Jurnal Tekno Insentif | Vol. 16 | No. 2 | Oktober 2022
DOI : https://doi.org/10.36787/jti.v16i2.852 Halaman 92 - 104

PENERAPAN METODE KRIPTOGRAFI AES UNTUK MENGAMANKAN FILE DOKUMEN

YUSUF JORDAN EL ANWAR[1], RONI HABIBI[2], NOVIANA RIZA[3]

[1,2,3]Politeknik Pos Indonesia, Indonesia
Email: 1184026@std.poltekpos.ac.id

ABSTRAK

Perkembangan ilmu pengetahuan dan teknologi pada era digital berkembang dengan sangat pesat. Keamanan file dokumen adalah salah satu dampak tersendiri dari datangnya era digital. Tentunya perusahaan x perlu memiliki keunggulan manajemen keamanan file yang efektif dalam menghadapi hal tersebut. Sangat disayangkan, perkembangan perusahaan x saat ini belum memiliki suatu media untuk melakukan pengamanan file dokumen. Oleh karena itu, tujuan utama penelitian ini adalah membuat model pengamanan file dokumen. Proses pengamanan file dokumen yang digunakan terdiri dari enkripsi dan dekripsi. Selanjutnya proses pengamanan file dokumen akan di implementasikan menggunakan pendekatan kriptografi dengan metode advanced encryption standard (aes). Tentunya pengamanan file dokumen perlu divisualisasikan secara realtime untuk dapat digunakan oleh perusahaan x untuk mengamankan file dokumen dengan cepat. Visualisasi hasil prediksi tersebut akan ditampilkan berbasis web base dengan bahasa pemrograman php.

Kata kunci: keamanan file, enkripsi, dekripsi, dokumen, kriptografi

ABSTRACT

The development of science and technology in the digital era is growing very rapidly. The security of document files is one of the impacts of the advent of the digital era. Of course company x needs to have an effective file security management advantage in dealing with this. Unfortunately, the development of company x currently does not have a media to protect document files. Therefore, the main purpose of this research is to create a document file security model. The process of securing document files used consists of encryption and decryption. Furthermore, the document file security process will be implemented using a cryptographic approach with the advanced encryption standard (AES) method. Of course, document file security needs to be visualized in real time to be used by company x to secure document files quickly. Visualization of the prediction results will be displayed based on a web base with the PHP programming language.

Keywords*: file security, encryption, decryption, document, cryptography*

1. PENDAHULUAN

Dokumen digital merupakan salah satu media untuk memberikan informasi baik informasi yang berbentuk tulisan, audio dan video untuk mempermudah manusia dalam berkomunikasi secara digital **(Hawa & Valiant Salomo, n.d.)**. Dengan adanya kemudahan tersebut banyak perusahaan yang beralih menggunakan dokumen digital untuk mengembangkan komunikasinya agar lebih cepat **(Amanuha et al., 2021)**. Disamping itu perusahaan dapat bertahan diera digital ini juga dapat dilihat bagaimana perusahaan memanfaatkan teknologi informasi **(Fardani et al., n.d.)**. Meskipun dengan menggunakan dokumen digital komunikasi menjadi lebih cepat ternyata tidak menjamin keamanan dokumen tersebut dari kejahatan siber **(Setyawati et al., 2021)**. Kejahatan siber adalah kejahatan yang dilakukan dengan cara menanamkan sebuah virus menggunakan teknik-teknik tertentu kedalam sistem atau perangkat lunak sehingga dokumen elektronik menjadi rusak dan tidak dapat digunakan **(Homepage et al., n.d.)**. Dengan adanya kejahatan siber dokumen elektronik perlu diamankan ketika disalurkan melalu internet supaya dokumen tidak rusak dan tidak dapat diakses oleh orang yang tidak memiliki akses untuk melihat dokumen tersebut **(Iswandari, 2021)**. Kritografi adalah metode pengamanan data agar data aman dari serangan kejahatan siber **(Maazouz et al., 2022)**. Kriptografi memiliki kunci dimana kunci tersebut digunakan sebagai kunci untuk mengamankan data ketika dienkripsi maupun dekripsi **(Daemen & Rijmen, n.d.)**. Didalam kriptografi data atau informasi yang dapat dibaca dengan jelas disebut *plaintext* dan data atau informasi yang tidak dapat dibaca dengan jelas disebut *chipertext* **(Rioja et al., 2021)**. Salah satu algoritma kriptografi yang saat ini masih dogunakan adalah algoritma kriptografi AES *(Advancen Encryption Standard)* **(Ibtihaji Ilham et al., 2021)**. Penggunaan metode kriptografi diatas ini didasarkan pada penelitian yang telah ada seperti pengunaan AES untuk mengamankan gambar **(Bal et al., 2021)**, mengamankan sebuah sistem **(Shahbazi et al., 2017)** dan mengamankan dari serangan injeksi **(Bedoui et al., 2022)**. Penelitian ini bertujuan untuk mejaga kerahasiaan data menggunakan AES pada pemrograman *php* dan menjaga kerahasiaan data dokumen elektronik dari proses distribusi data melalui media internet **(Kesuma et al., 2021)**. Dimana pada penelitian ini mengangkat teknik untuk mengamankan data dokumen eletronik menggunakan kriptografi saat sebuah perusahaan menyalurkan dokumennya melalui internet sehingga data dokumen tidak dapat dibaca oleh pengguna yang tidak memiliki akses **(Al-Shaarani & Gutub, 2021)**. Hal tersebut terjadi dikarenakan data telah dienkripsi dan meybabkan informasi menjadi sulit untuk diketahui pengguna yang tidak memiliki akses **(Thabit et al., 2021)**. Dengan pengamanan maka dokumen elektronik perusahaan terhindar dari pencurian data penting. Proses enkripsi pada penelitian ini menggunakan kombinasi algoritmat Md5 & AES yang menghasilkan chipertext **(Farisi, 2018)**. Dengan demikian penelitian ini tentang pengamanan dokumen elektronik menggunakan Md5 dan AES untuk enkripsi dan dekripsi data. Kombinasi ini diharapkan dapat memperkuat pengamanan data **(Az et al., 2021)** dari kejahatan siber berupa pencurian data yang bersifat rahasia, sehingga tidak dapat dipecahkan pengguna yang tidak memiliki akses terhadap data tersebut.

2. METODE

2.1 Identifikasi Masalah

Pada tahap ini peneliti melakukan magang ke perusahaan x untuk melakukan analisis bagaimana proses bisnis yang terjadi di dalam perusahaan. Selama pelaksanaan magang peneliti juga melakukan beberapa diskusi mengenai kendala apa saja yang menghambat proses bisnis perusahaan. Salah satu kendalanya adalah bagaimana cara perusahaan untuk

mengamankan dokumen. Kendala ini yang diangkat oleh peneliti menjadi topik yang akan dibahas didalam penelitian ini.

2.2 Studi Literatur

Setelah menentukan permasalahan didalam perusahaan yang dijadikan topik, selanjutnya peneliti mencoba untuk mencari jurnal, skripsi maupun buku yang memuat informasi bagaimana cara mengamankan surat. Dari beberapa jurnal dan buku yang telah peneliti analisis, peneliti kemudian menentukan Algoritma Kriptografi Advanced Encryption Standard (AES) untuk menyelesaikan permasalahan yang telah dirumuskan pada identifikasi masalah.

2.3 Pengumpulan Data

Tahapan selanjutnya adalah peneliti melakukan pengumpulan data. Tentunya data yang dikumpulkan merupakan data – data yang didapatkan dilapangan dan dapat dipublikasikan. Sehingga ketika data yang terdapat didalam penelitian ini juga dapat digunakan untuk penelitian yang selanjutnya. Data yang digunakan dalam penelitian ini adalah data dokumen perusahaan x.

2.4 Perancangan

Pada tahapan ini peneliti membuat rancangan untuk menentukan bagaimana desain sebuah aplikasi dan bagaimana aplikasi tersebut berjalan dan berinteraksi dengan pengguna

2.5 Implementasi

Setelah peneliti memahami bagaimana cara algortima ini bekerja, tahapan selanjutnya adalah bagaimana cara mengimplementasikan algoritma kedalam sistem. Karena algoritma ini tergolong rumit dan memakan waktu jika digunakan secara manual maka mengimplementasikan kedalam sebuah sistem adalah solusi agar algoritma ini dapat digunakan dengan mudah dan efisien. Sehingga meskipun tidak mengetahui bagaimana cara algoritma ini bekerja, perusahaan tetap dapat menggunakannya. Bahasa pemrograman php dipilih karena implementasi penelitian ini berupa sebuah website yang dapat digunakan dimana saja dan kapan saja.

2.7 Hasil dan Evaluasi

Hasil dari penelitian ini berupa sebuah aplikasi berbasis web untuk mengenkripsi dan mendekripsi berkas menggunakan metode aes serta laporan dan jurnal.

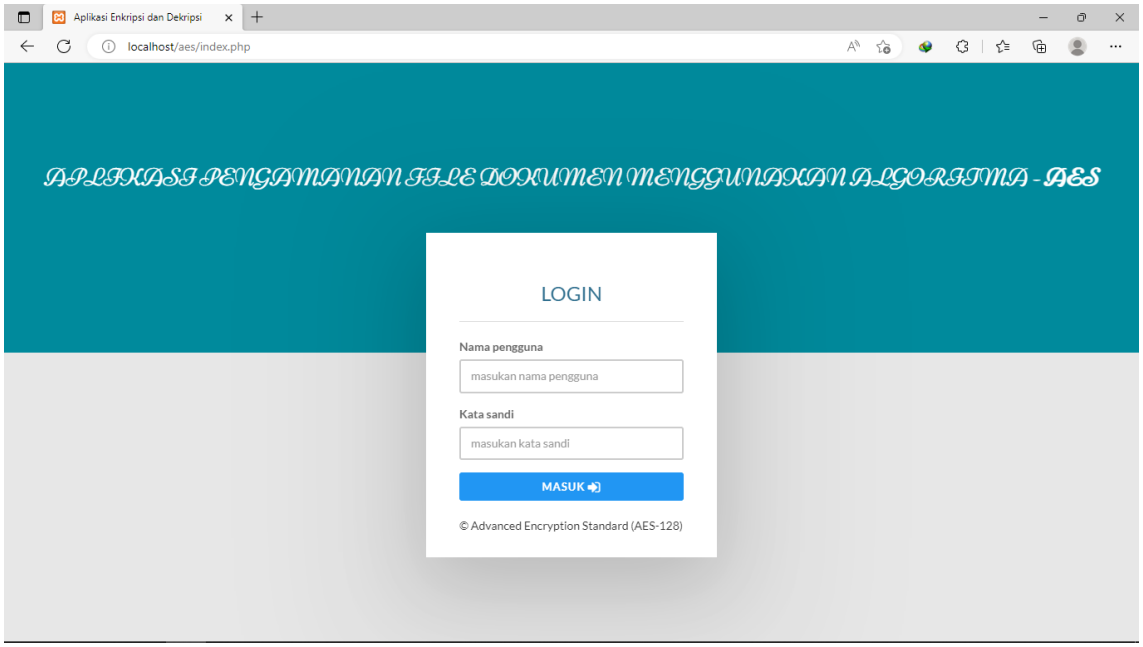
3. HASIL DAN PEMBAHASAN

3.1 Rancangan Prototype

Untuk hasil dari tahapan metode penelitian, penulis membuat prototype berupa sebuah website yang dapat digunakan untuk melakukan enkripsi dan dekripsi file dokumen. Website ini hanya dapat diakses melalui localhost dan dirancang menggunakan Bahasa pemrograman php.

3.1.1 Halaman Login

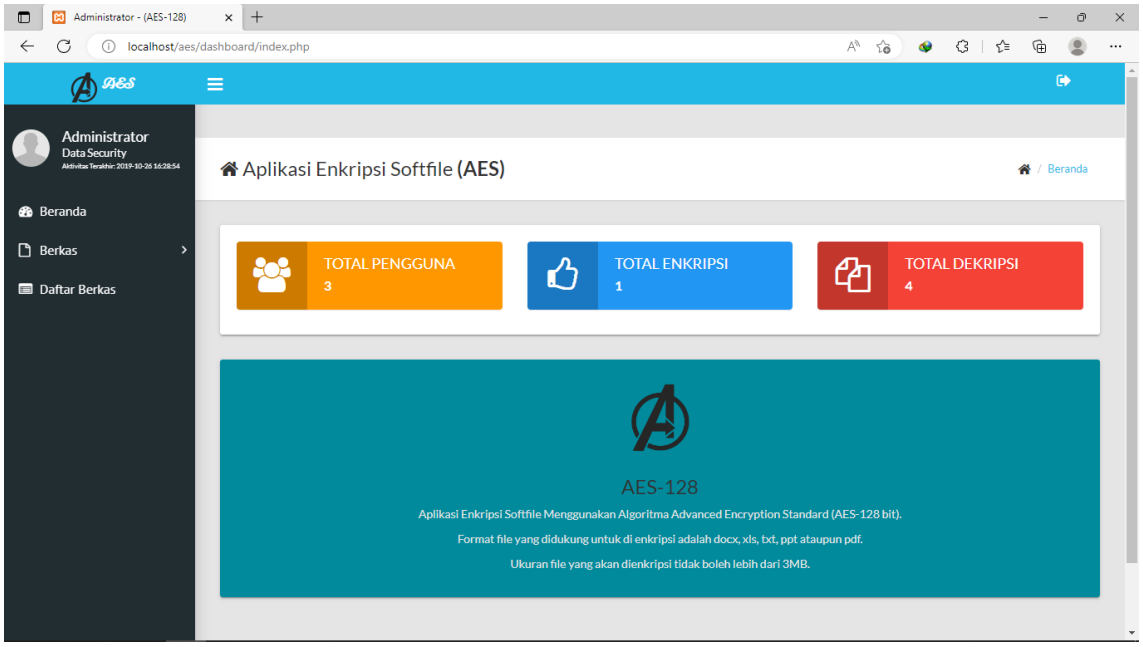
Pada halaman login ini. Pengguna harus masuk terlebih dahulu berdasarkan hak aksesnya. Di halaman login ini terdapat kolom input nama pengguna dan kata sandi.



Gambar 1. Halaman Login

3.1.2 Halaman Utama

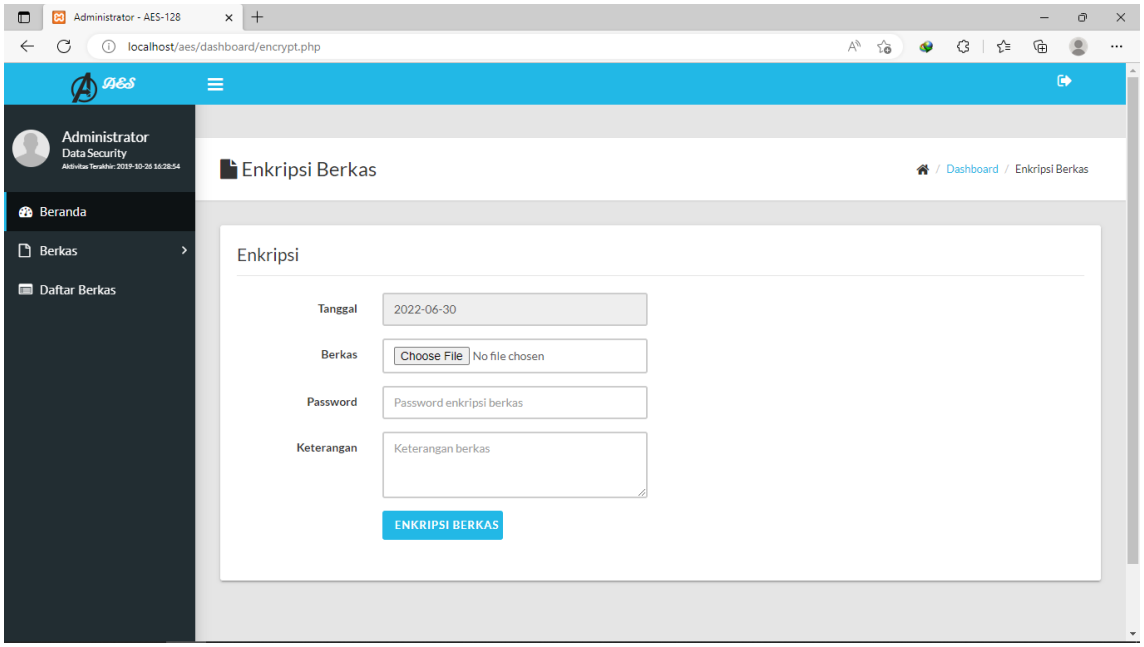
Pada halaman utama terdapat menu statistic mengenai informasi jumlah user yang terdaftar dan jumlah berapa banyak dokumen yang telah di enkripsi maupun dokumen yang telah di deskripsikan. Kemudian di sebelah kiri terdapat menu terdapat informasi user yang login, menu beranda, menu berkas dimana didalamnya terdapat sub menu enkripsi berkas dan dekripsi berkas dan terakhir adalah menu daftar berkas. Sedangkan di pojok kanan atas terdapat logo logout.



Gambar 2. Halaman Utama/Beranda

3.1.3 Halaman Enkripsi Berkas

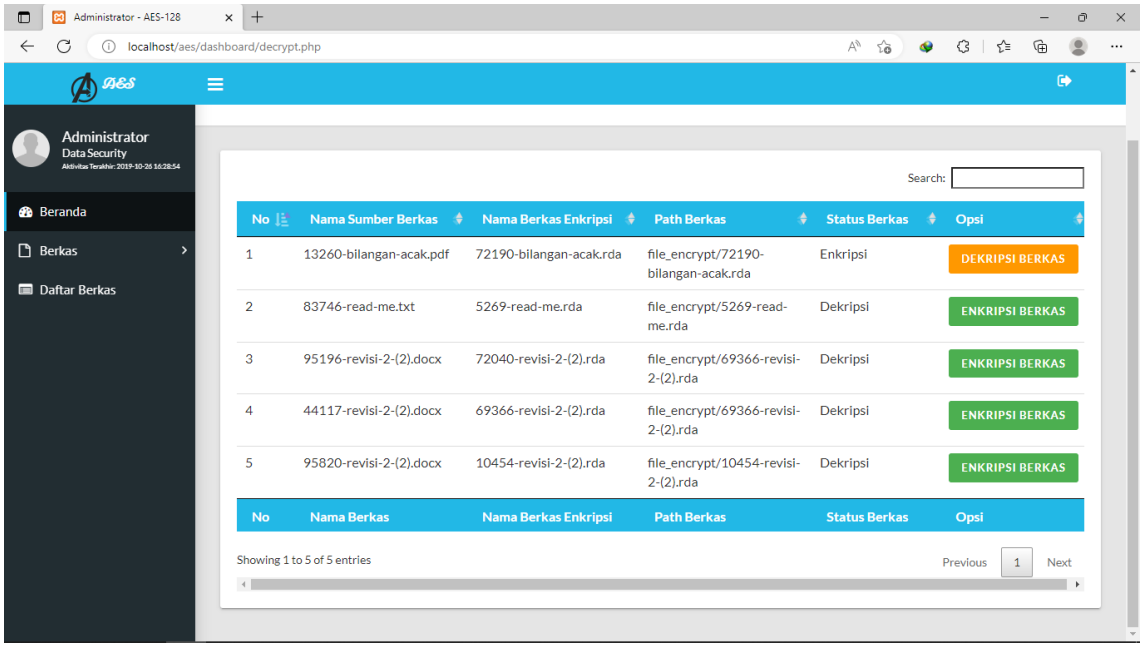
Pada halaman enkripsi berkas terdapat beberapa form inputan. Yang pertama form input tanggal yang akan terisi secara otomatis, kemudian form input berkas yang ingin di enkripsi dan jangan lupa untuk memberikan kunci untuk proses enkripsi dan keterangan.



Gambar 3. Halaman Enkripsi Berkas

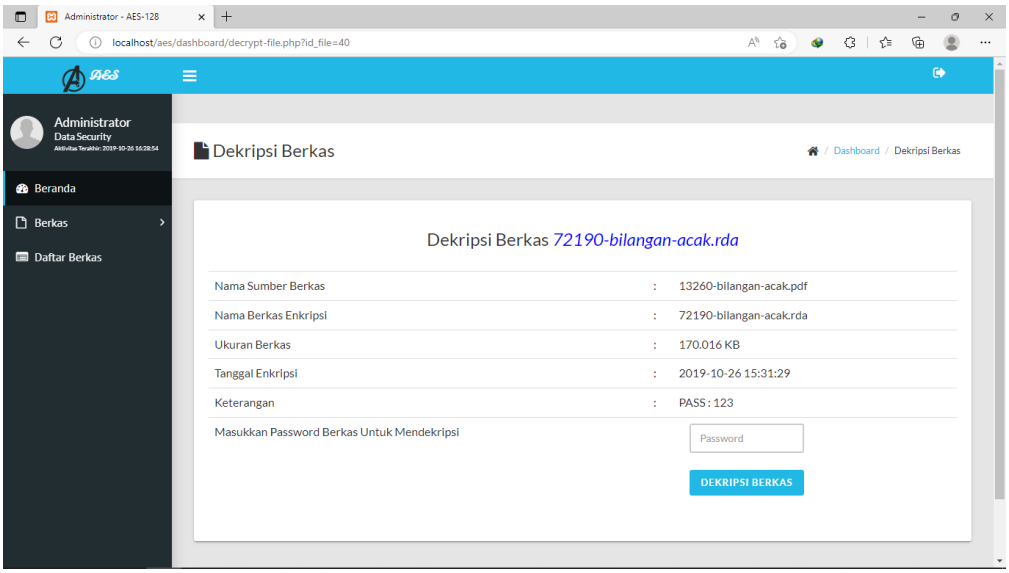
3.1.4 Halaman Dekripsi Berkas

Pada halaman dekripsi berkas akan ditampilkan table yang berisi informasi daftar berkas apa saja yang telah di enkripsikan dan status mengenai berkas. Apakah berkas sudah di dekripsikan atau masih terenkripsi.



Gambar 4. Halaman Dekripsi Berkas

Di dalam table terdapat tombol opsi. dimana jika keterangannya dekripsi berkas, maka ketika ditekan maka akan muncul halaman untuk mendekripsikan berkas. Pada halaman tersebut akan berisi mengenai informasi file yang terenkripsi dan terdapat form input key. Key yang dimasukan harus sama pada saat enkripsi.



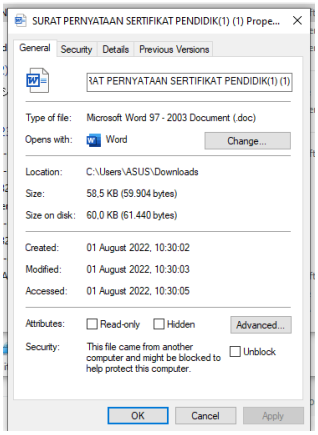
Gambar 5. Halaman Input Dekripsi Berkas

3.2 Pengujian Prototype

Setelah prototype dapat berfungsi, maka dilakukan pengujian untuk mengetahui apakah prototype dapat bekerja dengan baik atau tidak. Berikut ini adalah beberapa pengujian yang dilakukan

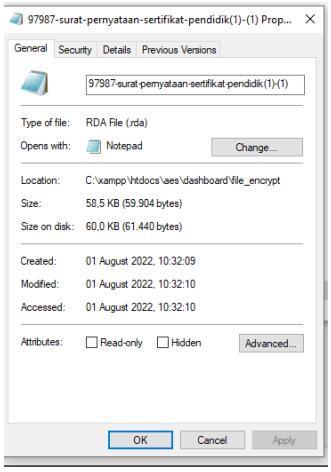
3.2.1 Ujicoba dengan menggunakan format file .doc

Pada ujicoba ini, digunakan sebuah file berformat .doc yang memiliki ukuran file sebesar 58,5 KB.



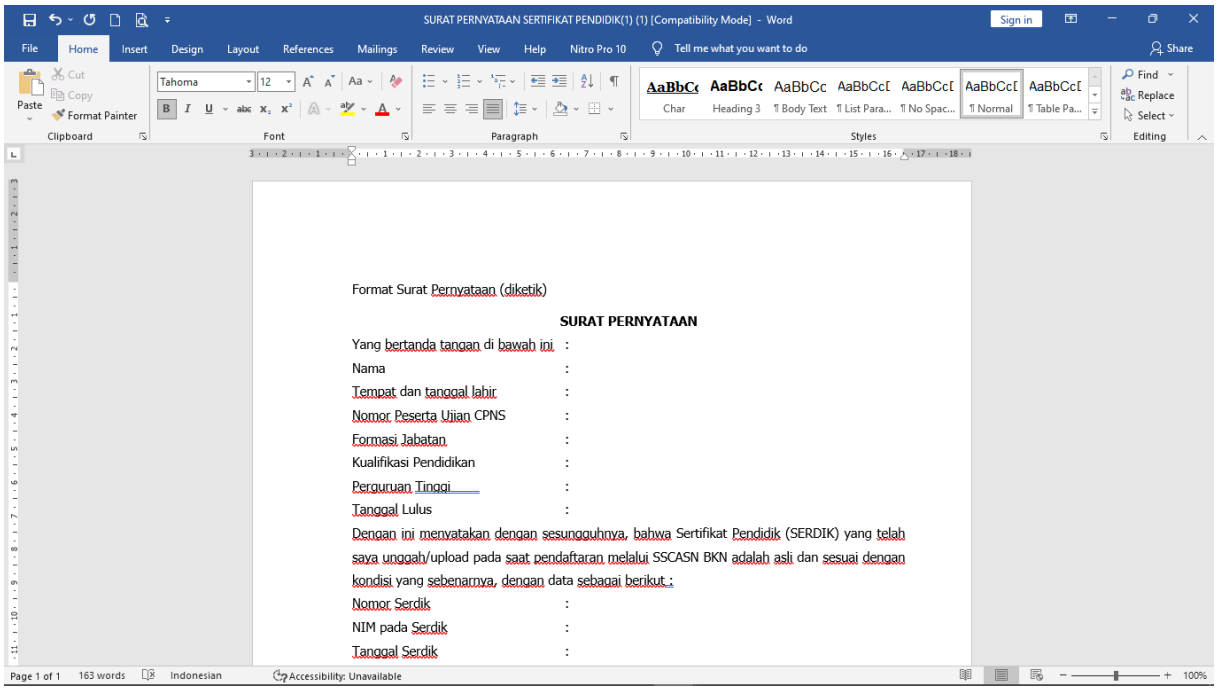
Gambar 6. Ujicoba File .doc

Maka setelah dilakukan enkripsi file akan berubah format menjadi rda dan ukuran file masih sama.

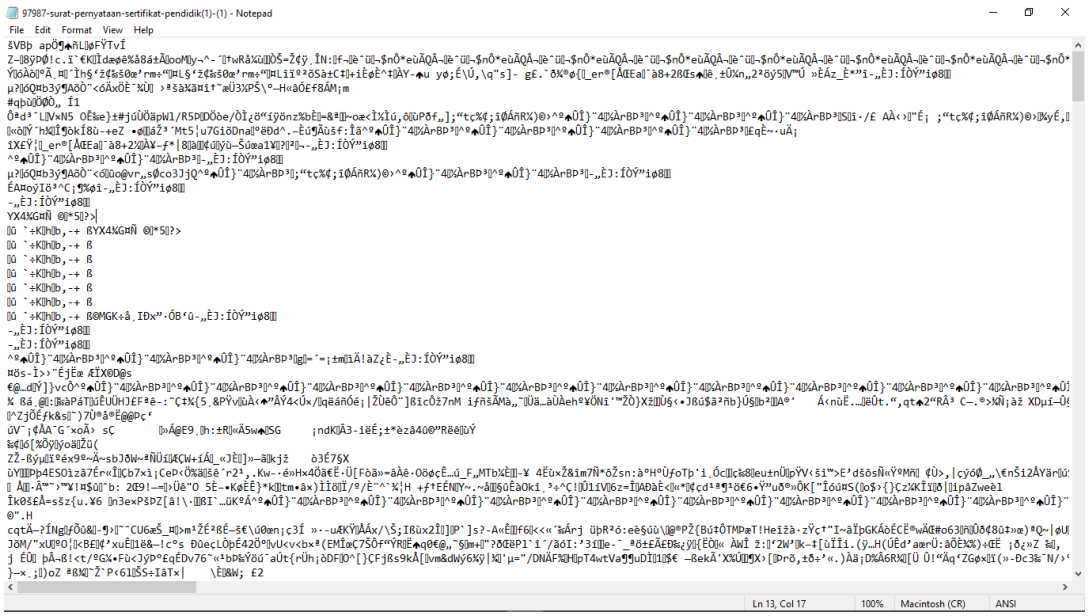


Gambar 7. Hasil Ujicoba File doc

Meskipun hanya berubah format dan ukuran filenya sama setelah dibuka maka file doc yang berisi berupa scan surat berubah menjadi file rda yang berisi karakter random.

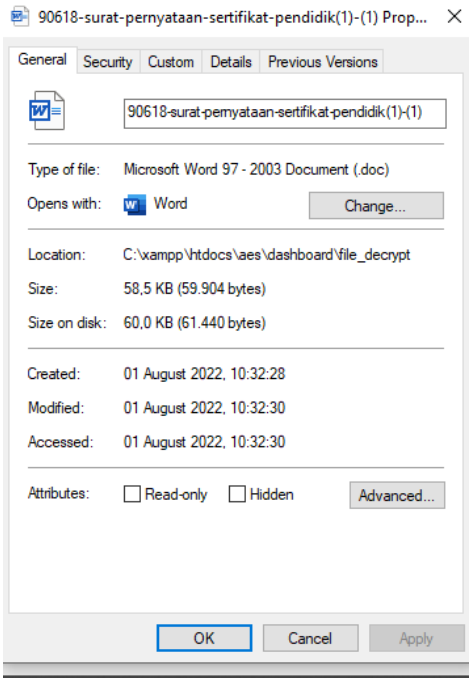


Gambar 8. File Doc Sebelum di Enkripsi

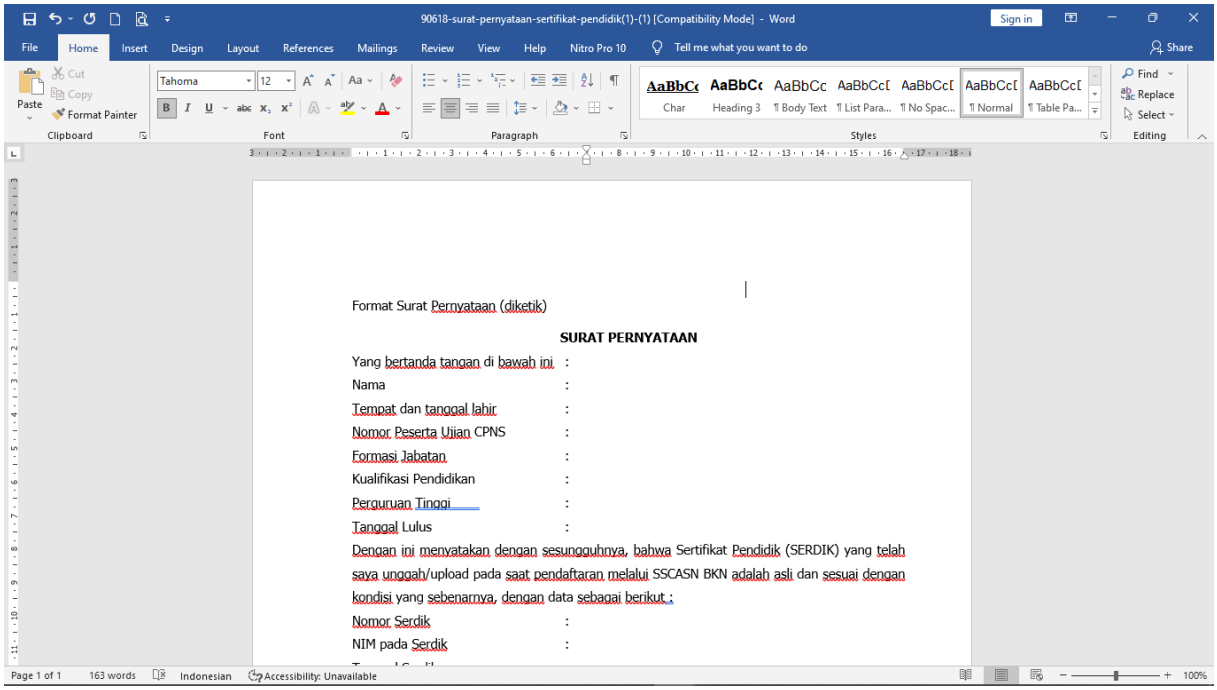


Gambar 9. File Doc Setelah Di Enkripsi

Kemudian Ketika file yang telah dienkripsikan dilakukan dekripsi file berubah menjadi seperti semula. Baik dari format, ukuran file dan isi file.



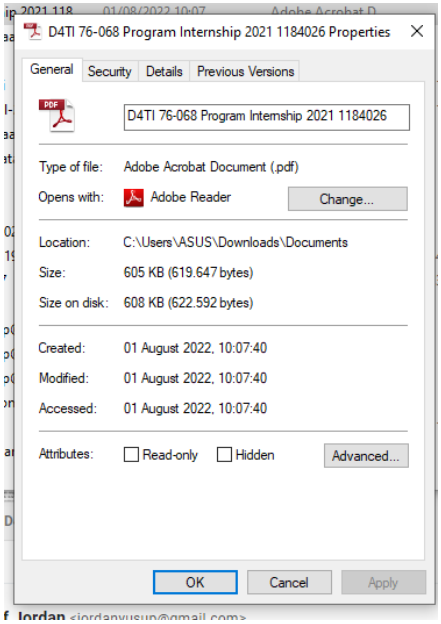
Gambar 10. File Dekripsi Ujicoba Doc



Gambar 11. Hasil Dekripsi Ujicoba Doc

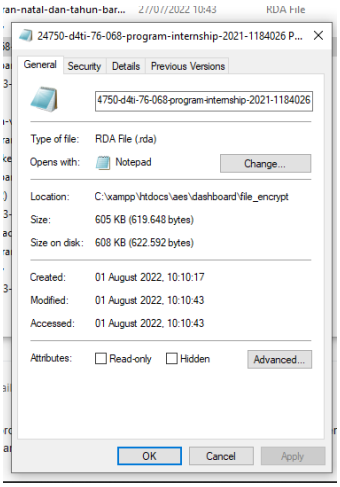
3.2.2 Ujicoba dengan menggunakan format file .pdf

Selanjutnya ujicoba menggunakan file dengan format pdf yang memiliki ukuran file sebesar 608KB



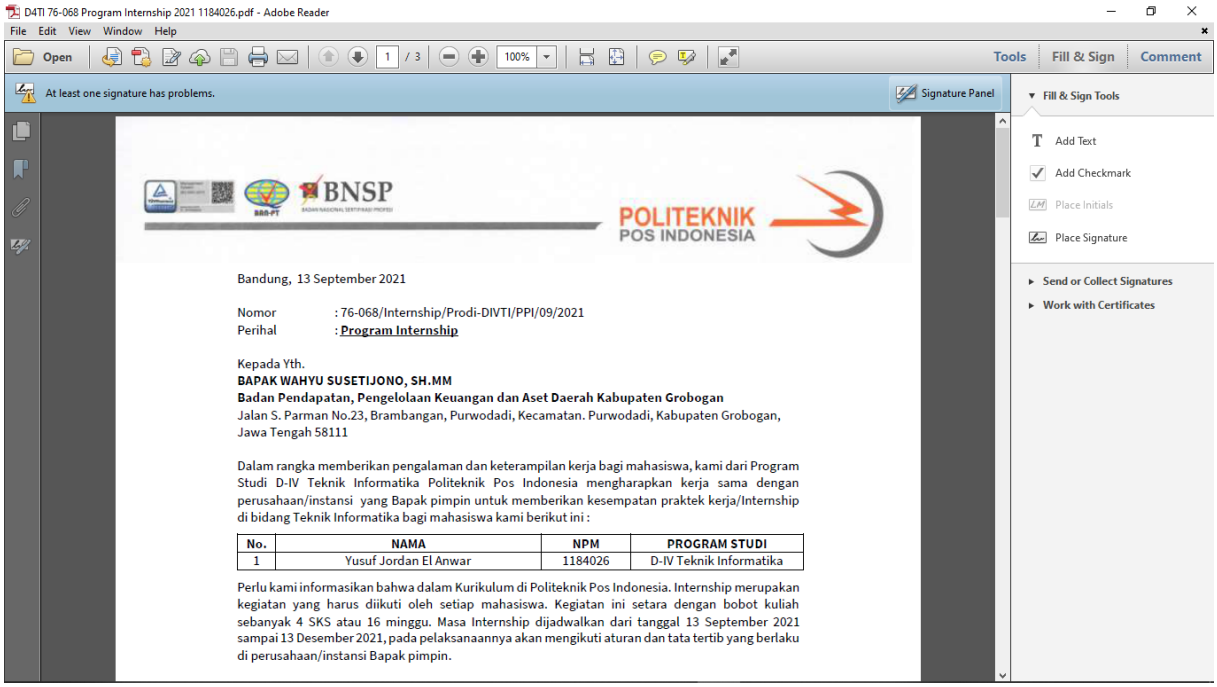
Gambar 12. Ujicoba File Pdf

Tidak jauh berbeda dengan ujicoba sebelumnya. Untuk file yang berubah hanyalah format file dari pdf menjadi rda dan ukuran file tidak berubah sedikitpun.



Gambar 13. Hasil Ujicoba File Pdf

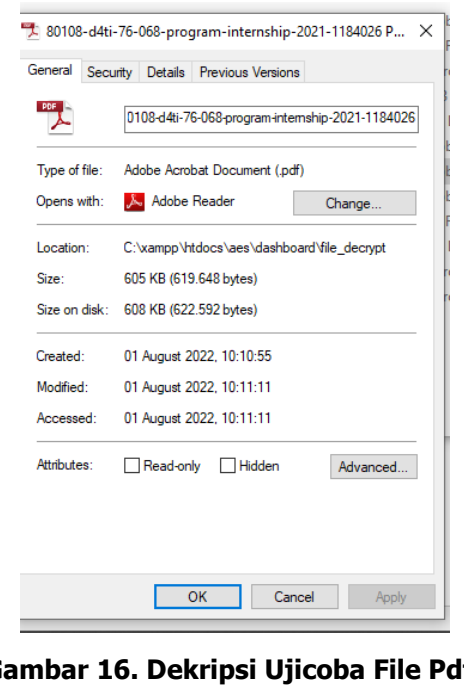
Meskipun hanya berubah format dan ukuran filenya sama setelah dibuka maka file pdf yang berisi berupa surat berubah menjadi file rda yang berisi karakter random.



Gambar 14. Isi File Ujicoba Pdf

Gambar 15. Hasil Ujicoba Pdf Setelah Enkripsi

Kemudian Ketika file yang telah dienkripsikan dilakukan dekripsi file berubah menjadi seperti semula. Baik dari format, ukuran file dan isi file.



Gambar 16. Dekripsi Ujicoba File Pdf

Gambar 17. Hasil Dekripsi Ujicoba File Pdf

4. KESIMPULAN

Berdasarkan studi literatur, analisis, perancangan dan implementasi, maka kesimpulan yang didapat adalah sebagai berikut:

1. Sistem pengamanan dokumen elektronik berbasis web dapat mengamankan dokumen elektronik
2. Sistem pengamanan dokumen elektronik berbasis web dapat mengenkripsi dan mendekripsi dokumen elektronik menggunakan metode kriptografi advanced encryption standard.

UCAPAN TERIMA KASIH

Terima kasih kepada Bapak Roni Habibi dan Ibu Noviana Riza selaku pembimbing Internal kampus yang berkenan membimbing ketika melaksanakan penelitian ini.

DAFTAR RUJUKAN

Al-Shaarani, F., & Gutub, A. (2021). Securing matrix counting-based secret-sharing involving crypto steganography. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.09.009

Amanuha, G., Hasanah, B., Sururi, A., & Sukendar, S. (2021). Digitalisasi Pemerintahan Melalui Implementasi SIMRAL dalam Mendukung Keberlanjutan Pembangunan Daerah. JURNAL TERAPAN PEMERINTAHAN MINANGKABAU, 1(2), 126–134. https://doi.org/10.33701/jtpm.v1i2.2086

Az, M., Pane, S. F., & Awangga, R. M. (2021). Cryptography: Cryptography: Perancangan Middleware Web Service Encryptor menggunakan Triple Key MD5. Base64, dan AES. Jurnal Tekno Insentif, 15(2), 65–75. https://doi.org/10.36787/jti.v15i1.497

Bal, S. N., Nayak, M. R., & Sarkar, S. K. (2021). On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. Journal of King Saud University - Computer and Information Sciences, 33(5), 552–561. https://doi.org/10.1016/j.jksuci.2018.04.006

Bedoui, M., Mestiri, H., Bouallegue, B., Hamdi, B., & Machhout, M. (2022). An improvement of both security and reliability for AES implementations. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.12.012

Daemen, J., & Rijmen, R. V. (n.d.). The Rijndael Block Cipher. http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

Fardani, I., Rochman, G. P., Akliyah, L. S., Burhanuddin, H., Bandung, U. I., & Kunci, K. (n.d.). DIGITALISASI DESA DI DESA CIKOLE LEMBANG (Vol. 5, Issue 2).

Farisi, A. (2018). Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone. In Maret (Vol. 4, Issue 2).

Hawa, P., & Valiant Salomo, R. (n.d.). READINESS OF DIGITALIZATION SERVICES FOR ELECTRONIC-BASED GOVERNMENT SYSTEMS IN AGENCY FOR THE ASSESSMENT AND APPLICATION OF TECHNOLOGY (BPPT). https://doi.org/10.33084/restorica.v5i2

Homepage, J., Ulfah, A. N., Lizarti, N., Sudyana, D., & Anam, M. K. (n.d.). J-PEMAS STMIK Amik Riau Pelatihan Secure Computer User Untuk Meningkatkan Kesadaran Siswa Terhadap Keamanan Data dan Informasi.

Ibtihaji Ilham, L., Pramita Widyassari, A., Sekolah Tinggi Teknologi Ronggolawe Cepu, ab, & Teknik Elektro, J. (2021). Pengembangan Aplikasi Pesan Instan Terenkripsi Menggunakan Algoritma Kriptografi AES (Advanced Encryption Standard). In Jurnal Teknik Elektro Smart) (Vol. 1, Issue 1).

Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. Jurnal Hukum Ius Quia Iustum, 28(1). https://doi.org/10.20885/iustum.vol28.iss1.art6

Kesuma, A. A. N. D. H., Budiartha, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik. Jurnal Preferensi Hukum, 2(2), 411–416. https://doi.org/10.22225/jph.2.2.3350.411-416

Maazouz, M., Toubal, A., Bengherbia, B., Houhou, O., & Batel, N. (2022). FPGA implementation of a chaos-based image encryption algorithm. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.12.022

Rioja, U., Batina, L., Flores, J. L., & Armendariz, I. (2021). Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis. Computer Networks, 198. https://doi.org/10.1016/j.comnet.2021.108405

Setyawati, E., Widjayanti, C. E., Siraiz, R. R., & Wijoyo, H. (2021). Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5. Jurnal Manajamen Informatika Jayakarta, 1(1), 56. https://doi.org/10.52362/jmijayakarta.v1i1.367

Shahbazi, K., Eshghi, M., & Faghih Mirzaee, R. (2017). Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5. Engineering Science and Technology, an International Journal, 20(4), 1308–1317. https://doi.org/10.1016/j.jestch.2017.07.002

Thabit, F., Alhomdy, A. P. S., Al-Ahdal, A. H. A., & Jagtap, P. D. S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91–99. https://doi.org/10.1016/j.gltp.2021.01.013