4th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITME KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN DATA AHLI WARIS PADA KELURAHAN GROGOL SELATAN

Ahmad Fauzi[1*], Mufti[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1*]1911501680@student.budiluhur.ac.id, [2]mufti@budiluhur.ac.id
(* : corresponding author)

Abstrak- Kemajuan dalam dunia teknologi informasi saat ini membuat pencarian data semakin mudah. Kemajuan dalam teknologi komputer memungkinkan orang saling bertukar data satu sama lain dengan berbagai informasi melalui internet. Kelurahan Grogol Selatan, yang terletak di kecamatan Kebayoran Lama, menghadapi masalah karena tidak adanya sistem keamanan yang memadai untuk menyimpan informasi seperti data ahli waris. Oleh karena itu, orang yang tidak memiliki wewenang dapat mengubah data penting di dalamnya kapan saja. Termasuk informasi yang diberikan oleh ahli waris. Salah satu tujuan keamanan data ahli waris agar tidak dimanfaatkan oleh pihak tertentu yang menyalahgunakan data karena tidak tersedianya sistem yang melindungi informasi ahli waris. Penelitian ini berkonsentrasi pada pembuatan aplikasi bertema web yang akan melindungi data ahli waris Grogol Selatan dengan menggunakan algoritme kriptografi *AES 128 bit*. Untuk mencegah kebocoran, pencurian, dan penyalahgunaan informasi ahli waris. *AES 128 bit* menggunakan kunci *random byte*. Aplikasi ahli waris berbasis web ini melindungi data menggunakan bahasa pemrogram *PHP*. Dokumen yang didukung hanya *xlsx, xls, docx, doc, txt, pdf,* dan *ppt*. Dalam pengamanannya, metode *AES-128* mengubah kuncinya dengan *byte random*, sehingga yang dihasilkan saat enkripsi selalu acak. Dengan dekripsi, *file* dapat dikembalikan dengan menggunakan kunci acak yang disimpan di database di masa mendatang. Sebagai hasil dari tes yang dilakukan pada data ahli waris di Kelurahan Grogol Selatan, algoritme kriptografi yang menggunakan metode *AES-128* berhasil menjaga keamanan *file*. Hasil penelitian dihasilkan setelah proses enkripsi menggunakan *AES-128*. Dokumen dengan ukuran rata-rata 2,788 kilobyte membutuhkan waktu enkripsi sekitar 70.37 detik dan dekripsi sekitar 68.81 detik, menurut tabel hasil pengujian *file. File* dengan ukuran rata-rata 547 kilobyte membutuhkan waktu enkripsi 14.21 detik dan dekripsi 13.46 detik.

Kata Kunci: *AES-128,* Kriptografi, *Byte Random*, Dekripsi, Enkripsi, *file*

IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD (AES-128) CRYPTOGRAPHY ALGORITHM FOR SECURING HEIRS' DATA IN THE GROGOL SELATAN DISTRICT

Abstract- *Advances in the world of information technology today make searching for data increasingly easier. Advances in computer technology allow people to exchange data with each other and various information via the internet. Grogol Selatan sub-district, which is located in Kebayoran Lama sub-district, is facing problems because there is no adequate security system to store information such as heir data. Therefore, unauthorized people can change important data in it at any time. Including information provided by the heirs. One of the goals of protecting heirs' data is to prevent it from being exploited by certain parties who misuse the data because there is no system that protects heirs' information. This research concentrates on creating a web-themed application that will protect the data of South Grogol heirs using the AES 128 bit cryptographic algorithm. To prevent leaks, theft and misuse of heir information. AES 128 bit uses random byte keys. This web-based heir application protects data using the PHP programming language. Supported documents are only xlsx, xls, docx, doc, txt, pdf, and ppt. In terms of security, the AES-128 method changes the key with random bytes, so that what is generated during encryption is always random. With decryption, files can be restored using a random key stored in the database in the future. As a result of tests carried out on heir data in South Grogol Village, a cryptographic algorithm using the AES-128 method succeeded in maintaining file security. The research results were produced after the encryption process using AES-128. Documents with an average size of 2,788 kilobytes took about 70.37 seconds to encrypt and about 68.81 seconds to decrypt, according to the file test results table. Files with an average size of 547 kilobytes required encryption time of 14.21 seconds and decryption time of 13.46 seconds.*

Keywords*: AES-128, Cryptography, Random Bytes, Decryption, Encryption, file*

1. PENDAHULUAN

Kemajuan yang terjadi di dunia teknologi informasi saat ini membuat pencarian data semakin mudah. Kemajuan dalam teknologi komputer memungkinkan orang saling bertukar data satu sama lain dengan berbagai

informasi melalui internet. Kriminalitas yang berhubungan dengan TI dan komputer meningkat seiring perkembangan zaman. Salah satu efek buruk dari kemajuan teknologi adalah pencurian data dan kebocoran informasi. Oleh karena itu, sangat penting untuk menjaga keamanan penyimpanan data di era modern. Salah satunya adalah data ahli waris, termasuk data sensitif karena menjadi salah satu data penting. Akibatnya, tindak kejahatan dapat muncul. Sebuah sistem yang dapat menyimpan dan mengamankan data diperlukan untuk memastikan bahwa data ahli waris aman. *Advanced Encryption Standard (AES)* adalah salah satu algoritme kriptografi yang digunakan.

Menurut [1](Eka Putri, Kartikadewi, and Abdul Rosyid 2021), kriptografi yaitu bidang yang membahas metode matematika yang digunakan untuk melindungi data dan informasi, seperti autentikasi, legalitas, dan kredibilitas. Berasal dari kata Yunani *"crypto"*, yang mengandung arti rahasia, dan *"graphia"*, yang berfaedah tulisan.

Kelurahan Grogol Selatan, yang terletak di kecamatan Kebayoran Lama, menghadapi masalah karena tidak adanya sistem keamanan yang memadai untuk menyimpan informasi seperti data ahli waris. Oleh karena itu, orang yang tidak memiliki wewenang dapat mengubah data penting di dalamnya kapan saja. termasuk informasi yang diberikan oleh ahli waris. Kelurahan hanya memiliki hasil scan dari sekumpulan data-data yang diberikan dari pihak keluarga ke kelurahan yang telah disatukan, hasilnya akan dikirim ke kecamatan kebayoran lama untuk diproses lebih lanjut. Selain itu, pihak kelurahan khawatir bahwa informasi ahli waris dapat hilang atau digunakan oleh pihak yang menggunakan dengan mengambil data dalam kasus Dimana sistem keamanan tidak tersedia.

Studi sebelumnya, [2] "Implementasi Metode *Advanced Encryption Standard (AES 128* Bit) Untuk Mengamankan Data Keuangan" berfokus atas perlindungan dokumen sekolah SMK Harapan Bangsa, terutama uang SPP. Format yang dienkripsi dan basis program berbeda dari penelitian sebelumnya. Untuk melindungi data ahli waris, yang terdiri dari *file* yang tersedia di Kelurahan Grogol Selatan, studi ini menerapkan sistem yang melindungi data dengan berbasis web yang menggunakan algoritme *AES-128*. dengan memodifikasi kuncinya menggunakan *random byte*.

Kriptografi simetris dan asimetris adalah dua jenis utama. Baik enkripsi maupun dekripsi memerlukan kunci yang sama. Namun, akan metode asimetris, memerlukan kunci publik sebagai enkripsi dan kunci privat untuk dekripsi. Keamanan algoritme kriptografi asimetris lebih tinggi daripada algoritme kriptografi simetris. [3]

Menurut [4] Untuk mengenkripsi dan mendekripsi data, *Advanced Encryption Standard (AES)* merupakan algoritme kriptografi simetris paling umum dipakai. *AES* mempunyai kecepatan yang lebih cepat daripada algoritme kriptografi simetris lainnya.

Oleh karena itu, proses pengembangan aplikasi ini adalah untuk membantu kelurahan membangun sistem yang aman untuk data ahli waris sehingga orang yang tidak berkewenangan tidak dapat mengaksesnya. Sistem ini juga akan mencegah data ahli waris hilang atau disalahgunakan oleh orang yang tidak berkewenangan. Penulis berharap dapat membantu pihak kelurahan mengurangi kekhawatiran masyarakat tentang kebocoran data ahli waris dengan menggunakan algoritme *Advance Encryption Standard (AES) 128*.

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Pembahasan ini, semua informasi yang diperlukan untuk penelitian telah dikumpulkan. Berikut adalah beberapa cara untuk mengumpulkan data:

a. Wawancara *(Interview)*

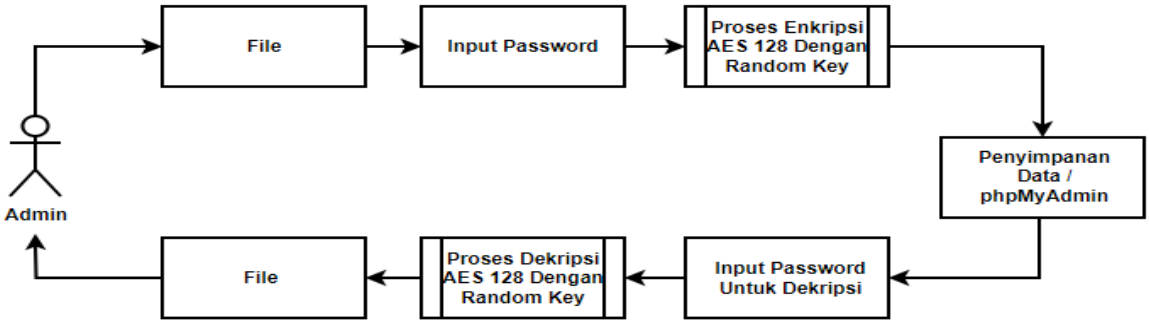
Wawancara dilakukan dengan cara berinteraksi langsung dan bertanya jawab dengan anggota. Kelurahan Grogol Selatan mengenai masalah yang sedang dibahas. Untuk mengetahui tentang keamanan data perusahaan dan kekhawatiran ahli waris, wawancara ini dilakukan.

b. Observasi *(Observation)*

Untuk mengetahui sistem kemananan dan informasi ahli waris, observasi tidak langsung dilakukan di Kelurahan Grogol Selatan.

2.2 Implementasi Metode *AES-128* dengan Pemodifikasian Kunci.

Kelurahan Grogol Selatan menghadapi masalah kekurangan program enkripsi dan dekripsi untuk menjaga data ahli waris aman. Oleh karena itu, program ini diperlukan untuk memastikan kerahasiaan dan keamanan data tersebut. Gambar 1 menunjukkan bagaimana metode diterapkan pada program yang dibuat, yang menggunakan metode *AES-128* dengan *key random*.



Gambar 1. Proses Penerapan Metod

Penerapan Metode *AES-128* melibatkan modifikasi kunci program. *Administrator* memasukkan *password* atau kunci yang telah ditetapkan, dan *password* tersebut digabungkan dengan kunci acak berukuran 16 *byte* untuk proses enkripsi. Pada tahap dekripsi, *administrator* menggunakan kunci atau *password* yang telah ditetapkan saat enkripsi dan mengambil kunci acak yang telah disimpan dalam database. Dengan cara ini, teknik *AES-128* akan diterapkan.

Tujuan algoritme yang dikenal sebagai *generator* bilangan acak adalah untuk menghasilkan urutan nilai yang sulit diprediksi sehingga dapat dianggap sebagai acak. [5]

2.3 Tahap Pengujian

Pada titik ini, uji coba dilaksanakan untuk memverifikasi kesesuaian sistem dengan desain dan hasil analisis, serta untuk menentukan sejauh mana sistem memenuhi harapan yang didasarkan pada masalah yang dihadapi. Untuk mencapai tujuan ini, diperlukan penerapan metode pengujian sebagai ukuran atau patokan untuk menetapkan bahwa sistem mampu mencapai arah yang ditentukan. Untuk mendeteksi kesalahan dan mengevaluasi kinerja aplikasi ketika beroperasi, teknik pengecekan yang dikenal sebagai *"black box"* digunakan.

Pengujian *black box* adalah bagian penting dari pengetesan perangkat lunak karena mereka memverifikasi apakah fungsi keseluruhan sistem berjalan dengan efektif.[6]

Black box testing yakni sebuah metode percobaan perangkat lunak yang menekankan detail fungsi program. Ini dapat menemukan kecacatan dalam struktur data, antarmuka, akses basis data, dan performa, serta kekeliruan dalam proses inisialisasi dan terminasi. [7]

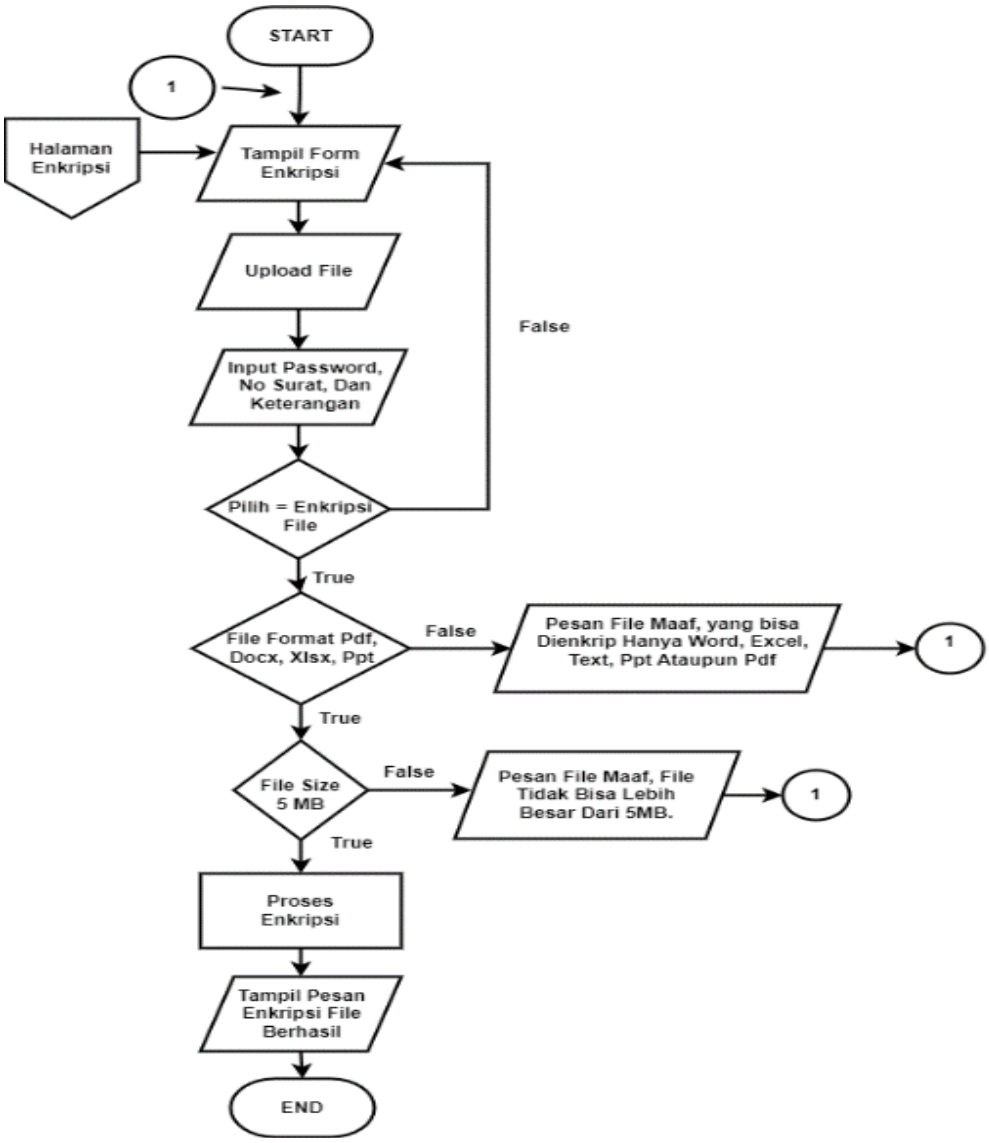
2.4 *Flowchart*

Penulis menggunakan representasi visual dari skema proses program untuk menunjukkan urutan proses dalam program ini. *Flowchart* tampilan layar program dan metode yang digunakan disertakan di sini.

Proses *flowchart* menunjukkan bagaimana algoritme aplikasi menjalankan perintah.[8]

2.4.1 *Flowchart* Halaman Enkripsi

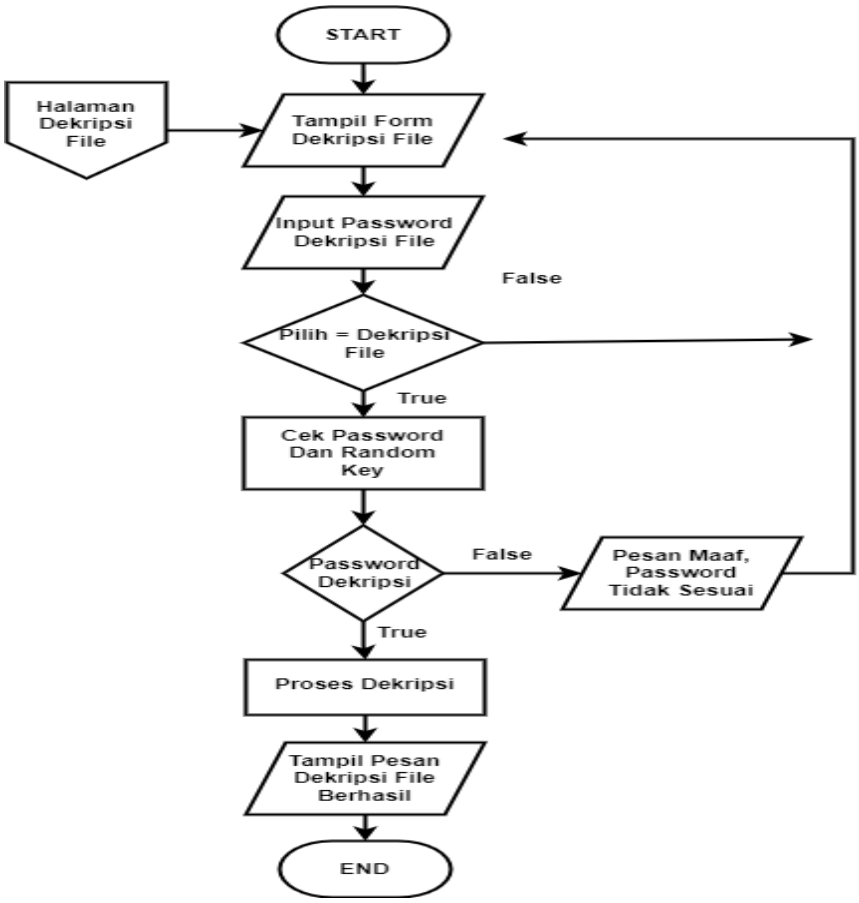
Gambar 2 menunjukkan diagram *flowchart* pada halaman enkripsi yang menjelaskan proses manajemen yang digunakan untuk mengenkripsi *file*. *Upload file* dan masukkan *password* adalah langkah pertama. Selain itu, *administrator* memiliki wewenang untuk mengisi nomor surat dan keterangan. Jenis *file* yang dapat dimasukkan termasuk *Microsoft Excel*, *Word*, *Text*, *PDF*, atau *PowerPoint*. *File* tidak boleh melebihi batas 5MB.



Gambar 2. *Flowchart* Halaman Enkripsi

2.4.2 *Flowchart* Halaman Dekripsi

Ilustrasi Gambar 3 menggambarkan rangkaian langkah pada halaman dekripsi *file*, yang memungkinkan pengguna untuk mengolah *file* terenkripsi dan mengembalikannya ke bentuk aslinya. Tahap awal melibatkan pemilihan *file* berdasarkan statusnya, dan ketika pengguna memilih opsi dekripsi, mereka diminta untuk memasukkan *password file*. Jika *password* sesuai, proses dekripsi akan mengembalikan *file* ke bentuk aslinya.



Gambar 3. *Flowchart* Halaman Dekripsi *File*

2.5 *Advanced Encryption Standard (AES)*

Menurut penjelasan [9] sejarah *AES* adalah *NIST* meluncurkan *Advance Encryption Standard (AES)* guna mewakilkan *Data Encryption Standard (DES)* pada tahun 1997. Algoritme *AES* dirancang untuk memastikan bahwa berbagai industri dapat diatur dengan menggunakan minimal blok input 128-bit. Algoritme ini mendukung pada tiga buah ukuran kunci yaitu: 128-bit, 192-bit, dan 256-bit. *NIST* mengumumkan di Agustus pada tahun 1998 bahwa lima belas proposal setelah proses seleksi algoritme yang dikirim, saran *AES* telah diterima dan dievaluasi. *NIST* menyatakan dengan lima algoritme yang diterima di tahun 1999. Algoritme *RC6*, *MARS*, *Snake*, *Rijdnael*, dan *Twofish*. 5 algoritme ini akan diuji dengan berbgai cara pengujian. *Rijndael* diumumkan sebagai algoritme pilihan untuk standar *AES* yang baru pada Oktober 2000.

Advanced Encryption Standard (AES) merupakan teknik kriptografi yang mempertahankan integritas data dengan memakai kunci kriptografi berpanjang 128, 192, atau 256 bit untuk mengenkripsi serta mendekripsi blok data berukuran 128 bit. Saat dienkripsi, *Ciphertext* adalah bentuk data yang tidak dapat dibaca lagi yang diciptakan ketika data dienkripsi. Selain itu, ketika proses dekripsi selesai, data dikembalikan ke bentuk aslinya, yang dapat dibaca disebut *plaintext*.[10]

3. HASIL DAN PEMBAHASAN

Setelah metodologi penelitian dibuat sebelumnya, komponen ini berisi penjabaran, hasil penerapan, dan percobaan pengujian, serta pembahasan materi penelitian. Komponen ini juga menampilkan penjelasan pada tabel, gambar, serta hal lainnya.

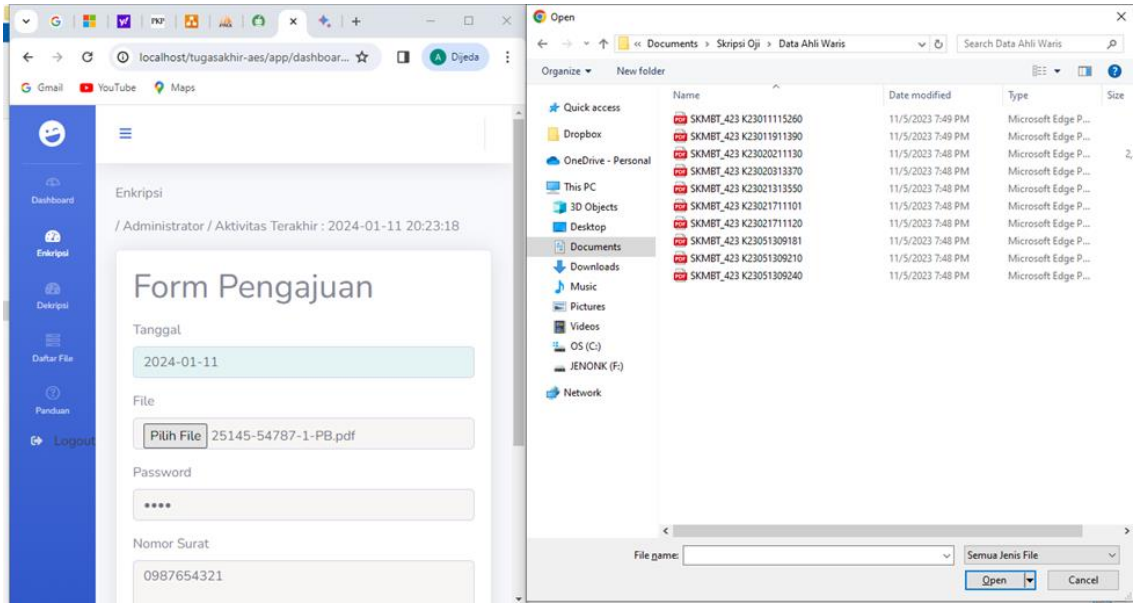
3.1 Implementasi Sistem

Penjelasan tentang cara metode *AES-128* bekerja dengan *key random* saat digunakan diberikan di sini.

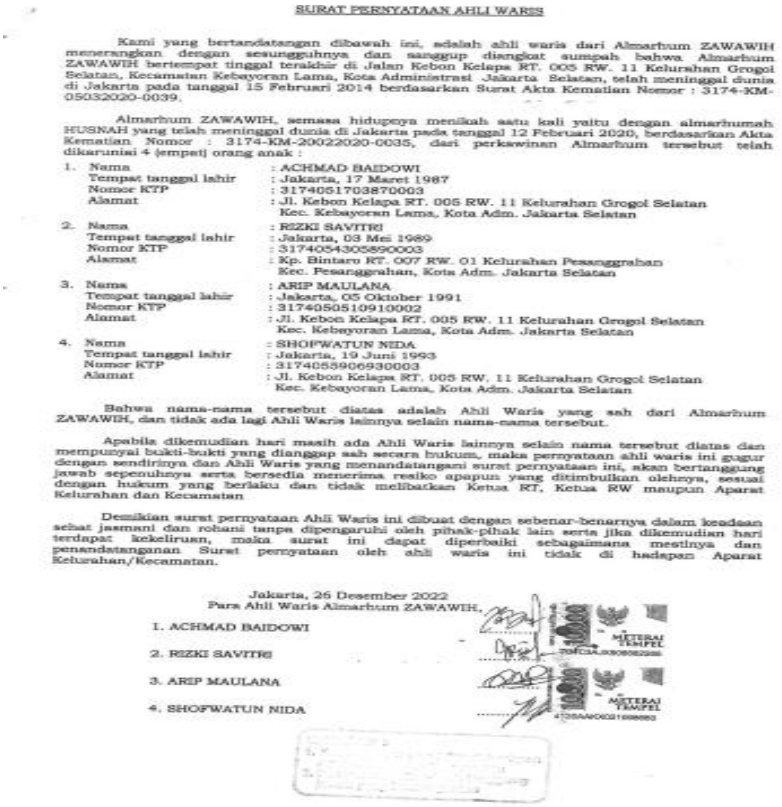
3.1.1 Proses Enkripsi *File*

Setelah berhasil masuk ke akun *administrator*, Anda dapat mengakses program dan memulai proses enkripsi *file*. *Administrator* akan memilih dan *mengimpor file* dalam bentuk *docx*, *doc*, *xlsx*, *xls*, *txt*, *pdf*, *ppt*, dan *pptx* dari Data Ahli Waris Kelurahan Grogol Selatan ke dalam program. Setelah *mengimpor file*, *administrator* memberikan *pasword*, no surat, dan juga keterangan, yang akan digunakan

bersama dengan *button* pilihan. Gambar 4 menunjukkan bagaimana *file* dimasukkan untuk pengujian program, Gambar 5 menunjukkan analisis data sebelum enkripsi, serta Gambar 6 menunjukkan perolehan enkripsi dari *file* data ahli waris Kelurahan Grogol Selatan, yang diubah dari format *pdf* ke format *rda*. Proses enkripi berjalan dengan baik.



Gambar 4. Proses enkripsi *File*



SURAT PERNYATAAN AHLI WARIS

Kami yang bertandatangan dibawah ini, adalah ahli waris dari Almarhum ZAWAWIH menerangkan dengan sesungguhnya dan sanggup disangkat sumpah bahwa Almarhum ZAWAWIH bertempat tinggal terakhir di Jalan Kebon Kelapa RT. 005 RW. 11 Kelurahan Grogol Selatan, Kecamatan Kebayoran Lama, Kota Administrasi Jakarta Selatan, telah meninggal dunia di Jakarta pada tanggal 15 Februari 2014 berdasarkan Surat Akta Kematian Nomor : 3174-KM-05032020-0039.

Almarhum ZAWAWIH, semasa hidupnya menikah satu kali yaitu dengan almarhumah HUSNAH yang telah meninggal dunia di Jakarta pada tanggal 12 Februari 2020, berdasarkan Akta Kematian Nomor : 3174-KM-20022020-0035, dari perkawinan Almarhum tersebut telah dikaruniai 4 (empat) orang anak :

1. Nama : ACHMAD BAIDOWI
   Tempat tanggal lahir : Jakarta, 17 Maret 1987
   Nomor KTP : 3174051703870003
   Alamat : Jl. Kebon Kelapa RT. 005 RW. 11 Kelurahan Grogol Selatan Kec. Kebayoran Lama, Kota Adm. Jakarta Selatan
2. Nama : RIZKI SAVITRI
   Tempat tanggal lahir : Jakarta, 03 Mei 1989
   Nomor KTP : 3174054305890003
   Alamat : Kp. Bintaro RT. 007 RW. 01 Kelurahan Pesanggrahan Kec. Pesanggrahan, Kota Adm. Jakarta Selatan
3. Nama : ARIP MAULANA
   Tempat tanggal lahir : Jakarta, 05 Oktober 1991
   Nomor KTP : 3174050510910002
   Alamat : Jl. Kebon Kelapa RT. 005 RW. 11 Kelurahan Grogol Selatan Kec. Kebayoran Lama, Kota Adm. Jakarta Selatan
4. Nama : SHOFWATUN NIDA
   Tempat tanggal lahir : Jakarta, 19 Juni 1993
   Nomor KTP : 3174055906930003
   Alamat : Jl. Kebon Kelapa RT. 005 RW. 11 Kelurahan Grogol Selatan Kec. Kebayoran Lama, Kota Adm. Jakarta Selatan

Bahwa nama-nama tersebut diatas adalah Ahli Waris yang sah dari Almarhum ZAWAWIH, dan tidak ada lagi Ahli Waris lainnya selain nama-nama tersebut.

Apabila dikemudian hari masih ada Ahli Waris lainnya selain nama tersebut diatas dan mempunyai bukti-bukti yang dianggap sah secara hukum, maka pernyataan ahli waris ini gugur dengan sendirinya dan Ahli Waris yang menandatangani surat pernyataan ini, akan bertanggung jawab sepenuhnya serta bersedia menerima resiko apapun yang ditimbulkan olehnya, sesuai dengan hukum yang berlaku dan tidak melibatkan Ketua RT, Ketua RW maupun Aparat Kelurahan dan Kecamatan.

Demikian surat pernyataan Ahli Waris ini dibuat dengan sebenar-benarnya dalam keadaan sehat jasmani dan rohani tanpa dipengaruhi oleh pihak-pihak lain serta jika dikemudian hari terdapat kekeliruan, maka surat ini dapat diperbaiki sebagaimana mestinya dan penandatanganan Surat pernyataan oleh ahli waris ini tidak di hadapan Aparat Kelurahan/Kecamatan.

Jakarta, 26 Desember 2022
Para Ahli Waris Almarhum ZAWAWIH,

1. ACHMAD BAIDOWI
2. RIZKI SAVITRI
3. AREP MAULANA
4. SHOFWATUN NIDA

Gambar 5. Data Sebelum dienkripsi

Gambar 6. Hasil Enkripsi *File*

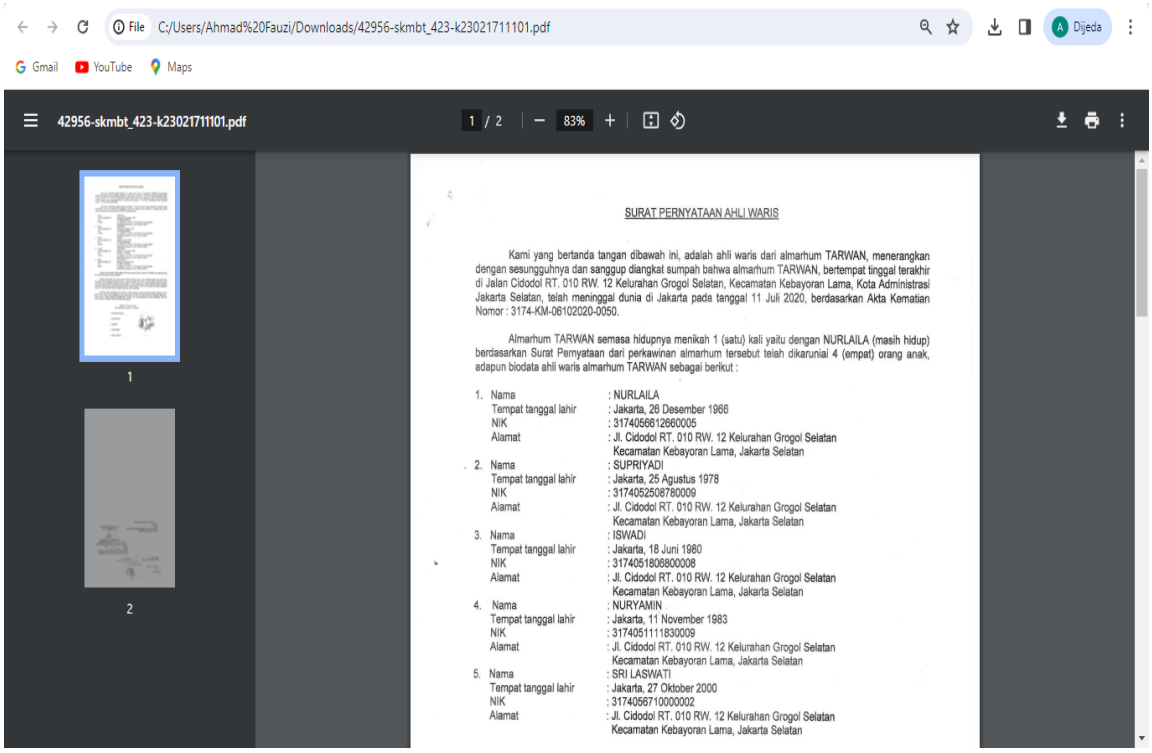
3.1.2 Proses Dekripsi

Selama tahap dekripsi *file* ini, Anda tidak akan dapat mengakses program sampai Anda masuk ke akun admin Anda. Gambar 7 menunjukkan, *administrator* akan mendekripsi *file* dengan memilih *file* statusnya enkripsi dan menekan *button* dekripsi. Seperti yang ditunjukkan pada Gambar 8, pengekripsi *file* data ahli waris dari Kelurahan Grogol Selatan dilakukan dengan menggunakan *password* yang sama. Sedangkan yang ditunjukkan pada Gambar 9, Hasil dekripsi *file* data ahli waris dari Kelurahan Grogol Selatan menunjukkan data asli *file* data ahli waris dari Kelurahan Grogol Selatan setelah pengisian *password* yang tepat.

No	Nama File	Nama File Enkripsi	Path File	Status File	Opsi
1	42956-skmbt_423-k23021711101.pdf	32860-skmbt_423-k23021711101.rda	file_encrypt/32860-skmbt_423-k23021711101.rda	Enkripsi	Dekripsi

Gambar 7. *List File* Terenkripsi

Gambar 8. Proses Dekripsi *File*



Gambar 9. Hasil Dekripsi *File*

3.2 Hasil Pengujian

Rancangan berikut diuji untuk menu dan kecepatan enkripsi dan dekripsi menggunakan *black box*, seperti yang dilakukan pada versi sebelumnya. Salah satu tujuan pengujian fungsional aplikasi berikut, untuk membuktikan bahwa aplikasi tersebut berfungsi sebanding atas perincian fungsional yang sudah ditentukan sebelumnya.

Table 1. Pengujian Fungsional Aplikasi

No.	Desain Proses	Hasil yang diperkirakan	Hasil Tes	Hasil Akhir
1.	Di *sidebar*, klik pada menu enkripsi.	Halaman dengan *form* enkripsi muncul.	Seperti yang diharapkan	*User* dapat mengisi formulir yang tersedia pada halaman enkripsi setelah mengeklik opsi enkripsi.
2.	Klik tombol enkripsi	Berhasil mengenkripsi *file*	Sesuai harapan	Data akan dienkripsi
3.	Di *sidebar*, pilih menu dekripsi.	Muncul tabel *list file* yang sudah di enkripsi dan juga di dekripsi	Sesuai harapan	Jika pengguna memilih opsi dekripsi, mereka akan menemui daftar tabel *file*.
4.	Klik pada tombol dekripsi	Akan muncul halaman untuk dekripsi *file*	Sesuai harapan	Jika pengguna mengeklik tombol "dekripsi" di tabel, halaman akan dibuka untuk melakukan dekripsi *file*.
5.	Klik tombol untuk mendekripsi *file*.	Mendekripsi *file* dengan sukses	Seperti yang diharapkan	Data bakal didekripsi

Metode *black box* digunakan untuk menguji *file* dari Kelurahan Grogol Selatan. Ini menghitung lamanya proses enkripsi dan dekripsi, serta ukuran *file* setelah program dienkripsi dan didekripsi. Faktanya bahwa *file* berukuran sekitar 2,788 kilobyte, untuk prosesnya membutuhkan waktu sekitar 70.37 detik untuk hasil enkripsinya, dan 68.81 detik untuk dekripsi ditunjukkan dalam tabel hasil pengujian *file*nya. *File* berukuran rata-rata 547 kilobyte memerlukan waktu enkripsi rata-rata 14.21 detik, dan dekripsi rata-rata 13.46 detik. Hasil pengujian data ahli waris dari Kelurahan Grogol Selatan yang dienkripsi dan didekripsi ditunjukkan dalam Tabel 2.

Table 2. Hasil Pengujian *File*

Nama *File*	Ukuran *File* (Kilobyte)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
SKMBT_423K23011115260	708 KB	707.214 KB	708 KB	17.61	18.42
SKMBT_423K23011911390	723 KB	722.731 KB	723 KB	18.97	18.28
SKMBT_423K23020211130	2,788 KB	2787.51 KB	2,788 KB	70.37	68.81
SKMBT_423K23020313370	661 KB	660.046 KB	661 KB	16.28	16.3
SKMBT_423K23021313550	547 KB	546.924 KB	547 KB	14.21	13.46
SKMBT_423K23021711101	610 KB	609.356 KB	610 KB	16.16	16.56
SKMBT_423K23021711120	685 KB	684.829 KB	685 KB	17.66	17.99
SKMBT_423K23051309181	810 KB	809.248 KB	810 KB	19.84	21.08
SKMBT_423K23051309210	791 KB	790.777 KB	791 KB	22.38	19.47
SKMBT_423K23051309240	861 KB	860.924 KB	861 KB	21.1	22.65

4. KESIMPULAN

Penulis dapat mencapai kesimpulan berikut setelah menyelesaikan proses pembuatan program web yang memungkinkan enkripsi dan dekripsi *file* serta mengevaluasi masalah yang disebutkan sebelumnya. Dengan

demikian, dapat disimpulkan bahwa program ini berhasil mencapai tujuan utamanya, yaitu menjaga data ahli waris Kelurahan Grogol Selatan aman. Algoritme *AES-128* meminimalkan kemungkinan penyalahgunaan oleh pihak yang tidak berwenang dan memastikan *file* ahli waris aman. Oleh karena itu, program ini sangat aman untuk mengamankan dan mengembalikan data ahli waris, serta membantu pihak kelurahan. Selain itu, program ini dapat mengambil data dalam berbagai format, termasuk *teks, pdf, word, dan excel*.

5. DAFTAR PUSTAKA

[1] A. Eka Putri, A. Kartikadewi, and L. A. Abdul 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," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[2] 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.

[3] T. H. Saputro *et al.*, "Survei tentang algoritma kriptografi asimetris," pp. 67–72, 2019.

[4] M. Fajar, A. B. Kambodji, and I. A. Musdar, "Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle," *J. Algoritm.*, vol. 20, no. 2, pp. 398–409, 2023, doi: 10.33364/algoritma/v.20-2.1466.

[5] 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.

[6] R. Parlika, T. A. Nisaa', S. M. Ningrum, and B. A. Haque, "Studi Literatur Kekurangan Dan Kelebihan Pengujian Black Box," *Teknomatika*, vol. 10, no. 02, pp. 131–140, 2020.

[7] N. W. Rahadi and C. Vikasari, "Pengujian Software Aplikasi Perawatan Barang Milik Negara Menggunakan Metode Black Box Testing Equivalence Partitions," vol. 11, no. 01, pp. 57–61, 2020, doi: 10.35970/infotekmesin.v11i1.124.

[8] T. F. A.-K. . Nabila Oper, Sabri Balafif, "MODIFIKASI ALGORITMA KRIPTOGRAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE," vol. 4, no. 3, pp. 179–184, 2022.

[9] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. Faizal Prianggara, and M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digit. Transform. Technol.*, vol. Vol.03, no. No.1, pp. 1–10, 2023, [Online]. Available: https://jurnal.itscience.org/index.php/digitech/article/view/2293.

[10] F. Ardianto and T. Fatimah, "PENERAPAN ALGORITMA KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN DATA PEGAWAI PADA PT MULTIJAYA IMPLEMENTATION OF AES-128 CRYPTOGRAPHIC ALGORITHM TO SECURE EMPLOYEE DATA AT PT MULTIJAYA SPARINDO," vol. 2, no. September, pp. 93–102, 2023.