Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
Jakarta – Indonesia, 06 September 2022

PENERAPAN *ADVANCED ENCRYPTION STANDARD*-128 DAN *RIVEST CODE*4 UNTUK PENGAMANAN DATA PADA CV.TRISTA JAYA ABADI

Kamal Saputra[1], Alexander J.P. Sibarani[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1]kamalsaputra219@gmail.com, [2]alexander.sibarani@budiluhur.ac.id
(* : corresponding author)

Abstrak- CV. Trista Jaya Abadi merupakan perusahaan yang bergerak di bidang perdagangan pakan burung, pakan ikan dan alat-alat pemancingan yang menggunakan metode *Business to Customer* (B2C) untuk menjalankan bisnisnya. CV. Trista Jaya Abadi memiliki banyak data-data penting seperti data pegawai, data pelanggan dan data *reseller*, yang masih menggunakan pendataan secara manual dengan menggunakan *Microsoft excel*. Semakin banyaknya data-data tersebut yang disimpan di dalam folder komputer mengakibatkan rawan terjadinya kehilangan maupun pencurian data. Selain itu *file* penting masih disimpan di dalam dokumen fisik dimana hal tersebut rawan kerusakan apabila terjadinya bencana dan juga rawan akan pencurian. Maka diimplementasikan algoritma kriptografi *Advanced Encryption Standard* (AES-128) dan *Rivest Code 4* (RC4) untuk melakukan pengamanan data-data penting perusahaan seperti *database* yang berisikan informasi data pegawai, data pelanggan dan data *reseller* serta pengamanan *file* penting perusahaan, sehingga data-data penting dan *file* penting perusahaan yang tersimpan menjadi lebih aman karena sudah terenkripsi. Penelitian ini diharapkan dapat membantu CV. Trista Jaya Abadi dalam pengamanan *database* yang berisikan informasi data pegawai, data pelanggan, data *reseller* dan *file* bersifat rahasia agar terhindar dari pencurian data perusahaan. Hasil pengujian, aplikasi ini diperoleh hasil proses enkripsi rata-rata ukuran dokumen 972.021 byte, lama waktu proses 30.260.321 milidetik dan hasil proses dekripsi rata-rata ukuran dokumen 546.754 byte, lama waktu proses 33.182.193 milidetik. Hasil penelitian, aplikasi ini dapat mempermudah dan mempercepat dalam melakukan pendataan data serta data menjadi rapih karena tersimpan di *database*, selain itu aplikasi ini dapat mengamankan *database* yang berisikan informasi data pegawai, data pelanggan, data *reseller* dan dapat menyimpan dan mengamankan *file* penting.

Kata Kunci: Kriptografi, *Advanced Encryption Standard* (AES-128), *Rivest Code 4* (RC4)

IMPLEMENTATION ADVANCED ENCRYPTION STANDARD-128 AND RIVEST CODE4 FOR DATA SECURITY IN CV.TRISTA JAYA ABADI

Abstract- *CV. Trista Jaya Abadi is a company engaged in trading bird feed, fish feed and fishing equipment that uses the Business to Customer (B2C) method to run its business. CV. Trista Jaya Abadi has a lot of important data such as employee data, customer data and reseller data, which still uses manual data collection using Microsoft excel. The more data that is stored in computer folders, it is prone to data loss and theft. In addition, important files are still stored in physical documents where they are prone to damage in the event of a disaster and also prone to theft. Then the Advanced Encryption Standard (AES-128) and Rivest Code 4 (RC4) cryptographic algorithms are implemented to secure important company data such as databases containing employee data information, customer data and reseller data as well as securing important company files, so that data important and important company files stored are more secure because they are encrypted. This research is expected to help CV. Trista Jaya Abadi in securing databases containing information on employee data, customer data, reseller data and confidential files to avoid theft of company data. The test results, this application obtained the results of the encryption process an average document size of 972,021 bytes, a long processing time of 30,260,321 milliseconds and the results of the decryption process an average document size of 546,754 bytes, a long processing time of 33,182,193 milliseconds. The results of the study, this application can make it easier and faster to collect data and the data to be neat because it is stored in the database, besides this application can secure a database that contains information on employee data, customer data, reseller data and can store and secure important files.*

Keywords*: Cryptography, Advanced Encryption Standard (AES-128), Rivest Code 4 (RC4)*

1. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari bagaimana cara menjaga kerahasiaan suatu data atau pesan dengan cara mengubah data kedalam bentuk yang tidak dapat dibaca atau dimengerti lagi maknanya. Kriptografi bertujuan untuk menjaga kerahasiaan suatu informasi penting yang ada di dalam data sehingga informasi tidak dapat diketahui isinya oleh pihak yang tidak bertanggung jawab [1].

Kriptografi memiliki tujuan dalam menjaga keamanan data yaitu dengan *confidentiality* merupakan layanan yang digunakan untuk melindungi atau menjaga suatu informasi dari pihak yang tidak berhak untuk mengaksesnya. *Integrity* merupakan layanan yang bertujuan untuk mencegah terjadinya manipulasi informasi atau mengubah isi informasi oleh pihak-pihak yang tidak berhak. Untuk meyakinkan integritas data dengan cara dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi atau mengubah isi informasi. *Authentication* merupakan layanan yang terkait dengan pembuktian identifikasi terhadap kebenaran suatu informasi bagi pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) dan cara untuk melakukan pembuktian datanya yaitu dengan menggunakan sistem informasi itu sendiri. *Non-repudiation* untuk mencegah terjadinya entitas yang berkomunikasi dengan melakukan penyangkalan dapat menggunakan sebuah layanan ketiadaan penyangkalan, proses penyangkalan dengan cara melakukan sebuah pengiriman informasi penyangkalan dengan cara pengiriman atau penerima pesan informasi menyangkal telah menerima pesan informasi [2].

CV. Trista Jaya Abadi merupakan perusahaan yang bergerak di bidang perdagangan pakan burung, pakan ikan dan alat-alat pemancingan yang menggunakan metode *(Business to Customer)* B2C untuk menjalankan bisnisnya. Saat ini CV. Trista Jaya Abadi mengalami permasalahan pada pendataan data yang dilakukan masih menggunakan pendataan secara manual, adanya resiko kehilangan data-data penting yang diakibatkan dari tidak rapihnya data di dalam folder dan kurangnya keamanan untuk menjaga data tersebut serta belum memiliki tempat penyimpanan untuk dokumen penting milik perusahaan yang aman.

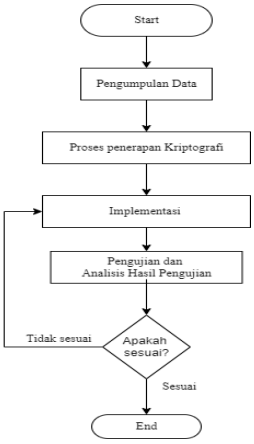
Studi mengenai sistem keamanan *database* dan *file* dengan metode *Advanced Encryption Standard* (AES-128) untuk mengamankan *database* telah dilakukan oleh K. Zalukhu [3] dan J. Prayudha [4], selain itu untuk mengamankan *file* telah dilakukan oleh D. Widyawan [5] dan metode *Rivest Code* 4 (RC4) untuk pengamanan *database* dilakukan oleh A. Setiawan [6] dan A. Kodir [7], selain itu untuk mengamankan *file* dilakukan oleh Z. Basim [8]. Dari penelitian terdahulu masih sedikit yang menggunakan kombinasi metode AES-128 dan RC4 dalam mengamankan *database* dan *file*. Algoritma *Advanced Encryption Standard* (AES-128) merupakan suatu algoritma *block chiper* yang menggunakan sebuah kunci yang sama, yaitu kunci simetris pada saat melakukan proses enkripsi dan dekripsi data. Saat ini AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) [9]. Algoritma *Rivest Code 4* (RC4) merupakan sebuah jenis aliran kode yang melakukan operasi enkripsinya per karakter, yaitu 1 byte untuk sekali melakukan sebuah operasi. *RSA Data Security Inc* (RSADSI) membuat salah satu algoritma yang menggunakan kunci simetris dalam bentuk *stream cipher* yaitu algoritma *Rivest Code 4* (RC4) [10].

Penelitian ini bertujuan untuk membangun sistem pendataan data pegawai, data pelanggan, data *reseller* dan penyimpanan *file* dan untuk mengamankan *database* yang berisi informasi data pegawai, data pelanggan dan data *reseller* serta *file* dengan menerapkan algoritma AES-128 Mode ECB dan RC4 pada aplikasi berbasis web.

Penelitian ini diharapkan dapat membantu CV. Trista Jaya Abadi dalam pengamanan *database* yang berisikan informasi data pegawai, data pelanggan, data *reseller* dan *file* bersifat rahasia agar terhindar dari pencurian data perusahaan.

2. METODE PENELITIAN

Dalam penelitian ini metode yang digunakan menggunakan metode *waterfall*. Metode ini untuk menyelesaikan permasalahan secara berurutan dan sistematis. Berikut ini adalah alur dari metode penelitian ditunjukkan dalam gambar 1.



Gambar 1. Metode Penelitian

Pengumpulan Data

Tahap ini dilakukan pengumpulan data dengan rincian sebagai berikut:

a. Wawancara (*interview*)

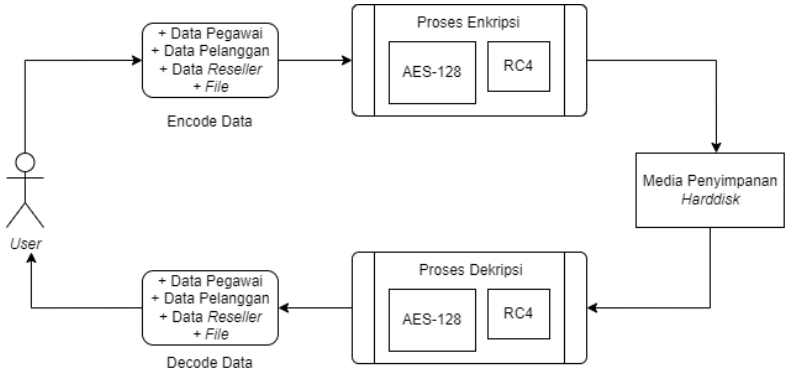
Proses wawancara dilakukan dengan melalui wawancara atau tanya jawab langsung dengan pihak-pihak yang berhubungan dengan aplikasi dan pembuatan program, atau mendapatkan informasi tentang aplikasi dan keamanan yang ada.

b. Observasi (*observation*)

Observasi merupakan salah satu teknik pengumpulan data yang dilakukan melalui pengamatan secara langsung terhadap proses sistem yang sedang berjalan pada CV. Trista Jaya Abadi.

2.1 Proses Penerapan Kriptografi

Dari permasalahan yang ada, maka diperlukan sebuah aplikasi yang berguna untuk menjaga suatu kerahasiaan data dan *file*. Aplikasi yang dibuat nantinya dapat mengubah sebuah data menjadi data yang tidak dapat dibaca dan dapat membuat *file* tidak dapat dibuka setelah melalui proses enkripsi. Data dan *file* dapat dilihat dan dibuka kembali saat melalui proses dekripsi. Berikut ini adalah gambar 2 menunjukkan proses enkripsi dan dekripsi data serta *file* berikut:



Gambar 2. Proses penerapan Kriptografi Data Pegawai, Data Pelanggan, Data *Reseller* dan *File*

2.2.1 Proses Enkripsi Dan Dekripsi AES-128

Proses enkripsi AES-128 *plaintext* atau data harus melewatkan beberapa proses tahapan dalam enkripsi seperti *AddRoundKey* yang dilakukan perulangan sebanyak 9 kali, pada perulangan ini dilakukan proses *SubBytes, Shift Rows, Mix Columns, AddRoundKey*. Selanjutnya setelah selesai melakukan perulangan, maka akan dilakukan kembali proses *SubBytes, Shift Rows, AddRoundKey* dan setelah melewati proses tersebut selanjutnya akan mendapatkan hasil *chipertext*.

Proses dekripsi AES-128 harus melakukan beberapa proses tahapan seperti *AddRoundKey*, selanjutnya dilakukan proses perulangan sebanyak 9 kali, di dalam perulangan dilakukan proses *Inverse ShiftRows, Inverse SubBytes, AddRoundKey, Inverse MixColumns* dan setelah melakukan proses perulangan, akan dilakukan kembali proses *Inverse ShiftRows, Inverse SubBytes* dan *AddRoundKey*.

2.2.2 Proses Enkripsi Dan Dekripsi RC4

Proses enkripsi RC4 *chipertext* harus melalui beberapa proses yaitu inisialisasi S-Box (*array* S), inisialisasi S-Box (*array* T), lalu dilakukan pengacakan S-Box, setelah itu dilakukan proses *psuedo* dan selanjutnya dilakukan proses Byte K di XOR dengan *plaintext*.

Proses dekripsi RC4 sama seperti proses enkripsi yaitu dengan melalui proses inisialisasi S-Box (*array* S), inisialisasi S-Box (*array* T), lalu dilakukan pengacakan S-Box, setelah itu dilakukan proses *psuedo* dan selanjutnya dilakukan proses Bytes K di XOR dengan *plaintext* dan mendapatkan hasil *plaintext*.

2.2 Implementasi

Tahap implementasi ini dilakukan tahap perancangan ke dalam bahasa pemrograman tertentu, dalam hal ini aplikasi yang akan digunakan sebagai berikut:

a. Perangkat lunak yang digunakan dalam penerapan pengamanan data pegawai, data pelanggan dan data *reseller* serta *file* menggunakan bahasa pemrograman PHP dengan *framework CodeIgniter 4* dan DBMS menggunakan MySQL.

b. Perangkat keras yang akan digunakan *Processor* Intel core I5, Ram 8GB, SSD 120 GB dan *Harddisk* 500 GB.

2.3 Pengujian Dan Analisa Hasil Pengujian

Dalam tahap pengujian akan dilihat apakah keamanan kriptografi yang dibuat sudah sesuai dengan kebutuhan atau belum, jika sudah sesuai maka proses penelitian akan selesai dan jika belum akan melakukan proses implementasi kembali.

3. HASIL DAN PEMBAHASAN

Berdasarkan metode yang diusulkan pada bab sebelumnya yaitu menggunakan algoritma kriptografi AES-128 dan RC4 untuk mengamankan *database* dan *file*. Metode yang digunakan dalam pengujian sistem menggunakan metode *black box testing* yaitu sebuah metode yang pengujiannya pada sisi fungsionalitas input/output pada suatu sistem khususnya pada aplikasi *website* kriptografi dan juga pengujian pada sisi kecepatan dan panjang teks aslinya sebelum dan sesudah di enkripsi dalam proses enkripsi dan dekripsi data, selain itu digunakan untuk melakukan pengujian dari sisi kecepatan dalam proses enkripsi dan dekripsi *file*.

3.1 Pengujian Sistem

Dalam pengujian sistem ini yang menjadi fokus pengujian adalah pada proses enkripsi dan dekripsi *database* dan *file* dengan menggunakan metode pengujian *black box testing*. Dalam pengujian ini yang menjadi hasilnya adalah pada sisi kecepatan dan panjang teks asli sebelum dan sesudah di enkripsi data, selain itu pada sisi kecepatan dalam proses enkripsi dan dekripsi *file*.

a. Tabel Pengujian Enkripsi Dan Dekripsi Data Pegawai

Dalam pengujian ini akan dibahas proses enkripsi dan dekripsi tabel data pegawai. Pengujian ini, akan dilakukan pengujian pada data dan data yang digunakan pada data pegawai hanya satu *field* di setiap *record* untuk mengetahui proses kecepatan enkripsi dan dekripsi serta panjang teks asli dan teks yang sudah di enkripsi di setiap recordnya. Pengujian enkripsi dan dekripsi data pegawai ditunjukkan dalam tabel 1.

Tabel 1. Pengujian Enkripsi Dan Dekripsi Data Pegawai

Karakter Asli	Jumlah Karakter (byte)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (byte)	Waktu Enkripsi (milidetik)	Waktu Dekripsi (milidetik)
amsalkristanto50@gmail.com	3.25	q1rWb/LZP8D70AZI3VwTZgv6/T1lRJEOmBcJ4hsrnqhzKtXElfj3JOhqDj0=	7.5	0.021756	0.010853
botokulo.ulo@gmail.com	2.75	twnXV8TDNOTokgEP+nQjCTr07nJCaJI6sUwOkwUeia9YCdX63dvYNs9tLD0=	7.5	0.027517	0.015009
ibnu63687@gmail.com	2.375	hUCrCqDUEeDY5z9azww0Bnab1RAueYQmv1gnk2oB2b13A/TH1vLyNqNrDj0=	7.5	0.021034	0.014698
tuenkkalaider@gmail.com	2.875	giWESK3+BOGI7jBNhG0IRRagwgpncr56uxUMoREe3qFkcMfEx4z2ULVLLD0=	7.5	0.023964	0.016657
teditadisyah@gmail.com	2.75	lh+DbqzAPN/a8hV+jlIofXrpghRjaJI6sUwOkwUeia9YCdX63dvYNs9tLD0=	7.5	0.022536	0.013403
Rata-Rata	2625 (byte)		7.5 (byte)	0.0233614 (milidetik)	0.0141240 (milidetik)

b. Tabel Pengujian Enkripsi Dan Dekripsi Data Pelanggan

Dalam pengujian ini akan dibahas proses enkripsi dan dekripsi pada tabel data pelanggan. Pengujian ini, akan dilakukan pengujian pada data dan data yang digunakan pada data pelanggan hanya satu *field* di setiap *record* untuk mengetahui proses kecepatan enkripsi dan dekripsi serta panjang teks asli dan teks yang sudah di enkripsi di setiap recordnya. Pengujian enkripsi dan dekripsi data pelanggan ditunjukkan dalam tabel 2.

Tabel 2. Pengujian Enkripsi Dan Dekripsi Data Pelanggan

Karakter Asli	Jumlah Karakter (byte)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (byte)	Waktu Enkripsi (milidetik)	Waktu Dekripsi (milidetik)
jojoksugito30@gmail.com	2.875	hAWnae3UJePl9Rdr8HB3BCib5DBUN756uxUMoREe3qFkcMfEx4z2ULVLLD0=	7.5	0.021344	0.013645
henkyheryadi12@gmail.com	3	mR6ZBvb8FuGM+CxT6UMySS6Y9ggvSqAHim4RnyUF2IgiN/C18IzFCepWXT0=	7.5	0.021722	0.013148
ronidwiseptiyadi56@gmail.com	3.5	oDCURO38Pvj5yQJp2lYmZA7z0QZPZbo3nhIIlmkFoJVzFJ3M/sq4Cs5mOD0=	7.5	0.022409	0.012071
dindinwahyudi10@gmail.com	3.125	+kjXC/zYQevoiCdz0ngIACyJ2QM5NY0M+G8R7zkVqK1WFdb8/tS4Jt5FJD0=	7.5	0.021513	0.020477
dwinanto45@gmail.com	2.5	4SOoaNHhNMTFyA5e/VMEBgKhmwElaLov5VASkhEIjJR0JtP0kvzlUsh6Aj0=	7.5	0.021460	0.013311
Rata-Rata	2.001 (byte)		7.5 (byte)	0.0216896 (milidetik)	0.0145303 (milidetik)

c. Tabel Pengujian Enkripsi Dan Dekripsi Data *Reseller*

Dalam pengujian ini akan dibahas proses enkripsi dan dekripsi pada tabel data *reseller*. Pengujian ini, akan dilakukan pengujian pada data dan data yang digunakan pada data *reseller* hanya satu *field* di setiap *record* untuk mengetahui proses kecepatan enkripsi dan dekripsi serta panjang teks asli dan teks yang sudah di enkripsi di setiap recordnya. Pengujian enkripsi dan dekripsi data *reseller* ditunjukkan dalam tabel 3.

Tabel 3. Pengujian enkripsi dan dekripsi data *reseller*

Karakter Asli	Jumlah Karakter (byte)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (byte)	Waktu Enkripsi (milidetik)	Waktu Dekripsi (milidetik)
agunghardityono23@gmail.com	3.375	4haLTMfMB9vL8htX+3g3VSyW3gF6crgqulgdrRIpi45jMMfp8oPzBsRYBj0=	7.5	0.024856	0.020868
bambangsudiarto23@gmail.com	3.375	4D+EeNuOLJ/26xpt7wAiSTeG7ixDTLgqulgdrRIpi45jMMfp8oPzBsRYBj0=	7.5	0.023243	0.012683
rikogunawan45@gmail.com	2.875	k0fUSezlM/3IzgVJzH4SVxeb8BNDN756uxUMoREe3qFkcMfEx4z2ULVLLD0=	7.5	0.028735	0.011537
erwankusuma78@gmail.com	2.875	/iCZC/PZTMv69D1W2WtvXgik93ZjN756uxUMoREe3qFkcMfEx4z2ULVLLD0=	7.5	0.022212	0.014905

achmatafandik67@gmail.com	3.125	tCKuefjaDOrS9Sx6jlE3YxmyzDcuNY0M+G8R7zkVqK1WFdb8/tS4Jt5FJD0=	7.5	0.022338	0.013686
Rata-Rata	3.125 (byte)		7.5 (byte)	0.0242768 (milidetik)	0.0147358 (milidetik)

d. Tabel Pengujian Enkripsi Dan Dekripsi *File*

Dalam pengujian ini, akan dibahas proses enkripsi dan dekripsi pada tabel *file*. Pengujiannya adalah pada proses kecepatan enkripsi dan dekripsi *file*. Pengujian enkripsi dan dekripsi *file* ditunjukkan dalam tabel 4.

Tabel 4. Pengujian Enkripsi Dan Dekripsi *File*

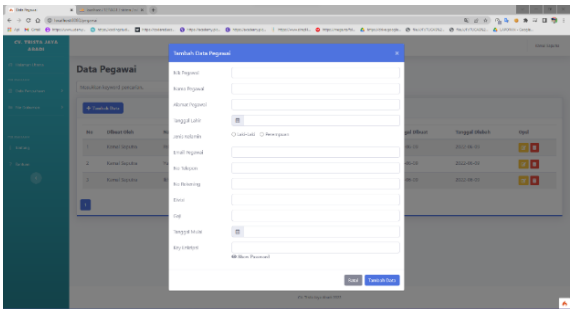
Nama File	Ukuran File (byte)			Waktu (milidetik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Tentang perusahaan.docx	59.587 byte	105.944 byte	59.587 byte	3.489467	3.067981
Bab I Kamal.docx	183.344 byte	325.952 byte	183.344 byte	7.822535	8.981868
Logo CV. Trista Jaya Abadi.pdf	158.705 byte	282.156 byte	158.705 byte	7.145148	7.199219
Bab II.pdf	738.150 byte	1.312.280 byte	738.150 byte	39.820341	43.276179
PMBN 2022.xlsx	90.818 byte	161.472 byte	90.818 byte	5.734215	6.247535
Data Order Maret.xlsx	123.452 byte	219.480 byte	123.452 byte	6.926618	7.789671
Presentasi 1.pptx	824.152 byte	1.465.176 byte	824.152 byte	49.861467	49.231033
Presentasi.pptx	2.195.822 byte	3.903.704 byte	2.195.822 byte	121.282778	139.664057
Rata-Rata	546.754 (byte)	972.021 (byte)	546.754 (byte)	30.260.321 (milidetik)	33.182.193 (milidetik)

3.2 Tampilan Layar

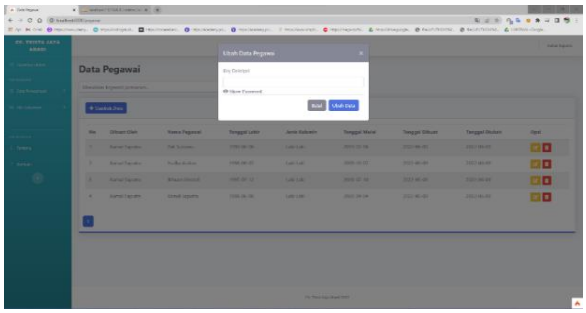
Bagian ini menjelaskan proses tampilan layar pada aplikasi sesuai dengan rancangan layar yang telah dibuat dari pertama hingga proses selesai.

a. Tampilan layar Enkripsi dan Dekripsi Data Pegawai

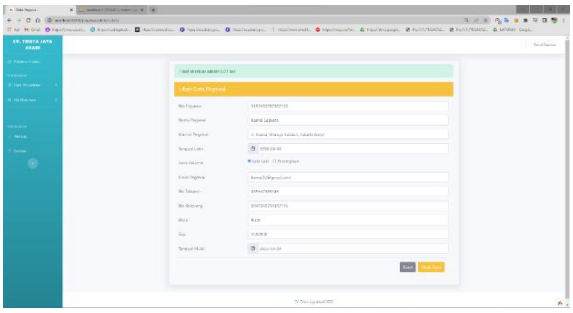
Tampilan layar enkripsi dan dekripsi merupakan tampilan layar yang digunakan untuk melakukan pendataan data dan melakukan proses enkripsi dan dekripsi data pegawai. Berikut ini adalah gambar 3 menunjukkan *form* enkripsi data pegawai, gambar 4 menunjukkan *form* dekripsi data pegawai, gambar 5 menunjukkan halaman *form* dekripsi *key* benar dan gambar 6 menunjukkan halaman *form* dekripsi *key* salah.



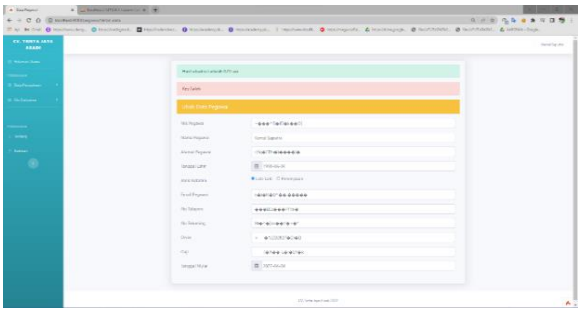
Gambar 3. *Form* enkripsi data pegawai



Gambar 4. *Form* dekripsi data pegawai



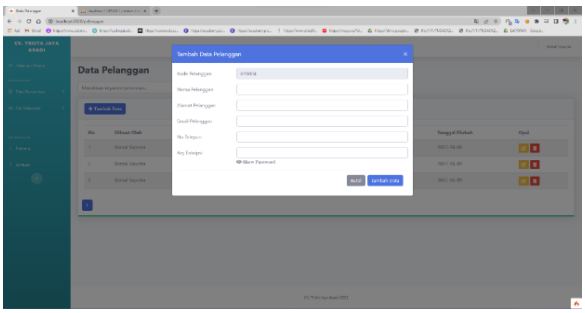
Gambar 5. Halaman *form* dekripsi *key* benar



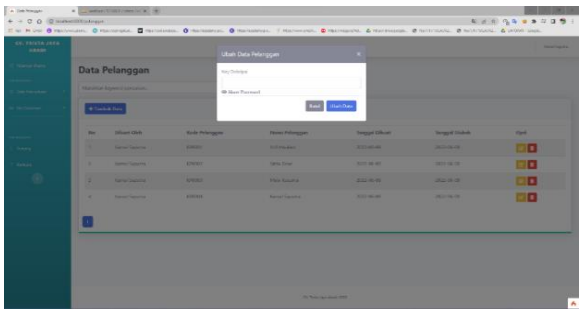
Gambar 6. Halaman *form* dekripsi *key* salah

b. Tampilan Layar Enkripsi Dan Dekripsi Data Pelanggan

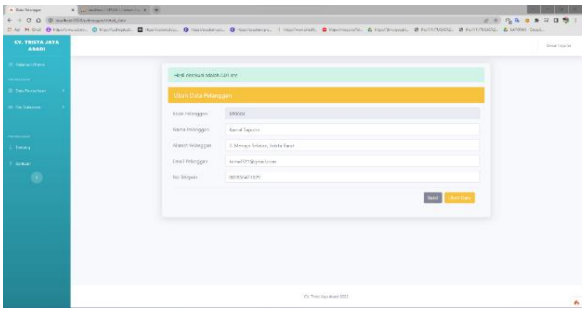
Tampilan layar enkripsi dan dekripsi merupakan tampilan layar yang digunakan untuk melakukan pendataan data dan melakukan proses enkripsi dan dekripsi data pelanggan. Berikut ini adalah gambar 7 menunjukkan *form* enkripsi data pelanggan, gambar 8 menunjukkan *form* dekripsi data pelanggan, gambar 9 menunjukkan halaman *form* dekripsi *key* benar dan gambar 10 menunjukkan halaman *form* dekripsi *key* salah.



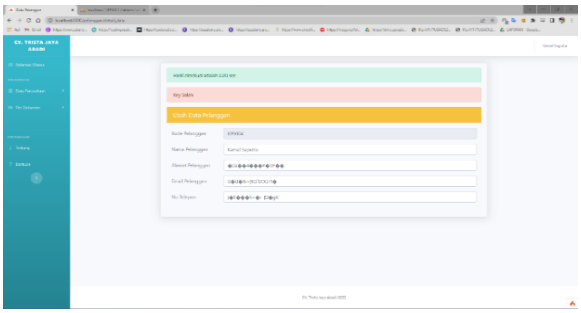
Gambar 7. *Form* enkripsi data pelanggan



Gambar 8. *Form* dekripsi data pelanggan



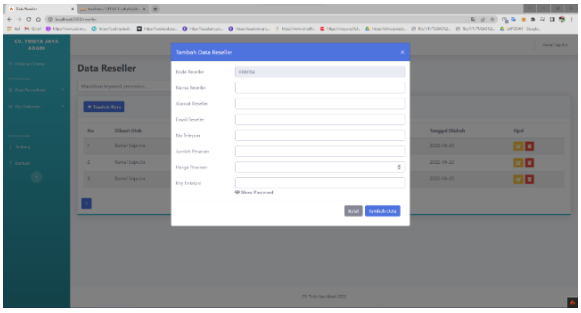
Gambar 9. Halaman *form* dekripsi *key* benar



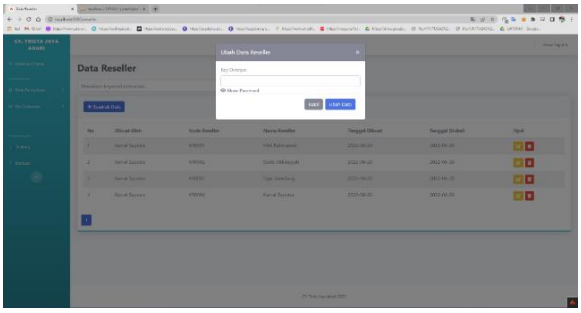
Gambar 10. Halaman *form* dekripsi *key* salah

c. Tampilan Layar Enkripsi Dan Dekripsi Data *Reseller*

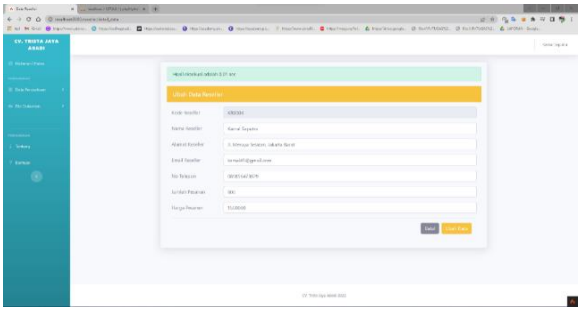
Tampilan layar enkripsi dan dekripsi merupakan tampilan layar yang digunakan untuk melakukan pendataan data dan melakukan proses enkripsi dan dekripsi data *reseller*. Berikut ini adalah gambar 11 menunjukkan *form* enkripsi data *reseller*, gambar 12 menunjukkan *form* dekripsi data *reseller*, gambar 13 menunjukkan halaman *form* dekripsi *key* benar dan gambar 14 menunjukkan halaman *form* dekripsi *key* salah.



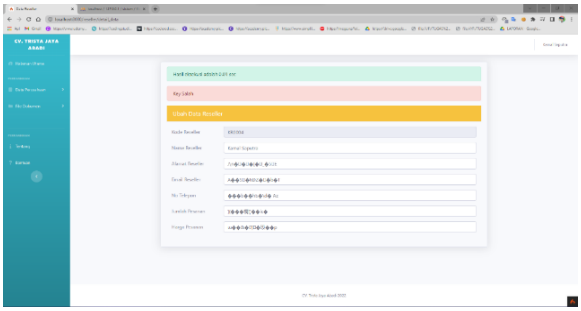
Gambar 11. *Form* enkripsi data *reseller*



Gambar 12. *Form* dekripsi data *reseller*



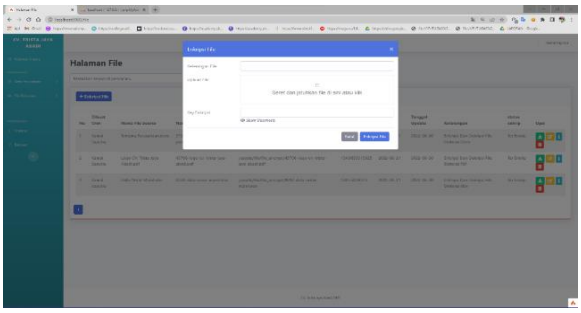
Gambar 13. Halaman *form* dekripsi *key* benar



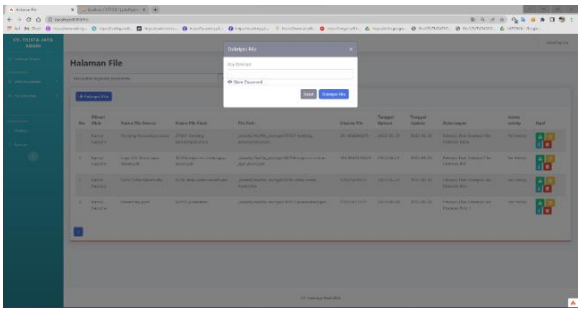
Gambar 14. Halaman *form* dekripsi *key* salah

d. Tampilan Layar Enkripsi Dan Dekripsi *File*

Tampilan layar enkripsi dan dekripsi merupakan tampilan layar yang digunakan untuk melakukan proses enkripsi dan dekripsi *file*. Berikut ini adalah gambar 15 menunjukkan *form* enkripsi *file* dan gambar 16 menunjukkan *form* dekripsi *file*.



Gambar 15. *Form* enkripsi *file*



Gambar 16. *Form* dekripsi *file*

4. KESIMPULAN

Dari pembahasan diatas dapat diambil kesimpulan bahwa kriptografi dengan metode *Advanced Encryption Standard* (AES-128) dan *Rivest Code* 4 (RC4) yang dibuat berhasil mencapai tujuan dimana dapat mengamankan *database* dan *file* penting perusahaan. Uji coba kriptografi dilakukan dengan menggunakan platform *website*, dimana *website* kriptografi yang dibuat dapat mempermudah dan mempercepat dalam melakukan pendataan data pegawai, data pelanggan dan data *reseller* serta data menjadi rapih karena tersimpan di dalam *database*. Selain itu

penggunaan metode AES-128 dan RC4 dapat mengamankan *database* yang berisikan informasi data pegawai, data pelanggan dan data *reseller* serta dapat menyimpan dan mengamankan *file* penting perusahaan. Terdapat hasil pengujian yang diperoleh dari proses enkripsi yaitu rata-rata ukuran dokumen 972.021 byte, lama waktu proses 30.260.321 milidetik dan hasil proses dekripsi rata-rata ukuran dokumen 546.754 byte, lama waktu proses 33.182.193 milidetik.

Penelitian selanjutnya diharapkan dapat menambahkan *level user* yang berguna untuk memberikan batasan kepada *user* dalam menggunakan aplikasi ini, selain itu dilakukan perbandingan metode kriptografi untuk menguji kecepatan dalam proses enkripsi dan dekripsi data dan *file*.

DAFTAR PUSTAKA

[1] A. E. Putri, A. Kartikadewi, and A. A. L. Rosyid, "Implementasi Kriptografi Dengan Algoritma *Advanced Encryption Standard* (AES) 128 Bit Dan Steganografi Menggunakan Metode *End of File* (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang," *Applied Information Systems and Management (AISM)*, vol. 3, no. 2, pp. 69-78, 2020.

[2] R. D. Saragi, M. J. Gultom, A. J. Tampubolon, and I. Gunawan, "Pengamanan Data *File* Teks (Word) Menggunakan Algoritma RC4," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, pp. 114–119, 2020.

[3] K. Zalukhu, Y. Syahra, and T. Syahputra, "Implementasi Sistem Keamanan *Database* Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma *Advanced Encryption Standard* 128 Bit Pada Pengadilan Militer I-02 Medan," *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, vol. 3, no. 2, pp. 138–150, 2020.

[4] J. Prayudha, Saniman, and Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (AES)," *Sains dan Komputer (SAINTIKOM)*, vol. 18, no. 2, pp. 119–129, 2019.

[5] D. Widyawan and Imelda, "Pengamanan *File* Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *SKANIKA*, vol. 4, no. 1, pp. 15–22, 2021.

[6] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan *Database* Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia," *SKANIKA*, vol. 4, no. 1, pp. 66–71, 2021.

[7] A. Kodir and W. Pramusinto, "Implementasi Kriptografi Dengan Menggunakan Metode RC4 Dan BASE64 Untuk Mengamankan *Database* Sekolah Pada SDN Grogol Utara 10," *SKANIKA*, vol. 4, no. 1, pp. 7–14, 2021.

[8] Z. Basim and Painem, "Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah," *SKANIKA*, vol. 3, no. 4, pp. 45–52, 2020.

[9] N. Cristy and F. Riandari, "Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]* , vol. 4, no. 2, pp. 75–85, 2021.

[10] D. Irwansyah, "Pengamanan Data Teks Dengan Algoritma Modifikasi RC4," *Jurnal Pelita Informatika*, vol. 6, no.3, 2018.