APLIKASI ENKRIPSI *FILE* DOKUMEN MENGGUNAKAN METODE ALGORITMA AES *(ADVANCED ENCRYPTION STANDARD)* DAN OTP *(ONE TIME PAD)* BERBASIS WEB PADA PT. MNC SKY VISION

Indra Nugraha Abdullah[1], Dewi Kusumaningsih[2], Mohammad Alawy[3]

[1)] Magister Ilmu Komputer, Universitas Budi Luhur
[2, 3)] Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5853752
[1]indraipb_it@yahoo.com, [2]dewi.kusumaningsih@budiluhur.ac.id, [3]mohammadallawy16@gmail.com

ABSTRAK

Keamanan merupakan salah satu faktor yang paling penting dalam dunia teknologi informasi terutama di dalam jalur-jalur komunikasi tersebut. Namun, banyak yang belum menyadari betapa pentingnya keamanan (security) itu dan juga tidak murahnya harga dari keamanan tersebut. Di dalam hal ini Teknologi kriptografi sangat berperan penting dalam proses komunikasi, yang digunakan untuk melakukan enkripsi (pengacakan) data yang ditransaksikan selama berada dalam perjalanan dari sumber menuju ke tujuan dan juga melakukan dekripsi (menyusun kembali) data yang telah diacak tadi setelah sampai ke tujuan. Waktu pengiriman informasi juga merupakan bagian utama dalam pertukaran informasi. Dan waktu pengiriman sangat bergantung pada ukuran file yang dikirimkan. Dengan memperkecil file akan bisa menghemat waktu pengiriman. Dalam penelitian ini akan dibangun aplikasi yang dapat meningkatkan keamanan pada jenis file dokumen DOCX, XLSX, dan PDF dengan menggunakan algoritma AES (Advanced Encryption Standard dan OTP (One Time Pad) sebagai metode kriptografi. Algoritma AES adalah blok ciphertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext, sedangkan One Time Pad adalah salah satu metode kriptografi yang cukup dikenal. One Time Pad merupakan algoritma berjenis symetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama.

Kata kunci : Enkripsi, Algoritma AES, Algoritma OTP.

I. PENDAHULUAN

Semakin meningkat teknologi komputer, maka semakin tinggi pula tingkat ancaman yang dapat mengancam keamanan para pengguna komputer. Salah satu dampak negatif di dalam perkembangan teknologi adalah adanya pencurian data, yang dikhawatirkan oleh para pengguna jaringan komunikasi. Dengan adanya pencurian data maka aspek keamanan data dalam pertukaran informasi serta penyimpanan data dianggap sangat penting, karena suatu komunikasi data jarak jauh, belum tentu memiliki jalur transmisi yang aman dalam penyadapan, serta penyimpanan data belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. PT. MNC SKY VISION merupakan perusahaan yang mengandalkan penggunaan teknologi komputer dan telekomunikasi dalam melakukan pertukaran data yang ada diperusahaan. Data yang dikirim merupakan data yang sangat rahasia dan penting. Dan pengiriman data tersebut dilakukan melalui media seperti *Local Area Network* (LAN), *internet, email* dan media lainnya. Yang pada dasarnya jika melakukan pengiriman data melalui media-media tersebut, konten yang dikirimkan belum dilakukan pengamanan, sehingga jika sewaktu-waktu terjadi penyadapan melalui jalur pengiriman tersebut data tersebut dapat langsung terbaca oleh si penyadap. Lalu dengan mudah pencuri dapat langsung membaca isi data tersebut karena tidak adanya pengamanan data. Untuk menghindari terjadinya hal seperti itu, maka sangat dibutuhkan suatu metode untuk mengamankan *file* yang akan dikirim dimana data yang dikirim akan diacak dengan suatu metode penyandian agar *file* tersebut hanya bisa dibaca oleh orang yang berhak.

Secara umum ada dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa dilakukan adalah substitusi dan transposisi. Sedangkan kriptografi Modern adalah algoritma yang lebih kompleks dari pada algoritma klasik, hal ini disebabkan algoritma ini menggunakan komputer. Operasi yang digunakan oleh kriptografi modern pada umumnya dalam mode bit. Sehingga semua sistem yang terlibat di dalamnya seperti kunci, plainteks, dan teks semuanya dinyatakan kedalam rangkaian bit-bit biner. Algoritma yang akan penulis gunakan adalah penggabungan kedua algoritma tersebut.

Algoritma kriptografi yang akan digunakan adalah dua metode kriptografi simetris yaitu AES (*Advanced Encryption Standard*), dan OTP (*One Time Pad*). AES dipilih penulis dalam menjaga keamanan pada sebuah data atau informasi tersebut, dikarenakan AES merupakan *cipher* yang berorientasi pada bit, sehingga memungkinkan untuk implementasi

algoritma yang efisien ke dalam software dan hardware, adapun OTP dipilih untuk mengkombinasikan masing masing karakter pada *plaintext* dengan satu karakter pada satu kunci dan dienkripsi dengan satu algoritma kemudian diteruskan dengan algoritma yang lainnya. Dengan tujuan teknik ini maka sebuah *file* rahasia terlindungi dari penyadapan dan pencurian data.

II. LANDASAN TEORI

2.1. Kriptografi

Menurut Rifki Sadikin (2012) Kriptografi (*cryptography*) ini berasal dari bahasa Yunani yang terdiri dari dua buah kata yaitu *crypto* dan *graphia*. Kata *crypto* berarti rahasia sedangkan *graphia* berarti tulisan. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana cara menyembunyikan pesan. Selain pengertian di atas, juga terdapat pengertian lain mengenai kriptografi. Yaitu, ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan kemananan informasi seperti kerahasaian data, keabsahan data, integritas data dan autentikasi entitas[1].

Dony Ariyus (2008) mengatakan aspek-aspek keamanan didalam kriptografi adalah :

a. Confidentiality (Kerahasiaan)

Kerahasiaan menjamin data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.

b. Authentication (Otentikasi)

Otentikasi merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi. Penerima pesan dapat memastikan keaslian pengirimnya.

c. Integrity (Integritas)

Integritas menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanda ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya dan ditambahkan. Integritas data bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut.

d. Non-repudiation (Penyangkalan)

Pengirim tidak dapat mengelak bahwa dia telah mengirim pesan, penerima juga tidak dapat mengelak bahwa dia telah menerima pesan tersebut.

Tujuan kriptografi secara umum adalah mewujudkan keempat aspek keamanan tersebut didalam teori dan praktek[2].

2.2. Algoritma Kriptografi

"Algoritma dalam kriptografi merupakan sekumpulan aturan (fungsi matematis yang digunakan) untuk proses enkripsi dan proses dekripsi. Dalam beberapa metode kriptografi terdapat perbedaan antara fungsi enkripsi dan fungsi dekripsi."[3].

Konsep matematis yang mendasari algortima adalah relasi antara himpunan, yaitu relasi antara himpunan yang berisi elemen-elemen *ciphertext.* Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. Misalkan himpunan *plaintext* dinotasikan P dan himpunan elemen *ciphertext* dinotasikan C, maka fungsi E memetakan himpunan P ke himpunan C.

$$\mathbf{E(P) = C}$$

Dan fungsi dekripsi memetakan himpunan C ke himpunan P

$$\mathbf{D(C) = P}$$

Karena fungsi dekripsi D mengembalikan himpunan C menjadi himpunan P asal, maka algoritma kriptografi harus memenuhi persamaan

$$\mathbf{D(E(P)) = P}$$

Tingkat keamanan suatu algoritma dalam kriptografi seringkali diukur dari kuantitas proses yang dilakukan dalam suatu fungsi, baik itu fungsi enkripsi maupun fungsi dekripsi. Proses tersebut juga dapat dihubungkan dengan sumber data yang dibutuhkan, menunjukkan semakin kuat algoritma kriptografi tersebut.

Berikut ini adalah istilah-istilah atau komponen yang digunakan dalam bidang kriptografi :

a. Enkripsi adalah proses pengubahan *plaintext* menjadi *ciphertext.*
b. Dekripsi adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal atau asli.
c. *Key* atau kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.
d. *Ciphertext* adalah pesan yang terenkripsi (tersandi) yang merupakan hasil dari enkripsi.
e. *Plaintext* adalah pesan yang hendak dikirim (berisi data asli).
f. Pesan, dapat berupa data maupun informasi yang dikirim melalui kurir, media, komunikasi data, atau yang disimpan di dalam media perekaman.
g. *Cryptanalisis*, merupakan ilmu untuk mendapatkan teks-teks asli tanpa harus mengetahui kunci yang sah secara wajar.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenal sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah bentuk teracak tersebut menjadi informasi awal.

Algortima kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

a. Algoritma Simetris

Pada Algoritma simetris, kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang sama. Dalam kriptografi kunci simetris dapat diasumsikan bahwa si penerima dan pengirim pesan telah terlebih dahulu berbagi kunci sebelum pesan dikirimkan. Keamanan dari sistem ini terletak pada kerahasiaan kuncinya[2]

b. Algoritma Asimetris

Berbeda dengan kriptografi kunci simetris, kriptografi kunci publik memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsinya. Dimana kunci yang digunakan untuk proses enkripsi atau sering disebut dengan *public key* dan dekripsiatau sering disebut *private key* menggunakan kunci yang berbeda. Entitas pengirim akan mengenkripsi dengan menggunakan kunci publik, sedangkan entitas penerima mendekripsi menggunakan kunci *private* [2].

2.3 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamakan data. Algoritma AES adalah blok *ciphertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext* sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES is mengunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

Panjang kunci algoritma rijndael memiliki pajang kunci antara 128 bit sampai dengan 256 bit. Namun dalam penerapan AES menetapkan panjang kunci yang dibutuhkn adalah 128 bit, 192 bit, dan 256 bit sehingga kemudian dikenal sebutan AES-128, AES-192, dan AES-256 walaupun dalam penggunananya paling banyak menggunakan AES-128 dn AES-256. Untuk lebih jelasnya dapat dilihat pada table dibawah ini

Tabel 1 : Perbandingan Tipe AES

	Panjang Kunci (*Nk words*)	Ukuran Blok (*Nb words*)	Jumlah Putaran (*Nr*)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.4 *One Time Pad* (OTP)

Menurut Paar & Pelzl (2010) *One Time Pad* adalah salah satu metode kriptografi yang cukup dikenal. *One Time Pad* merupakan algoritma berjenis *symetric* key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama [4]. *One Time Pad* (*Pad* = kertas bloknot) berisi barisan karakter karakter kunci yang dibangkitkan secara acak. Aslinya, satu buah *One Time Pad* adalah sebuah pita (*tape)* yang berisi barisan karakter-karakter kunci.

Algoritma *One Time Pad* dalam proses enkripsi menggunakan cara *stream cipher* yang berasal dari hasil *XOR* antara bit *Plaintext* dan bit *Key*. Pada metode ini *Plaintext* diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII. Enkripsi dapat digambarkan sebagai penjumlahan modulo 26 dari satu karakter plaintext dengan satu karakter kunci *One Time Pad.*

Ci = (pi + ki) mod 26

Sedangkan persamaan untuk mendekripsikan adalah

Pi + (ci + ki) mod 26

Yang didalam hal ini,

Pi : karakter plainteks

ki : karakter kunci

ci : karakter cipherteks

setiap karakter kunci digunakan tepat satu kali. Pengirim mengirim pesan dan kemudian menghancurkan halaman kunci yang telah digunakan. Penerima menerima kunci yang identic dan menggunakan kunci tersebut untuk mendekripsi setiap karakter pada cipherteks, setalah pengirim mengenkripsikan pesan dengan *One Time Pad,* tersebut (makanya disebut satu kali pakai atau *One Time).* Sebuah pesan baru sama dengan sebuah kunci baru

III. ANALISIS DAN PERANCANGAN PROGRAM

3.1 Analisa dan Penyelesaian Masalah

Setiap perusahaan memiliki informasi yang sangat sensitif oleh pesaingnya. kerahasiaan suatu informasi tersebut, selalu menjadi masalah tersendiri bagi setiap perusahaan. Mereka mengggap jalur-jalur media yang sering mereka gunakan seperti *internet, email* dan *Local Area Network* (LAN) sudah cukup aman bagi mereka untuk melakukan pertukaran data. Padahal jalur-jalur tersebut masih belum aman. Jalur-jalur tersebut belum terdapat pengamanan untuk konten yang dikirim. Sehingga apabila terjadi penyadapan di jalur-jalur tersebut, maka data yang tersebut dapat langsung terbaca oleh si penyadap. Selain itu, pencurian data juga sering terjadi bukan hanya melalui jalur-jalur media seperti *internet, email* dan *Local Area Network* (LAN). Tetapi pencurian data juga dilakukan dengan cara langsung mengambil dari komputer pribadi. Dimana *File* tersebut berisi data pribadi pelanggan seperti alamat, nomor *HandPhone* pelanggan, nomor *Handphone* kerabat/keluarga, Email, Bilamana data tersebut dicuri oleh kompetitor perusahaan lain. hal-hal itu menyebabkan kerugian bagi PT. MNC SKY VISION.

Salah satu cara untuk mengamankan sebuah dokumen yaitu dengan mengubah dokumen asli menjadi dokumen yang tidak bisa dibaca oleh orang lain atau sering disebut dengan enkripsi. Untuk mengimplementasikan enkripsi dokumen dibutuhkan algoritma enkripsi agar dokumen tersebut bisa dienkripsi dan kemudian di kembalikan seperti semula atau dekripsi tanpa mengalami perubahan. Sehingga diperlukan suatu aplikasi yang dapat memberikan solusi dari permasalahan yang ada, yaitu dengan dua algoritma AES dan OTP.

Dengan adanya aplikasi ini diharapkan suatu dokumen atau data penting dapat disimpan dan dikirim ke pihak yang benar-benar berwenang dan tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

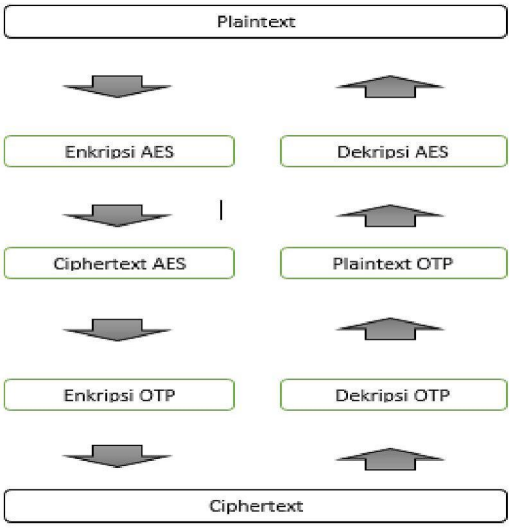
3.2 Perancangan Program

Tahap perancangan program dilakukan untuk mencari bentuk yang optimal dan program yang akan dibuat dengan mempertimbangkan faktor permasalahan dan kebutuhan yang telah dijelaskan sebelumnya. Upaya yang dilakukan adalah dengan berusaha mencari kombinasi penggunaan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang tepat sehingga diperoleh hasil yang maksimal dan mudah untuk diimplementasikan.

Program yang dibuat terdiri dari *Form Login* dan *Form Menu* Utama. *Form Menu* Utama terdiri dari *Form Home*, *Form* Enkripsi, *Form* Dekripsi, *Form Management user*, *Form* Bantuan, *Form* Tentang Saya dan *Form* Keluar.

Untuk melakukan enkripsi *file*, *user* dapat memilih *menu* enkripsi. Pada *menu* ini, *user* diharuskan memilih *file* dokumen docx, xlsx, pdf terlebih dahulu, baru kemudian melakukan proses enkripsi dengan AES kemudian mendapatkan hasil *file ciphertext* AES lalu dilanjutkan menggunakan algoritma enkripsi OTP . Sedangkan untuk mengembalikan *file* yang

sudah dienkripsi menjadi *file* semula, *user* dapat memilih *menu* dekripsi. Pada menu ini user harus memilih *File* yang sudah di enkripsi sebelumnya, kemudian melakukan dengan dekripsi OTP kemudian dilanjutkan plaintext OTP lalu didekripsi AES dan *File* menjadi kebentuk semula. Secara umum, rancangan program yang akan dibuat dapat dilihat pada gambar 1.



Gambar 1 : Alur Rancangan Program

3.3 Rancangan Database MySQL

Berikut ini adalah beberapa spesifikasi database dalam aplikasi ini :

a. tbl_decrypt

Nama Tabel : tbl_decrypt
Primary Key : file_id

Tabel 1 : tbl_decrypt

Nama *Field*	Tipe	Panjang	Deskripsi
File_id	char	8	Berisikan id pengguna (PK)
File_name	varchar	100	Berisikan nama pengguna
File_type	char	20	Berisikan type pengguna
userid	char	4	Berisikan userid pengguna
File_date	date	-	Berisikan date pengguna
File_time	Time	-	Berisikan time pengguna
File_dir	varchar	255	Berisikan dir pengguna
File_size	Varchar	11	Berisikan size pengguna
File_protime	double	-	Berisikan protime pengguna

b. tbl_encrypt

Nama Tabel : tbl_encrypt
Primary Key : file_id

Tabel 2 : tbl_encrypt

Nama *Field*	Tipe	Panjang	Deskripsi
File_id	char	8	Berisikan id pengguna (PK)
File_name	varchar	100	Berisikan nama pengguna
File_type	char	20	Berisikan type pengguna
userid	char	4	Berisikan userid pengguna
File_date	date	-	Berisikan date pengguna
File_time	Time	-	Berisikan time pengguna
File_dir	varchar	255	Berisikan dir pengguna
File_size	Varchar	11	Berisikan size pengguna
File_protime	double	-	Berisikan protime pengguna
File_key	Char	32	Berisikan key pengguna

c. tbl_user

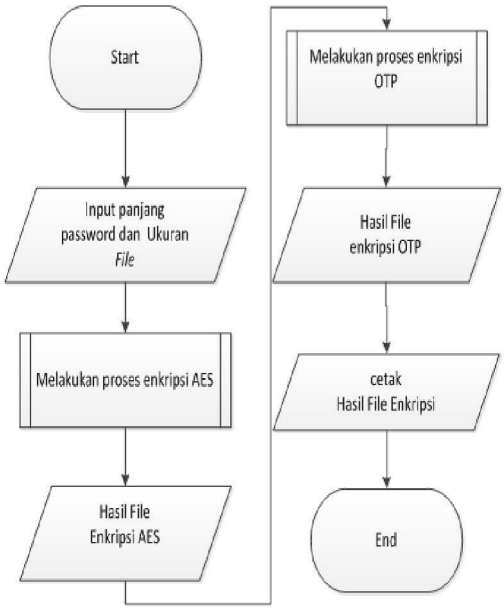
Nama Tabel : tbl_user
Primary Key : userid

Tabel 3 : tbl_user

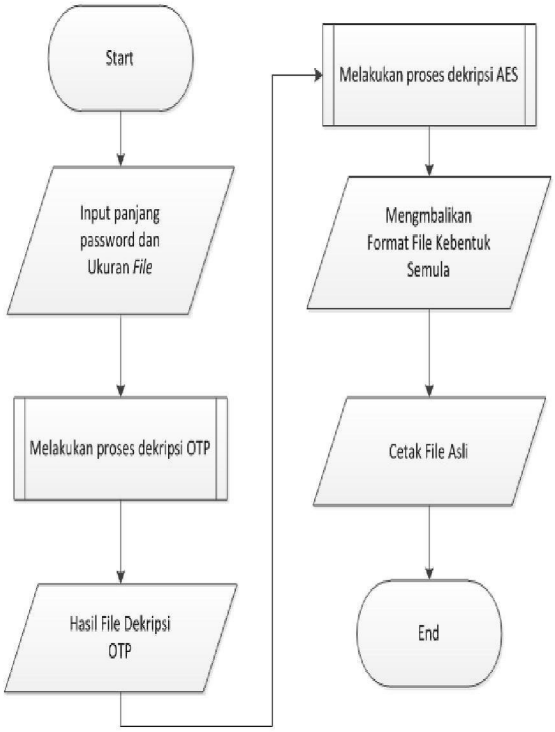
Nama *Field*	Tipe	Panjang	Deskripsi
Userid	Char	4	Berisikan id pengguna (PK)
Username	Varchar	30	Berisikan user name pengguna
userpass	Varchar	32	Berisikan user pass pengguna
Userlevel	varchar	13	Berisikan user level pengguna

3.4 Flowchart Program

Berikut ini adalah *flowchart* yang digunakan untuk menelusuri proses program pada aplikasi Kriptografi algoritma Caesar Cipher dan Base64 untuk keamanan pada *file* dokumen docx, xlsx dan pdf.



Gambar 2 : Proses Enkripsi



Gambar 3 : Proses Dekripsi

IV. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan-tampilan yang ada pada aplikasi enkripsi *file* dokumen DOCX, XLSX atau PDF.

Gambar 4: Tampilan Menu Utama

Gambar 5 : Menu Cryptography Form Encrypt

Gambar 6: Menu Cryptography Form Decrypt

4.2 Tabel Pengujian

Dalam pengujian kali ini, akan dibahas perbandingan antara proses enkripsi dan dekripsi *file*. Pengujianya yaitu antara lain ukuran *file*,waktu proses enkripsi,waktu proses dekripsi hingga hasil yang dicapai dalam proses enkripsi maupun dekripsi.

Tabel 4 : Hasil Pengujian Enkripsi

Nama File Awal	Ukuran File (KB)	Waktu Enkripsi (Seconds)	Ukuran Hasil Enkripsi (KB)	Nama File Hasil Enkripsi
1.Master Report	10	0.01	12.37	1^(encrypted
2. Master Report1	12	0.01	12.75	2^(encrypted
3. Master Report2	13	0.02	13.09	3^(encrypted
4. Master Report3	14	0.01	13.77	4^(encrypted
5. Master Repor4t	15	0.01	14.09	5^(encrypted

Tabel 5: Hasil Pengujian Dekripsi

Nama File Awal	Ukuran File (KB)	Waktu Dekripsi (Seconds)	Ukuran Hasil Dekripsi (KB)	Nama File Hasil Dekripsi
1^(encrypted	13	0.01	12.76	1. (decrypted-2016
2^(encrypted	14	0.09	13.09	2. (decrypted-2016
3^(encrypted	14	0.01	13.42	3. (decrypted-2016
4^(encrypted	14	0.01	13.78	4. (decrypted-2016
5^(encrypted	14	0.01	14.09	5. (decrypted-2016

Berdasarkan pengujian program untuk proses enkripsi dan dekripsi yang telah dilakukan,baik itu berupa *file* dokumen DOCX, XLSX maupun *file* PDF. Dari hasil pengujian program yang telah dilakukan,ditemukan beberapa kelebihan dan kekurangan dari apikasi ini,yaitu semakin besar *file* maka akan semakin lama proses nya dan *file* hasil enkripsi akan menjadi lebih besar ukurannya dari file aslinya.

V. KESIMPULAN

Dari hasil pengujian dan analisa yang telah dilakukan dapat disimpulkan bahwa:

a. Aplikasi ini menggunakan algoritma AES dan OTP untuk Enkripsi. Dibangun untuk dapat mengamankan jenis *file* dokumen DOCX, XLSX, dan PDF.
b. Aplikasi yang telah terenkripsi tidak dapat dibuka atau dikembalikan seperti semula tanpa *key* yang diinput saat enkripsi.
c. Waktu proses enkripsi lebih cepat dari pada waktu proses dekripsi.
d. Dengan adanya aplikasi kriptografi ini, proses penyimpanan dan pertukaran informasi menjadi lebih aman.

Aplikasi kriptografi menggunakan algoritma AES dan OTP ini belum sempurna dan masih memerlukan banyak perbaikan untuk meningkatkan efektifitas pekerjaan. Untuk meningkatkan kinerja aplikasi ini maka diusulkan beberapa saran yang dapat menjadi pertimbangan, antara lain:

a. Kunci sandi (*password*) yang digunakan sebaiknya hanya diketahui oleh seorang pengirim dan penerima informasi saja.
b. Salah satu algoritma mungkin akan lebih baik apabila dijalankan disisi client seperti algoritma AES yang ditulis dengan bahasa *javascipt* agar berjalan disisi *client* dan tidak terlalu membebankan server.
c. Aplikasi ini bisa mengenkripsi semua jenis file tanpa terkecuali.

Pentingnya penelitian lebih lanjut untuk mengembangkan aplikasi sistem keamanan data dengan berbagai layanan yang ada di internet.

DAFTAR PUSTAKA

[1] Sadikin, Rifki. 2012, Kriptografi Untuk Keamanan Jaringan, Yogyakarta

[2] Arius, Dony. 2008. *Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi*. Yogyakarta, STMIK Amikom Yogyakarta

[3] Munir, Rinaldi. 2013. *Pengantar Kriptografi* (IF3058), Departemen Teknik Informatika. Institut Teknologi Bandung.

[4] Paar, Christof dan Pelzl, Jan. 2010. *Understanding Cryptography*. New York, Springer-Verlag.