

Pengamanan Disposisi Dokumen secara online menggunakan Kriptografi Twofish dan Kompresi Huffman pada CV. TMU

Imelda Imelda¹⁾, Ega Prawira²⁾

^{1),2)}Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Cileduk Raya Petukangan Utara Jakarta Selatan 12260
Email : imelda@budiluhur.ac.id, egayage21@yahoo.com

Abstrak. Disposisi merupakan petunjuk singkat tentang tindak lanjut terhadap suatu urusan atau surat masuk. Banyak dokumen yang membutuhkan disposisi dari pimpinan. Padahal pimpinan tidak selalu berada di kantor. Dokumen yang di disposisi sangat penting. Tidak sembarang orang boleh mendistribusikan dokumen. Oleh karena itu pengamanan disposisi dokumen merupakan hal mutlak yang harus dilakukan. Penyelesaiannya dibuatlah pengamanan disposisi dokumen secara online berbasis web dengan algoritma Twofish dan algoritma Huffman. Pengamanan ini dapat melindungi data yang memiliki file yang berformat Microsoft Word, Microsoft Excel, dan PDF. Dengan pengamanan ini maka dapat mencegah terjadinya pencurian, kerusakan dan penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Alasan pemilihan algoritma Twofish dan Huffman karena kedua algoritma ini sederhana. Ada dua tahap dalam mengamankan disposisi dokumen. Pertama, proses encode untuk enkripsi dan kompresi. Pada proses ini, pesan diisi lalu pilih file yang ingin disertakan, kemudian isi password, klik ok untuk menjalankan proses encode. Kedua, proses decode untuk melakukan dekompresi dan dekripsi. Pada proses ini, buka inbox lalu ambil file yang sudah di encode, masukkan password yang sama saat enkripsi, klik ok untuk menjalankan proses decode. Berdasarkan 9 data pengujian diperoleh rata-rata proses encode 7,1 KB/s dan decode 6 KB/s.

Kata kunci : Disposisi, Kriptografi, Twofish, Kompresi, Huffman

1. Pendahuluan

Disposisi merupakan petunjuk singkat tentang tindak lanjut terhadap suatu urusan atau surat masuk [1]. Disposisi adalah petunjuk tertulis mengenai tindak lanjut pengelolaan Surat bersama lembar disposisi diantarkan oleh kurir ke dinas atau biro yang dituju. Kemudian apabila diperlukan pejabat yang berwenang dapat melakukan disposisi lanjutan kepada bawahannya hingga surat sampai ke tangan pelaksana untuk ditindaklanjuti. Setelah surat ditindaklanjuti, maka pelaksana akan memberikan laporan kepada pimpinan yang telah memberikan disposisi.

Disposisi dokumen pada CV. TMU dilakukan melalui *email* yang diterima staf administrasi, lalu staf mencatat ke dalam buku agenda kemudian diteruskan kepada pimpinan lalu akan diteruskan kepada bagian yang akan dituju. Keragaman tugas dan fungsi unit kerja semakin menyulitkan dalam mengantisipasi keberadaan dokumen sejak awal masuk sampai menjadi arsip. Tugas dan fungsi organisasi pengendalian dokumen tidak diterapkan secara optimal.

CV. TMU yang memiliki berbagai macam data yang harus dirahasiakan seperti dokumen perjanjian, kontrak kerja, laporan keuangan, transaksi, legalitas perusahaan, pajak, dan sebagainya yang didistribusikan baik dalam perusahaan itu sendiri maupun di luar perusahaan. Oleh karena itu, sebuah data harus dijaga kerahasiaannya supaya tidak disalahgunakan oleh orang yang tidak berwenang. Dimana, ketika sudah dilakukan pengamanan data, orang yang telah mencuri data tersebut tidak bisa menyalahgunakan karena tidak dapat dibaca oleh orang tersebut.

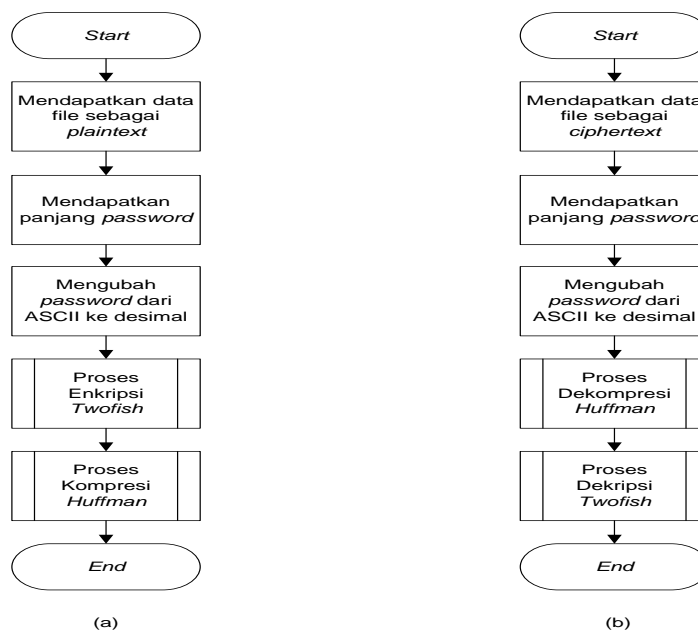
Oleh karena itu, dibutuhkan suatu mekanisme yang dapat mengamankan informasi tersebut dengan baik, dapat mudah digunakan dengan fitur yang dapat diandalkan sehingga aman dari pihak yang tidak memiliki kepentingan. Salah satunya dengan memanfaatkan kriptografi sebagai sistem keamanan. Kriptografi adalah sebuah teknik yang digunakan untuk melindungi data dengan melakukan pengacakan terhadap isi data sehingga sulit untuk diartikan [2]. Kemudian dilanjutkan dengan teknik kompresi data yang diketahui untuk mengurangi ukuran suatu file menjadi lebih kecil. Proses kompresi data dikombinasikan dengan kriptografi diperlukan untuk mempercepat waktu dalam proses pengiriman data.

Kontribusi penelitian ini adalah mengamankan disposisi dokumen secara online berbasis web menggunakan kriptografi dengan algoritma *Twofish* dan kompresi dengan algoritma *Huffman*.

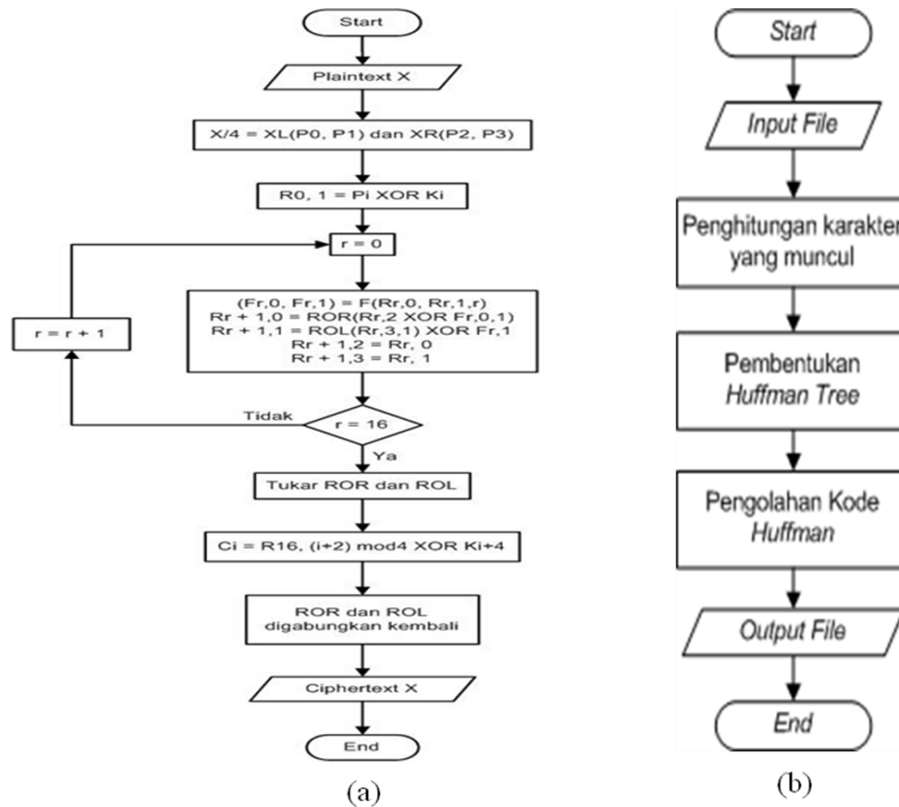
2. Disposisi Dokumen secara online dengan Kriptografi Twofish Dan Kompresi Data Huffman

Pada penelitian ini terdapat kegiatan pengiriman pesan dan dokumen disertai dengan proses *encode* terhadap isi dokumen. Proses *encode* adalah proses enkripsi menggunakan kriptografi *Twofish* dan kompresi menggunakan algoritma *Huffman*. Ada beberapa langkah dalam melakukan *encode*. Pada saat proses *encode*, langkah pertama adalah memasukan kunci privat yang digunakan untuk enkripsi data. Setelah memasukan kunci, kemudian dilakukan proses enkripsi menggunakan algoritma *Twofish* menggunakan kunci privat yang telah dimasukan sebelumnya. Langkah selanjutnya adalah mengkompresi data yang telah di enkripsi menggunakan algoritma *Huffman*. Setelah proses *encode* selesai, maka pesan dan dokumen di kirim atau di disposisi sesuai bagian yang dituju. Detil proses dapat dilihat pada Gambar 1a dan Gambar 2.

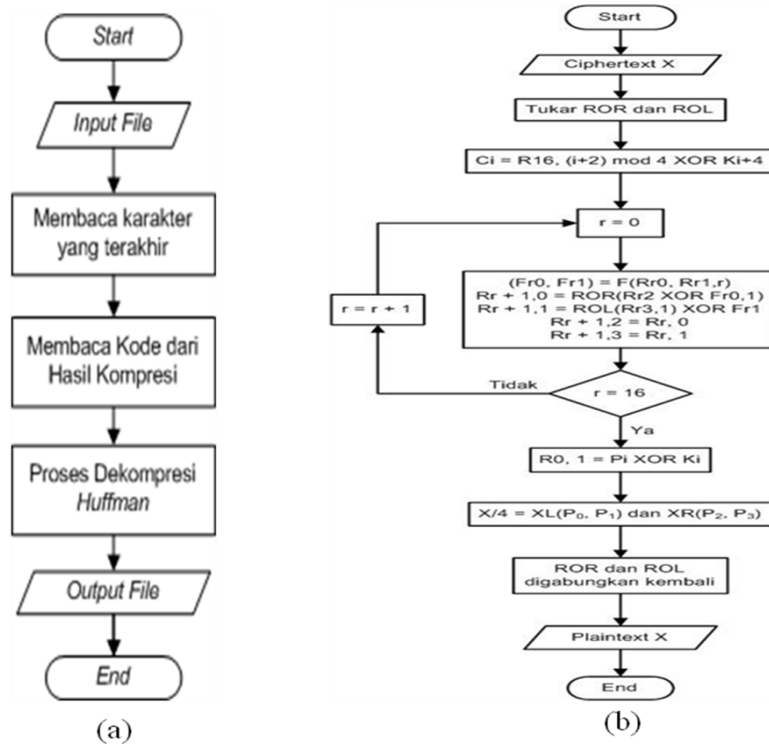
Bagian yang dituju menerima pesan dan dokumen yang telah di *encode*. Bagian ini membutuhkan dokumen asli agar dapat mengetahui isi dokumen penting yang telah dikirimkan. Dokumen yang telah di *encode* perlu dikembalikan ke bentuk semula. Caranya dokumen perlu di *decode*. Proses *decode* adalah melakukan dekompresi menggunakan algoritma *Huffman* dan dekripsi menggunakan algoritma *Twofish*. Ada beberapa langkah untuk melakukan *decode*. Langkah pertama adalah dokumen di dekompresi menggunakan algoritma *Huffman*. Langkah selanjutnya, data di dekripsi menggunakan algoritma *Twofish*. Dekripsi yang dilakukan algoritma *Twofish* menggunakan kunci privat yang telah digunakan karena algoritma *Twofish* termasuk dalam algoritma kriptografi simetris yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Detil proses dapat dilihat pada Gambar 1b dan Gambar 3.



Gambar 1. Flowchart Proses Encode dan Decode yang diusulkan (a) Encode (b) Decode



Gambar 2. Flowchart Proses Encode dengan Enkripsi *Twofish* dan Kompresi *Huffman*
(a) Enkripsi *Twofish* (b) Kompresi *Huffman*



Gambar 3. Flowchart Proses Decode dengan Dekompresi *Huffman* dan Dekripsi *Twofish*
(a) Dekompresi *Huffman* (b) Dekripsi *Twofish*

2.1. Algoritma Twofish

Twofish adalah algoritma kriptografi yang beroperasi dalam mode *block cipher*. Algoritma *Twofish* sendiri merupakan pengembangan dari algoritma *Blowfish*. Perancangan *Twofish* dilakukan dengan memperhatikan kriteria-kriteria yang diajukan *National Institute of Standards and Technology* (NIST) untuk kompetisi *Advanced Encryption Standard* (AES) dan menjadi salah satu finalis. *Twofish* adalah block cipher yang berukuran 128 bit yang dapat menerima kunci dengan panjang mencapai 256 bit. *Twofish* merupakan algoritma yang beroperasi dalam mode blok [3]. Algoritma *Twofish* terdiri dari 3 (tiga) tahapan proses, yaitu penjadwalan kunci, proses enkripsi, dan proses dekripsi [4].

2.2. Algoritma Huffman

Prinsip kode *Huffman* adalah karakter yang paling sering muncul di dalam data dikodekan dengan kode yang jumlah bitnya lebih sedikit, sedangkan karakter yang jarang muncul dikodekan dengan kode yang jumlah bitnya lebih panjang. Algoritma *Huffman* menggunakan tabel frekuensi kemunculan karakter untuk frekuensi dua buah pohon yang digabungkan [5]. Oleh karena itu, total *cost* pembentukan pohon *Huffman* adalah jumlah seluruh penggabungan daun-daun.

Metode kode huffman merupakan salah satu metode yang terdapat pada teknik kode entropy [6]. Dalam kode huffman, panjang blok dari keluaran sumber dipetakan dalam blok berdasarkan panjang variabel. Cara seperti ini disebut sebagai *fixed to variable-length coding*. Ide dari kode huffman adalah memilih panjang *codeword* dari yang paling besar probabilitasnya sampai dengan urutan *codeword* yang paling kecil probabilitasnya. Apabila dapat dipetakan setiap keluaran sumber dari probabilitas p_i ke sebuah *codeword* dengan panjang $1/p_i$ dan pada saat yang bersamaan dapat dipastikan bahwa dapat didekodekan secara unik, dengan dicarikan rata-rata panjang kode $H(x)$. Kode Huffman dapat didekodekan secara unik dengan $H(x)$ minimum dan optimum pada keunikan dari kode-kode tersebut. Algoritma dari kode huffman adalah :

- a. Pengurutan keluaran sumber dimulai dari probabilitas paling tinggi.
- b. Menggabungkan dua keluaran yang sama dekat ke dalam satu keluaran yang probabilitasnya merupakan jumlah dari probabilitas sebelumnya.
- c. Apabila setelah dibagi masih terdapat dua keluaran, maka lanjut ke langkah berikutnya, namun apabila masih terdapat lebih dari dua, kembali ke langkah satu.
- d. Memberikan nilai 0 dan 1 untuk keluaran. Apabila sebuah keluaran merupakan hasil dari penggabungan dua keluaran dari langkah sebelumnya, maka berikan 0 dan 1 untuk *codeword*-nya, ulangi sampai keluaran merupakan satu keluaran yang berdiri sendiri. Untuk menentukan kode-kode dengan kriteria bahwa kode harus unik dan karakter yang sering muncul dibuat kecil jumlah bitnya, dapat digunakan algoritma *Huffman*.

3. Pembahasan

3.1. Hasil

Pengamanan disposisi dokumen berbasis web ini menggunakan bahasa pemrograman PHP. Perangkat yang dibutuhkan dalam melakukan implementasi ini terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*).

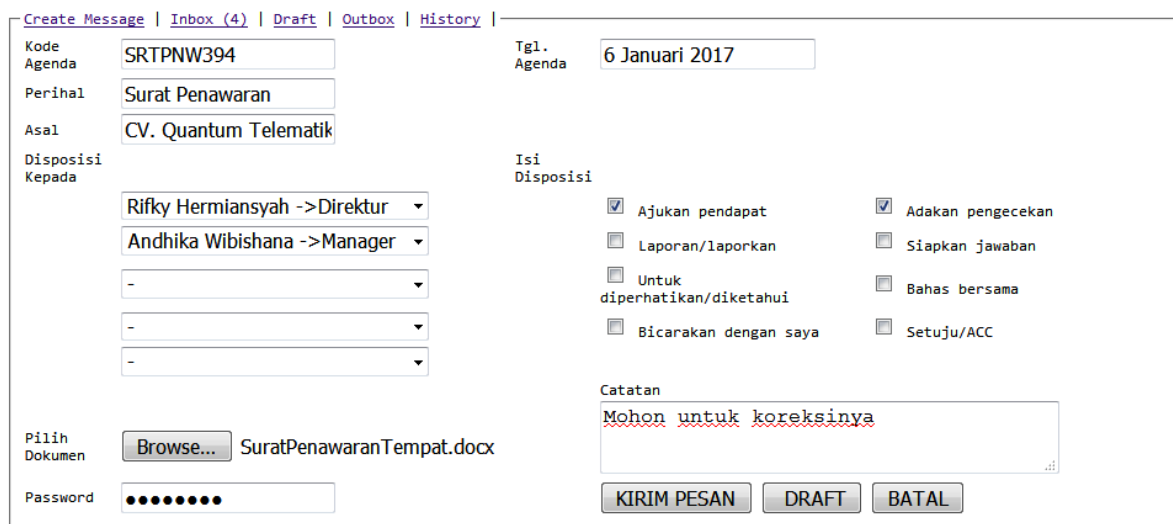
Spesifikasi perangkat keras / *hardware* yang digunakan adalah sebagai berikut:

- a. *Processor* : Intel(R) Pentium(R) CPU P6100 2.0 GHz
- b. *RAM* : 3 GB
- c. *Harddisk* : 320 GB
- d. *Monitor* : 14.0"
- e. *Mouse* : USB Mouse
- f. *Keyboard* : Internal Keyboard Laptop

Spesifikasi perangkat lunak / *software* yang digunakan dalam pembuatan aplikasi adalah sebagai berikut :

- a. Sistem Operasi : Windows 7 Ultimate 32-bit
- b. Bahasa Pemrograman : PHP
- c. Editor : Adobe Dreamweaver CS5, Notepad++
- d. Database Server : MySQL Server 5.1.41

Implementasi disposisi dokumen ini memiliki dua tahap utama. Pertama, Buat Pesan. Kedua, tahap *Inbox*. Pada tahap Buat Pesan, user perlu mengisi *form* pesan disertai dengan mempersiapkan file dokumen. Kemudian user memilih file dokumen yang akan disertakan untuk dikirim. Setelah itu user memasukan password minimal 8 karakter lalu tekan tombol Kirim Pesan untuk menjalankan proses encode, seperti Gambar 4. Hasil dari *encode* merupakan file yang berisikan *ciphertext* (file acak). Waktu proses encode di mulai pada saat tombol Kirim Pesan di klik dan berakhir pada saat pesan terkirim.



Gambar 4. Tahap Buat Pesan

Tahap *Inbox* dilakukan apabila *user* ingin melihat pesan yang masuk dan melakukan pengembalian *file* yang telah di-*encode*. Tahap *inbox* dimulai dengan memilih pesan yang ingin dilihat. Setelah memilih pesan, kemudian *user* melihat pesan masuk lalu *user* meng-*input password* yang sama dengan password yang digunakan pada tahap Buat Pesan, seperti Gambar 5. Hasil dari decode merupakan file yang berisi *plaintext* (file asli). Waktu proses decode dimulai pada saat tombol Download di klik dan berakhir saat muncul kotak dialog save file.



Gambar 5 Tahap Inbox

3.2. Pengujian

Pengujian ini membahas perbandingan antar proses *encode* dan *decode file*. *File* yang diuji meliputi jenis *file*, yaitu *file* berformat .doc, .docx, .xls, .xlsx, atau .pdf. Pengujiannya membandingkan antara ukuran *file* asli dan ukuran *file* setelah melakukan *encode*, waktu proses pada saat *encode*, waktu proses dekripsi hingga hasil yang dicapai dalam proses *encode* maupun *decode*.

3.2.1. Pengujian Proses Encode

Tabel 1 menunjukkan hasil pengujian proses encode. Pengujian proses encode dilakukan pada 9 dokumen yang berekstensi .doc, docx, xls,xlsx, dan pdf. Tabel 1 menunjukkan 9 pengujian yang telah dilakukan. Tabel 1 terdiri dari nama file asli, size asli, waktu proses, nama file encode, size file encode. Berdasarkan hasil pengujian ukuran file yang telah di-encode memiliki sedikit selisih dengan file asli. Dengan rata-rata ukuran file asli 816,8 KB dan output file 817,94 KB dan waktu proses 115,15 detik.

Tabel 1. Hasil Pengujian Proses *Encode*

Nama <i>File</i> Asli	Size Asli	Waktu Proses (detik)	Nama <i>File</i> Encode	Size <i>File</i> Encode
Dokumen1.doc	53 KB	12,2	Encode_Dokumen1.doc	54 KB
Dokumen2.docx	173 KB	38,3	Encode_Dokumen2.docx	174 KB
Dokumen3.xls	300 KB	67,7	Encode_Dokumen3.xls	301 KB
Dokumen4.xlsx	83 KB	18,8	Encode_Dokumen4.xlsx	84 KB
Dokumen5.pdf	401 KB	88,9	Encode_Dokumen5.pdf	402 KB
Dokumen6.docx berisi "aa.." sebanyak 1000 kata	9,71 KB	2,55	Encode_Dokumen6.docx	10,47 KB
Dokumen7.docx berisi "abc..xyzABC..XYZ" sebanyak 1000 kata	10,07 KB	2,176	Encode_Dokumen7.docx	10,83 KB
Dokumen8.pdf	5671,94 KB	585,07	Encode_Dokumen8.pdf	5675,42 KB
Dokumen9.pdf	1466,25 KB	220,65	Encode_Dokumen9.pdf	1467,71 KB
Rata-rata:	816,8	115,15		817,94

3.2.2. Pengujian Proses Decode

Tabel 2 menunjukkan hasil pengujian proses decode. Pengujian proses decode dilakukan pada 9 dokumen. Input dokumen pada proses decode adalah 9 dokumen yang telah di-encode. Tabel 2 menunjukkan 9 pengujian yang telah dilakukan. Tabel 2 terdiri dari nama file encode, size file, waktu proses, nama file decode, size file decode. Berdasarkan hasil pengujian ukuran dokumen asli sama dengan dokumen hasil decode. Dengan rata-rata ukuran file encode 817,94 KB dan output file 815,51 KB dan waktu proses 134,699 detik.

Tabel 2. Hasil Pengujian Proses Decode

Nama <i>File</i> Encode	Size <i>File</i> Encode	Waktu proses (detik)	Nama <i>File</i> decode	Size <i>File</i> decode
Encode_Dokumen1.doc	54 KB	14	Decode_Dokumen1.doc	53 KB
Encode_Dokumen2.docx	174 KB	44,3	Decode_Dokumen2.docx	174 KB
Encode_Dokumen3.xls	301 KB	77,3	Decode_Dokumen3.xls	301 KB
Encode_Dokumen4.xlsx	84 KB	21,6	Decode_Dokumen4.xlsx	83 KB
Encode_Dokumen5.pdf	402 KB	103,8	Decode_Dokumen5.pdf	401 KB
Encode_Dokumen6.docx	10,47 KB	2,004	Decode_Dokumen6.docx	9,71 KB
Encode_Dokumen7.docx	10,83 KB	2,109	Decode_Dokumen7.docx	10 KB
Encode_Dokumen8.pdf	5675,42 KB	680,77	Decode_Dokumen8.pdf	5671 KB
Encode_Dokumen9.pdf	1467,71 KB	266,41	Decode_Dokumen9.pdf	1452,40 KB
Rata-rata:	817,94	134,699		815,51

3.3. Evaluasi Sistem

Evaluasi sistem bertujuan untuk mengetahui hasil yang telah dicapai berdasarkan analisa dan implementasi dari hasil pengujian aplikasi. Dari pengujian diperoleh informasi bahwa isi dokumen mempengaruhi waktu *encode* dan *decode*. Hal ini dapat dilihat dari pengujian untuk dokumen 6.docx dan dokumen 7.docx yang memiliki perbedaan waktu *encode* dan *decode*. Kelebihan aplikasi adalah aplikasi ini mempermudah disposisi karena tidak memerlukan dokumen dalam bentuk fisik, rata-rata proses *encode* mencapai 7,1 KB/s, rata-rata proses

decode mencapai 6 KB/s, *file* yang telah di-*encode* tidak dapat dibaca dan dibuka oleh orang lain sebelum di-*decode*, dan ukuran *file* hasil *encode* tidak jauh berbeda dengan ukuran *file* asli. Sedangkan kekurangan aplikasi ini adalah semakin besar file maka semakin lama prosesnya dan aplikasi ini hanya meng-*encode* jenis file yang berformat .doc, .docx, .xls, .xlsx, dan .pdf.

4. Simpulan

Pengamanan disposisi dokumen berbasis web dengan kriptografi *Twofish* dan kompresi *Huffman* membuat penyimpanan dan pertukaran informasi menjadi lebih aman. Format file yang digunakan adalah file .doc, .docx, xls, xlsx, dan pdf. Aplikasi ini dapat digunakan dengan mudah karena dirancang sesederhana mungkin sehingga user dengan mudah menggunakannya. Waktu yang diperlukan untuk meng-*encode* dan men-*decode* file tergantung pada ukuran file dan spesifikasi komponen komputer yang digunakan, jika ukuran file yang di proses semakin besar maka diperlukan waktu yang semakin lama, sedangkan jika ukuran file yang di proses semakin kecil maka diperlukan waktu yang semakin cepat. Tidak terjadi kerusakan pada file dokumen yang telah didekripsi, sehingga sama sekali tidak ada perubahan terhadap isi data sedikitpun dari file asli. Pada penelitian selanjutnya dapat dikembangkan kriptografi asimetris karena keabsahannya diakui sebagai tanda tangan digital.

Ucapan Terima Kasih

Ucapan terima kasih diberikan kepada Yayasan Budi Luhur Cakti yang telah memberikan dukungan sehingga penelitian ini dapat dipublikasikan.

Daftar Pustaka

- [1]. Aji, Sapto., Migunani., Fitro Nur Hakim., 2014, *Rancang Bangun Sistem Informasi Disposisi Surat Berbasis Web*, Semarang, Indonesian Journal on Networking and Security, 3(3), hal. 25-27.
- [2]. Munir, Rinaldi., 2006, *Kriptografi*, Bandung: Informatika.
- [3]. Randy, Adhitya., 2012, Studi dan Perbandingan Algoritma Blowfish dan Twofish, Tugas Akhir Institut Teknologi Bandung.
- [4]. Radhiah, Ainatul., 2014, Rancang Bangun Secure Chatting Pada Platform Android Dengan Algoritma Twofish, Tugas Akhir Institut Teknologi Bandung.
- [5]. Putra, Darma., 2004, Perbandingan Kinerja Algoritma Kompresi Huffman, LZW, dan DMC pada Berbagai Tipe File., Jurnal Integral, 9(1), hal. 7-16.
- [6]. Musril, Hari Antoni., 2012, Studi Komparasi Metode Arithmetic Coding Dan Huffman Coding Dalam Algoritma Entropy Untuk Kompresi Citra Digital, Jurnal Teknologi Informasi & Pendidikan, 5(2), hal.135-149.