Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018
SENSITEK 2018
STMIK Pontianak, 12 Juli 2018

Kriptografi Email menggunakan Algoritma Rivest Code 6 (Rc6) berbasis Java Pada PT. XYZ

Rizky Saleh[1)], **Imelda Imelda**[2)]

[1,2)]Program Studi Teknik Informatikai, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753
e-mail: *rizkypane45@gmail.com* [1)], *imelda@budiluhur.ac.id* [2)]

Abstrak

Saat ini email merupakan alat komunikasi yang umum dipakai oleh banyak orang. Dengan email kita dapat begitu mudah bertukar pesan tanpa batasan jarak dan waktu. Secara umum email tidak menjamin kerahasiaan pesan yang dikirimkan oleh pengguna. Suatu pesan teks yang dikirim dapat bersifat rahasia atau pribadi, sehingga pengguna menginginkan pesan email tersebut tidak ingin diketahui oleh pihak-pihak yang tidak memiliki hak atau wewenang untuk mengaksesnya. Pada penelitian ini akan dibuat suatu aplikasi yang mengimplementasikan teknik kriptografi. Penerapan kriptografi ini akan difokuskan bagaimana kriptografi dapat mengamankan pesan email dan file yang dikirim dengan tetap memperhatikan integritas pesan yang menggunakan algoritma Rivest Code 6 (RC6) yaitu algoritma yang menggunakan ukuran blok hingga 128 bit, dengan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit terhadap plaintext untuk menghasilkan chipertext, diharapkan proses pengiriman email yang dilakukan melalui perangkat komputer menjadi lebih aman. Output yang dihasilkan merupakan chipertext yang mana ketika penerima ingin membacanya, perlu untuk melakukan proses dekripsi. Selain itu, proses enkripsi pada plaintext yang sama diperoleh chipertext yang berbeda-beda, namun pada proses dekripsi diperoleh plaintext yang sama. Sehingga, membuat email menjadi lebih secure dibanding sebelumnya dan pesan dapat disandikan sehingga keamanan isi pesan sangat terjaga dalam kerahasiaan data.

Kata kunci: *algoritma RC6, kriptografi, email*

1. Pendahuluan

Saat ini email merupakan alat komunikasi yang umum dipakai oleh banyak orang. Dengan email kita dapat begitu mudah bertukar pesan tanpa batasan jarak dan waktu. Secara umum email tidak menjamin kerahasiaan pesan yang dikirimkan oleh pengguna. Suatu pesan teks yang dikirim dapat bersifat rahasia atau pribadi, sehingga pengguna menginginkan pesan email tersebut tidak ingin diketahui oleh pihak-pihak yang tidak memiliki hak atau wewenang untuk mengaksesnya.

Penyampaian pesan email membutuhkan suatu sistem keamanan. Pembuatan sistem keamanan tersebut menggunakan suatu teknik penyandian yang disebut dengan kriptografi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi / pesan dengan suatu algoritma tertentu yang membuat informasi tersebut tidak dapat dibaca. Supaya pesan tersebut dapat dibaca, dilakukan proses yang disebut dengan dekripsi. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Dalam melakukan proses dekripsi pesan dibutuhkan suatu pengetahuan khusus, yaitu kunci. Berbagai jenis layanan komunikasi tersedia di internet seperti pengiriman pesan melalui email yang semakin diminati masyarakat. Meningkatnya pemanfaatan layanan email melalui internet menyebabkan permasalahan juga bermunculan selain permasalahan hacker dan cracker [1].

Penelitian sebelumnya aplikasi yang dibuat bekerja untuk data text pada proses enkripsi dan dekripsi RC6 yang dijalankan saat mengirim ataupun menerima pesan, namum aplikasi masih belum bisa digunakan untuk mengarsisipkan sebuah file ke dalam aplikasi yang juga bisa dienkripsi dan dikirimkan melalui aplikasi [2].

Pada penelitian ini telah dibuat suatu aplikasi yang mengimplementasikan teknik kriptografi. Penerapan kriptografi ini berfokus pada bagaimana kriptografi dapat mengamankan pesan email dan file yang dikirim dengan tetap memperhatikan integritas pesan yang menggunakan algoritma Rivest Code 6 (RC6) yaitu algoritma yang menggunakan ukuran blok hingga 128 bit, dengan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit terhadap plaintext untuk menghasilkan chipertext.Aplikasi Kriptografi email dianggap penting oleh penulis karena sangat berguna untuk keamanan pesan email pada PT. XYZ.Pengiriman data email ataupun pesan telah menjadi masalah penting. Terkadang data-data ini harus bersifat rahasia agar tidak diketahui secara umum. Apabila diketahui maka data tersebut akan disalahgunakan untuk kejahatan orang lain.

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, identifikasi masalah pada penelitian ini

yaitu bagaimana mengimplementasikan algoritma RC6 untuk mengamankan pesan dan file dokumen dalam email. Karena RC6 menggunakan 4 register maka akan terdapat 2 operasi rotasi pada setiap half-round yang ada, dan juga akan lebih banyak bit-bit yang akan digunakan untuk mempengaruhi banyaknya bit yang dirotasi. Operasi perkalian ini sangat efektif dalam menghasilkan efek "diffusion" atau penyebaran yang tentu saja mengakibatkan RC6 lebih aman.Tujuan dari penelitian ini adalah mengamankan pesan email supaya hanya dapat dibaca oleh orang yang dimaksud dengan mengimplementasikan algoritma RC6 [3].

Adapun batasan masalah dalam penelitian ini :

a. Algoritma kriptografi yang digunakan untuk mengenkripsi dan mendekripsi adalah RC6.
b. Tipe file dibatasi: doc, docx, xls, xlsx, pdf, txt.
c. Pesan yang dikirimkan dalam bentuk teks.
d. File yang dikirim tidak lebih dari 25MB.
e. Aplikasi menggunakan bahasa pemograman Java.
f. *Login* aplikasi hanya bisa menggunakan domain gmail saja.

2. Kriptografi Email menggunakan Algoritma RC6

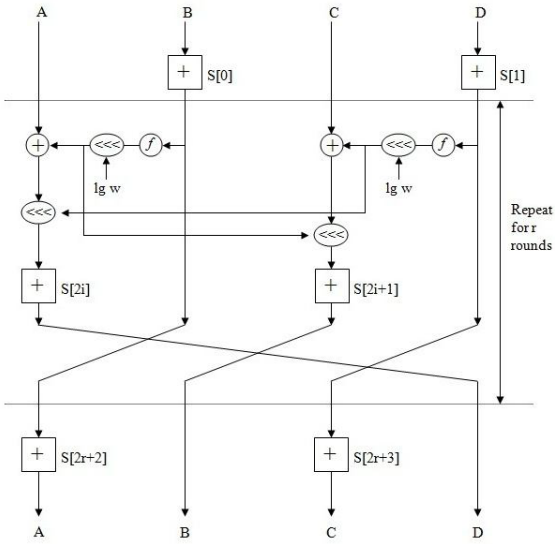
2.1. Algoritma RC6

RC6 merupakan salah satu dari algoritma simetri kriptografi yaitu algoritma yang menggunakan satu kunci untuk enkripsi dan dekripsinya. RC6 adalah algoritma blok kode yang sangat aman, padat, sederhana dan menawarkan performansi yang sangat bagus dan fleksibel, dikembangkan dari algoritma RC5 [4].

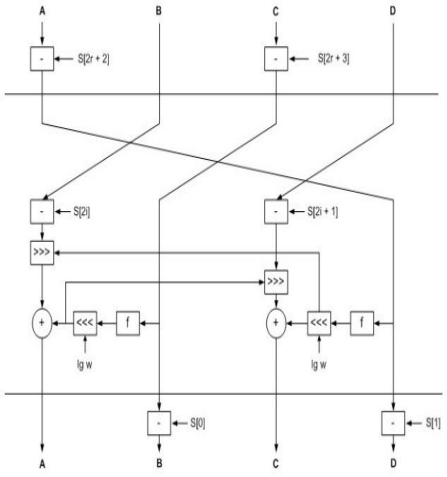
Algoritma RC6 adalah versi yang dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b, dimana parameter w merupakan ukuran kata dalam satuan bit, r adalah bilangan bulat bukan negatif yang menunjukan banyaknya iterasi selam proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam byte. Ketika algoritma ini masuk sebagai kandidat AES, maka ditetapkan nilai parameter w = 32, r = 20 dan b bervariasi antara 16, 24, dan 32 byte [5].

Karena RC6 memecah blok 128 bit menjadi 4 buah blok 32 bit, maka algoritma ini bekerja dengan 4 buah register 32-bit A, B, C, D. Byte yang pertama dari plaintext atau ciphertext ditempatkan pada byte A, sedangkan byte yang terakhirnya ditempatkan pada byte D. Dalam prosesnya akan didapatkan (A, B, C, D) = (B, C, D, A) yang diartikan bahwa nilai yang terletak pada sisi kanan berasal dari register disisi kiri. Diagram blok Gambar 1 menjelaskan proses enkripsi yang terjadi pada algoritma RC6.

Proses dekripsi ciphertext pada algoritma RC6 merupakan pembalikan dari proses enkripsi. Pada proses whitening, bila proses enkripsi menggunakan operasi penjumlahan, maka pada proses dekripsi menggunakan operasi pengurangan. Sub kunci yang digunakan pada proses whitening setelah iterasi terakhir diterapkan sebelum iteasi pertama, begitu juga sebaliknya sub kunci yang diterapkan pada proses whitening sebelum iterasi pertama digunakan pada whitening setelah iterasi terkahir. Akibatnya, untuk melakukan dekripsi, hal yang harus dilakukan semata-mata hanyalah menerapkan algoritma yang sama dengan enkripsi, dengan tiap iterasi menggunakan sub kunci yang sama dengan yang digunakan pada saat enkripsi, hanya saja urutan sub kunci yang digunakan terbalik. Diagram blokGambar 2 menjelaskan proses dekripsi yang terjadi pada algoritma RC6.



Gambar 1. *Proses Enkripsi Algoritma RC6*



Gambar 2. *Proses Dekripsi Algoritma RC6*

Pengguna memasukkan sebuah kunci yang besarnya b byte, dimana $0 \leq b \leq 255$. bytekunci ini kemudian ditempatkan dalam array c w-bit words L[0]…L[c-1]. Byte pertama kunci akan ditempatkan sebagai pada L[0],

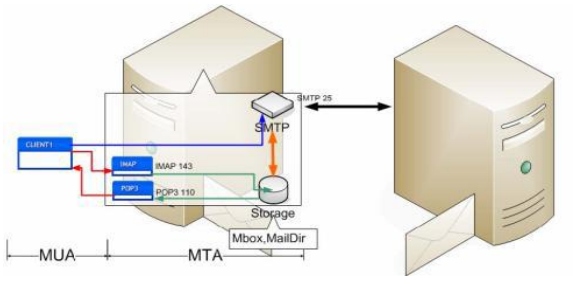
byte kedua pada L (Dewi, 2013), dan seterusnya. (Catatan, bila b=0 maka c=1 dan L[0]=0). Masing-masing nilai kata w-bit akan dibangkitkan pada penambahan kunci round 2r+4 dan akan ditempatkan pada array S[0,…,2r+3]. Konstanta P32 = B7E15163 dan Q32 = 9E3779B9 (dalam satuan heksadesimal) adalah "konstanta ajaib" yang digunakan dalam penjadwalan kunci pada RC6. nilai P32 diperoleh dari perluasan bilangan biner e-2, dimana e adalah sebuah fungsi logaritma. Sedangkan nilai Q32 diperoleh dari perluasan bilangan biner Ø-1, dimana Ø dapat dikatakan sebagai "*golden ratio*" (rasio emas) [6].

2.2. E-Mail

Electronic-Mail (E-Mail) merupakan aplikasi TCP/IP yang paling banyak di-gunakan. E-mail adalah pesan yang terdiri atas kumpulan string ASCII dalam format RFC 822 dikembangkan thn 1982 [7].

a. Cara Kerja Email

Gambar 3 menunjukkan gambaran dari cara kerja email. Cara kerja email dapat dilihat pada Gambar 3. E-mail yang dikirim be-lum tentu akan diteruskan ke komputer penerima (end user), tapi disim-pan/dikumpulkan dahulu dalam sebuah komputer server (host) yang akan online secara terus menerus (continue) dengan media penyimpanan (storage) yang relatif lebih besar dibanding komputer biasa. Hal ini bisa diibaratkan dengan sebuah kan-tor pos, jika sesorang mempunyai alamat (mailbox), maka dia dapat memeriksa secara berkala jika dia mendapatkan surat. Komputer yang melayani penerimaan email secara terus-menerus tersebut biasa disebut dengan mailserver atau mailhost.

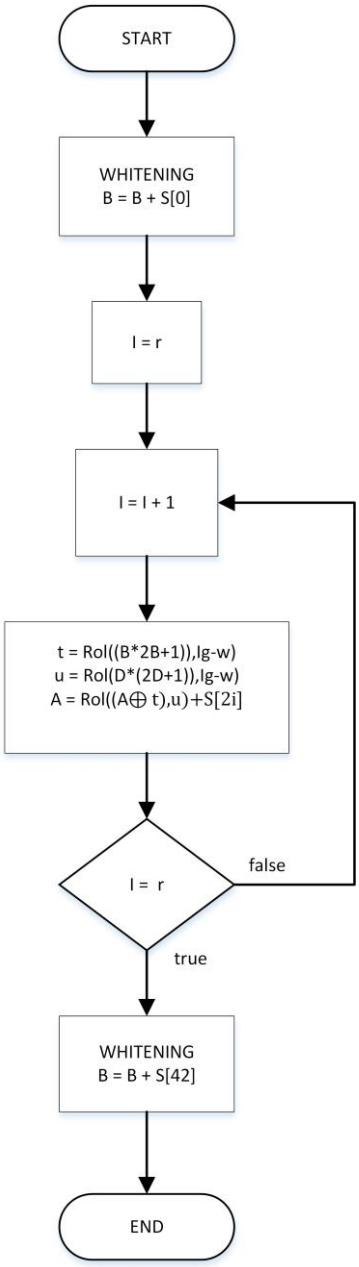


Gambar 3. *Cara Kerja Email*

3. Perancangan

3.1. Algoritma Enkripsi

RC6 memecah blok 128 bit menjadi 4 buahy blok bit, maka algoritma ini bekerja dengan 4 buah register 32-bit A, B, C, D. Bytepertama plainteks atau chiperteks ditempatkan pada byte A, sedangkan byte terakhirnya ditempatkan pada byte D. Dalam prosesnya akan didapatkan (A, B, C, D) = (B, C, D, A) yang diartikan bahwa nilai yang terletak pada sisi kanan berasal dari register sisi kiri. Gambar 4 menjelaskan proses yang terjadi pada algoritma RC6.

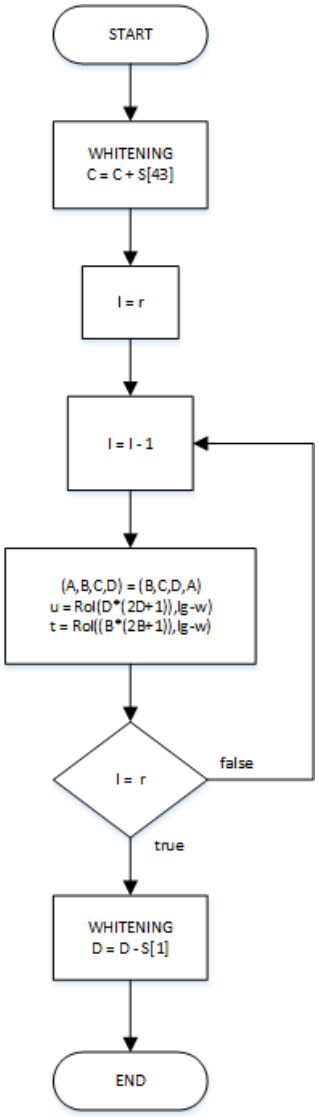


Gambar 4. *Proses Enkripsi RC6*

3.2. Algoritma Dekripsi

Proses dekripsi cipherteks pada algoritma RC6 merupakan pembalikan dari proses enkripsi. Pada proses whitening, bila proses enkripsi menggunakan operasi penjumlahan, maka pada proses dekripsi menggunakan operasi pengurangan. Sub kunci yang digunakan pada proses whitening setelah iterasi terakhir diterapkan sebelum iterasi pertama, begitu juga sebaliknya sub kunci yang diterapkan pada proses whitening sebelum iterasi pertama digunakan pada whitening setelah iterasi terakhir. Akibatnya, untuk melakukan dekripsi, hal yang

harus dilakukan semata-mata hanyalah menerapkan algoritma yang sama dengan enkripsi, dengan tiap iterasi menggunakan sub kunci yang sama dengan yang digunakan pada saat enkripsi, hanya saja urutan sub kunci yang digunakan terbalik.



Gambar 5. *Proses Dekripsi RC6*

4. Hasil Dan Pembahasan

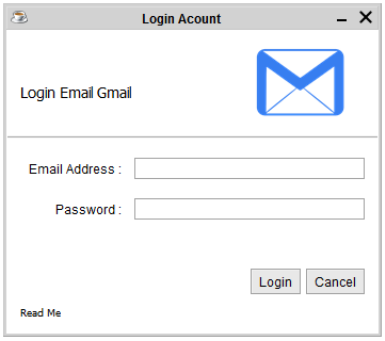
Pada tahapan ini menjelaskan hasil rancangan, tampilan program aplikasi dan kesimpulan dari uji coba baik dari analisa hasil serta kelebihan dan kekurangan dari hasil perancangan.

4.1. Tampilan Aplikasi

Tampilan Aplikasi berisi tentang tampilan hasil aplikasi keamanan data email menggunakan algoritma enkripsi RC6 berbasis Dekstop.

a. Tampilan Form Login

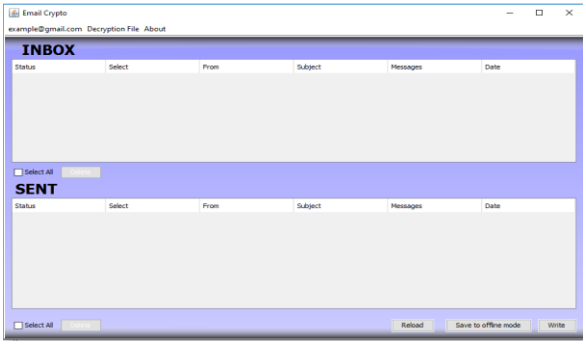
Form login pada Gambar 6 menunjukkan form yang pertama akan muncul saat pertama kali membuka program. Awalnya user mengisi email address dan password sebagai syarat untuk masuk ke tampilanhome.



Gambar 6. *Tampilan Layar FormIndex/Login*

b. Tampilan Home

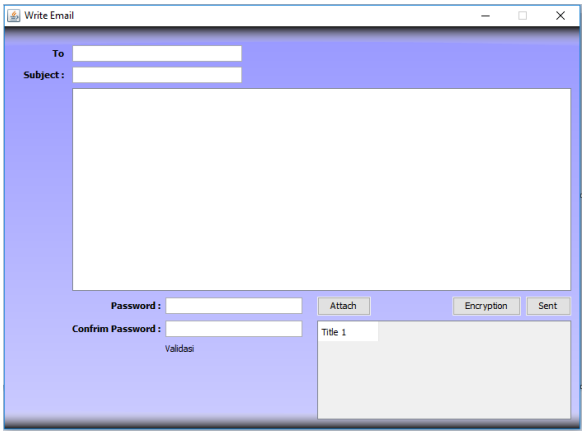
Halaman home pada Gambar 7 menunjukkan halaman pertama dituju oleh user. Pada halaman ini user bisa memilih menu dan fitur.



Gambar 7. *Tampilan Layar Home*

c. Tampilan Form Write Email

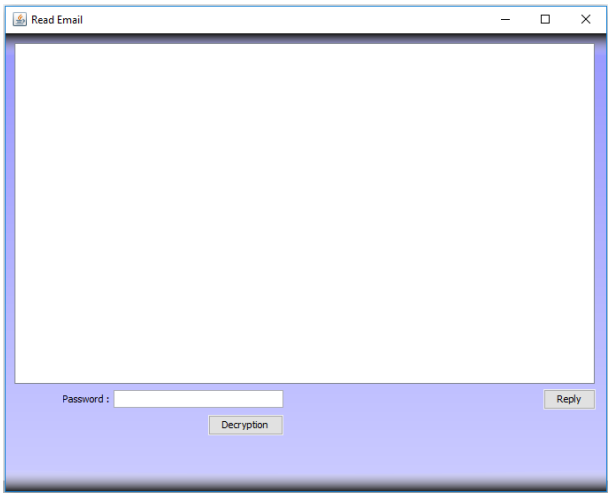
Tampilan Form *write email* dapat ditunjukkan pada Gambar 8. Form writeemailadalah fungsi utama dari aplikasi ini. Form write email berfungsi untuk membuat dan mengirim pesan email yang sudah terenkripsi pada alamat email tujuan.



Gambar 8. *Tampilan Form Write Email*

d. Tampilan Form Read Email

Gambar 9 menunjukkan tampilan formreademail. Form ini berfungsi untuk melihat pesan email dan dekripsi pesan email yang sudah terenkripsi.



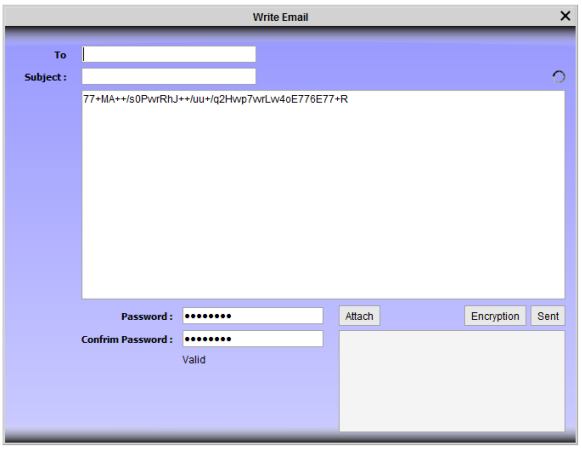
Gambar 9. *Tampilan Form Read Email*

4.2. Pengujian Program

Pengujian enkripsi dan dekripsi pesan/file. Pengujian ini bertujuan untuk mendapatkan hasil perbandingan pesan/file asli dan pesan/file hasil enkripsi.

a. Tampilan Pesan Teks Sudah di Enkripsi

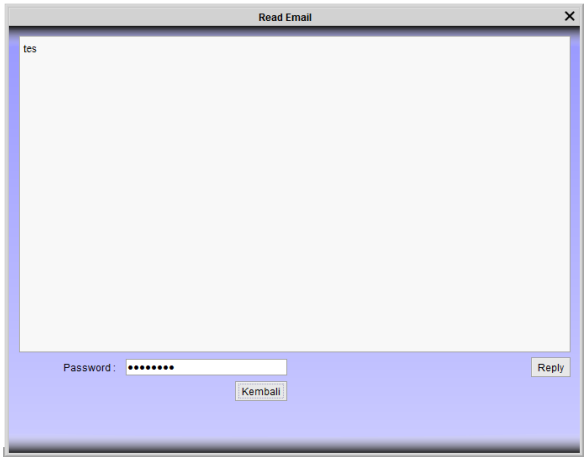
Gambar 10 menunjukkan hasil tampilan pesan teks yang sudah di enkripsi. Setelah memasukkan teks yang ingin dienkrip lalu menginput password dan confirm password lalu klik encryption. Bila ingin mengirim pesan klik sent.



Gambar 10. *Tampilan Pesan Teks Sudah di Enkripsi*

b. Pesan Teks Sudah di Dekripsi

Setelah pesan chipper text dibuka dan menginput password dengan benar maka akan di dekripsi bisa ditunjukkan pada Gambar 11. Untuk melakukan dekripsi cukup menginput passward yang sama pada saat enkripsi email.



Gambar 11. *Tampilan Pesan Teks Sudah di Dekripsi*

Tabel 1 menunjukkan tabel pengujian yang membahas tentang perbandingan pengiriman email, proses enkripsi, dan dekripsi file doc, pdf, xls dan txt yang berisi file teks. Pengujiannya antara lain key yang diberikan, ukuran file,waktu pengiriman email, waktu proses enkripsi dan waktu proses dekripsi hingga hasil yang dicapai dalam proses enkripsi maupun dekripsi.

5. Kesimpulan

Adapun kesimpulan dari perancangan, pembuatan, serangkaian uji coba dapat dianalisa program kriptografi email ini, maka dapat dibuat suatu kesimpulan antara lain:

a. Dengan adanya aplikasi ini pesan dapat disandikan sehingga keamanan isi pesan sangat terjaga dalam kerahasiaan data.

b. Perangkat lunak ini hanya mengamankan isi text email bukan mengamankan jalur transfer email.
c. Tidak terjadi kerusakan dokumen yang sudah di dekrip.
d. Pesan dan file tidak dapat di dekrip tanpa kunci.
e. Aplikasi sinkron dengan server gmail.
f. Sebelum login diaplikasi harus membuka akun gmail dan mengaktifkan aplikasi tidak aman.
g. Dokumen yang bisa di enkripsi di aplikasi ini berupa doc, docx, xls, xlsx, txt dan pdf.

Daftar Pustaka

[1] M. S. Lubis, M. A. Budiaman, and K. L. Manik, "Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email," *J. Semin. Nas. Apl. Teknol. Inf.*, pp. 28–33, 2013.

[2] M. Zulham, H. Kurniawan, and I. F. Rahmad, "PERANCANGAN APLIKASI KEAMANAN DATA EMAIL MENGGUNAKAN ALGORITMA ENKRIPSI RC6," *J. Semin. Nas. Inform.*, pp. 96–101, 2014.

[3] A. Zelvina, S. Efendi, and D. Arisandi, "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," *J. Dunia Teknol. Inf.*, vol. 1, no. 1, pp. 56–62, 2012.

[4] Defni and I. Rahmayun, "Enkripsi SMS (Short Message Service) Pada Telepon Seluler Berbasis Android Dengan Metode RC6," *J. Momentum*, vol. 16, no. 1, pp. 63–73, 2014.

[5] A. Subari, Mustafid, and K. I. Satoto, "Desain web secure login dengan algoritma enkripsi simetri rc-6," *J. Semin. Nas.*, vol. 2, pp. 3–4, 2007.

[6] N. K. K. Dewi, M. Aswin, and W. Djurianto, "IMPLEMENTASI ALGORITMA RC6 UNTUK PROTEKSI FILE MP3," *Publ. J. Skripsi*, pp. 2–3, 2013.

[7] Y. Taufan, I. Winarno, and K. Fathoni, "Enkripsi email dengan menggunakan metode elgamal pada perangkat mobile," *J. Tek. Inform.*, pp. 2–3, 2011.

Tabel 1. *Tabel Pengujian Kirim Email dan File*

Pesan / Nama File	Key	Waktu Enkripsi (detik)	Nama File Setelah Enkripsi	Waktu Dekripsi (detik)	Waktu Kirim (detik)	Nama File Setelah Dekripsi	Ukuran File asli (KB)	Ukuran File Setelah Di Enkripsi (KB)
Pesan Text	12345678	0.001	-	0.001	5.58	-	-	-
Design Tools.docx	enkripdoc01	0.069	en_Design Tools.docx	0.154	4.37	de_en_Design Tools.docx	1.919	1.919
02.Rekayasa Web.pdf	enkrippdf04	0.051	en_02.Rekayasa Web.pdf	0.031	10.09	de_en_02.Rekayasa Web.pdf	1.056	1.056
02Tem HPS & Proposal Biaya - CONTOH 2010.xls	enkripxls02	0.015	en_02Tem HPS & Proposal Biaya - CONTOH 2010.xls	0.005	4.78	de_en_02Tem HPS & Proposal Biaya - CONTOH 2010.xls	51	51
controller robot.txt	enkriptxt03	0.001	en_controller robot.txt	0.001	4.11	de_en_controller robot.txt	1	1