IMPLEMENTASI ALGORITMA KRIPTOGRAFI *RIVEST CODE 4, RIVEST SHAMIR ADLEMAN*, DAN METODE STEGANOGRAFI UNTUK PENGAMANAN PESAN RAHASIA PADA BERKAS TEKS DIGITAL

Rizal Yunan Rifai[*)], Yuli Christyono, and Imam Santoso

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH. Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-Mail: rifaiyunan@gmail.com*

Abstrak

Kriptografi adalah salah satu cara untuk menjaga keamanan dan kerahasiaan data dengan melakukan penyandian terhadap data, sehingga pihak yang tidak berkepentingan tidak dapat mengetahui isi data tersebut. Saat proses pengiriman, data rahasia memerlukan perlindungan ekstra dengan memanipulasi media cover agar hanya dapat dibaca oleh penerima saja dengan memanfaatkan steganografi. Dalam penelitian ini dibangun aplikasi yang dapat melakukan enkripsi dan dekripsi pesan teks memanfaatkan metode kriptografi algoritma simetris Rivest Code 4, algoritma asimetris Rivest Shamir Adleman, kemudian pesan tersebut disembunyikan dengan menggunakan metode steganografi mode ukuran font atau warna font dengan variabel jumlah karakter pesan asli, pesan palsu, ukuran font, intensitas warna dan password. Berdasarkan hasil uji kriptografi dengan plaintext sama, algoritma simetris RC4 kecepatan operasi algoritma RC4 lebih cepat dibandingkan algoritma RSA. Untuk hasil uji steganografi, jumlah karakter pesan asli, pesan palsu, ukuran font, dan intensitas warna berpengaruh terhadap ukuran file. Selanjutnya hasil uji pengiriman online berkas adalah kondisi file sebelum upload dan setelah download tetap sama. Penelitian ini menghasilkan aplikasi untuk mengamankan pesan teks yang dapat dijaga kerahasiaan dan keamanannya.

Kata kunci : Kriptografi, Steganografi, RC4, RSA

Abstract

Cryptography is one way to maintain the security and confidentiality of data by encoding the data, so that unauthorized parties can not know the contents of the data. When the delivery process, need the extra protection of confidential data by manipulating the media cover that can only be read by the addressee only by using steganography. In this study built an application that can encrypt and decrypt text messages utilizing cryptographic methods symmetric algorithms Rivest Code 4 , asymmetric algorithms Rivest Shamir Adleman, then the message is hidden using steganography mode font size or font color with variable the number of characters of the original message, fake message, font size, color intensity and password. Based on the test results with the plaintext cryptographic equal, symmetrical algorithm RC4 operating speed faster than the RSA algorithm. For the test results of steganography, the number of characters of the original message, fake message, font size, and color intensity affect the file size. Further test results online delivery of files is the condition of the file before uploading and after downloading remains the same. This research resulted in an application to secure a text message to confidentiality and security.

Keyword: Cryptography, Steganography, RC4, RSA

1. Pendahuluan

Masalah privasi dan keamanan pesan, data, informasi menjadi hal yang penting di era kemajuan teknologi komputer. Pengiriman suatu pesan, data, informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi. Dengan perkembangan teknologi informasi sekarang ini yang begitu pesat, setiap orang dapat dengan mudah mendapatkan suatu pesan, data, dan informasi. Berbagai cara dilakukan orang untuk mendapatkan pesan, data, dan informasi tersebut. Dan dengan berbagai cara pula orang berusaha melindungi pesan, data, dan informasi tersebut agar tidak dapat diketahui oleh orang yang tidak memiliki hak untuk mengakses pesan, data, dan informasi tersebut. Karena itu, dibutuhkan suatu metode yang tepat dan berguna untuk melindungi pesan. data, dan informasi tersebut dari serangan orang-orang

yang tidak bertanggung jawab. Metode yang dimaksud adalah kriptografi dan steganografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Di dalam ilmu kriptografi terdapat algoritma-algoritma yang membantu untuk melakukan enkripsi dan dekripsi data. Enkripsi adalah proses penyandian dari pesan asli menjadi pesan yang tidak dapat diartikan. Sedangkan dekripsi sendiri berarti mengubah pesan yang sudah disandikan menjadi pesan aslinya. Sedangkan steganografi atau teknik *hidden message* adalah suatu teknik untuk menyembunyikan suatu pesan di dalam pesan yang lain. Di dalam steganografi terdapat media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program atau pesan lain.
Menurut penelitian kriptografi yang telah dilakukan menjelaskan bahwa faktor keamanan menjadi hal yang sulit untuk dipecahkan. Perkembangan teknik kriptografi yang beredar saat ini sudah semakin banyak. Namun penggunaan kriptografi dalam teknologi informasi masih sangat sedikit, apalagi untuk pengguna yang belum mengetahui fungsi keamanan data[1]**.** Salah satu cara untuk menjaga keamanan dan kerahasiaan data atau informasi pada saat ditransmisikan adalah dengan melakukan penyandian terhadap data atau informasi, sehingga pihak lain yang tidak berkepentingan tidak dapat mengetahui isi dari informasi tersebut. Dalam penelitian ini dihasilkan aplikasi *e-mail client* dengan algoritma *RSA*[2]. Dalam penelitian kriptografi yang lain menyebutkan bahwa kriptografi terdapat berbagai macam sistem sandi (*cryptosystem*) yang memiliki algoritma, tujuan penggunaan, dan tingkat kerahasiaan berbeda[3]**.** Selanjutnya menurut penelitian steganografi yang telah dilakukan menerangkan bahwa dengan solusi steganografi, maka pada prinsipnya masalah yang terkait dengan hak cipta dan kepemilikan dapat dipecahkan, hal ini mengacu pada sifat dasar steganografi yaitu menyembunyikan pesan. Namun demikian steganografi bukan solusi tunggal untuk menyelesaikan masalah tersebut[4]**.** Data rahasia yang akan dikirim memerlukan perlindungan ekstra agar hanya dapat dibaca oleh target penerima saja. Penelitian ini menghasilkan aplikasi steganografi yang diterapkan pada *image* dengan tidak mengubah *cover image*[5]**.** Sehubungan dengan hal di atas, maka dalam penelitian ini membangun aplikasi yang dapat melakukan enkripsi dan dekripsi pesan teks dengan memanfaatkan algoritma kriptografi simetris *Rivest Code 4 (RC4)* serta algoritma asimetris *Rivest Shamir Adleman (RSA)* kemudian pesan tersebut dapat disembunyikan menggunakan metode steganografi dengan mengubah mode ukuran *font* atau warna *font*. Sehingga dengan aplikasi ini dapat dihasilkan suatu metode pengamanan pesan teks yang dapat dijaga kerahasiaan dan keamanannya dan pesan yang hendak disampaikan dapat diterima dengan aman dari pengirim ke penerima tanpa gangguan dari pihak yang tidak bertanggungjawab.

2. Metode

2.1. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu "*cryptos*" yang artinya "*secret*" (rahasia) dan "*graphein*" yang artinya tulisan. Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Ada beberapa definisi kriptografi yang telah dikemukakan dalam berbagai literatur. Kriptografi merupakan suatu seni atau ilmu untuk menjaga kerahasiaan sebuah tulisan agar tetap aman tanpa diketahui oleh pihak yang tidak berhak. Namun saat ini kriptografi bukan hanya sekedar seni dan kerahasiaan tetapi juga integritas, otentikasi dan keabsahan data.

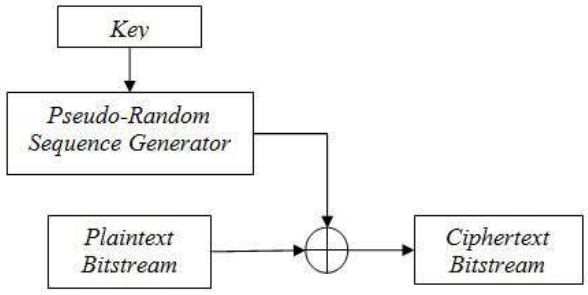
2.2. Algoritma Kriptografi RC4

Algoritma kriptografi *Rivest Code 4 (RC4)* merupakan salah satu algoritma kunci simetris dibuat oleh *RSA Data Security Inc* (*RSA*DSI). Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan *RSA* (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). Algoritma *RC4* menggunakan dua buah *S-Box* yaitu *array* sepanjang 256 yang berisi permutasi dari bilangan 0 sampai 255, dan *S-Box* kedua, yang berisi permutasi merupakan fungsi dari kunci dengan panjang yang variabel. Cara kerja algoritma *RC4* yaitu inisialisasi *S-Box* pertama, S[0],S[1],...,S[255], dengan bilangan 0 sampai 255. Pertama isi secara berurutan S[0] = 0, S[1] = 1,...,S[255] = 255. Kemudian inisialisasi *array* lain (*S-Box* lain), misal *array* K dengan panjang 256. Isi *array* K dengan kunci yang diulangi sampai seluruh *array* K[0], K[1],...,K[255] terisi seluruhnya.

1) Proses inisialisasi *S-Box* (*Array* S) dirumuskan dengan persamaan berikut :
   for i = 0 to 255
   S[i] = i (1)
2) Selanjutnya proses inisialisasi *S-Box* (*Array* K) persamaannya adalah :
   Array kunci dengan panjang kunci "length"
   for i = 0 to 255
   K[i] = Kunci [i mod length] (2)
3) Kemudian langkah pengacakan *S-Box* dirumuskan dengan persamaan :
   I = 0 ; j = 0
   for i = 0 to 255
   j = (j + S[i] + K[i]) mod 256
   swap S[i] dan S[j] (3)

4) Lalu membuat *pseudo random byte* dengan rumus persamaan :
   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   swap S[i] dan S[j]
   t = (S[i] + S[j]) mod 256
   K = S[t] (4)

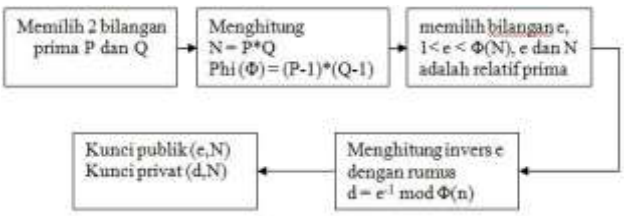
Byte K di-XOR-kan dengan *plaintext* untuk menghasilkan *ciphertext* atau di-XOR-kan dengan *ciphertext* untuk menghasilkan *plaintext.*



Gambar 1. Diagram algoritma RC4

2.3. Algoritma Kriptografi RSA

Algoritma kriptografi RSA merupakan algoritma kriptografi kunci publik (nirsimetri). Ditemukan pertama kali pada tahun 1977 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci rahasia hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Algoritma kriptografi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.



Gambar 2. Diagram algoritma RSA

2.3.1. Proses Pembentukan Pasangan Kunci

Berikut ini adalah proses pembentukan kunci dalam algoritma kriptografi RSA :
1) Memilih dua bilangan prima yang diberi simbol sebagai p dan q (nilai $p \neq q$).
2) Menghitung nilai n = p.q ($p \neq q$, karena jika p = q , maka nilai $n = p^2$ sehingga nilai p dapat diperoleh dengan menarik akar pangkat dua dari n).
3) Hitung $\varphi(n) = (p - 1)(q - 1)$.
4) Memilih kunci publik e yang relatif prima terhadap (n).
5) Bangkitkan kunci privat dengan persamaan $e \cdot d \equiv 1 \pmod{\varphi(n)}$ dimana $1<d<\varphi(n)$. Perhatikan bahwa persamaan $e \cdot d \equiv 1 \pmod{\varphi(n)}$ ekivalen dengan $e \cdot d = 1 + k\,\varphi(n)$, sehingga untuk mencari nilai d dapat dihitung dengan $d = \frac{1 + k\,\varphi(n)}{e}$

Hasil dari pembentukan pasangan kunci di atas adalah :
a) kunci publik (e, n)
b) kunci rahasia (d, n)

2.3.2. Proses Enkripsi

Berikut ini adalah proses enkripsi dalam algoritma kriptografi RSA :
1) Ambil kunci publik penerima pesan *e* dan modulus *n* atau (*e*,*n*).
2) Pilih plainteks *m* dan ubah isi pesan *m* menjadi pesan dengan nilai ASCII.
3) Potong pesan menjadi blok-blok pesan m_1, m_2, m_3, ... dengan nilai setiap bloknya adalah $0 \leq m \leq n - 1$.
4) Setiap blok *m* dihitung dengan rumus $c_i = m_i^e$ **mod** *n*.
5) Susun nilai *c* hasil enkripsi dengan susunan c_1, c_2, c_3,....,c_n sehingga diperoleh cipherteks dari pesan *m*.

2.3.3. Proses Dekripsi

Berikut ini adalah proses dekripsi dalam algoritma kriptografi RSA :
1) Ambil pesan (cipherteks) yang telah diterima.
2) Kemudian ambil kunci rahasia *d* dan modulus *n* atau (*d*,*n*).
3) Potong pesan menjadi blok-blok pesan c_1, c_2, c_3, ... dengan nilai setiap bloknya adalah $0 \leq c \leq n - 1$.
4) Hitung $m_i = c_i^d$ **mod** *n*.
5) Susun nilai *m* hasil dekripsi dengan susunan m_1, m_2, m_3,....,m_n sehingga diperoleh plainteks (pesan asli) dari cipherteks yang diterima.

2.4. Steganografi

Steganografi adalah ilmu dan seni menulis atau menyembunyikan pesan ke dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut. Metode steganografi sangat berguna jika digunakan pada steganografi komputer karena banyak format *file digital* yang dapat dijadikan media untuk menyembunyikan pesan. Steganografi yang dibahas di sini adalah penyembunyian data di dalam teks *digital* saja. Meskipun demikian, penyembunyian data dapat juga dilakukan pada wadah berupa suara *digital*,

teks, ataupun *video*. Penyembunyian data rahasia ke dalam teks *digital* akan mengubah *size* teks tersebut.

Kriteria yang harus diperhatikan dalam penyembunyian data adalah :

1) *Fidelity*
   Mutu *covertext* penampung tidak jauh berubah. Setelah penambahan data rahasia, teks hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam teks tersebut terdapat data rahasia.
2) *Robustness*
   Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada *covertext* penampung. Bila pada teks dilakukan operasi pengolahan teks, maka data yang disembunyikan tidak rusak.
3) *Recovery*
   Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah data *hiding*, maka sewaktu-waktu data rahasia di dalam *covertext* penampung harus dapat diambil kembali untuk digunakan lebih lanjut.
4) *Imperceptible*
   Keberadaan pesan rahasia tidak dapat dipersepi.

Gambar 3. Diagram Steagnografi Teks

3. Hasil dan Analisa

3.1. Pengujian Fungsionalitas Program

Hasil pengujian fungsionalitas program kriptografi yang terdiri dari algoritma simetris RC4 dan algoritma asimetris RSA secara umum terdiri dari pengujian terhadap proses enkripsi, proses dekripsi, dan pembuatan kunci. Sedangkan hasil pengujian fungsionalitas program steganografi secara umum terdiri dari pengujian mode ukuran font, mode warna font, proses enkripsi, dan proses dekripsi dengan media cover berupa teks. Dari hasil pengujian fungsionalitas program kriptografi RC4, RSA, serta program steganografi dengan dua mode atribut teks dapat disimpulkan bahwa seluruh bentuk pengujian fungsionalitas program yang dilakukan telah sesuai dengan hasil yang diharapkan.

Tabel 1. Data hasil uji fungsionalitas program kriptografi.

Nama Pengujian	Bentuk Pengujian	Hasil yang Diharapkan	Hasil Uji
Pengujian Enkripsi *RC4*	*Input plaintext, kunci, enkrip*	Muncul *ciphertext*	v
Pengujian Dekripsi *RC4*	Memasukkan *ciphertext* dan kunci, klik tombol Enkripsi	Muncul p*laintext*	v
Pengujian *Generate Keys RSA*	Klik Tombol *Generate Keys*	Muncul pembangkitan kunci P, Q, N, Phi, E, D secara acak	v
Pengujian Enkripsi *RSA*	Klik *Generate Keys,* masukkan *plaintext,* klik tombol Enkrip	Muncul *ciphertext*	v
Pengujian Dekripsi *RSA*	Masukkan *ciphertext*, klik tombol Dekrip	Muncul *plaintext*	v

keterangan : v =berhasil ; x = gagal

Tabel 2. Data hasil uji fungsionalitas program steganografi.

Nama Pengujian	Bentuk Pengujian	Hasil yang Diharapkan	Hasil Uji
Pengujian Mode Ukuran	Klik *radio button* ubah ukuran, keluar *MsgBox Mode Font Size*, isi ukuran, klik OK	Muncul info ukuran yang dimasukkan	v
Pengujian Mode Warna	Klik *radio button* ubah warna, keluar *GroupBox* pilih warna, isi warna *RGB* 8 bit	Muncul warna yang dipilih	v
Pengujian Tombol *Reset* Mode	Klik *Reset* Mode	Mode kembali mengulang dari awal	v
Pengujian *Password* pesan	Pilih mode, masukkan pesan asli, pesan palsu, klik tombol *password* pesan, masukkan *password,* klik OK	Muncul notifikasi OK Selesai dan hasil pesan keluar	v
Pengujian Buka *password* pesan diterima	Klik *load from file,* pilih *file*, klik *Open*, klik Buka *password* pesan diterima, isi *password,* klik OK	Muncul pesan asli dan notifikasi OK Selesai	v

3.2. Pengujian Enkripsi dan Dekripsi Kriptografi

Pengujian dilakukan dengan menguji hasil enkripsi dan dekripsi kriptografi dengan menggunakan kunci enkripsi dan dekripsi yang sama hasil ujinya berhasil dengan parameter *plaintext* kembali seperti semula sebelum saat dienkripsi. Sedangkan dengan menggunakan kunci enkripsi dan kunci dekripsi yang berbeda maka hasil ujinya gagal.

Tabel 3. Data hasil uji enkripsi dan dekripsi program kriptografi RC4.

Plaintext	Kunci Enkripsi	Enkripsi	Kunci Dekripsi	Dekripsi	Hasil Uji
INDONESIA	JAYA	70316723 173E194C 21	JAYA	INDONESIA	v
Merah Putih	suci	E5C55461 C796DB4 DAEB30C	suci	Merah Putih	v
INDONESIA	JAYA	70316723 173E194C 21	Jaya	<ÿk4Çg	x
Merah Putih	suci	E5C55461 C796DB4 DAEB30C	SUCI	¤ ¬™ÁpÄ-ê`	x

keterangan : v =berhasil ; x = gagal

Tabel 4. Data hasil uji enkripsi dan dekripsi program kriptografi RSA.

Plaintext	Kunci Enkripsi	Enkripsi	Kunci Dekripsi	Dekripsi	Hasil Uji
HAI	81222563, 87699083	36920842, 62108193, 74671944	81222563, 60594707	HAI	v
Pusat	21276341, 65523277	3951236, 4415089, 7267249, 15678412, 12663010	21276341, 14569381	Pusat	v
HAI	21276341, 87699083	36920842, 62108193, 74671944	36831269, 16517489	-	x
Pusat	21276341, 65523277	3951236, 4415089, 7267249, 15678412, 12663010	49405273, 41399833	-	x

keterangan : v =berhasil ; x = gagal

3.3. Pengujian Kecepatan Waktu Operasi Kriptografi

Pengujian yang telah dillakukan didapatkan hasil uji waktu enkripsi dan dekripsi dari algoritma RC4 lebih cepat dibandingkan dengan waktu enkripsi dan dekripsi algoritma RSA. Sehingga sesuai dasar teori bahwa kecepatan operasi dari algoritma simetris lebih tinggi bila dibandingkan dengan algoritma asimetris.

Tabel 5. Data hasil perbandingan kecepatan waktu operasi kriptografi RC4 dan RSA

Plaintext ke-	Waktu Enkripsi *RC4*	Waktu Enkripsi *RSA*	Waktu Dekripsi *RC4*	Waktu Dekripsi *RSA*
1	1 *min* 18 *sec* 633 *ms*	3 *min* 31 *sec* 590 *ms*	25 *sec* 652 *ms*	6 *min* 51 *sec* 348 *ms*
2	6 *min* 6 *sec* 41 *ms*	7 *min* 3 *sec* 259 *ms*	1 *min* 54 *sec* 884 *ms*	13 *min* 19 *sec* 522 *ms*
3	19 *min* 26 *sec* 319 *ms*	22 *min* 29 *sec* 272 *ms*	6 *min* 4 *sec* 457 *ms*	43 *min* 29 *sec* 20 *ms*

3.4. Pengujian Enkripsi dan Dekripsi Steganografi

Pengujian program steganografi menggunakan mode ukuran dan mode warna dilakukan dengan menggunakan beberapa pesan yang berbeda yang di dalamnya terdapat hasil enkripsi dari dua algoritma *RC4* atau *RSA* yang disembunyikan oleh pesan palsu yang diberikan.

Tabel 6. Data hasil uji program kriptografi dan steganografi parameter ukuran.

Pesan ke-	Jumlah karakter pesan palsu	Ukuran *font*	Enkripsi	Dekripsi	*Size file (bytes)*
1	145	7 pt	v	v	599
2	376	43 pt	v	v	782
3	1348	94 pt	v	v	2447

keterangan : v =berhasil ; x = gagal

Tabel 7. Data hasil uji program kriptografi dan steganografi parameter warna.

Pesan ke-	Jumlah karakter pesan palsu	Warna (R,G,B)	Enkripsi	Dekripsi	*Size file (bytes)*
1	213	50,101,110	v	v	727
2	585	50,0,150	v	v	1518
3	1305	250,150,90	v	v	2204

keterangan : v =berhasil ; x = gagal

3.5. Pengujian Pengiriman Pesan secara Online

Pengujian dilakukan dengan mengirimkan *file* steganografi secara *online* menggunakan *e-mail*, media sosial dan media penyimpanan *online*. Hal ini untuk menguji *file* steganografi yang dikirimkan mengalami kerusakan atau tidak dan setelah dikirim apakah terjadi perubahan terhadap *file* seperti ukuran *file* serta untuk mengetahui proses enkripsi dekripsi berjalan dengan baik atau tidak. Secara keseluruhan proses pengujian berhasil dengan ukuran *upload* sama dengan ukuran *download*.

Tabel 8. Data hasil uji pengiriman pesan melalui *e-mail* dan sosial media.

Pesan ke-	Mode *file*	Ukuran *upload (bytes)*	Pengiriman *via*	Ukuran *download (bytes)*	Enkripsi	Dekripsi
1	*RC4*, ukuran	616	*Gmail*	616	v	v
2	*RSA*, ukuran	1583	*Outlook Mail*	1583	v	v
3	*RSA*, warna	2150	*Yandex Mail*	2150	v	v
4	*RC4*, ukuran	848	*Facebook*	848	v	v
5	*RSA*, warna	1518	*Line*	1518	v	v

keterangan : v =berhasil ; x = gagal

Tabel 9. Data hasil uji pengiriman pesan melalui *cloud storage*.

Pesan ke-	Mode *file*	Ukuran *upload (bytes)*	Pengiriman *via*	Ukuran *download (bytes)*	Enkripsi	Dekripsi
1	*RC4*, ukuran	*762*	*Google Drive*	*762*	v	v
2	*RC4*, ukuran	*782*	*Dropbox*	*782*	v	v
3	*RC4*, warna	*841*	*4shared*	*841*	v	v
4	*RSA*, ukuran	*2430*	*Mediafire*	*2430*	v	v
5	*RC4*, warna	*923*	*Tusfiles*	*923*	v	v

4. Kesimpulan

Proses awal dari enkripsi kriptografi adalah menentukan kunci. Untuk algoritma *RC4* kunci ditentukan oleh pengguna sendiri sedangkan untuk algoritma *RSA* proses pembangkitan kunci ditentukan dengan diacak menggunakan program untuk membuat kunci publik dan kunci privat. Kecepatan waktu operasi pada algoritma *RC4* lebih cepat dibandingkan dengan algoritma *RSA*. Pada proses steganografi untuk proses dekripsi pada steganografi mode ukuran atau mode warna, penerima harus mengetahui *password*, ukuran *font* atau intensitas warna yang dipakai pengirim untuk melakukan enkripsi pesan steganografi apabila terdapat perbedaaan pada *password*, ukuran *font* atau intensitas warna saat dekripsi pesan maka program gagal untuk melakukan dekripsi.

Pada proses pengiriman *online file via e-mail*, sosial media, dan *cloud storage* ukuran *file* sebelum *upload* dan setelah *download* adalah sama serta isi *file* tidak mengalami kerusakan untuk mode ukuran maupun mode warna dan berhasil terdekripsi kembali. Pada penelitian selanjutnya untuk kriptografi agar dapat melakukan enkripsi dan dekripsi pada berkas lainnya seperti gambar, video, audio dan dapat menggunakan panjang kunci dengan bit yang lebih besar. Sedangkan untuk steganografi untuk bisa menggunakan lebih banyak atribut teks lainnya seperti tipe *font*, *style*, *effect*, *kerning*,*leading* dan juga dapat menggunakan media *cover* lainnya seperti gambar, audio, dan video.

Referensi

[1]. Muzakir, Ari, 2014, *Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standard (DES) dengan Mode Operasi Cipher Block Chaining (CBC).* Seminar Nasional Inovasi dan Tren (SNIT) 2014.

[2]. Paramita, Anang, *Implementasi Algoritma Kriptografi RSA pada Surat Elektronik*, Tugas Akhir, Universitas Diponegoro, Semarang. 2014.

[3]. Dwi, Asti, 2007, *Metode Pengamanan Enkripsi RC4 Stream Cipher untuk Aplikasi Pelayanan Gangguan.* Seminar Nasional Aplikasi Teknologi Informasi (SINATI) 2007.

[4]. Mahmud, Amir, 2013, *Pengaman Data dengan Metode Steganografy dan Algoritma RC4.* Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM) 2013.

[5]. Saefullah, Asep, 2012, *Aplikasi Stegaografi untuk Menyembunyikan Teks dalam Media Image dengan Menggunakan Metode LSB.* Seminar Nasional Teknologi Informasi dan Komunikasi Terapan (Semantik) 2012.

[6]. Scheiner, Bruce., *Applied Cryptography, 2nd Edition*. USA. 1996.

[7]. Fauzan, Firda, *Pengamanan Transmisi Hasil dan Data Query Basis Data dengan Algoritma Kriptografi RC4*, Tugas Akhir, Institut Teknologi Bandung, Bandung, 2008.

[8]. Rivest R.L., Shamir A., Adleman L, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. MIT: Massachusetts. 1977.

[9]. Mohanty, Saraju, *Digital Watermarking: Tutorial Review.* Dept of Comp Sc and Eng. University of South Florida: Tampa, FL 33620. 1999.

[10]. Lee, Christopher, *Pintar Pemrograman Microsoft Visual Basic 2010.* Jakarta : Elex Media Komputindo, 2014.