APLIKASI KEAMANAN EMAIL DATA PRODUKSI PT KUNYUN GRAVURE INDUSTRIES INDONESIA DENGAN RC4 DAN BASE64

Wahyu Eko Winanto[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
E-mail : 1211510209@student.budiluhur.ac.id[1)], mufti@budiluhur.ac.id[2)]

ABSTRAK

Pembuatan aplikasi ini di dasari oleh masalah yang ada pada PT. Kunyun Gravure Industries Indonesia yaitu pengiriman data teknik produksi yang dikirim melalui email, karena banyaknya pengguna email perusahaan. Pihak perusahaan ingin membatasi akses terhadap email tersebut, terutama email yang menyangkut data produksi. Yang mungkin akan menyebabkan bocornya data perusahaan kepada pihak *competitor* yang akan berdampak pada kepercayaan *customer* dan berkurangnya *order* perusahaan, untuk mengatasi potensi terjadinya pencurian atau manipulasi data tersebut adalah dengan menggunakan aplikasi keamanan email berbasis web dengan bahasa pemograman PHP dan teknik kriptografi RC4 dan base64. Dengan adanya teknik Kriptografi maka data perusahaan yang bersifat rahasia akan memiliki tingkat keamanan yang baik karena berkas yang disimpan sudah mengalami pengacakan yang sulit dibaca oleh orang yang ingin mencuri data tersebut. Sehingga orang lain yang tidak memiliki aplikasi keamanan email tidak dapat mengetahui isi email yan sudah di enkripsi.

Kata kunci: Kriptografi, *RC4, Base64*, Email, Enkripsi, Dekripsi

1. PENDAHULUAN

1.1 Latar Belakang

Dengan pesatnya perkembangan dunia informatika saat ini membuat pertumbuhan dunia ke dalam masa teknologi informasi menjadi salah satu faktor utama menuju kesuksesan. Oleh Karena itu nilai informasi saat ini sangat penting dan tinggi. Teknologi informasi saat ini berada di atas lebih unggul dari pada media komunikasi sebagai suatu media untuk menyampaikan informasi pada suatu tempat antar tempat lainnya. Informasi-informasi yang akan disampaikan berjalan melalui media komunikasi yang ada saat ini.

Media komunikasi yang biasanya digunakan adalah sebuah media yang mudah dijangkau dan digunakan oleh orang banyak. Contoh media komunikasi saat ini yang sering digunakan adalah jaringan internet, telephone, dan email. Kemudahan dalam pengaksesan media komunikasi oleh semua orang membawa dampak besar bagi keamanan informasi atau pesan yang sudah memakai media komunikasi saat ini. Informasi jadi sangat mudah untuk diambil, diketahui dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab.

Pembuatan aplikasi ini dilatar belakangi oleh suatu masalah di pada PT. Kunyun Gravure Industries Indonesia yaitu masalah keamanan dalam melakukan pengiriman data perusahaan yaitu data teknik produksi, dikarenakan adanya kendala jarak antaran kantor dengan pabrik maka data teknik produksi dikirim melalui email oleh karena itu memungkinkan terjadinya manipulasi data atau pencurian data perusahaan. Menyebabkan bocornya data perusahaan kepada pihak *competitor* yang akan berdampak pada kepercayaan *customer* dan berkurangnya *order* perusahaan, untuk mengatasi potensi terjadinya pencurian atau manipulasi data adalah dengan menggunakan teknik kriptografi RC4 dan base64.

Berdasarkan pernyataan di atas, diperlukan suatu system pengamanan informasi baik saat mengirimkan maupun menerima email. Untuk mengatasi masalah ini ada suatu cara yang biasa digunakan yaitu dengan membuat penyandian data. Dalam penilitian ini akan mencoba menerapkan suatu cabang ilmu matematika yang biasa disebut dengan kriptografi. Dengan kriptografi, data yang ada dapat diubah menjadi sandi-sandi yang tidak dimengengerti oleh orang awam pada umumnya serta dapat mengembalikannya ke dalam bentuk sebenarnya, proses ini yang disebut Enkripsi dan Deskripsi. Algoritma enkripsi yang ada saat ini sudah cukup banyak. Pada laporan Tugas Akhir yang saya buat ini, akan menerapkan metode enkripsi dan deskripsi menggunakan algiritma RC4(rivest cipher4) dan base64.

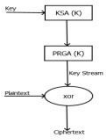
2. LANDASAN TEORI

2.1 Algoritma RC4 (Rivest Code 4)

Algoritma RC4 pertama kali di rancang oleh Ron Rivest RSA pada tahun 1987 dari Laboratorium. RC adalah sebuah singkatan resmi yaitu "*Rivest Chiper*", namun biasa di kenal "*Ron's Code*". RC4 pada awalnya dirahasiakan dan tidak dipublikasikan kepada khalayak umum, akan tetapi pada september 1994 algoritma tersebut telah diketahui adanya, kode tersebut dikirim oleh seseorang yang mengetahuinya dan menyebar ke banyak situs-situs internet. Kode yang telah bocor tersebut akhirnya dipastikan sebagai RC4 karena mempunyai output yang serupa dengan software RC4 berlisensi di dalam programnya. Karena algoritma sudah banyak diketahui, RC4 tidak menjadi rahasia. Nama RC4 akhirnya dipatenkan,

sehingga sering disebut sebagai "ARC4" atau "ARCFOUR" (Alleged RC4) untuk menghindari lisensi yang dipatenkan. RSA Security secara resmi tidak penah merilis algoritma tersebut, akan tetapi Rivest secara pribadilah yang merilisnya dengan menghubungkan kedalam wikipedia Inggris ke catatan yang ia miliki. RC4 telah menjadi sebuah aturan enkripsi yang umum dan banyak digunakan. Faktor utama atas kesuksesan RC4 adalah keserdahanaannya dan kecepatanya dalam menangani berbagai aplikasi, sehingga mudah untuk mengembangkan implementasi yang efisiensi ke hardware dan software. RC4 termasuk algoritma kriptografi simetris. Disebut algoritma kriptogarfi simetris karena kunci untuk mengenkripsi atau mendekripsi menggunakan kunci yang sama dalam suatu pesan, informasi, ataupun data (Rosyidi, M. U. 2014).

RC4 adalah jenis stream cipher yang mempunyai sebuah S-Box, S0,S1,S2,S3,S4....,S225, yang berisi permutasi mulai dari bilangan 0 sampai 225, dan permutasi ialah fungsi dari kunci atas panjang variable. Dalam algoritma metode enkripsi ini akan membangkitkan psedo random byte dari key yang nanti akan digunakan operasi XOR pada plaintext untuk dapat menghasilkan ciphertext. Untuk mengetahui proses enkripsi dari algoritma RC4, dapat dilihat pada keterangan gambar di berikut ini :



Gambar 1. Stream Cipher Enkripsi RC4

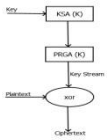
Pada dasarnya algoritama dari metode RC4 stream *cipher* ini terbagi atas dua bagian, yaitu : *key schedulling Algoritma* (KSA)dan *key setup* dan *Pseudo Random Generation Algoritma* (PRGA) atau *system generation* dan proses XOR dengan *stream* data. Berikut ini penjelasan atas bagian bagian dari algoritma Rivest Code 4 *stream cipher* ini.

1) *key schedulling Algoritma* (KSA) atau *key setup*
   Pada proses ini diperoleh tiga tahapan proses didalamnya yaitu :
   a) inisialisai proses S-Box
      Pada proses ini, S-Box akan dimasukan dengan nilai seperti indeksnya demi mendapatkan nilai S-Box awal. Berikut algoritmanya:
      (1). Maka i=0 hingga i=255 proses
      (2). Masukan i pada nilai s
      (3). Jumlahkan i dan 1, dan akan kembali pada point 2.
   b) Menyimpan kunci dalam *Key Byte Array*
      Pada proses kunci (*key*) yang akan kita lakukan untuk mengenkripsi atau dekripsi akan dimasukan kedalam *array* berukuran 256 berulang terus menerus hingga semua *array* terisi. Algoritmanya adalah sebagai berikut:
      (1). Masukan nilai 1
      (2). Pada i = 0 hingga i=255 proses
      (3). Jika j > jumlah kunci lalu
      (4). j dimasukan nilai 1
      (5). Jika berakhir
      (6). Masukan nilai K dan I dalam nilai ASCII karakter pada kunci j
      (7). Maka Nilai j akan naik 1
      (8). Jumlahkan i dan 1, dan akan kembali pada point 2.

   c) Permutasi pada S-Box
      Pada tahapan ini, akan dibandingkan pada nilai yang telah ditetapkan sebagai aturan permutasi pada proses S-Box. Mulai dengan isi berurutan s(0)=0, s(1) = 1,….,s(255)= 255. Setelah itu isi seluruh array k(0),K(1),….,<K(255). Setelah indeks j dengan nol. Algoritmanya adalah sebagai berikut:
      (1). Jika nilai j dengan 0
      (2). Untuk i=0 sehingga i=panjang *plaintext*
      (3). Masukan nilai j beserta hasil dari operasi (j + s(i) + k(i)) mod2356
      (4). Tukar nilai s(i) dan s(j)
      (5). Jumlahkan i dan 1, dan akan kembali pada point 2.

2) *Pseudo Random Generation Algoritma* (PGRA) atau *Stream Generation*
   Pada tahapan ini akan dihasilkan *pseudo Random* yang akan dikenalkan operasoi XOR demi mendapatkan *ciphertext* maupun sebaliknya yaitu untuk mendapatkan *plaintext*. Berikut adalah algoritmanya :
   (1). Isi indeks I dengan nilai 0, dan indeks J isi juga dengan nilai 0
   (2). Pada i=0 sampai i=panjang *ciphertext*, panjang *ciphertext* = panjang *plaintext*
   (3). Isi nilai I beserta hasil dari operasi (i+1) mod 256
   (4). sedangkan nilai j dengan hasil dari operasi (j+S(i)) mod 256
   (5). Tukar nilai antara S(j) dan S(i)
   (6). masukan nilai t beserta hasil dari operasi (S(i)+(S(j) mod 256)) mod 256
   (7). Masukan nilai y dan nilai S(t)
   (8). Nilai y digunakan pada operasi XOR kepada *ciphertext*
   (9). Jumlahkan i dan 1, dan akan kembali pada point 2

2.2 Algoritma Dekripsi Rivest Code 4(RC4)



Gambar 2. Stream Cipher Dekripsi RC4

Alogaritma dekripsi Rivest Code 4(RC4) serupa dengan algoritma enkripsinya, yang membedakan hanya pada saat *stream generation*, yaitu untuk menghasilkan *plaintext* asli oleh karena itu *ciphertext* nya akan menggunakan operasi XOR kepada *pseudo random byte* nya. Dan algoritma *key setup* pada proses dekripsi serupa dengan algoritma enkripsinya yang telah inisialisasi proses S-Box, penyimpanan kunci kedalam *key byte array* sampai proses enkripsi dan dekripsi akan medapatkan *key stream* sama. Perbedaannya ada pada *stream generation* nya, yaitu yang diproses bersamaan dengan *key stream* adalah *ciphertext* untuk mendapatkan kembali plaintext. Berikut adalah Algoritmanya :

1) Isi indeks I dengan nilai 0, dan indeks J isi juga dengan nilai 0
2) Pada i=0 sampai i=panjang *ciphertext*, panjang *ciphertext* = panjang *plaintext*
3) Isi nilai I beserta hasil dari operasi (i+1) mod 256
4) sedangkan nilai j dengan hasil dari operasi (j+S(i)) mod 256
5) tukar nilai antara S(j) dan S(i)
6) masukan nilai t beserta hasil dari operasi (S(i)+(S(j) mod 256)) mod 256
7) masukan nilai y dan nilai S(t)
8) Nilai y digunakan pada operasi XOR kepada *ciphertext*
9) Jumlahkan i dan 1, dan akan kembali pada point 2

2.3 Algoritma Base64

Base64 merupakan sistem untuk mewakili data byte dalam bentuk karakter *ASCII*. Pada Base64 menyiapkan 6-bit encoding dan 8-bit untuk ASCII karakter. Dalam Base64 sendiri istilah generik untuk sejumlah skema pengkodean serupa yang encode data biner dengan numerik dan menerjemahkannya ke dalam basis 64. Base64 istilah berasal tertentu MIME konten transfer encoding. Skema pengkodean Base64 biasanya digunakan ketika ada kebutuhan untuk mengkodean data biner yang perlu disimpan lalu ditransferkan melalui media yang dibuat untuk mengatasi data tekstual. Ini untuk memastikan bahwa data tetap utuh tanpa modifikasi selama transportasi. Base64 biasa digunakan dalam berbagai aplikasi termasuk email melalui MIME, dan menyimpan data yang kompleks dalam XML. Base64 berbentuk dalam format yang dicetak menggunakan karakter, memungkinan data binari yang akan dikirim dalam bentuk data email, dan disimpan di database atau file.

Skema enkripsi Base64 pada umumnya juga digunakan saat diperlukan sandi terhadap data biner yang didesain untuk mengatasi data dalam bentuk teks, hal ini bertujuan untuk menjaga data saat dalam pengiriman ke email server. Karakter yang didapatkan pada transformasi Base64 ini adalah dari 0...9, A...Z dan a...z, serta ditambah adanya 2 karakter terakhir + dan / serta sebuah karakter sama dengan (=) yang berfungsi untuk menyesuaikan dan menggenapkan data binary atau istilah lainya disebut sebagai pengisi pas. Karakter simbol yang akan dihasilkan itu tergantung dari proses algoritma yang berjalan. Kriptografi Base64 di dunia internet banyak digunakan sebagai media data format untuk mengirim data, hal ini disebabkan karena hasil dari Base64 berupa plaintext, maka data tersebut akan jauh lebih mudah dalam proses pengirim, dari pada dengan format data yang berupa binary. Dalam Encoding_Base64 dapat dikatagorikan dan dibedakan menjadi kriteria yang tertera dan dapat dilihat di dalam table. Teknik encoding Base64 pada dasarnya sederhana, contohnya pada satu (string) byte yang akan disandikan ke Base64 caranya adalah sebagai berikut :

1) Buat pecahan string bytes menjadi ke per 3 bytes.
2) Satukan 3 bytes menjadi 24 bits. Dengan syarat 1 bytes = 8 bit, dan dijumlahkan 3x8=24 bits.
3) Selanjutnya 24 bits yang tersimpan di-buffer dipecahkan menjadi 6 bits, maka akan mendapatkan 4 pecahan.
4) Pecahan masing-masing diubah ke dalam nilai decimal, dengan maksimal nilai 6 bit adalah 63.
5) Terakhir, nilai-nilai decimal tersebut ubah menjadi indeks untuk memilih karakter penyusunan dari Base64 dan maksimum adalah 63. Bisa lihat pada indeks ke 64.

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						pad	=

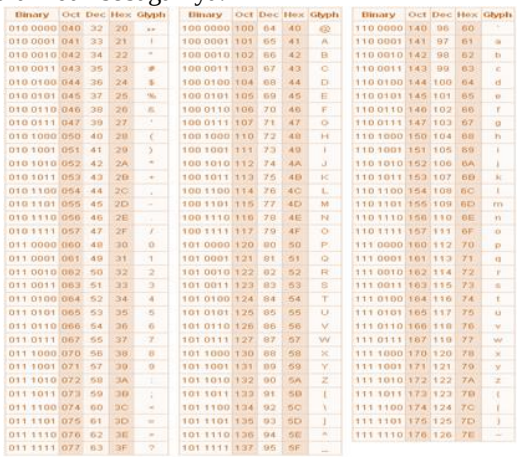
Gambar 3. Tabel index Base64

Transformasi Base64 merupakan salah satu algoritma untuk melakukan proses encoding dan decoding suatu data yang diubah dalam format *ASCII*, dengan berdasarkan pada bilangan 64.

karakter yang didapatkan pada Base64 adalah dari 0...9, A-Z dan a-z, serta ditambah adanya 2 karakter terakhir + dan /. Seperti itulah langkah – langkah enkripsi menggunakan algoritma Base64.

2.4 Pengertian ASCII

ASCII adalah karakter kode standar yang ditetapkan untuk digunakan dalam pertukaran informasi antara sistem pengolahan informasi, sistem komunikasi, dan peralatan terkait standar berikutnya yang akan meresepkan cara menerapkan standar ini di media *participal*, seperti *perforated tape*, *punched cards*, dan *magnetic tape*. Standar ini akan digunakan untuk pertukaran informasi digital. komunikasi lain untuk menunjukkan teks. Sebenarnya kode *ASCII* memanfaatkan biner sebanyak 8 bit. Dimulai dari 0000 0000 hingga 1111 1111. Dalam pengkodean, kode *ASCII* memanfaatkan 8 bit. Saat ini pada kode *ASCII* sudah tergantikan oleh kode *UNICODE (Universal Code)*. *UNICODE* dalam pengkodeannya menggunakan 16 bit sehingga mengizinkan untuk menyimpan kode-kode lainnya yaitu kode bahasa Cina, Jepang, Vietnam dan sebagainya.

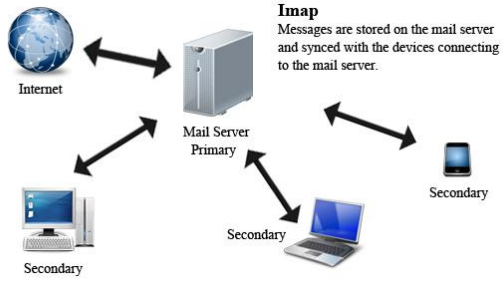


Gambar 4.Kode ASCII

2.5 Pengertian IMAP

IMAP *(Internet Message Access Protocol*) IMAP adalah sebuah singkatan dari *Internet Message Access Protocol*, dan untuk POP adalah merupakan singkatan dari *Post Office Protocol*., keduanya termasuk dalam *protocol email*. Pada sistem (IMAP dan POP) mengizinkan kamu dapat mengakses email melalui software email client, seperti Mozilla, Thunderbird dan Microsoft Outlook.

POP3 (*Post Office Protocol version 3*) adalah protocol yang dapat digunakan untuk mengambil email dari email server. Protokol POP3 ditujukan agar adanya server email yang menampung email sementara waktu hingga email tersebut diambil oleh penerimanya yang berhak.



Gambar 5.Diagram IMAP

3. ANALISA MASALAH DAN RANCANGAN PROGRAM

3.1. Analisa Masalah

PT. Kunyun Gravure Industries Indonesia adalah perusahaan yang bergerak dalam bidang film printing yang sudah 11 tahun berdiri. Dengan banyaknya persaingan, maka mungkin saja ada beberapa orang yang mencuri informasi penting secara diam-diam untuk diberikan kepada perusahaan yang bertindak sebagai pesaing demi mengambil keuntungan pribadi. PT. Kunyun Gravure Industries Indonesia sendiri belum mempunyai sistem keamanan untuk menjaga informasi penting yang dikirim atau diterima melalui email dari perusahaan-perusahaan pesaing. Oleh karena itu dibutuhkan suatu aplikasi yang dapat mengamankan informasi penting tersbut dari perusahaan pesaing.

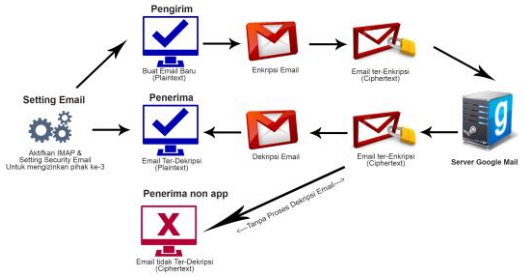
3.2. Penanganan Masalah

Karena masih kurangnya faktor keamanan dari informasi penting yang terdapat di email, maka perlu dibuatkan suatu aplikasi untuk mengenkripsi informasi tersebut, sehingga hanya dapat diakses oleh orang yang berkepentingan untuk melihat informasi tersebut. Orang lain yang tidak berkepentingan tidak dapat melihat isi dari email yang telah dienkripsi tersebut tanpa tahu email dan password login serta metode yang digunakan untuk mengenkripsi dan dekripsi informasi tersebut.

3.3. Arsitektur Sistem

Arsitektur sistem atau skema aplikasi dari program yang akan dibangun adalah seperti berikut. Yaitu dengan melakukan pengaturan pada email untuk mengaktifkan IMAP yang ada dalam email, lalu akses email pada perangkat komputer yang telah memilikir aplikasi ini. Maka sebelum email sampai pada server isi email tersebut akan dapat diproses enkripsi ataupun dekripsi untuk membacanya. Berikut adalah gambar dari arsitektur sistem aplikasi

ini:



Gambar 6.Arsitektur Sistem

4. HASIL DAN PEMBAHASAN

4.1. Pengukuran Kinerja Aplikasi

Aplikasi yang telah buat ini harus dilakukan pengukuran kinerja untuk mengetahui tingkat keberhasil terhadap teknik kriptografi yang digunakan, sudah cukup baik atau belumnya kinerja aplikasi ini sudah dilakukan percobaan pengiriman email dan pembacaan emaik melalui aplikasi ini dengan email yang berbeda.

Tabel 1 : Tabel Pengujian Enkripsi pesan *email*

Nama *Email*	Ukuran *Email* Asli (Byte)	Ukuran *Email* Enkripsi (*Byte*)	Waktu Enkripsi *Email* (detik)
Detik	3381	3381	0.01
Wikipeda_hewan	6139	6139	0.02
Wikipedia_gunung kidul	4559	4559	0.02
Wikipedia_Sejarah Komputer	5092	5092	0.01
Produksi kunyun	5092	5092	0.01
Tshoot link monitoring	5208	5208	0.01

Tabel 2 : Tabel Pengujian dekripsi pesan *emai*

Nama *Email*	Ukuran *Email* Asli (Byte)	Ukuran *Email* Enkripsi (*Byte*)	Waktu Dekripsi *Email*(detik)
Detik	3381	3381	1.17
Wikipeda_hewan	6139	6139	2.05
Wikipedia_gunung kidul	4559	4559	2.08
Wikipedia_Sejarah Komputer	5092	5092	0.01
Produksi kunyun	5092	5092	0.01
Tshoot link monitoring	5208	5208	1.96

4.2. Kelebihan Dan Kekurangan Aplikasi

Kelebihan Aplikasi :

Teks *email* yang dikirim dengan aplikasi dapat langsung terenkripsi dan tidak dapat dibaca bila tidak menggunakan aplikasi kemanan data email yang sama. Perangkat lunak dan perangkat yang keras yang akan digunakan untuk menjalakan aplikasi ini tidak memerlukan spesifikasi yang tinggi.Karena Tampilan yang digunakan sangat sederhana, memudahkan penguna aplikasi ini dalam menjalakanya, dan ditambah lagi dilengkapi dengan panduan bagi pengguna di dalam aplikasi tersebut sudah sangat membantu pengguna yang tidak mengerti.

Kekurangan Aplikasi:

Karakter penulisan memiliki keterbatasan max 5500 karakter.belum dapat mengirimkan *file attachment* saat mengunakan aplikasi ini.Belum terdapat kolom CC dan BCC oleh karena itu hanya bisa memasukkan satu alamat email tujuan saja. Sehingga tidak dapat mengirimkan email ke banyak email sekaligus. Dalam email yang terdapat banyak pesan saat proses enkripsi atau dekripsi akan terasa lama dalam prosesnya.

5. KESIMPULAN

5.1. Kesimpulan

Berdasarkan analisa yang ada telah dilakukan terhadap proses aplikasi keamanan email data produksi ini adalah :

1) Aplikasi ini mudah dimengerti dan mudah digunakan sebagai alat keamanan suatu perusahaan.
2) Isi email tidak dibaca oleh pengguna tanpa masuk kedalam aplikasi, karena tidak melalui proses dekripsi, sehingga keamanan informasi lebih terjaga.
3) Aplikasi ini dapat di gunakan dengan banyak akun akun email yang ada.

5.2. Saran

Aplikasi Keamanan Email ini pada dasarnya belum dapat dibilang sempurna, karena masih memerlukan beberapa perbaikan untuk meningkatkan efektifitas, efisiensi dan penambahan fitur untuk mendukung pekerjaan, Adapun saran yang perlu untuk perbaikan aplikasi ini adalah sebagai berikut :

1) Aplikasi ini dapat mengirim file yang diattacment
2) Aplikasi ini harus dapat mengunakan semua jenis email yang ada.
3) Dalam kinerja proses enkripsi dan dekripsi pada email yang memiliki banyak pesan bisa lebih cepat.
4) Dapat dibuat versi web, karena masih dalam localhost.

6. DAFTAR PUSTAKA

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

[2]Eko, W. (n.d.). *Share Information.* Retrieved November 21, 2017, from

http://sharewelcome.blogspot.co.id/2013/01/tabel-ascii-lengkap.html

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

[4] Hakim, E. L. dkk. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rivest Code 4 Dengan Menggunakan Bahasa Pemrograman PHP. *Jurnal Media Infotama Vol.10 No.1, Februari, Bengkulu*.

[5]Hendriyawan, M. A. (2004). Enkripsi Data Menggunakan Algoritma Rivest Code 4. *Jurnal Ilmiah, Teknik Elektro Politeknik Negeri Padang*.

[6]Irawan, H. (2009). *Aplikasi Java Mobile.* Palembang.

[7]Militia, S. (n.d.). Retrieved November 11, 2017, from http://computer-muter.blogspot.co.id/2011/12/imap- access--message-internet - protocol.html

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

[9] Nugraha, A. P. Gunadhi, E. (2016). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal umum*, Sekolang Tinggi Teknologi, *Garut*.

[10] Rosyidi, M. U. (2014). Implementasi Algoritma Kriptografi RC4 Pada Aplikasi SMS Berbasis Java. *Jurnal umum, Sekolah Tinggi Manajement Informatika dan Komputer, AMIKOM, Yogyakarta*.

[11] Sholeh, A. T. dkk. (2013). Mengamankan Skrip Pada Bahasa Program PHP Dengan Menggunakan Kriptografi Base 64. *Jurnal Algoritma Sekolah Teknologi Garut*, 1-9.

[12] Suryani, K. N. (2009). Algoritma RC4 Sebagai Metode Enkripsi. *Jurnal Umum, Program Studi Teknik Informatika - Sekolah Teknik Elektro Dan Informatika ITB, Bandung*.

[13]Septian, D. (n.d.). Retrieved November 03, 2017, from https://en.wikipedia.org/wiki/Base64.

[14]Wahyu, F. dkk. (2012). Penerapan Algoritma Gabungan Rivest Code 4 Dan Base64 Pada Sistem Keamanan E-Commerce. *Jurnal umum. Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Yoyakarta*.