IMPLEMENTASI KRIPTOGRAFI PADA PENGIRIMAN PESAN *EMAIL* DENGAN MENGGUNAKAN METODE *RC4* DAN *BLOWFISH* BERBASIS *WEB* PADA PT.DASCOM JAYA SAKTI

Frengki Danil Zain Rohman[1)], Mufti[2)]
Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : frengkidanil100@gmail.com[1)], muftyhayat@gmail.com[2)]

Abstrak

Informasi saat ini sangat mudah untuk diperoleh, email adalah media komunikasi yang sering digunakan pada saat ini. Di era perkemabangan teknologi komputer dan teknologi saat ini yang mengalami kemajuan yang sangat pesat, pentingnya keamanan data dalam bertukar informasi menggunakan email.. Dulu manusia berkomunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu salah satunya dengan cara mengirim surat. Dengan adanya teknologi saat ini maka berkomunikasi jarak jauh dapat dilakukan dengan mudah dan cepat menggunakan email. Bermodalkan internet manusia bisa saling berkomunikasi maupun bertukar informasi menggunakan email. Namun saat ini email semakin rentang terhadap penyadapan data atau informasi penting lainya. Penyadapan adalah salah satu masalah yang ditakuti oleh para pengguna media komunikasi. Maka dibuatkanlah sebuah keamanan enkripsi pada PT.DASCOM JAYA SAKTI. Tujuan pembuatan kemanan data ini adalah untuk menjaga kemanan data ataupun informasi yang tersimpan dalam bentuk pesan ataupun file, mengenkripsi email adalah salah satu cara yang digunakan untuk mengamankan email dengan menggunakan metode kriptografi. Algoritma kriptografi yang digunakan adalah menggunakan metode algoritma Rivrest Cipher 4 (RC4) dan Blowfish yang merupakan suatu algoritma yang simestris dan berbentuk chiper block.

Kata kunci: Kriptografi, Email, Rivest Chiper 4, Blowfish

1. PENDAHULUAN

Teknologi komputer saat ini mengalami perubahan yang sangat signifikan, bukan hanya di negara maju, di negara berkembang pun terjadi peningkatan terhadap pengguna komputer baik dalam aktifiatas Pendidikan dan bisnis. Pada zaman dahulu berkomunikasi jarak jauh menggunakan cara konvensional, salah satu diantaranya dengan cara mengirim surat. Dengan adanya teknologi, berkomunikasi jarak jauh dapat dilakukan dengan mudah menggunakan E-mail. Bermodalkan internet manusia bisa saling bekomunikasi maupun bertukar informasi menggunakan E-mail. Namun saat ini E-mail semakin rentan terhadap penyadapan data atau informasi penting lainya.

PT.DASCOM JAYA SAKTI merupakan suatu perusahaan yang bergerak pada bidang penjualan printer.metrix dan lampu LED () dan memiliki banyak customer di perusahaan-perusahaan logistic dan perbankan, Sehingga E-mail sering digunakan untuk melakukan komunikasi. Keamanan data pada PT.DASCOM JAYA SAKTI sangatlah penting seperti data service report, permintaan barang, dan permintaan maintance. Data tersebut merupakan data dari konsumen yang bersifat rahasia, oleh karena itu dibutuhkan tingkat keamanan data yang sangat tinggi.

Aplikasi E-mail pada dasarnya sudah memiliki keamanan karena telah memiliki password, namun jika password user tersebut di hack oleh orang yang tidak bertanggung jawab maka orang tersebut bisa masuk ke dalam email, hal tersebut membuat para karyawan pada PT.DASCOM JAYA SAKTI khawatir jika akan bertukar informasi melalui pesan E-mail. Untuk itu dibuatkanlah sebuah keamanan data pada E-mail.

Rivest Chiper 4 merupakan algoritma yang mempunyai kunci simestris yang berbentuk stream cipher. Faktor kesuksesan dari RC4 adalah kecepatan dan kesederhanaanya dalam menangani segala banyak aplikasi. Blowfish merupakan algoritma cipher block yang menerpakan teknik kunci yang berukuran sembarang.

2. LANDASAN TEORI

2.1. Sejarah Kriptografi

Sejarah kriptografi mempunya cerita yang sangat panjang. Banyak sumber informasu yang menuliskan tentang penjelasan kriptografi diantaranya terdapat pada buku David yang berjudul The Codebreakers.

Menurut sejarah ada beberapa golongan atau kelompok yang telah ikut ambil alih terhadap perkembangan kriptografi. Diantaranya yaitu kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang sangatlah dibutuhkan karena terdapat pesan rahasia yang harus diinformasikan oleh pasukan. Kalangan gereja Kristen menggunakan kriptografi untuk menjaga tulisan relijus daro gangguan otoritas politik atau budaya domain saat ini.

2.2. Tujuan Kriptografi

Ada empat aspek yang medasar tujuan dari ilmu kriptografi ini yang juga merupakan aspek-aspek keamanan didalam kriptografi yaitu :

1) *Confidentiality* (Kerahasiaan)
   Membuat pesan sangat sulit dipahami oleh orang lain sehingga menjadi pesan yang rahasia.
2) *Data Integrity* (Integritas)
   Membuat pesan masih terlihat asli atau belum pernah termanipulasi sebelumnya.
3) *Autentication* (Otentikasi)
   Mencari layanan untuk mencari kebenaran oleh pihak yang berkomunikasi
4) *Non-repudiation* (Penyangkalan)
   Mencegah terjadinya penyangkalan oleh si pengirim yang telah melakukan pengiriman pesan dan begitupun sebaliknya.

2.3. Proses Kriptografi

Untuk *Publik Key Cryptography* diperlukan teknik enkripsi asimetris dimana kunci dkeripsi tidak sama dengan kumci enkripsi. Pembuatan kunci untuk teknik enkripsi asimetris memprlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar.

Gambar1: Konsep Dasar Enkripsi dan Dekripsi

Secara garis besar, proses enkripsi merupakan proses yang digunakan untuk melakukan pengacakan kata sehingga pesan yang diterima tidak dapat dibaca dan harus melakukan proses dekripsi untuk menjadikan pesan dabat terbaca.

2.4. Kunci Simetris

Kriptografi simetris (*Symmetric Cryptography)* atau dikenal kunci rahasia (*Secret-Key Criptography)* yaitu dimana kunci enkripsi dan dekripsinya menggunakan kunci yang sama.

e = d = k
Ek(m) = c
Dk(c) = m

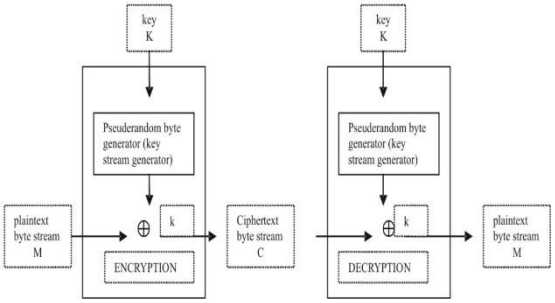
Kriptografi simetris sangat menekankan kerahasiaan *key* yang telah dibuat pada saat enkripsi dan dekripsinya. Oleh karena itu kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia.

Secara umum dalam proses enkripsi dan dekripsi pada kunci simetris dikenal dua macam cipher berdasarkan cara kerja penyajiannya, yaitu :

1) **Stream Chiper.** *Stream chiper* merupakan suatu proses enkripsi dan dekripsinya dilakukan dengan cara bit per bit.
2) **Block Chiper.** *Block Chiper* merupakan suatu proses enkripsi dan dekripsi dengan cara perblok dengan tidak mengubah ukuran data.

2.5. Algoritma RC4

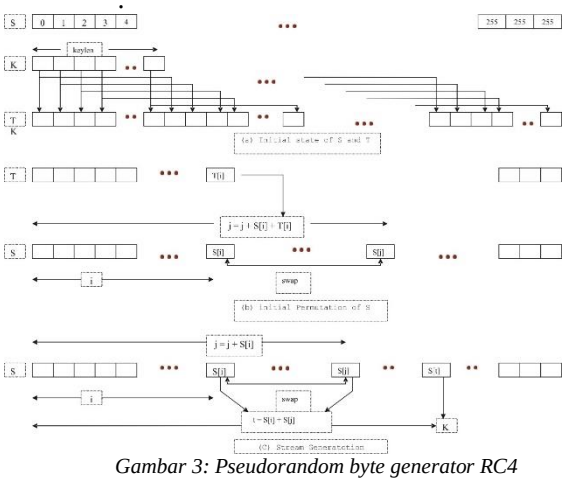
RC4 merupakan jenis aliran kode yang operasi enkripsinya dilakukan karakter 1 *byte* untuk sekali operasi. Ronald Rivest menemukan algortima ini pada tahun 1987. Faktor utama yang menjadi kesuksesan dari RC4 adalah kecepatan dan dan kemudahan dalam melakukan pengembangan sehingga memudahkan untuk mengimplementasikan.



Gambar 2: Stream cipher diagram RC4

RC4 mempunyai 2 metode, yaitu :

1) *Key setup*
2) *Stream generation.*



Gambar 3: Pseudorandom byte generator RC4

2.6. Algoritma *Blowfish*

Algoritma *Blowfish* terdiri atas dua bagian yaitu ekspansi kunci dan enkripsi data :

1) Ekspansi Kunci (*Key-Expansion*)
   Berfungsi untuk merubah kunci menjadi beberapa *array* subkunci dengan total 4168 *byte*(18x32 bit)

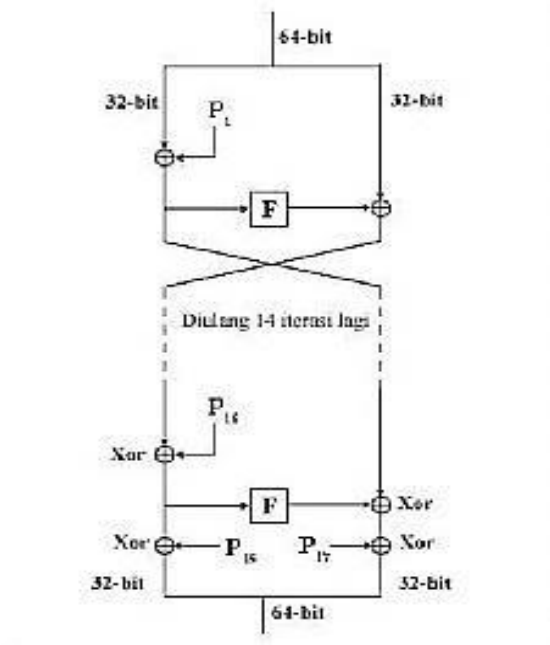
2) Enkripsi data
   a) Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit : X_L, X_R
   b) Lakukan langkah berikut :
      For i = 1 to 16;
      $X_L = X_L$ XOR P_1
      X_R = F(X_L) XOR X_R
      Tukar X_L dengan X_R

c) Setelah iterasi ke-16, tukar X_L dengan X_R lagi untuk melakukan membatalkan pertukaran terakhir.

$X_R = P_{17}$ XOR X_R

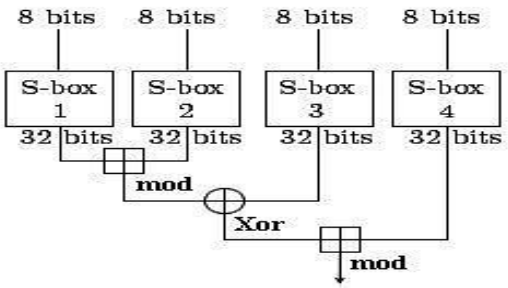
$X_L = P_{18}$ XOR X_L

d) Terakhir gabungkan kembaki X_R dengan X_L untuk mendapatan ciphertext untuk lebih jelasnya, ambaran pada tahapan jaringan feistel yang digunakan *blowfish* seperti pada gambar berikut ini.



Gambar 4 : *Blok Diagram Enkripsi Algoritma Blowfish*

Pada langkah kedua, telah dituliskan mengenai penggunaan fungsi F. yaitu seperti gambar dibawah ini :



Gambar 5 : Fungsi F dalam Blowfish

3) Dekripsi Data

Dekripsi sama persis dengan enkripsi, kecuali bahwa P_1, P_2, … P_{18} digunakan pada urutan yang berbalik (reverse). Algoritmanya dapat dinyatakan sebagai berikut :

For I = 1 to 16 do

$XR_i = XL_i$ – 1 xor P_{18}-i;

XL_i = F[XR_i] xor XR_i-1;

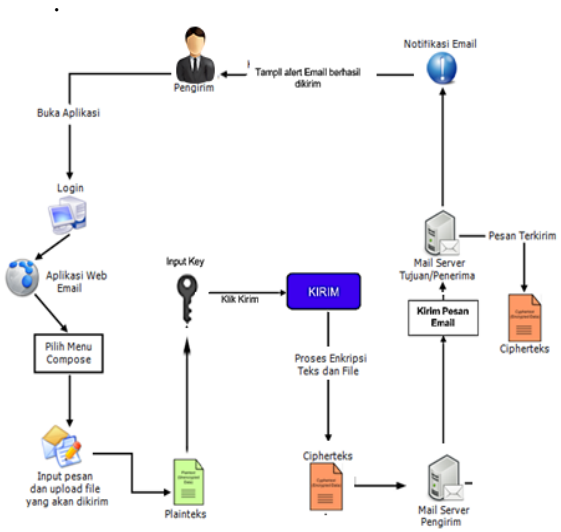
$XL_{17} = XR_{16}$ xor P_1;

$XR_{17} = XR_{16}$ xor P_2;

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Rancangan Program

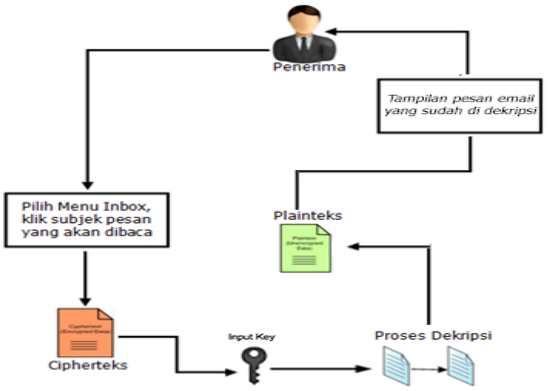
Terdapat alur rancangan program untuk cara menggunakan aplikasi dan cara untuk membuka pesan yang masuk di dalam email.



Gambar 6 : Alur Pengiriman Email

Berikut ini adalah tahapan untuk proses penerimaan email :

1) User halus melakukan login terlebih dahulu.
2) Jika berhasil login maka user masuk ke menu compose untuk membuat pesan email.
3) Lalu masukkan key untuk proses enkripsi.
4) Setelah itu klik tombol "KIRIM".
5) Proses enkripsi pesan email dilakukan.
6) Setelah pengekripsian pesan email selesai, maka pesan akan dikirim ke penerima.

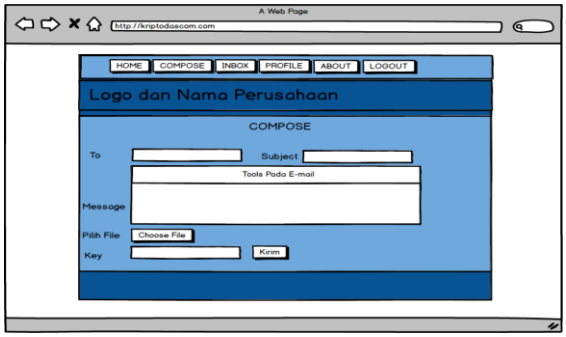


Gambar 7 : Alur Peneriamaan Email

Berikut ini adalah tahapan proses penerimaan email :

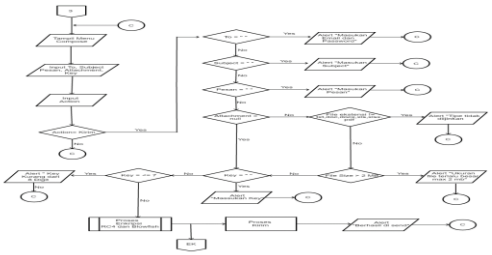
1) Penerima harus login terlebih dahulu ke aplikasi.

2) Jika sudah berhasil login maka penerima pilih menu inbox lalu akan tampil daftar inbox email
3) Klik pesan email yang telah masuk di inbox email.
4) Lalu masukkan key yang telah dibuat oleh pengirim untuk melakukan proses dekripsi.
5) Klik tombol dekripsi untuk melakukan proses pendekripsian.
6) Setelah proses dekripsi selesai maka email akan ditampilkan.

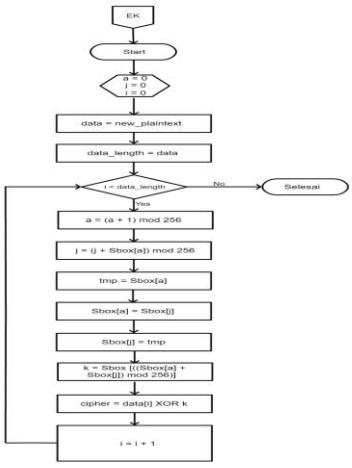


Gambar 8 : Rancangan Layar Compose

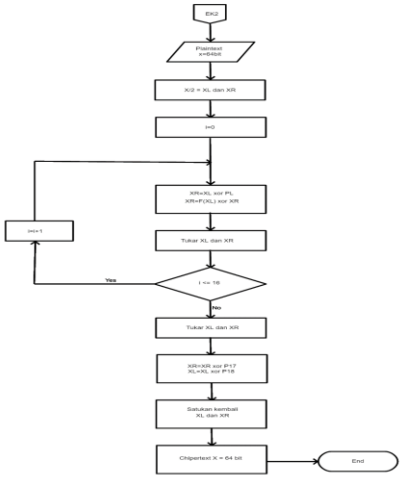
Pada rancangan layar menu compose ini ditampilkan form untuk menulis sebuah pesan atau *email* yang akan dienkripsi dan dikirim kepada seseorang. Dengan cara mengisi *form* tersebut dan memasukkan *key* untuk mengenkripsi isi *email* yang telah dibuat oleh pengguna, dan selanjutnya mengkilik tombol kirim untuk mengenkripsi sekaligus mengirim pesan.



Gambar 9 : Flowchart Menu Compose

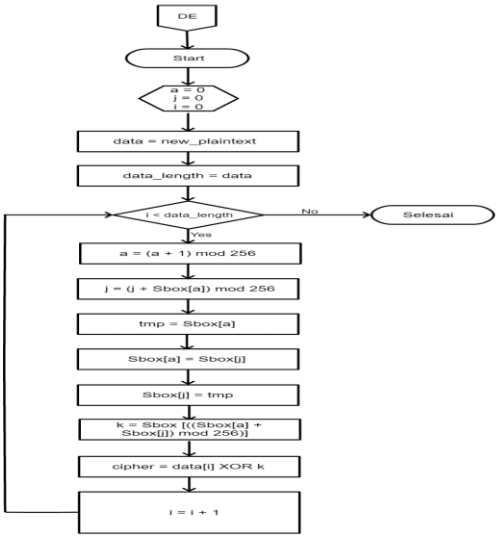


Gambar 10 : Flowchart Enkripsi RC4

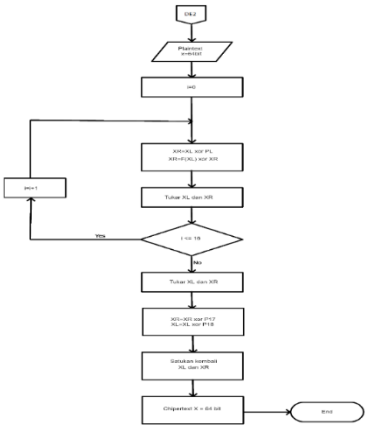


Gambar 11: Flowchart Enkripsi Blowfish

Flowchart diatas menjelaskan alur dari proses enkripsi RC4 dan *Blowfish* dan menjelaskan langkah apa saja yang terdapat pada proses enkripsi RC4 dan *Blowfish.*



Gambar 12 : Flowchart Dekripsi RC4



Gambar 13 : Flowchart Dekripsi Blowfish

Flowchart diatas menjelaskan alur dari proses dekripsi RC4 dan *Blowfish* dan menjelaskan langkah apa saja yang terdapat pada proses dekripsi RC4 dan *Blowfish.*

4. HASIL DAN PEMBAHASAN

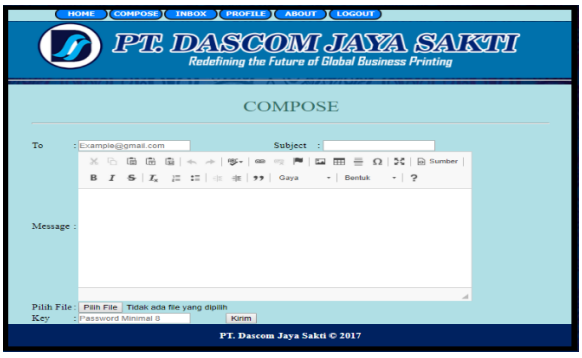
4.1. Menu *Login*

Langkah awal untuk menggunakan program ini adalah pengguna harus melakukan *login* terlebih dahulu, dengan menggunakan *email* dan *password* yang sama dengan akun gmail google. Berikut tampilan menu login

Gambar 14 : Tampilan Menu Login

4.2. Menu *Compose*

Pada menu ini pengguna harus mengisi *form* yang telah tersedia pada menu tersebut. Kemudian langkah selajutnya adalah untuk mengisi *key* kemudian mengklik tombol kirim agar proses enkripsi dapat berjalan. Berikut tampilan menu *compose.*



Gambar 15 : Tampilan Menu Compose

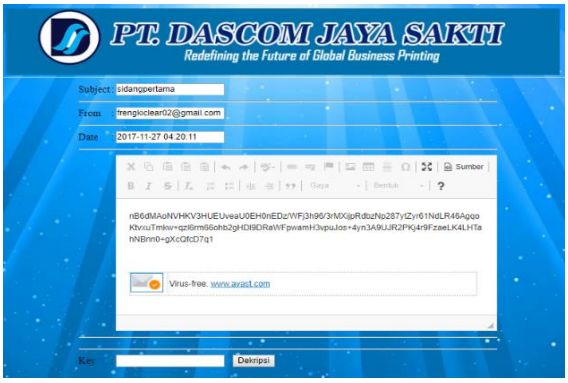
4.3. Menu *Inbox*

Menu *inbox* merupakan menu yang digunakan untuk pengecekan pesan yang telah masuk pada *emai*. Berikut tampilan menu *inbox*

Gambar 16 : Tampilan Menu Inbox

4.5. Proses Dekripsi

Dekripsi merupan proses untuk mengembalikan pesan yang telah di enkripsi atau pesan yang sudah mengalami perubahan sehingga pesan sudah tidak dapat terbaca dengan baik. Berikut proses dekripsi.



Gambar 17 : Tampilan Pesan Sebelum Didekripsi

Untuk mendekripsi pesan tersebut adalah pengguna harus memasukkan *key* yang telah dibuat sebelum pada saat enkripsi pesan. Jika *key* yang dimasukkan benar makan pesan akan berhasil didekripsi. Berikut tampilan pesan yang berhasil didekripsi.

Gambar 18 : Tampilan Pesan Sudah Didekripsi

4.6. Pengujian Tabel Enkripsi dan Dekripsi

Dalam table pengujian akan terlihat perbandingan antara proses enkripsi dan dekripsi file .doc, .txt, .xls, dan .pdf dengan parameter meliputi ukuran awal file, waktu proses enkripsi atau dekripsi, ukuran akhir file dan hasil file yang dicapai dalam proses enkripsi maupun dekripsi.

Tabel 1 : Hasil Proses Enkripsi

No	Nama File	Ukuran File Awal	Ukuran Sesudah Enkripsi	Waktu
1	File.txt	1 Kb	56 Bytes	0:06:4
2	File.doc	22 Kb	29.3 Kb	0:04:9
3	File.xls	26 Kb	34.0 Kb	0:05:6

4	File.pdf	62 Kb	82.91 Kb	0:05:8

Tabel 2 : Hasil Proses Dekripsi

No	Nama File	Ukuran File Enkripsi	Ukuran Sesudah Enkripsi	Wakru
1	File.txt	56 Byte	1 Kb	0:06:2
2	File.doc	29.3 Kb	22 Kb	0:05:1
3	File.xls	34.0 Kb	26 Kb	0:06:3
4	File.pdf	82.91 Kb	62 Kb	0:06:6

5. KESIMPULAN

5.1. Kesimpulan

a. Algoritma RC4 dan Blowfish dapat digunakan untuk mengimplementasikan aplikasi pengiriman pesan email.
b. Pengguna harus memasukan key untuk melakukan proses dekripsi email. Key yang dimasukkan harus sama dengan key pada saat enkripsi email.

5.2. Saran

a. Bisa digunakan untuk file selain ektensi : .txt, .doc, .xls,dan .pdf.
b. Tampilan masih sederhana diharapkan ada beberapa fitur tambahan.
c. Dapat digunakan tanpa harus terkoneksi dengan internet.

6. DAFTAR PUSTAKA

[1] A. Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan. Yogyakarta:Andi.355-400
[2] C, Febrian. Wahyu, Rahagiar, A. P., & Fretes, F. (2012). Penerapan Algoritma Gabungan Rc4 Dan Base64 Pada Sistem Keamanan E-Commerce, Seminar Nasional Aplikasi Teknologi Informasi. 47-52.
[3] Halim Dermawan, D.A., 2014. Penerapan Algoritma RC4 untuk Enkripsi dan Dekripsi SMS Berbasis Android 1,2. Seminar Perkembangan dan Hasil penelitian ilmu komputer (SPHP-ILKOM), pp.79–87.
[4] Menezes, A.J., Oorschot, P.C. Van & Vanstone, S. a, 1996. Handbook of Applied Cryptography. Stanford University, Electrical Engineering.
[5] Munir, Rinaldi, 2006, Diktat Kuliah Kriptografi, Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika, Insitut Teknologi Bandung, Bandung.
[6] Sarangih Sholihah U, (2017). "Implementasi enkripsi dan dekripsi dengan metode rc4 untuk pengamanan data sistem informasi, Universitas Bandar Lampung.13(1)1-92.
[7] Setyawan., A. (2015) "Perancangan Mail Server Intranet Berbasis Web Base Dengan Optimalisasi Operasi Sistem Client," Teknik Komputer, I(1), hal. 1–10.
[8] Sutiono, A. P. (2011) "Algoritma RC4 sebagai Perkembangan Metode Kriptografi," Institut Teknologi Bandung, 38(2),1–6.