dengan menggunakan angka dilakukan dengan pertukaran huruf dengan angka, hampir seperti pada kode geser.contoh:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 2.3. Tabel Perpindahan Algoritma Kriptografi Vigenere Cipher

Plaintext: PLAINTEXT
Kunci: CIPHER

Plain	15	11	0	8	13	19	4	23	19
Kunci	2	8	15	7	4	17	2	8	15
Hasil	17	19	15	15	17	10	6	5	8
Ciphertext	R	T	P	P	R	K	G	F	I

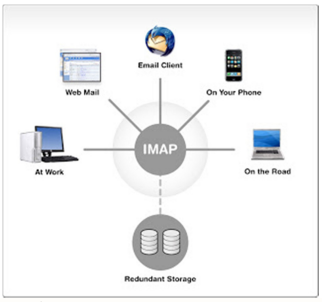
Gambar 2.3. Tabel Kriptografi dengan Algoritma Vigenere Cipher

Dengan metode Subsitusi angka dengan huruf , didapatkan ternyata teks asli (PLAINTEXT) mempunyai kode bilangan (15,11, 0, 8, 13, 19, 4, 23, 19), seterusnya kode bilangan untuk teks kunci (CIPHER) berupa(2, 8, 15, 7, 4, 17). Setelah itu lakukan perhitungan, maka menghasilkan kode angka yang berupa *ciphertext* (17, 19, 15, 15, 17, 10, 6, 5, 8). Jika diterjemahkan kembali menjadi huruf sesuai urutan awal,yang berhurufkan RTPPRKGF.

2.5. IMAP

Internet Message Access Protocol ialah protokol standar untuk mengakses email dari server. IMAP memungkinan pengguna memilih pesan email yang akan ia ambil, membuat folder diserver, mencari pesan email tertentu, bahkan menghapus pesan email yang ada. Kemampuan ini jauh lebih baik dari pada POP (Post Office Protocol) yang hanya memperbolahkan kita mengambil atau mendownload semua pesan yang ada tanpa kecuali.

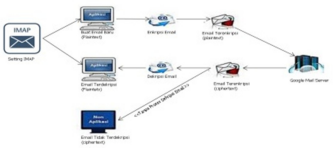
Internet Message Accsess Protocol merupakan salah satu dari protocol penerimaan email (*email retrieval protocol*). Juga diketahui dengan nama *IMAP*, merupakan *Internet protocol* yang beroperasi pada *layer Application.*
Dengan *IMAP*, kotak pesan masuk bisa dibaca dan diprose secara multitask (bersamaan) oleh sebagian besar *email client* yang tidak sama. *IMAP* selalu digunakan oleh sebagian banyak para pengguna Internet untuk men-*download* email dari *web mail server*.biasa disebut sebagai Interim Mail Accsess Protocol, versi IMAP pertama telah menjalani beberapa versi sejak tahun 1986 saat dibuat. Saat ini disebut menjadi Internet Message Accsess Protocol,versi yang digunakan adalah versi keempat yang sudah menjadi standart saat tahun 1994,dan dipublikasi oleh RFC 1730.IMAP memiliki beberapa keunggunalan termasuk kemampuan untuk memuat bagian dari email kerimbang menunggu semua attachmen didalamnya. IMAP juga dapat meneriam isi pesan memiliki mekanisme MIME. IMAP client juga selalu akan bisa terhubung dengan mail server dalam jangka waktu yang sangat lama, yang dapat meningkatan respond time secara keseluruhan.



Gambar 2.4. IMAP Diagram

III. PERANCANGAN SISTEM

3.1. Proses Sistem



Gambar 2.5. Arsiktektur Sistem

IV. HASIL DAN PEMBAHASAN

4.1. Pengukuran Kinerja Aplikasi

Pengukuran kinerja aplikasi dilakukan untuk melakukan evaluasi tingkat keberhasilan terhadap teknik yang digunakan. Dalam hal ini sudah dilakukan percobaan mengirim email melalui aplikasi kepada penerima dan dibuka dengan menggunakan aplikasi maupun tidak yang nantinya akan digunakan sebagai pembanding. Nantinya akan terlihat perbedaan antara isi email yang dibuka dengan aplikasi dan yang tidak.

Tabel 4.1 : Tabel pengujian pada enkripsi pesan

Nama Pesan	Ukuran Pesan Asli (Byte)	Ukuran *Pesan* Enkripsi (*Byte*)	Waktu Enkripsi (detik)
Wiki11	5381	10038	4.06
Rc4	6229	10045	5.65
Kriptografi	8008	12159	5.63
Sejarah Komputer	7669	11805	6.72
Test 15	1047	5196	0.14
Rata-rata :	5666,8	9848,6	4.44

Tabel 4.2 : Tabel pengujian pada dekripsi pesan

Nama Pesan	Ukuran Pesan Asli (Byte)	Ukuran Pesan Dekripsi (*Byte*)	Waktu Dekripsi (detik)
Wiki11	5381	5381	6.82
Rc4	6229	6229	7.74
Kriptografi	8008	8008	9.18
Sejarah Komputer	7669	7669	9.53
Test15	1047	1047	0.22
Rata-rata :	5666,8	5666,8	6,7

4.2. Kelebihan Dan Kekurangan Aplikasi

Kelebihan Aplikasi :

Aplikasi ini tidak terlalu membutuhkan spesifikasi perangkat lunak dan perangkat yang keras yang tinggi.Karena Tampilannya yang simpel, pengguna dapat dengan mudah menggunakanya, ditambah dengan adanya bantuan pemakaian pada apliksi tersebut.

Kekurangan Aplikasi:

Keterbatasan karakter penulisan max 5500 karakter.Masih belum dapat mengirim *attachment* pada aplikasi ini.Belum adanya kolom CC dan BCC sehingga hanya bisa memasukkan satu email tujuan saja.Untuk email tujuan baru bisa menapung 1 akun saja, belum bisa kirim email kepada beberapa akun sekaligus.

V. KESIMPULAN

Berdasarkan analisa yang telah dilakukan terhadap aplikasi Client Email terenkripsi yang telah saya buat, maka dapat diambil kesimpulan dan saran yang di perlukan membuat sistem yang lebih baik lagi.

5.1. Kesimpulan

Berdasarkan hasil dan pembahasan pengujian aplikasi sebelumnya terhadap permasalahan dan aplikasi yang telah diterapkan, akan sehingga dapat diperoleh kesimpulan mengenai proses enkripsi dan dekripsi terhadap masalah keamanan data perusahaan, antara lain:

Dari hasil tabel pengujian enkripsi dan dekripsi email diketahui bahwa ukuran rata-rata email yang di enkripsi 9488,6 *byte* dengan waktu rata-rata 4,44 detik dan rata-rata ukuran email yang di dekripsi 5666,8 *byte* dengan waktu rata-rata 6,7 detik.

5.2. Saran

Aplikasi Client Email Terenkripsi ini masih belum sempurna, karena masih memerlukan perbaikan untuk meningkatkan kegunaan, kemudahan dan penambahan tambahan aplikasi untuk mendukung kegiataan, Beberapa saran yang perlu diajukan untuk perbaikan adalah sebagai berikut :

Aplikasi dapat mengirimkan file yang di attachment melalui aplikasi ini.Aplikasi bisa mendukung banyak jenis akun layanan email.

DAFTAR PUSTAKA

[1]Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta.

[2]Efrandi,Asnawati,Yupianti.(2014).Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher.Bengkulu

[3]Elkas Lukman Hakim,Khairil,Ferry Hari Utami.(2014).Aplikasi Enkripsi dan Dekripsi Data Menggunakan Pemograman PHP.Bengkulu

[4]Erima Oneto, Y. S. (2009). *Anti Gaptek Internet.* jakarta: Penerbit PT Kawan Pustaka.

[5]Hakim, F.Wiwiek Nurwiyati, Indra Yatini B.(2013).Enkripsi Deskripsi Data Menggunakan Metode Stream Dan Vigenere Cipher.Yogyakarta.

[6]Militia, S. (n.d.). Retrieved November 11, 2017, from http://computer-muter.blogspot.co.id/2012/11/imap-internet-message-access-protocol.html

[7]Munir,R.(2013).*Kriptografi.* Bandung: Teknik Informatika.

[8]Munir,Rinaldi., 2006, *Kriptografi*. Penerbit Informatika, Bandung.

[19] Nurcahyo Budi,Zulfian Asmi,Saiful Nur Arif.(2016).Aplikasi Keamanan Email Menggunakan RC4.Jakarta.

[10] Yuli Praptomo, (2015).Implementasi Algoritma Kriptografi Vigenere Cipher untuk mengamankan File Text Menggunakan Java NETBEAN 8.0. Yogyakarta.