Perancangan dan Realisasi Aplikasi Berbasis *Web* untuk Enkripsi dan Dekripsi Data dengan Algoritma 3DES dan Twofish

Mera Kartika Delimayanti
Jurusan Teknik Informatika dan Komputer
Politeknik Negeri Jakarta
Depok, Indonesia
mera.kartika@tik.pnj.ac.id

Danu Sudirko
Jurusan Teknik Elektro
Politeknik Negeri Jakarta
Depok, Indonesia
danu.sardiko@gmail.com

Diterima: 15 Maret 2015. Disetujui: 15 April 2015. Dipublikasikan: Mei 2015

***Abstrak* - Penelitian ini membahas perancangan dan realisasi sistem berupa aplikasi berbasis *web* untuk enkripsi dan dekripsi data dengan algoritma 3DES dan Twofish yang berfungsi untuk mengamankan sebuah data. Sistem dapat digunakan untuk mencegah tindakan pencurian informasi data dengan cara menyandikan informasi menggunakan teknik kriptografi berupa enkripsi dan dekripsi dengan menggunakan 2 metode yakni 3DES dan Twofish. Fungsi enkripsi adalah untuk menyandikan data sebenarnya (*plaintext*) menjadi data sandi (*chipertext*) dan fungsi dekripsi adalah sebaliknya. 3DES adalah salah satu algoritma enkripsi yang cukup populer dan perkembangan dari DES dengan menggunakan panjang kunci 168 bit, sedangkan Twofish merupakan algoritma dengan panjang kunci bervariasi 128-bit, 192-bit, dan 256-bit. Sistem dirancang dan dibangun berbasis *web* untuk mempermudah penggunaan yang dapat multi *platform*. Implementasi sistem telah dilakukan dengan menggunakan berbagai macam tipe file dengan ukuran tertentu dan aplikasi telah berfungsi dengan baik tanpa mengubah file asli dengan teknik penyandian yang dipilih.**

Kata Kunci: enkripsi-dekripsi, algoritma 3DES, algoritma Twofish, aplikasi web.

I. PENDAHULUAN

Perkembangan teknologi telah banyak mengubah data keras menjadi data lunak sehingga ancaman pencurian data lunak wajib diantisipasi. Salah satu cara pengamanan data dengan teknik kriptografi. Kriptografi berupa teknik penyandian yang dapat digunakan untuk merahasiakan data yang terdiri dari dua proses enkripsi dan dekripsi. Proses enkripsi adalah proses *encode* data agar berubah kedalam bentuk data sandi yang tidak dapat dibaca. Proses dekripsi adalah proses *decode* data agar berubah ke dalam bentuk data aslinya [1].

Salah satu algoritma kriptografi yang lazim digunakan pada algoritma simetris adalah algoritma 3DES dan Twofish selain jenis-jenis algoritma lainnya seperti Blowfish, DES, 3DES, Twofish, Rijndael [2]. Implementasi penggunaan algoritma simetris dalam aplikasi sehari-hari sebagai contoh pembangunan aplikasi *web event calendar* dengan algoritma Rijndael untuk enkripsi data [3]. Aplikasi tersebut mampu mengatur *data event* agar terorganisir sesuai konsep.

Pada penelitian Muhamad, telah dilakukan implementasi kombinasi Algoritma 3DES dan Algoritma Base64 pada sistem keamanan *handshaking animation store*. Algoritma dimaksudkan untuk menghindari proses *upload*, *download* dan jual beli konten animasi tanpa melalui verifikasi aplikasi *client* (ilegal) [4]. Aplikasi dikembangkan berbasis *desktop* menggunakan Delphi sehingga tidak dapat diimplementasikan multi *platform* sistem operasi komputer.

Pada penelitian ini telah dilakukan rancang bangun suatu sistem berupa aplikasi berbasis *web*.

II. TINJAUAN PUSTAKA

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti : keabsahan, integritas data, serta autentikasi data. Ada 3 tujuan dari ilmu kriptografi, yaitu [1]:

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah seperti penyisipan, penghapusan, dan pensubtitusian data lain ke dalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi data mengenai keaslian data, keaslian pengirim, keaslian informasi data.

A. *Algoritma Simetris*

Algoritma simetris (*symetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*.

B. *Enkripsi - Dekripsi*

Enkripsi adalah proses penyandian *plaintext* menjadi *chipertext* dimana *plaintext* disebut dengan pesan asli (pesan yang ingin dikirim), sedangkan *chipertext* adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi seperti pada Gambar 1.

Gambar 1. Proses Enkripsi

Dekripsi adalah kebalikan dari enkripsi yakni mengubah *chipertext* menjadi *plaintext*, sehingga berupa data awal/asli seperti pada Gambar 2.

Gambar 2. Proses Dekripsi

Kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci yang digunakan adalah kunci rahasia (*private key*), yaitu kunci yang sama saat enkripsi dan dekripsi dilakukan.

C. *Triple Data Encryption Standard (3DES)*

DES (*Data Encryption Standard*) merupakan salah satu algoritma simetris pada kriptografi yang merupakan *Block Chiper* yang menerima 64 bit data *input* dan mengeluarkan 64 bit data *output*. Panjang kunci yang digunakan adalah 64 bit (8 bit untuk *parity*, jadi panjang sebenarnya 56 bit). Skema global dari algorima DES adalah sebagai berikut [1]:

1. Blok *plaintext* dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasil permutasi awal kemudian di-*enchipering* sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *enchipering* kemudian dipermutasikan dengan matriks permutasi balikan (*invers initial permutation* atau IP-1) menjadi blok *chipertext*.

1. *Proses Enkripsi*

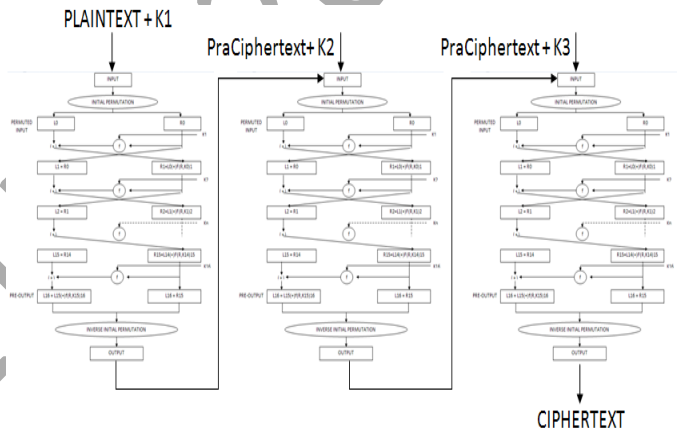
Plaintext yang dimasukan pertama akan disubtitusikan pada matrik permutasi awal (*initial permutation*) atau IP panjangnya 64-bit. Kemudian dibagi menjadi 2 bagian, yaitu kiri (L) dan kanan (R) masing-masing panjangnya menjadi 32-bit. Kedua bagian ini masuk ke dalam 16 putaran *enchipering*.

2. *Proses Dekripsi*

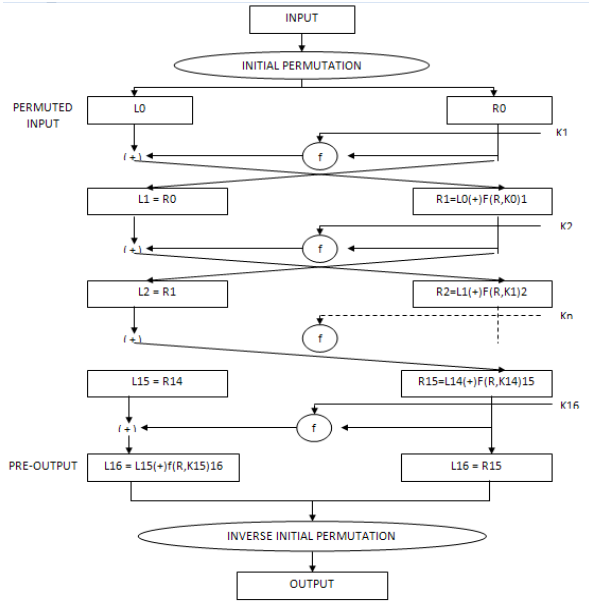
Proses dekripsi terhadap *chipertext* merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah k1, k2, ..., k16 maka pada proses dekripsi urutan kunci internal yang digunakan adalah k16, k15, ..., k1.

3DES (*Triple Data Encryption Standard*) merupakan suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Algoritma yang digunakan adalah melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES).

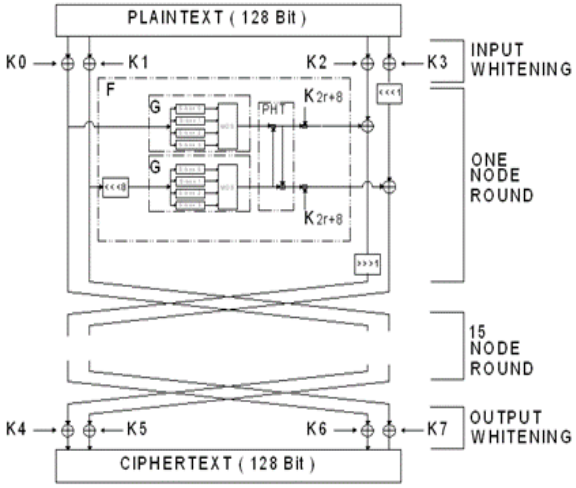
Pada algoritma 3DES seperti pada Gambar 3 dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Proses enkripsi ditunjukkan pada Gambar 4.



Gambar 3. Algoritma 3DES



Gambar 4. Proses Enkripsi DES



Gambar 5. Algoritma Twofish

Algoritma Twofish seperti pada Gambar 5 dibangun untuk memenuhi kriteria yang ditetapkan oleh NIST (*National of Standard*) pada sayembara penentuan standar algoritma. Kriteria tersebut diantaranya adalah [5]:

a. Menggunakan 128-bit enkripsi dengan metode *block chiper*.
b. Panjang kunci 128 bit, 192 bit, dan 256 bit.
c. Tidak memiliki kunci lemah.
d. Efisien baik jika digunakan di Intel Pentium Pro maupun perangkat lunak ataupun keras lainnya.
e. Memiliki desain yang fleksibel sehingga dapat digunakan untuk *stream chiper, hash function*, dan MAC.
f. Desain yang sederhana.

D. Teknologi Berbasis Web

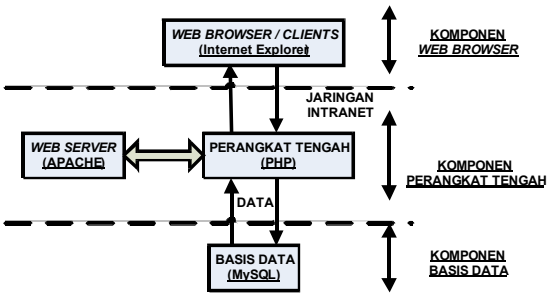
Perangkat lunak berbasis web dibangun atas tiga komponen yakni komponen basis data, komponen perangkat tengah dan komponen *web browser*. Gambar 6 menunjukkan arsitektur perangkat lunak berbasis *web* dilengkapi dengan perangkat lunak pembangun yang bersifat sumber terbuka [6]. Perangkat lunak berbasis *web* adalah salah satu penerapan *multi tier application* yakni aplikasi yang terbagi menjadi beberapa bagian dalam menjalankan fungsi masing-masing.

a) *Server Side Business Logic*

Server side business logic, sering disebut juga *middle tier*, adalah bagian yang bertanggung jawab atas cara kerja aplikasi.

b) *Back End Storage*

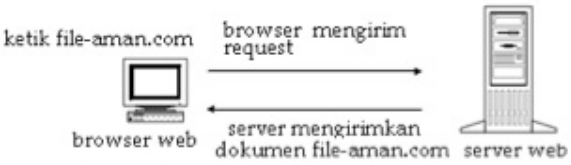
Bagian ini mengatur cara penyimpanan data yang merupakan materi yang cukup kompleks dalam pembangunan aplikasi. Gambar 6 Arsitektur Perangkat Lunak Berbasis *Web*.



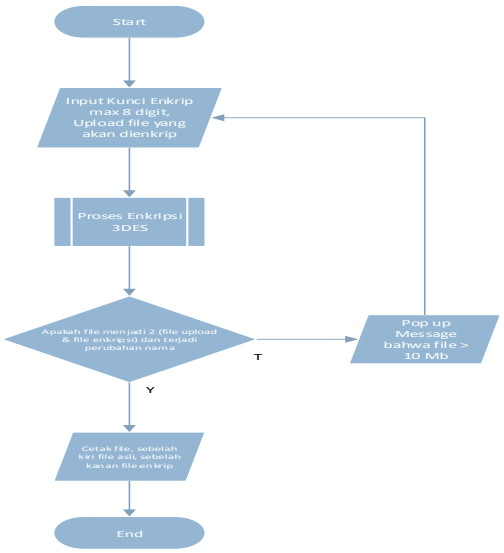
Gambar 6. Arsitektur Perangkat Lunak Berbasis *Web*

III. HASIL DAN PEMBAHASAN

Sistem dirancang untuk dapat melakukan proses enkripsi dan dekripsi dalam jaringan LAN maupun jaringan internet dengan menggunakan *web browser* sebagai alat untuk mengimplementasikan sistem. Diagram blok sistem seperti tercantum pada Gambar 7. Prinsip kerja situs *web* adalah untuk melakukan proses enkripsi dan dekripsi berbagai macam data. Pencatatan bagi pengguna yang mengunggah data akan tersimpan di basis data kriptografi pengguna supaya di kemudian hari dapat dilihat kembali data yang pernah diunggah dan dienkripsi atau didekripsi. Setiap pengguna dapat menentukan kunci enkrip-dekrip sebanyak maksimal 8 karakter. Gambar 8 menunjukkan salah satu diagram alir untuk proses enkripsi untuk algoritma 3DES.

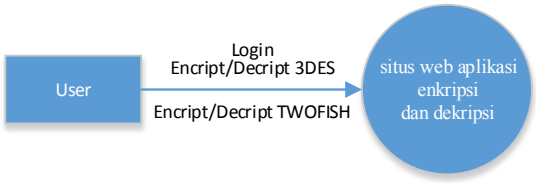


Gambar 7. Diagram Blok *System*



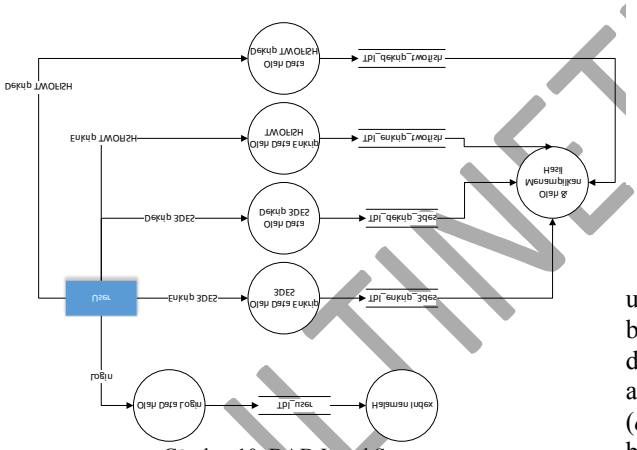
Gambar 8. Diagram Alir Enkripsi dengan Algoritma 3DES

Selanjutnya adalah merancang Diagram Aliran Data (DAD) yang merupakan gerakan data melalui sebuah sistem, mulai dari masuk sampai ke tujuannya. Diagram DAD level teratas sebagai *context* diagram. Dari *context* diagram ini kemudian akan digambarkan dengan lebih rinci lagi disebut DFD level 1. Tiap-tiap proses akan digambarkan secara lebih terinci lagi pada Gambar 9 dan 10.



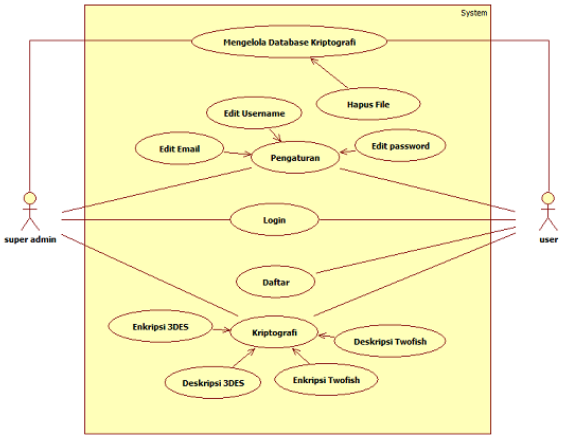
Gambar 9. Diagram Konteks Sistem

User atau pengguna dapat *login* dan langsung menggunakan aplikasi *web* untuk enkripsi dan dekripsi semua jenis data. Dimana pada DFD level 1, sistem dapat mengolah proses enkripsi dan dekripsi data. Sistem juga dapat menampilkan data asli dan data *chipper*. Selanjutnya seluruh data tersimpan dalam tabel data di basis data.

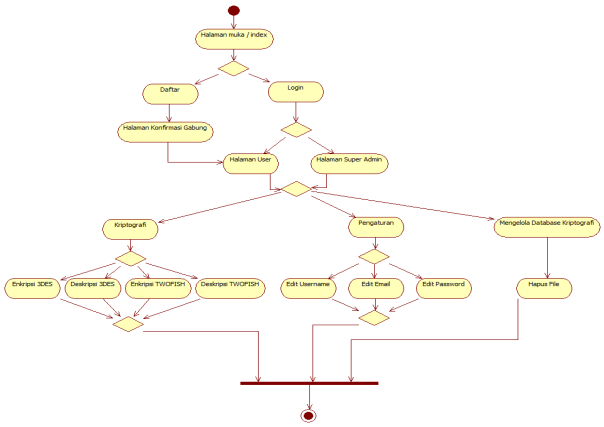


Gambar 10. DAD Level Satu

Untuk rancangan aplikasinya, telah dilakukan perancangan dengan membuat *use case diagram* dan *activity diagram* seperti yang terlihat di gambar 11 dan 12.



Gambar 11. *Use Case Diagram*



Gambar 12. *Activity Diagram*

Menu yang terdapat dalam sistem ialah menu untuk pengaturan pengguna, menu kriptografi yang berisi enkripsi dan dekripsi dengan algoritma yang dipilih serta pengelolaan basis data kriptografi oleh admin. Data asli (*plain*) maupun data tersandikan (*chipper*) dapat dihapus dalam menu pengelolaan basis data oleh admin.

Tahapan selanjutnya ialah implementasi aplikasi dengan membuat aplikasi *web* menggunakan script HTML, CSS dan pemrograman *web* dengan PHP dan basis data MySQL. Pada Gambar 13 merupakan halaman indeks sistem. Apabila pengguna telah berhasil *login* maka akan tampil menu beranda, tentang kami, kriptografi, basis data, pengaturan dan logout.

Gambar 13. Tampilan Halaman Kriptografi

Menu kriptografi terdiri dari enkripsi *3DES*, enkripsi *Twofish*, dekripsi *3DES*, dan dekripsi *Twofish*. *Input* untuk menjalankan sistem berupa data (file) dan kunci kriptografi seperti pada gambar 13. Setelah proses enkripsi, akan ditampilkan tabel yang berisi *file upload*, *file* kriptografi, lama proses *upload*, kecepatan *upload*, lama proses kriptografi, kecepatan kriptografi, dan tampilan karakter *file* asli dan *file* ter-enkripsi.

Pada proses pengujian enkripsi-dekripsi menggunakan algoritma *3DES* dan *Twofish* dilakukan pada form enkripsi yaitu dengan memasukan *file* yang akan diproses dengan *browsing file*, kemudian memasukan kunci enkripsi, lalu menekan tombol enkrip untuk diproses. Hasil enkripsi atau dekripsi berupa tampilan *file* yang diunggah baik berupa *file* asli maupun *file* terenkripsi dan *file* yang telah diproses enkripsi atau dekripsi serta menampilkan karakter pembentuk *file* asli dan *file* terenkripsi/ terdekripsi. File yang dilakukan untuk uji coba berukuran tidak lebih dari 10MB. Tabel 1 dan 2 menunjukkan hasil percobaan dari beberapa ekstensi file dengan masing-masing sebanyak 10 data dengan metode *3DES* dan metode *Twofish*.

TABEL 1. HASIL PERCOBAAN DENGAN METODE 3DES

No	Jenis *File*	Ukuran (Mb)	Lama proses enkripsi	Kecepatan enkripsi (Mbps)	Lama proses dekripsi	Kecepatan dekripsi (Mb)	Hasil sama seperti asli
1	.docx	0,016	0,091 s	0,17	0,004 s	3,60	√
2	.doc	0,050	0,008 s	6,06	0,023 s	2,14	√
3	.pdf	0,185	0,024 s	7,56	0,025 s	7,50	√
4	.jpg	0,139	0,018 s	7,47	0,02 s	6,82	√
5	.txt	0,029	0,005 s	4,88	0,005 s	4,88	√
6	.mp3	2,654	0,345 s	7,85	0,345 s	7,86	√

TABEL 2. HASIL PERCOBAAN DENGAN METODE *TWOFISH*

No	Jenis *File*	Ukuran (MB)	Lama roses ıkripsi	Kecepatan enkrip (Mbps)	Lama proses dekripsi	Kecpatan ekrip (Mbps)	Hasil sama seperti asli
1	.docx	0,016	0,002 s	5,81	0,002 s	5,85	√
2	.doc	0,050	0,003 s	14,72	0,003 s	16,32	√
3	.pdf	0,185	0,007 s	26,34	0,006 s	28,38	√
4	.jpg	0,139	0,006 s	22,83	0,005 s	28,01	√
5	.txt	0,029	0,002 s	24,88	0,002 s	9,79	√
6	.mp3	2,654	0,091 s	29,74	0,071 s	37,92	√

Proses enkripsi dan dekripsi yang dilakukan dengan ukuran *file* kurang dari 10 MB dan kunci yang digunakan maksimal 8 karakter supaya kunci tidak terlalu panjang sehingga mudah diingat. Kecepatan proses enkripsi dan dekripsi bergantung pada spesifikasi perangkat keras komputer, kondisi jaringan *internet* dan terpengaruh pada program aplikasi lain pada komputer yang sedang berjalan. kunci enkripsi dan dekripsi harus sama. *File* yang ter-*upload* tersimpan di *folder* file_asli atau file_enkrip/dekrip, kemudian yang tersimpan di basis data adalah nama *file*, ukuran, *password file*, dan nama *file* rename. Penyimpanan *file* di *folder* karena *folder* dapat menyimpan lebih banyak *file* dan memiliki kapasitas yang besar. *File* yang diunduh adalah berupa *file* asli yang sebelumnya diunggah, dan *file* enkrip/dekrip. Penghapusan *file* dengan men-*ceklist* menu *list* yang mewakili *file* dan proses hapus berjalan setelah menekan tombol hapus.

IV.KESIMPULAN

Berdasarkan hasil perancangan dan realisasi sistem berupa aplikasi berbasis *web* enkripsi dekripsi dengan metode algoritma *3DES* dan *Twofish*, maka dapat disimpulkan sebagai berikut :

1. Aplikasi *web* telah mampu untuk melakukan enkripsi dan dekripsi bermacam-macam jenis *file* dengan ukuran kurang dari 10MB tanpa ada perubahan data atau hasil seperti *file* asli.
2. Berdasarkan hasil percobaan maka perbandingan dari kedua metode kriptografi bahwa algoritma *Twofish* lebih unggul karena waktu yang diperlukan untuk proses enkripsi dan dekripsi 4 kali lebih cepat daripada metode *3DES* yang sesuai dengan penelitian Marta [7].
3. Tambahan kemampuan aplikasi enkripsi-dekripsi yang dibutuhkan dengan adanya proses *rename file* yakni dengan penambahan string -*3DES*- atau -*Twofish*- pada *file* yang diproses.
4. Basis data yang dirancang telah berfungsi sesuai dengan perencanaan yakni mampu menyimpan seluruh file yang telah terproses unggah, enkripsi, dan dekripsi. Selain itu basis data menyediakan fungsi unduh *file* dan hapus *file*.

REFERENSI

[1] F.Fidens,. "*Dasar Kriptografi"*. Kuliah Umum Ilmu Komputer, 2004.

[2] I.Mansoor. Et.al. "*Symmetric Algorithm Survey: A Comparative Analysis"*. International Journal of Computer Applications (0975-8887) Vol. 61-No.20, January 2013.

[3] D. Rosmala. Hanif, Wibowo. " *Pembangunan Aplikasi Web Event Calendar Menggunakan Algoritma Rijndael Untuk Enkripsi Data"* . Jurnal Informatika. No. 2 Vol. IV. Mei 2013. ISSN: 2087-5276.

[4] M. Abdul Rahim, *"Implementasi Kombinasi Algoritma 3des Dan Algoritma Base64 Pada Sistem Keamanan Handshaking Animation Store Di CV. Edukreasi"*. Jurnal Informatika. Fakultas Ilmu Komputer. Udinus 2014.

[5] D. Mudeng, "*Kriptografi Twofish"*, Makalah, Magister Teknologi Informasi, ITB. 2004. Diakses melalui http://budi.insan.co.id/courses/ec7010/dikmenjur-2004/ [Maret 2014].

[6] J. Greenspan dan B. Bulger. "*MySQL/PHP Database Applications*." M&T Books. 20-24. Foster City, 2001

[7] R.F.Marta, "*Studi, Implementasi Dan Perbandingan Algoritma Kunci Simetri Triple Data Encryption Standard Dan Twofish",* Makalah PS Teknik Informatika, ITB, 2006. Diakses melalui http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1-2006.htm [Juni 2014]