3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENERAPAN ALGORITMA KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN DATA PEGAWAI PADA PT MULTIJAYA SPARINDO

Fikri Ardianto[1*], Titin Fatimah[2]

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

Email: [1*]1911501359@student.budiluhur.ac.id, [2]titin.fatimah@budiluhur.ac.id
(* : corresponding author)

Abstrak-Sebagai perusahaan yang bergerak di industri suku cadang penerbangan, solusi pencarian dan penyelamatan, serta peralatan penegak hukum, Dengan adanya penggunaan algoritma kriptografi yang canggih, PT Multijaya Sparindo dapat memberikan jaminan kepada pegawai bahwa informasi pribadi dan data penting mereka aman dari akses yang tidak sah. Keberhasilan penelitian ini juga membuka peluang untuk beradaptasi dengan perkembangan keamanan siber yang terus berkembang, mengukuhkan reputasi perusahaan dalam menjaga integritas data dan privasi pegawai. Data pegawai menjadi aset berharga yang mencakup informasi pribadi, identitas, dan informasi penting lainnya yang harus dijaga dengan cermat. Masalah yang sering terjadi adalah kurangnya tingkat keamanan yang memadai terhadap data pegawai di PT Multijaya Sparindo, menyebabkan potensi risiko akses tidak sah dan pelanggaran privasi yang dapat merugikan perusahaan dan pegawai.Oleh karena itu, implementasi algoritma kriptografi menjadi langkah yang sangat dibutuhkan. Algoritma kriptografi merupakan suatu sistem matematis yang kompleks yang bertujuan untuk mengubah data asli menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, yaitu *ciphertext.* PT Multijaya Sparindo menggunakan metode *Advanced Encryption Standard* 128 (AES-128) dalam penelitian ini. Metode ini telah dimodifikasi dengan memanfaatkan *random byte* dalam proses enkripsi kuncinya. Dengan demikian, setiap kali enkripsi dilakukan, *output* yang dihasilkan akan berbeda, meningkatkan tingkat keamanan data. Untuk memastikan keberhasilan dekripsi, *random key* yang sesuai telah disimpan di *database.* Proses ini memastikan bahwa hanya pihak yang sah yang memiliki kunci yang benar dapat mengembalikan data ke bentuk aslinya. Hasil penelitian menunjukkan bahwa aplikasi ini memberikan tingkat keamanan yang tinggi dalam mengamankan data pada PT Multijaya Sparindo. Modifikasi pada *random byte* berhasil meningkatkan efektivitas enkripsi dan dekripsi data. Hasil akhir pengujian rata-rata ukuran hasil proses enkripsi sebesar 181043,2 *byte*, lamanya 5073 millidetik dan rata-rata ukuran hasil proses dekripsi sebesar 181043,2 *byte*, lamanya 5021 milidetik.

Kata Kunci: Kriptografi,AES-128,*Random Byte*,*Random Key*,Enkripsi,Dekripsi,*File.*

IMPLEMENTATION OF AES-128 CRYPTOGRAPHIC ALGORITHM TO SECURE EMPLOYEE DATA AT PT MULTIJAYA SPARINDO

Abstract- *As a company operating in the aviation spare parts, search and rescue solutions, and law enforcement equipment industry, PT Multijaya Sparindo utilizes advanced cryptographic algorithms to provide employees with assurance that their personal and critical data remain protected from unauthorized access. The success of this research not only facilitates adaptation to the ever-evolving cybersecurity landscape but also bolsters the company's reputation for upholding the integrity of employee data and privacy. Employee data stands as a valuable asset encompassing personal information, identities, and crucial details that necessitate careful safeguarding. A recurring issue pertains to the insufficient level of security for employee data at PT Multijaya Sparindo, leading to potential risks of unauthorized access and privacy violations that could detrimentally impact the company and its employees. Consequently, the implementation of cryptographic algorithms becomes an essential step. Cryptographic algorithms, intricate mathematical systems, aim to transform original data into an unreadable form for unauthorized parties, referred to as ciphertext. In this study, PT Multijaya Sparindo employs the Advanced Encryption Standard 128 (AES-128) method, which has been adapted through the utilization of random bytes during the key encryption process. This modification ensures that each encryption iteration yields distinct outputs, consequently enhancing data security. To ensure successful decryption, the corresponding random key is stored within the database. This process guarantees that only authorized entities possessing the correct key can restore the data to its original form. Research findings underscore that this application confers a high level of security when safeguarding data at PT Multijaya Sparindo. The modification involving random bytes has successfully elevated the effectiveness of data encryption and decryption. Ultimately, test results reveal an average encryption process output size of 181,043.2 bytes, taking 5,073 milliseconds, and an average decryption process output size of 181,043.2 bytes, taking 5,021 milliseconds.*

Keywords*: Cryptography,AES-128,Random Byte,Random Key,Encrypt,Decrypt,File*

1. PENDAHULUAN

Teknologi Informasi memberikan dampak positif sekaligus negatif. Salah satu dampak negatifnya adalah adanya penyadapan data yang sering terjadi dalam perkembangan teknologi informasi. Keamanan dan kerahasiaan data, informasi, dan pesan menjadi aspek yang sangat penting. Data ini bisa berbentuk dokumen digital seperti .docx, .pdf, .xlsx, dan lain-lain.[1] Data dan informasi memiliki nilai yang sangat penting bagi perusahaan maupun individu. Setiap pengguna komputer selalu melakukan penyimpanan data untuk meningkatkan keamanan data yang disimpan dan menjaga kerahasiaan setiap informasi yang telah diolah.[2]

Sebagai perusahaan yang bergerak dibidang pemasok di industri suku cadang penerbangan, solusi pencarian dan penyelamatan, dan peralatan penegak hukum, PT Multijaya Sparindo membutuhkan keamanan data dengan upaya melindungi data pegawai yang dimilikinya. Data pegawai pada PT Multijaya Sparindo perlu diamankan dengan cermat dan teliti karena melibatkan informasi yang sangat penting dan sensitif. Maka dari itu, penerapan algoritma kriptografi sangat dibutuhkan oleh PT Multijaya Sparindo untuk mengamankan data pegawainnya.

Masalah yang sering terjadi adalah kurangnya tingkat keamanan yang memadai terhadap data pegawai di PT Multijaya Sparindo, menyebabkan potensi risiko akses tidak sah dan pelanggaran privasi yang dapat merugikan perusahaan dan pegawai. Penelitian ini bertujuan untuk menerapkan algoritma AES-128 pada platform enkripsi berbasis web dan meningkatkan keamanan file yang berisi informasi data pegawai agar terjaga secara efektif.[3] Dengan adanya penggunaan algoritma kriptografi yang canggih, PT Multijaya Sparindo dapat memberikan jaminan kepada pegawai bahwa informasi pribadi dan data penting mereka aman dari akses yang tidak sah.

Kriptografi berasal dari bahasa Yunani, di mana "*crypto*s" berarti rahasia dan "*graphein*" berarti tulisan. Jadi, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara mengenkripsinya menjadi bentuk yang tidak dapat dimengerti maknanya. Dalam menjaga kerahasiaan data menggunakan kriptografi, data asli yang dikirim diubah menjadi bentuk data terenkripsi, dan hanya bisa dikembalikan ke bentuk aslinya menggunakan kunci khusus yang dimiliki oleh pihak yang sah. Hal ini menyebabkan pihak lain tanpa kunci tidak dapat membaca data asli sehingga data tetap terjaga kerahasiaannya.[4]

Advanced Encryption Standard (AES) merupakan pengembangan dari algoritma enkripsi standar DES. AES adalah algoritma kriptografi yang diogunakan untuk mengamankan data. Algoritma AES beroperasi sebagai blok *ciphertext* simetrik yang mampu melakukan enkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Saat proses enkripsi, data diubah menjadi bentuk yang tidak dapat dibaca lagi yang disebut *ciphertext*, sedangkan proses dekripsi mengembalikan *ciphertext* menjadi bentuk semula yang dikenal sebagai *plaintext*. Untuk mengenkripsi dan mendekripsi data pada blok 128 bit, algoritma AES menggunakan kunci kriptografi dengan Panjang 128, 192, atau 256 bit. [5]

Proses enkripsi algoritma AES dimulai dengan melakukan operasi XOR antara *plaintext*/*state* yang akan dienkripsi dengan *roundkey*. Setelah dilakukan operasi XOR, dilakukan substitusi menggunakan *s-box*. Setelah proses substitusi selesai, dilakukan operasi *shiftrow*. Setelah hasil dari *shiftrow* didapatkan, langkah selanjutnya adalah melakukan operasi *Mix Columns* dengan mengalikan matriks khusus. Setelah perhitungan *Mix Columns* selesai, dilakukan operasi *addround key* dengan melakukan operasi XOR antara *state* hasil sebelumnya dengan *round key*. Proses ini diulang sebanyak 10 iterasi, namun pada iterasi ke-10, setelah langkah *shiftrow*, langkah *Mix Columns* dilewati dan langsung dilakukan operasi XOR antara hasil *state* saat *shiftrow* dengan *round key*.[6]

Terdapat perbedaan pada penelitian sebelumnya oleh Fadhlurrahman dan Ariyani yang berjudul "Aplikasi *Chatting* Notaris Berbasis Android Dengan Metode Kriptografi AES-128 dan *Blowfish*" [7] yang mengimplementasikan aplikasi berbasis Android dan menggunakan dua metode yaitu AES-128 dan *Blowfish* untuk mengamankan *chatting* notaris, penelitian oleh Rizki dan Ariyani yang berjudul "Penerapan Kriptografi Dengan Menggunakan Algoritma RSA Untuk Pengamanan Data Berbasis Desktop Pada PT Trias Mitra Jaya Manunggal" [8] yang mengimplementasikan aplikasi berbasis *Desktop* untuk mengamankan data populasi mesin, penelitian oleh Widiyanto dkk., yang berjudul "Pengamanan Pesan *Text* dengan menggunakan Kriptografi Klasik Metode *Shift Chipper* dan Metode *Substitution Chipper"*[9] untuk mengamankan pengiriman pesan teks, penelitian oleh Cristy dan Riandari yang berjudul "Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan" [10] untuk pengaman data keuangan SPP berbasis *Desktop*, sedangkan pada penelitian kali ini berbasis *web* untuk mengamankan data pegawai dan menggunakan satu metode yaitu AES-128, kelebihan pada penelitian kali ini yaitu adanya modifikasi pada proses enkripsi menggunakan kunci acak sehingga tingkat keamanan yang lebih tinggi.

2. METODE PENELITIAN

2.1 Pengumpulan Data

Metode pengumpulan data merupakan tahap yang digunakan dalam sebuah penelitian, berikut beberapa metode penelitian data :

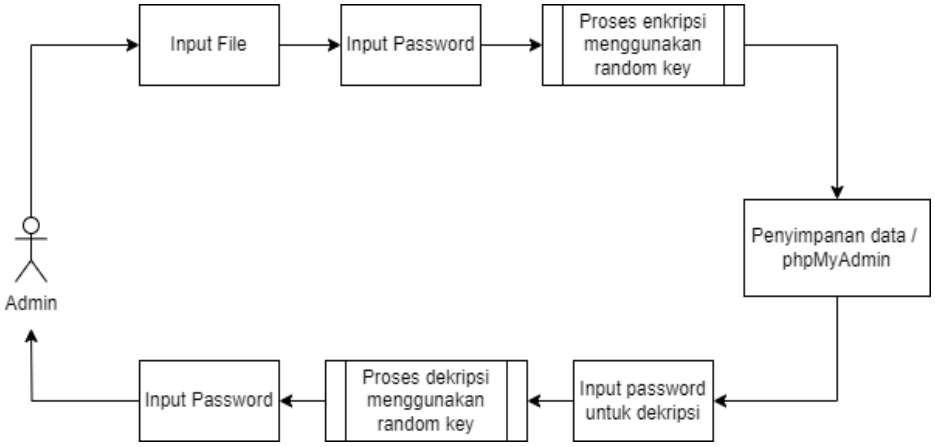
a. Wawancara

Wawancara adalah proses interaksi langsung antara peneliti dan responden dengan tujuan mengumpulkan data melalui pertanyaan-pertanyaan yang telah disusun sebelumnya. Untuk mendapatkan informasi dan data tentang keamanan pada PT Multijaya Sparindo, proses wawancara dilakukan dengan cara interaksi langsung melalui tanya jawab dengan salah satu petinggi perusahaan tersebut.

b. Observasi
Metode Observasi melibatkan pengamatan langsung terhadap kejadian, perilaku, atau fenomena yang ingin diteliti. Dalam observasi, peneliti secara aktif mengamati dan mencatat apa yang terjadi di lingkungan atau situasi yang diamati. Pada penelitian ini dilakukan observasi secara tidak langsung dengan tujuan untuk memperoleh pola kerja, lingkungan fisik, serta interaksi sosial pada PT Multijaya Sparindo.

2.2 Proses Penerapan Metode AES-128

Pada proses penerapan metode AES-128 ini menggunakan modifikasi pada kuncinya. Dalam kriptografi, bilangan acak sering dibangkitkan menggunakan pembangkit bilangan acak semu atau *Pseudo Random Number Generator* (PRNG). Meskipun luaran dari pembangkit bilangan acak semu hanya mendekati sifat-sifat bilangan acak, mereka masih banyak digunakan dalam simulasi ilmiah seperti fisika, matematika, biologi, dan bidang lainnya[11]. Proses penerapan metode AES-128 meliputi kunci acak, pengaturan mode operasi, pengolahan data blok, dan langkah-langkah enkripsi serta dekripsi. Melalui tahapan-tahapan tersebut, metode AES-128 mampu memberikan tingkat keamanan yang tinggi dalam melakukan enkripsi dan dekripsi data. Namun, penting untuk memastikan pengaturan kunci acak yang kuat, memilih mode operasi yang sesuai, dan menjaga kerahasiaan kunci untuk memastikan keamanan data yang optimal. Proses penerapan algoritma AES-128 dapat dilihat pada Gambar 1.



Gambar 1 Proses Penerapan Metode AES-128

2.3 Tahap Pengujian

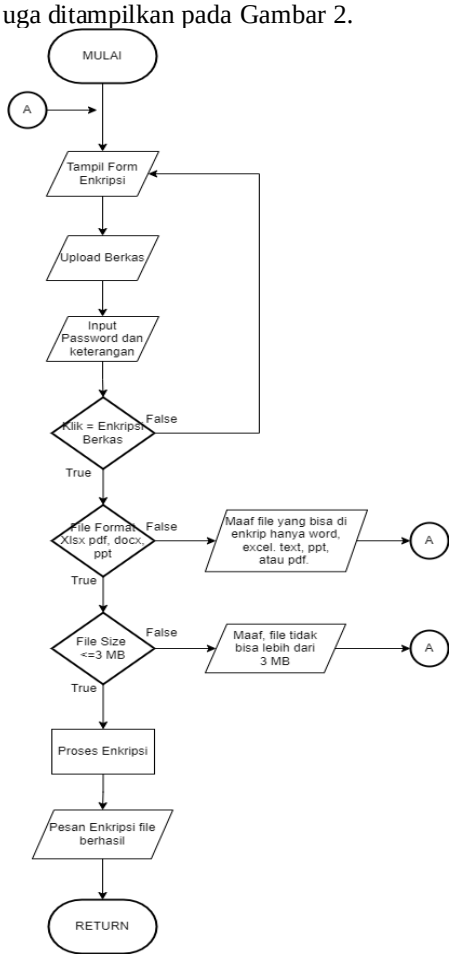
Dalam tahap ini, pengujian dilakukan dengan maksud untuk memastikan bahwa sistem yang telah dirancang sesuai dengan perencanaan dan analisis yang telah dilakukan, serta menghasilkan kesimpulan apakah sistem tersebut memenuhi harapan sesuai dengan permasalahan yang ada. Untuk mencapai tujuan tersebut, digunakan metode pengujian yang menjadi panduan atau parameter untuk menyimpulkan apakah sistem dapat beroperasi sesuai dengan tujuan yang telah ditetapkan. Salah satu metode pengujian yang digunakan adalah *Blackbox*, yang digunakan untuk menemukan kesalahan dan menguji fungsi aplikasi saat berjalan. Metode yang digunakan untuk pengujian aplikasi ini adalah metode *Black Box*. Pengujian *Black Box* adalah pendekatan pengujian yang menggunakan struktur kontrol yang telah dirancang secara prosedural untuk melaksanakan pengujian dan melihat bagaimana perangkat lunak beroperasi. Seluruh komponen internal perangkat lunak diuji untuk memastikan bahwa mereka berfungsi sesuai dengan spesifikasi dan desain yang telah ditentukan[12]. Metode pengujian *Black Box* digunakan untuk memverifikasi apakah semua fungsi aplikasi pada proses enkripsi dan dekripsi *file* sesuai dengan harapan. Metode pengujian ini juga akan digunakan untuk menguji kecepatan dalam proses enkripsi dan dekripsi *file*.

2.4 *Flowchart*

Flowchart digunakan sebagai cara untuk menjelaskan tahap-tahap pemecahan masalah secara visual, mudah digunakan, dan sesuai dengan standar. *Flowchart* juga berperan dalam perencanaan dan optimasi algoritma, sehingga membantu meningkatkan efisiensi dan efektivitas dalam menjalankan aplikasi.

2.4.1 *Flowchart* Halaman Enkripsi

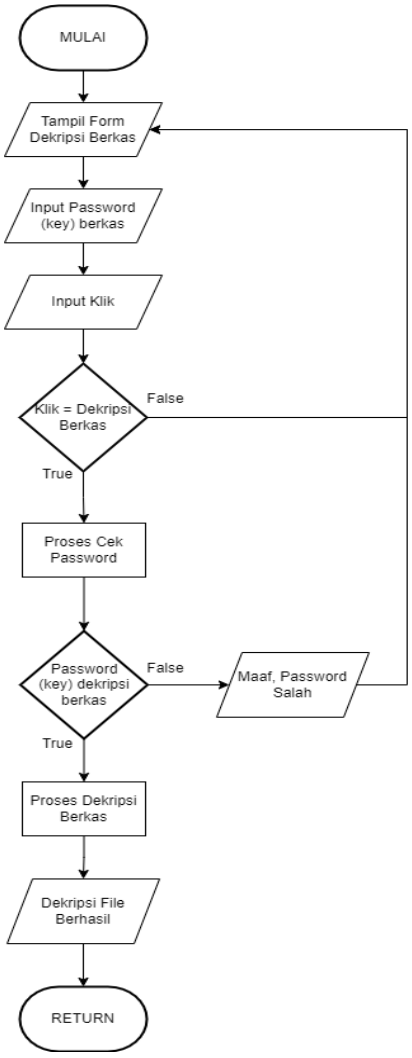
Pada halaman enkripsi, pengguna dapat melakukan proses enkripsi berkas yang dilakukan oleh *admin* dengan cara *upload* berkas yang berformat excel, word, text, pdf, dan ppt. Ukuran berkas yang dapat di *upload* tidak bisa lebih besar dari 3mb. Proses tersebut juga ditampilkan pada Gambar 2.



Gambar 2 Flowchart Halaman Enkripsi

2.4.2 *Flowchart* Halaman Dekripsi Berkas

Pada halaman dekripsi berkas, pengguna dapat melakukan proses dekripsi berkas yang sudah di enkripsi sesuai status pada daftar berkas pada menu halaman dekripsi sebelumnya yang dimana *admin* akan memilih berkas untuk di dekripsi lalu memasukkan *password* (*key*) sesuai dengan *password* yang telah di input pada proses enkripsi, dekripsi berkas ini berfungsi untuk mengembalikan data asli dari berkas tersebut. Proses tersebut dijelaskan pada Gambar 3.



Gambar 3 Flowchart Halaman Dekripsi Berkas

3. HASIL DAN PEMBAHASAN

Bagian ini mencakup analisis, implementasi, dan pengujian hasil, serta pembahasan mengenai topik penelitian, yang sebelumnya dapat disusun dengan menyusun metodologi penelitian terlebih dahulu. Selain itu, bagian ini juga berfungsi untuk menyajikan penjelasan melalui teks, gambar, tabel, dan elemen lain yang relevan untuk membahas topik penelitian.

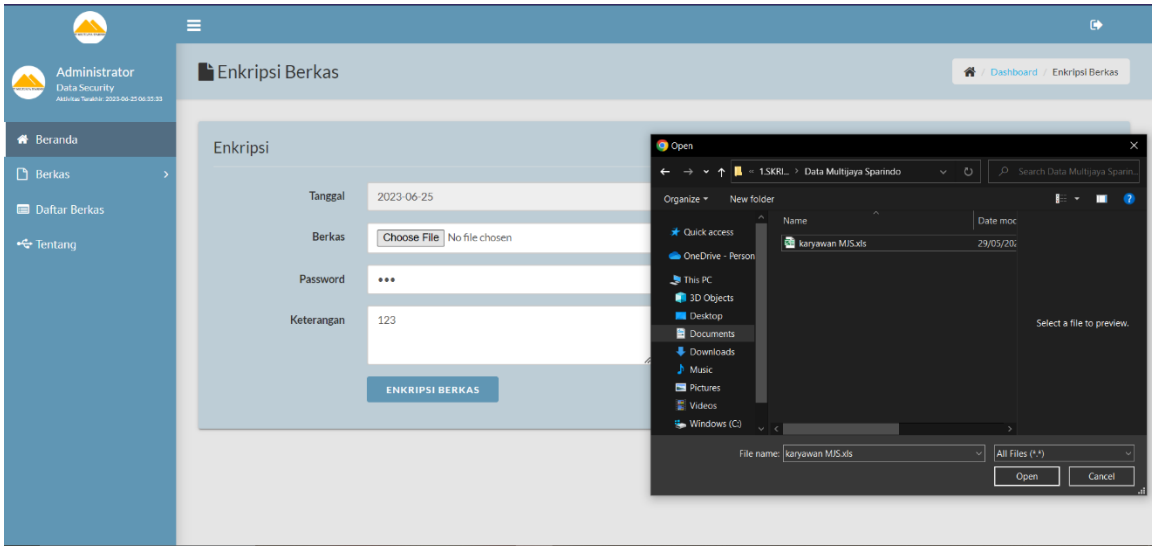
3.1 Implementasi Metode

Berikut ini akan dijelaskan serangkaian langkah yang menjelaskan bagaimana metode AES-128 bekerja dengan menggunakan kunci acak dalam proses implementasinya.

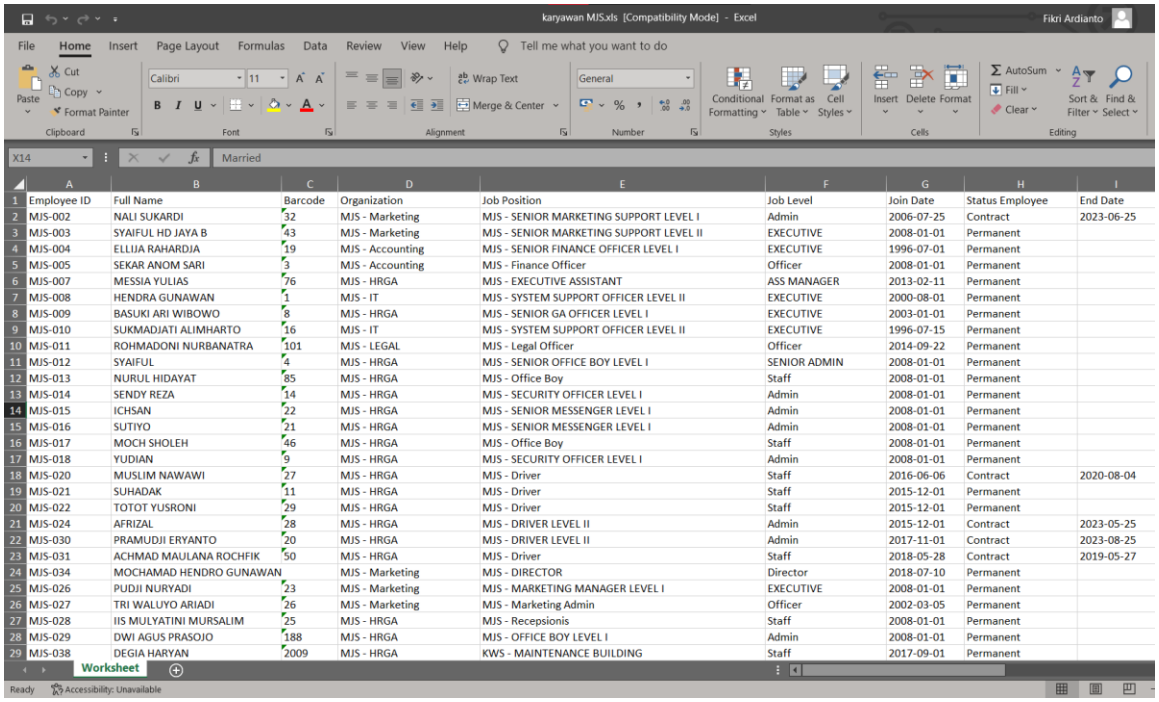
3.1.1 Proses Enkripsi *File*

Pada tahap ini, pengguna diharuskan *login* menggunakan akun *admin* untuk mengakses program. *Admin* akan melakukan *upload file* data pegawai PT Multijaya Sparindo dengan format xls. Setelah itu, *admin* akan melakukan *input password* (*key*) dan keterangan. Lebih lengkapnya dapat dilihat pada gambar 4.

Setelah melakukan enkripsi maka akan menghasilkan *file* berformat rda yang menandakan proses enkripsi berhasil dilakukan seperti pada Gambar 5.

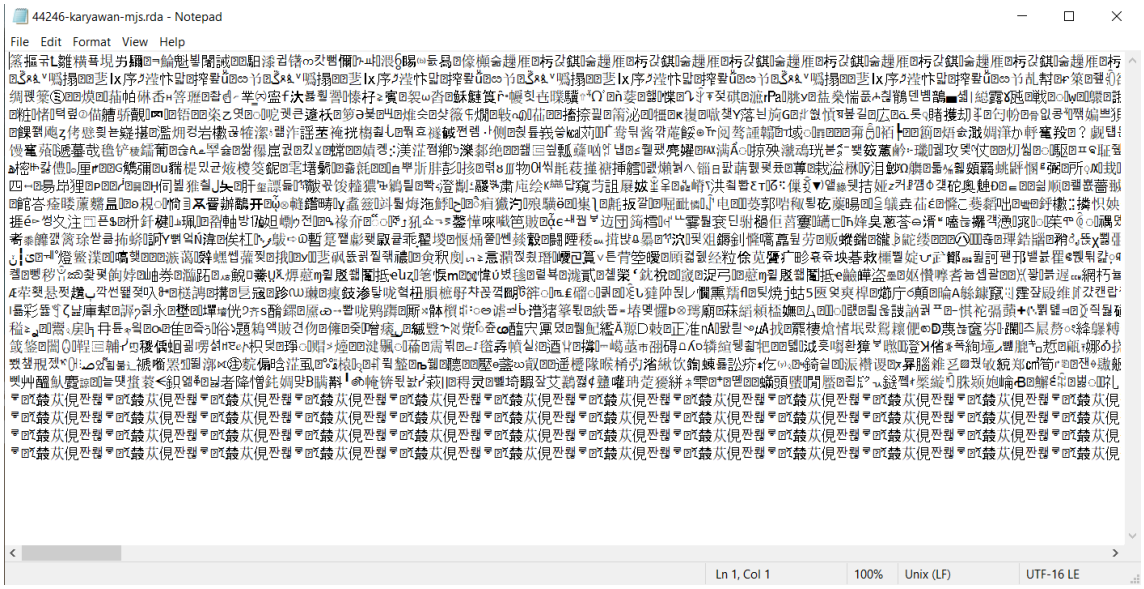


Gambar 4 Proses Enkripsi File



Employee ID	Full Name	Barcode	Organization	Job Position	Job Level	Join Date	Status Employee	End Date
MJS-002	NALI SUKARDI	32	MJS - Marketing	MJS - SENIOR MARKETING SUPPORT LEVEL I	Admin	2006-07-25	Contract	2023-06-25
MJS-003	SYAIFUL HD JAYA B	43	MJS - Marketing	MJS - SENIOR MARKETING SUPPORT LEVEL II	EXECUTIVE	2008-01-01	Permanent	
MJS-004	ELLIJA RAHARDJA	19	MJS - Accounting	MJS - SENIOR FINANCE OFFICER LEVEL I	EXECUTIVE	1996-07-01	Permanent	
MJS-005	SEKAR ANOM SARI	3	MJS - Accounting	MJS - Finance Officer	Officer	2008-01-01	Permanent	
MJS-007	MESSIA YULIAS	76	MJS - HRGA	MJS - EXECUTIVE ASSISTANT	ASS MANAGER	2013-02-11	Permanent	
MJS-008	HENDRA GUNAWAN	1	MJS - IT	MJS - SYSTEM SUPPORT OFFICER LEVEL II	EXECUTIVE	2000-08-01	Permanent	
MJS-009	BASUKI ARI WIBOWO	8	MJS - HRGA	MJS - SENIOR GA OFFICER LEVEL I	EXECUTIVE	2003-01-01	Permanent	
MJS-010	SUKMADJATI ALIMHARTO	16	MJS - IT	MJS - SYSTEM SUPPORT OFFICER LEVEL II	EXECUTIVE	1996-07-15	Permanent	
MJS-011	ROHMADONI NURBANATRA	101	MJS - LEGAL	MJS - Legal Officer	Officer	2014-09-22	Permanent	
MJS-012	SYAIFUL	4	MJS - HRGA	MJS - SENIOR OFFICE BOY LEVEL I	SENIOR ADMIN	2008-01-01	Permanent	
MJS-013	NURUL HIDAYAT	85	MJS - HRGA	MJS - Office Boy	Staff	2008-01-01	Permanent	
MJS-014	SENDY REZA	14	MJS - HRGA	MJS - SECURITY OFFICER LEVEL I	Admin	2008-01-01	Permanent	
MJS-015	ICHSAN	22	MJS - HRGA	MJS - SENIOR MESSENGER LEVEL I	Admin	2008-01-01	Permanent	
MJS-016	SUTIYO	21	MJS - HRGA	MJS - SENIOR MESSENGER LEVEL I	Admin	2008-01-01	Permanent	
MJS-017	MOCH SHOLEH	46	MJS - HRGA	MJS - Office Boy	Staff	2008-01-01	Permanent	
MJS-018	YUDIAN	9	MJS - HRGA	MJS - SECURITY OFFICER LEVEL I	Admin	2008-01-01	Permanent	
MJS-020	MUSLIM NAWAWI	27	MJS - HRGA	MJS - Driver	Staff	2016-06-06	Contract	2020-08-04
MJS-021	SUHADAK	11	MJS - HRGA	MJS - Driver	Staff	2015-12-01	Permanent	
MJS-022	TOTOT YUSRONI	29	MJS - HRGA	MJS - Driver	Staff	2015-12-01	Permanent	
MJS-024	AFRIZAL	28	MJS - HRGA	MJS - DRIVER LEVEL II	Admin	2015-12-01	Contract	2023-05-25
MJS-030	PRAMUDJI ERYANTO	20	MJS - HRGA	MJS - DRIVER LEVEL II	Admin	2017-11-01	Contract	2023-08-25
MJS-031	ACHMAD MAULANA ROCHFIK	50	MJS - HRGA	MJS - Driver	Staff	2018-05-28	Contract	2019-05-27
MJS-034	MOCHAMAD HENDRO GUNAWAN		MJS - Marketing	MJS - DIRECTOR	Director	2018-07-10	Permanent	
MJS-026	PUDJI NURYADI	23	MJS - Marketing	MJS - MARKETING MANAGER LEVEL I	EXECUTIVE	2008-01-01	Permanent	
MJS-027	TRI WALUYO ARIADI	26	MJS - Marketing	MJS - Marketing Admin	Officer	2002-03-05	Permanent	
MJS-028	IIS MULYATINI MURSALIM	25	MJS - HRGA	MJS - Recepsionis	Staff	2008-01-01	Permanent	
MJS-029	DWI AGUS PRASOJO	188	MJS - HRGA	MJS - OFFICE BOY LEVEL I	Admin	2008-01-01	Permanent	
MJS-038	DEGIA HARYAN	2009	MJS - HRGA	KWS - MAINTENANCE BUILDING	Staff	2017-09-01	Permanent	

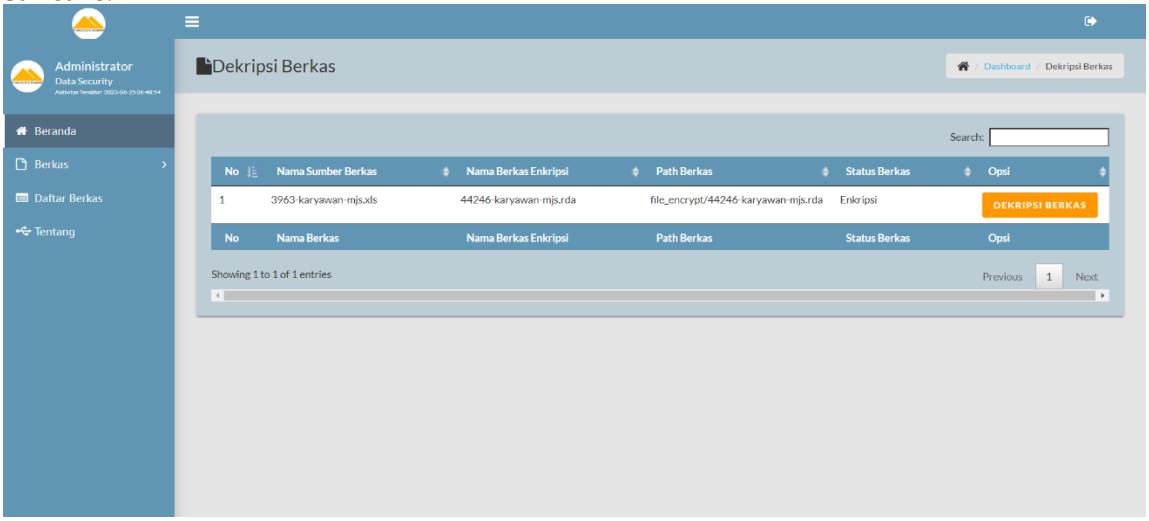
Gambar 5 File Sebelum Enkripsi



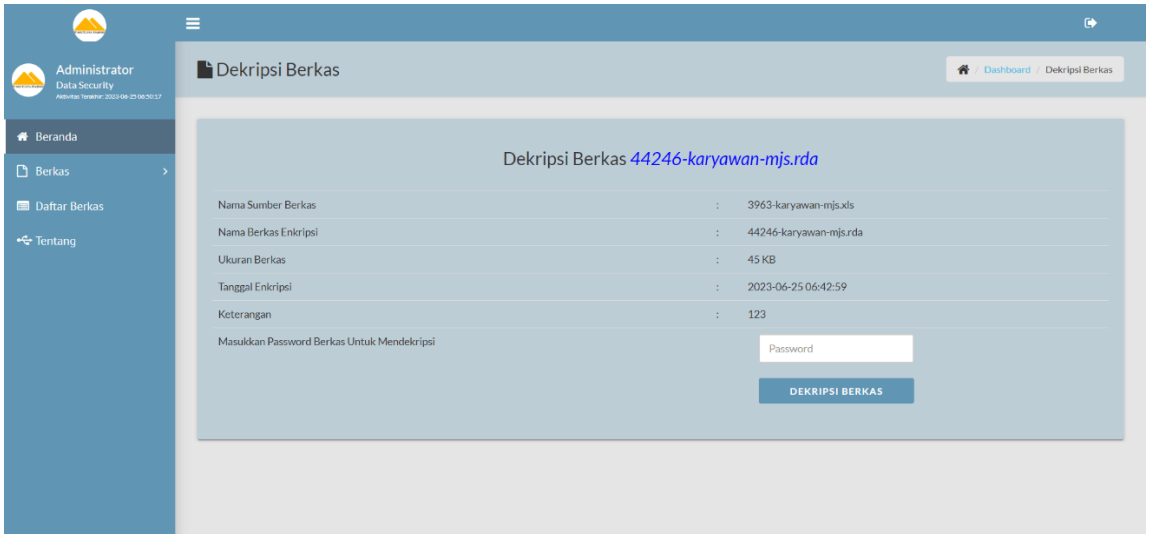
Gambar 6 Hasil Enkripsi

3.1.2 Proses Dekripsi *File*

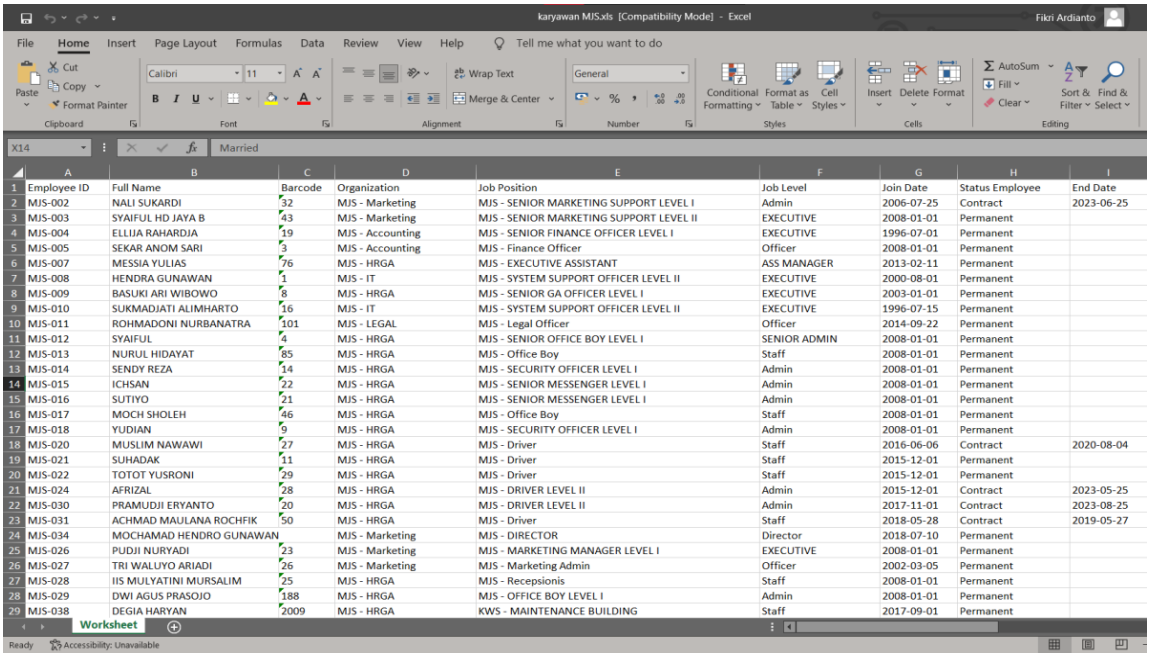
Pada tahap ini, pengguna diharuskan *login* menggunakan akun *admin* untuk bisa mendekripsi berkas. *Admin* akan memilih berkas yang berstatus enkripsi lalu menekan *button* dekripsi berkas, seperti pada Gambar 6. Setelah mengakses halaman yang ada pada Gambar 6, maka akan muncul halaman *form* yang menampilkan detail berkas yang terenkripsi, lalu *admin* akan memasukkan *password* (*key*) untuk mendekripsi berkas, seperti pada Gambar 7. Setelah berhasil mendekripsi berkas maka status berkas akan berubah menjadi terenkripsi, lalu jika menekan *button download* pada berkas yang terenkripsi tersebut akan menghasilkan data asli dari berkas tersebut, seperti pada Gambar 8.



Gambar 7 Daftar Berkas Terenkripsi



Gambar 8 Proses Dekripsi Berkas



Employee ID	Full Name	Barcode	Organization	Job Position	Job Level	Join Date	Status Employee	End Date
MJS-002	NALI SUKARDI	32	MJS - Marketing	MJS - SENIOR MARKETING SUPPORT LEVEL I	Admin	2006-07-25	Contract	2023-06-25
MJS-003	SYAIFUL HD JAYA B	43	MJS - Marketing	MJS - SENIOR MARKETING SUPPORT LEVEL II	EXECUTIVE	2008-01-01	Permanent	
MJS-004	ELLIJA RAHARDJA	19	MJS - Accounting	MJS - SENIOR FINANCE OFFICER LEVEL I	EXECUTIVE	1996-07-01	Permanent	
MJS-005	SEKAR ANOM SARI	3	MJS - Accounting	MJS - Finance Officer	Officer	2008-01-01	Permanent	
MJS-007	MESSIA YULIAS	76	MJS - HRGA	MJS - EXECUTIVE ASSISTANT	ASS MANAGER	2013-02-11	Permanent	
MJS-008	HENDRA GUNAWAN	1	MJS - IT	MJS - SYSTEM SUPPORT OFFICER LEVEL II	EXECUTIVE	2000-08-01	Permanent	
MJS-009	BASUKI ARI WIBOWO	8	MJS - HRGA	MJS - SENIOR GA OFFICER LEVEL I	EXECUTIVE	2003-01-01	Permanent	
MJS-010	SUKMADJATI ALIMHARTO	16	MJS - IT	MJS - SYSTEM SUPPORT OFFICER LEVEL II	EXECUTIVE	1996-07-15	Permanent	
MJS-011	ROHMADONI NURBANATRA	101	MJS - LEGAL	MJS - Legal Officer	Officer	2014-09-22	Permanent	
MJS-012	SYAIFUL	4	MJS - HRGA	MJS - SENIOR OFFICE BOY LEVEL I	SENIOR ADMIN	2008-01-01	Permanent	
MJS-013	NURUL HIDAYAT	85	MJS - HRGA	MJS - Office Boy	Staff	2008-01-01	Permanent	
MJS-014	SENDY REZA	14	MJS - HRGA	MJS - SECURITY OFFICER LEVEL I	Admin	2008-01-01	Permanent	
MJS-015	ICHSAN	22	MJS - HRGA	MJS - SENIOR MESSENGER LEVEL I	Admin	2008-01-01	Permanent	
MJS-016	SUTIYO	21	MJS - HRGA	MJS - SENIOR MESSENGER LEVEL I	Admin	2008-01-01	Permanent	
MJS-017	MOCH SHOLEH	46	MJS - HRGA	MJS - Office Boy	Staff	2008-01-01	Permanent	
MJS-018	YUDIAN	9	MJS - HRGA	MJS - SECURITY OFFICER LEVEL I	Admin	2008-01-01	Permanent	
MJS-020	MUSLIM NAWAWI	27	MJS - HRGA	MJS - Driver	Staff	2016-06-06	Contract	2020-08-04
MJS-021	SUHADAK	11	MJS - HRGA	MJS - Driver	Staff	2015-12-01	Permanent	
MJS-022	TOTOT YUSRONI	29	MJS - HRGA	MJS - Driver	Staff	2015-12-01	Permanent	
MJS-024	AFRIZAL	28	MJS - HRGA	MJS - DRIVER LEVEL II	Admin	2015-12-01	Contract	2023-05-25
MJS-030	PRAMUDJI ERYANTO	20	MJS - HRGA	MJS - DRIVER LEVEL II	Admin	2017-11-01	Contract	2023-08-25
MJS-031	ACHMAD MAULANA ROCHFIK	50	MJS - HRGA	MJS - Driver	Staff	2018-05-28	Contract	2019-05-27
MJS-034	MOCHAMAD HENDRO GUNAWAN		MJS - Marketing	MJS - DIRECTOR	Director	2018-07-10	Permanent	
MJS-026	PUDJI NURYADI	23	MJS - Marketing	MJS - MARKETING MANAGER LEVEL I	EXECUTIVE	2008-01-01	Permanent	
MJS-027	TRI WALUYO ARIADI	26	MJS - Marketing	MJS - Marketing Admin	Officer	2002-03-05	Permanent	
MJS-028	IIS MULYATINI MURSALIM	25	MJS - HRGA	MJS - Recepsionis	Staff	2008-01-01	Permanent	
MJS-029	DWI AGUS PRASOJO	188	MJS - HRGA	MJS - OFFICE BOY LEVEL I	Admin	2008-01-01	Permanent	
MJS-038	DEGIA HARYAN	2009	MJS - HRGA	KWS - MAINTENANCE BUILDING	Staff	2017-09-01	Permanent	

Gambar 9 Hasil Dekripsi

3.2 Hasil Pengujian

Pengujian program ini menggunakan metode *black box*. Metode *black box* adalah pendekatan pengujian yang berfokus pada *input* dan *output* program tanpa memperhatikan struktur internal kode program. Berikut pengujian fungsional yang digambarkan melalui Tabel 1 yang menggunakan metode *black box*.

Tabel 1 Tabel Pengujian Fungsional Aplikasi

No.	Rancangan Proses	Hasil Yang DIharapkan	Hasil Pengujian	Kesimpulan
1.	Mengisi form login	Berhasil Login	Sesuai harapan	Setelah berhasil langsung ke halaman dashboard
2.	Klik menu beranda di sidebar	Muncul halaman dashboard	Sesuai harapan	Jika berhasil, pengguna akan ke halaman dashboard dan dapat melihat informasi data yang di dekripsi dan enkripsi
3.	Klik menu dropdown berkas lalu pilih enkripsi di sidebar	Muncul form enkripsi	Sesuai harapan	Jika berhasil maka menu akan turun ke bawah (dropdown) lalu ada pilihan enkripsi dan dekripsi

4.	Klik button enkripsi	Berkas berhasil di enkripsi	Sesuai harapan	Jika berhasil, pengguna dapat mengisi form dan upload berkas yang akan di enkripsi
5.	Klik menu dropdown berkas lalu pilih dekripsi di sidebar	Muncul form tabel berkas yang sudah didekripsi dan enkripsi	Sesuai harapan	Jika berhasil maka menu akan turun ke bawah (dropdown) lalu akan ada pilihan enkripsi dan dekripsi
6.	Klik button dekripsi	Muncul form untuk dekripsi berkas	Sesuai harapan	Jika berhasil, maka pengguna dapat melihat list berkas terenkripsi dan terdekripsi
7.	Klik button dekripsi berkas	Berhasil mendekripsi berkas	Sesuai harapan	Jika berhasil, maka akan muncul halaman untuk dekripsi berkas dengan memasukkan password (key) yang sesuai

Berikut pengujian file yang digambarkan melalui Tabel 2 dan menggunakan metode *black box* untuk mengetahui ukuran serta waktu proses dalam mengenkripsi dan mendekripsi *file*.

Tabel 2 Tabel Pengujian File

Nama File	Bentuk File	Ukuran File (Byte)			Waktu (milidetik)	
		Asli (byte)	Enkripsi (byte)	Dekripsi (byte)	Enkripsi (milidetik)	Dekripsi (milidetik)
Karyawan MJS.xls	Excel	46080	46080	46080	1310	1270
Karyawan MJS.docx	Word	37888	37888	37888	1050	1200
Karyawan MJS.pdf	Pdf	467968	467968	467968	12890	12880
Karyawan MJS.pptx	powerpoint	38912	38912	38912	1270	1280
1911501359_Lembar Pengesahan.pdf	Pdf	17408	17408	17408	580	550
Surat Keterangan Riset.pdf	Pdf	120832	120832	120832	3390	3350
surat tidak plagiat.pdf	Pdf	710656	710656	710656	19930	19530
HASIL PENGUJIAN.docx	Word	22528	22528	22528	620	620
Hasil uji fungsi aplikasi.pdf	Pdf	173056	173056	173056	4820	4730
13260-bilangan-acak.pdf	Pdf	175104	175104	175104	4870	4800
	Rata-rata :	**181043,2**	**181043,2**	**181043,2**	**5073**	**5021**

Setelah melakukan pengujian pada Tabel 2 dapat dismpulkan bahwa waktu enkripsi lebih lama dari waktu dekripsi, semakin besar ukuran *file* yang dienkripsi maka semakin lama waktu yang dibutuhkan untuk enkripsi dan dekripsi *file* tersebut, serta berkas yang dienkripsi akan berupa tulisan acak dalam format rda. Hasil akhir pengujian rata-rata ukuran hasil proses enkripsi sebesar 181043,2 *byte*, lamanya 5073 millidetik dan rata-rata ukuran hasil proses dekripsi sebesar 181043,2 *byte*, lamanya 5021 milidetik.

4. KESIMPULAN

Setelah melakukan perancangan dan pengembangan aplikasi kriptografi berbasis *web* untuk enkripsi dan dekripsi *file* serta menghadapi permasalahan yang telah dibahas sebelumnya, diperoleh kesimpulan bahwa aplikasi ini dapat mengenkripsi dan mendekripsi *file* dengan baik, dengan Hasil akhir pengujian rata-rata ukuran hasil proses enkripsi sebesar 181043,2 *byte*, lamanya 5073 millidetik dan rata-rata ukuran hasil proses dekripsi sebesar 181043,2 *byte*, lamanya 5021 milidetik.

Berdasarkan kesimpulan diatas, berikut beberapa saran yang diberikan untuk meningkatkan fitur serta tingkat keamanan pada aplikasi, diantaranya diharapkan untuk dikembangkan lagi untuk program enkripsi dan dekripsi *file* ini dengan memodifikasi algoritma ataupun mengkombinasikan metode AES-128 dengan metode kriptografi lainnya supaya sistem semakin sulit untuk diretas, diharapkan untuk dikembangkan lagi dari sisi kompatibilitas dan fleksibilitas dengan membuat versi *mobile* dari aplikasi ini, serta diharapkan untuk ditambahkan format *file* yang dapat di enkripsi supaya aplikasi dapat menjangkau lebih banyak *file* yang ingin diamankan.

DAFTAR PUSTAKA

[1] N. U. Baidoi, M. Hardjianto, and A. Wibowo, "Implementasi Algoritma Advanced Encryption Standard Untuk Pengamanan File Pada Smp Negeri 189 Jakarta Barat," *Pros. Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 2, no. 1, pp. 1–9, 2023, [Online]. Available: http://senafti.budiluhur.ac.id/index.php/senafti/article/view/570

[2] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," *TECHSI - J. Tek. Inform.*, vol. 13, no. 1, p. 14, 2021, doi: 10.29103/techsi.v13i1.2395.

[3] D. Widyawan and I. 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, doi: 10.36080/skanika.v4i1.2216.

[4] S. D. Nurcahya, "Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.

[5] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[6] A. Pariddudin and F. Syauqi, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 2, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.87.

[7] Z. Fadhlurrahman and F. Ariyani, "Aplikasi Chatting Notaris Berbasis Android Dengan Metode Kriptografi AES-128 dan Blowfish," *Skanika*, vol. 1, no. 2, pp. 656–661, 2018.

[8] M. Rizki and F. Ariyani, "Algoritma Rsa Untuk Pengamanan Data Berbasis," vol. 4, no. 2, pp. 1–6, 2021.

[9] M. A. H. Septian Widiyanto, Govindo Adnan, Moh. Fatkuroji, Dwi Wahyu Handoyo, "Pengamanan Pesan Text dengan menggunakan Kriptografi Klasik Metode Shift Chipper dan Metode Substitution Chipper," *Riau J. Comput. Sci.*, vol. 7, no. 01, pp. 9–17, 2021.

[10] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

[11] M. Fahrizal and A. Solichin, "Pengamanan M-Commerce Menggunakan One Time Password Metode Pseudo Random Number Generator (PRNG)," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 5, no. 2, pp. 108–116, 2020, doi: 10.36341/rabit.v5i2.1363.

[12] R. Firdaus and R. R. Santika, "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," *Semin. Nas. Mhs. Fak. Teknol. Inf. Univ. Budi Luhur*, vol. 1, no. 1, pp. 111–120, 2022.