e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Comparison of the DES Cryptographic Algorithm and the AES Algorithm in Securing Document Files

Perbandingan Algoritma Kriptografi DES Dan Algoritma AES Dalam Pengamanan File Dokumen

Meli Suwarni [1)], Jusuf Wahyudi [2)], Khairil [3)]
[1,2,3)] ***Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu***
Email: [1)] melisuwarni05@gmail.com

How to Cite :
Suwarni, M., Wahyudi, J., Khairil. (2023). Comparison of the DES Cryptographic Algorithm and the AES Algorithm in Securing Document Files. Jurnal Media Computer Science, 2(1).

ARTICLE HISTORY
Received [01 Desember 2022]
Revised [27 Desember 2022]
Accepted [05 Januari 2023]

KEYWORDS
Perbandingan, Algoritma Kriptografi DES, Algoritma Kriptografi AES, File Dokumen

ABSTRAK

Aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu dibuat menggunakan bahasa pemrograman Visual Basic .Net. Pada aplikasi tersebut telah diterapkan 2 algoritma kriptografi yang dapat digunakan dalam mengamankan file dokumen khususnya file daftar pembayaran gaji pegawai yaitu algoritma DES dan algoritma AES. Selain itu pada aplikasi ini juga telah ditanamkan proses untuk menganalisis perbandingan algoritma DES dan AES, agar dapat diketahui algoritma mana yang lebih baik untuk digunakan. Adapun aspek perbandingan terdiri dari 2 aspek yaitu waktu proses dan ukuran file setelah proses. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu mampu melakukan proses enkripsi dan dekripsi file dokumen dan fungsional dari aplikasi telah berjalan sesuai harapan. Dari data uji yang telah dilakukan proses enkripsi dan dekripsi didapatkan hasil berdasarkan waktu proses enkripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES, berdasarkan waktu proses dekripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES, berdasarkan ukuran file setelah proses enkripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama, berdasarkan ukuran file setelah proses dekripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama

ABSTRACT

The document file security application at the Bengkulu City Education Office was made using the Visual Basic .Net programming language. In this application, 2 cryptographic algorithms have been implemented that can be used to secure document files, especially the employee payroll list file, namely the DES algorithm and the AES algorithm. In addition, this application has also embedded a process to analyze the comparison of the DES and AES algorithms, so that it can be known which algorithm is better to use. The comparison aspect consists of 2 aspects, namely processing time and file size after processing. Based on the tests that have been carried out, it can be concluded that the document file security application at the Bengkulu City Education Office is capable of carrying out the process of encrypting and decrypting document files and the functionality of the application has run as expected. From the test data that has been carried out by the encryption and decryption process, the results obtained based on the encryption processing time show that the AES algorithm is faster than the DES algorithm, based on

the decryption processing time it is found that the AES algorithm is faster than the DES algorithm, based on the file size after the encryption process it is found that the DES algorithm and the AES algorithm have the same file size, based on the file size after the decryption process it is found that the DES algorithm and the AES algorithm have the same file size.

PENDAHULUAN

Penerapan teknologi komputer sebagai salah satu media penyimpanan dan komunikasi menjadi suatu kebutuhan penting yang beruhubungan dengan sistem informasi. Berbagai macam data atau informasi yang diperoleh akan dimanfaatkan untuk berbagai kepentingan. Pertukaran data atau informasi sudah semakin mudah dilakukan dengan atau tanpa melalui media fisik.

Dalam proses pertukaran data atau informasi terdapat beberapa aspek penting yang perlu diperhatikan, yaitu: kerahasiaan, integritas data, autentikasi dan non repudiasi. Namun terkadang aspek tersebut kurang diperhatikan, sehingga memungkinkan adanya pencurian data. Oleh karena itu dibutuhkan suatu proses pengkodean data atau informasi sebelum dilakukan proses pengiriman. Sehingga data atau informasi yang dikirim terjaga kerahasiaannya dan tidak mudah untuk dapat mengubahnya.

Dinas Pendidikan Kota Bengkulu merupakan salah satu Instansi Pemerintah yang terdapat di Kota Bengkulu. Dinas Pendidikan Kota Bengkulu sudah memanfaatkan komputer sebagai media penyimpanan dan pengolahan data yang dilakukan baik yang bersifat terbuka maupun rahasia. Namun data-data yang telah diolah tersebut tidak sepenuhnya diberikan keamanan, karena selama ini pengamanan dilakukan hanya sebatas pemberian password login windows. Salah satu data yang sifatnya rahasia yaitu data daftar pembayaran gaji pegawai. Gaji pegawai tentunya sensitif karena pegawai satu tidak dapat mengetahui gaji pegawai lainnya.

Oleh karena itu dalam penelitian ini dilakukan pengamanan terhadap file daftar pembayaran gaji pegawai agar tidak dapat diakses oleh orang banyak. Walaupun file diperoleh, namun tidak dapat terbuka karena file tersebut telah dienkripsi menggunakan algoritma Kriptografi.

Algoritma kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data. Algoritma kriptografi terbagi menjadi 2 yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Algoritma DES dan AES termasuk ke dalam kriptografi modern dengan menggunakan kunci simetris. or kepastian, sehingga user atau pasien dapat memilih. kondisi sesuai gejala yang dialami dari penyakit bronkhitis.

LANDASAN TEORI

Kriptografi

Kriptografi merupakan seni dan ilmu dalam menciptakan sebuah sistem kripto yang mampu menyediakan keamanan informasi. Kriptografi berkaitan erat dengan pengamanan data digital. Ilmu ini terdiri dari mekanisme-mekanisme perancangan yang didasarkan pada algoritma-algoritma matematik yang menawarkan sejumlah layanan keamanan informasi fundamental (Siahaan & Sianipar, 2019)

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti dan hanya penerima yang dapat mengubah kode-kode tersebut menjadi pesan asli yang dapat dimengerti (Jamaludin & Romindo, 2020).

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas, dan autentikasi keaslian data. Dalam perkembangannya kriptografi juga digunakan untuk mengidentifikasi pesan tanda tangan digital dan keaslian pesan dengan sidik jari digital (fingerprint) (Mukhtar, 2018).

Algoritma DES

Penggunaan data sandi yang paling banyak didasarkan pada standard-standard data sandi (DES) yang diambil pada tahun 1977 oleh Standard-Standard Nasional Bureau, yang sekarang Institut Nasional Standard dan Tekhnologi (NIST), sebagai Standard Proses Informasi Umum. Untuk DES, data disandikan ke dalam 64 balok bit menggunakan 56 bit kunci. Transformasi algoritma 64 bitinput ke dalam satu serilangkah-langkah ke dalam 64 bitoutput. Langkah yang sama dengan kunci yang sama, digunakan untuk cadangan persandian (Adhar, 2019).

Algoritma Data Encryption Standard (DES) termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit dan mengenkripsikan 64 bit plainteks menjadi 64 bit cipher teks dengan menggunakan 56 bit kunci internal (internal key) atau up-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit (Adhar, 2019).

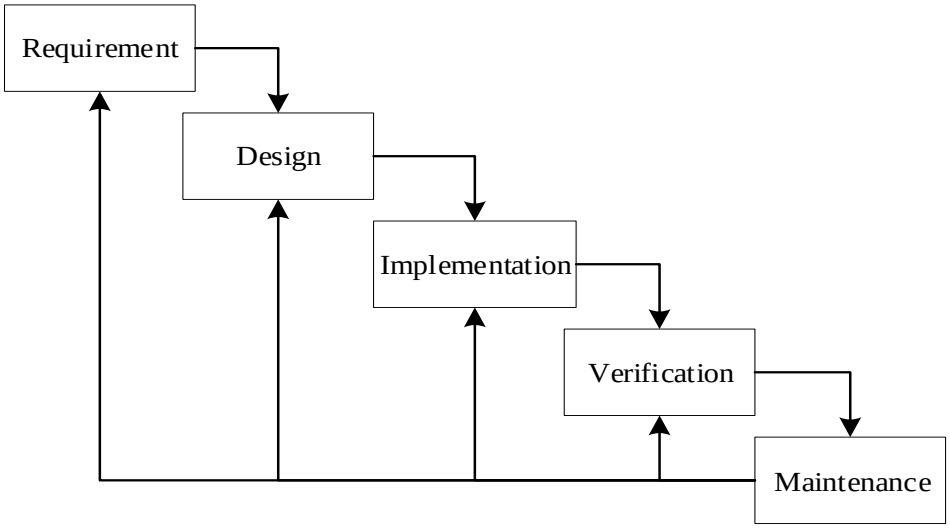
Algoritma AES

Algoritma AES merupakan standar pemrosesan informasi Federal Pemerintah Amerika Serikat yang digunakan untuk enkripsi simetris. Algoritma AES merupakan kombinasi dari suatu algoritma yang kuat dan kunci aman, di mana algoritma ini memiliki panjang kunci variabel seperti 128,192, dan 256 bit yang menghasilkan tingkat kecepatan dan keamanan. AES adalah Cipher blok simetris dengan 10 putaran untuk kunci 128-bit, 12 putaran dengan kunci 192-bit, dan juga 14 putaran untuk kunci 256-bit. Pada Gambar 4 dapat dilihat bagaimana alur diagram dari proses enkripsi dan dekripsi algoritma AES yang tidak dioptimalkan dengan 11 putaran. Proses enkripsi dengan menggunakan metode AES lebih cepat jika dibandingkan dengan DES, 3DES, CAST5, MARS, IDEA, Blowfish, dan RC6. Selain kecepatan, di dalam metode AES penggunaan memory pada proses enkrispi lebih ringan bila dibandingkan dengan ketujuh algoritma lainnya (Kirana & Sugianto, 2019).

Algoritma AES adalah algoritma kritografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut dengan round function. Round terakhir agak berbeda dengan round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns (Handoyo & Subakti, 2020).

METODE PENELITIAN

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode waterfall. Metode Waterfall memiliki tahapan-tahapan terlihat pada Gambar 1.



Gambar 1. Tahapan Metode *Waterfall*

Keterangan :

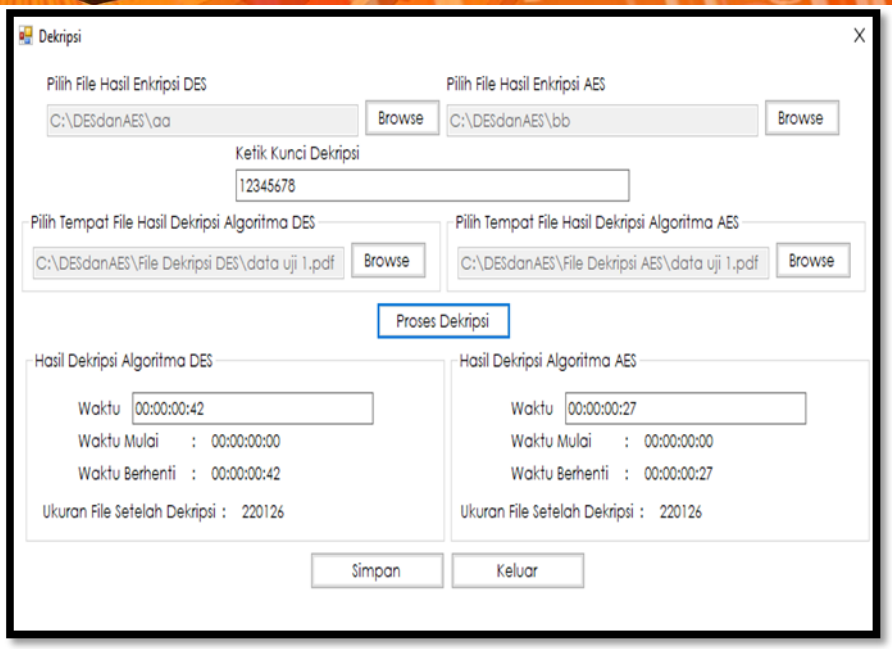
1) *Requirement analysis and definition*
   Pada tahap ini akan dilakukan analisis terhadap sistem yang akan dibuat berdasarkan kendala yang ditemukan, kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.
2) *System and software design*
   Pada tahap ini akan dilakukan perancangan sistem dengan mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.
3) *Implementation and unit testing*
   Pada tahap ini akan dilakukan realisasi terhadap perancangan perangkat lunak yang telah dibuat sebagai serangkaian program atau unit program. Kemudian dilakukan pengujian terhadap unit program tersebut.
4) *Integration and system testing*
   Pada tahap ini akan dilakukan penggabungan unit-unit program yang telah diuji sebagai sebuah sistem lengkap. Untuk memastikan apakah sesuai dengan kebutuhan, maka dilakukan pengujian perangkat lunak ke tempat penelitian.
5) *Operation and maintenance*
   Pada tahap ini akan dilakukan pengoperasian terhadap perangkat lunak dan melakukan perbaikan secara berkala untuk meningkatkan kinerja dari perangkat lunak tersebut.

HASIL DAN PEMBAHASAN

Adapun langkah proses enkripsi menggunakan algoritma AES antara lain :

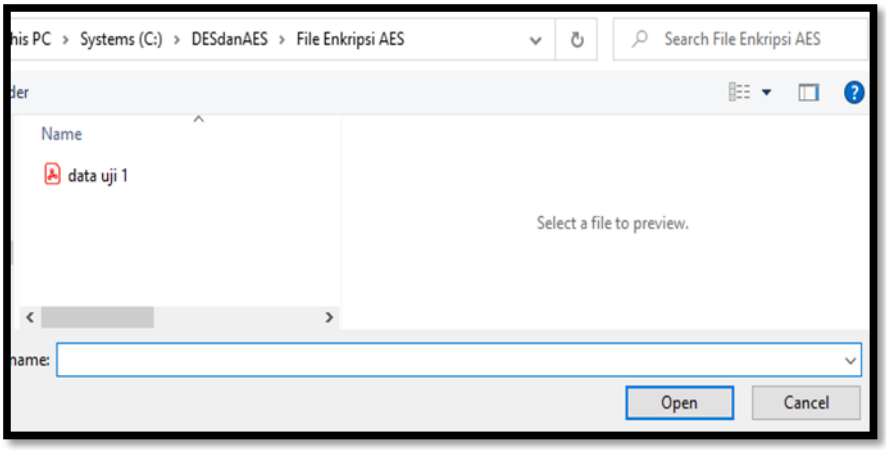
a) Membuka form dekripsi pada aplikasi, sehingga terdapat tampilan seperti Gambar 2

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE



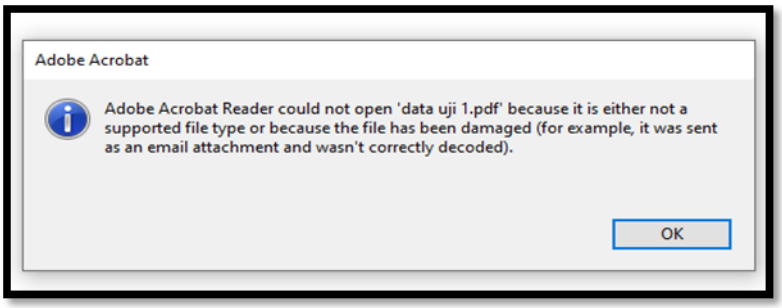
Gambar 2. Form Dekripsi

b) Memilih file dokumen yang terenkripsi, dengan klik tombol browse seperti Gambar 3.



Gambar 3. Memilih File Dokumen Yang Terenkripsi

c) Adapun isi file dokumen data uji 1 terenkripsi seperti Gambar 4

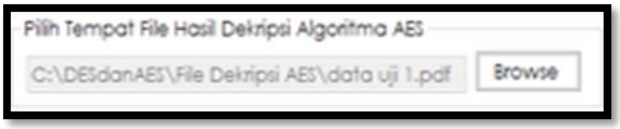


Gambar 4 Isi File Dokumen Terenkripsi

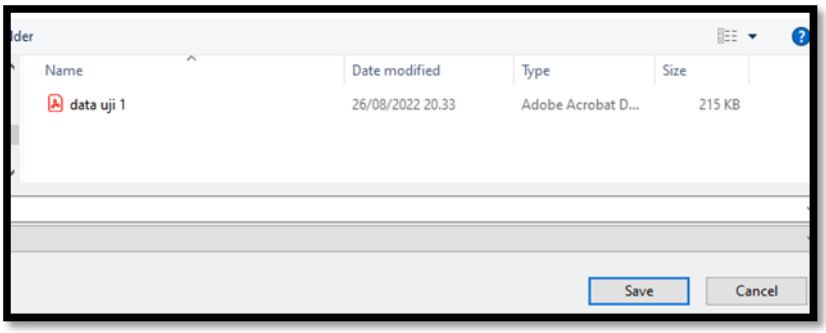
d) Masukkan kunci dekripsi yang digunakan untuk melakukan proses dekripsi file dokumen yang telah dipilih seperti Gambar 5.

Gambar 5. Kunci Dekripsi

e) Menjalankan proses dekripsi, dan menampilkan pesan seperti Gambar 4.34. untuk memilih tempat file baru yang sudah di dekripsi seperti Gambar 6



Gambar 6. Pilih Tempat Penyimpanan File Baru

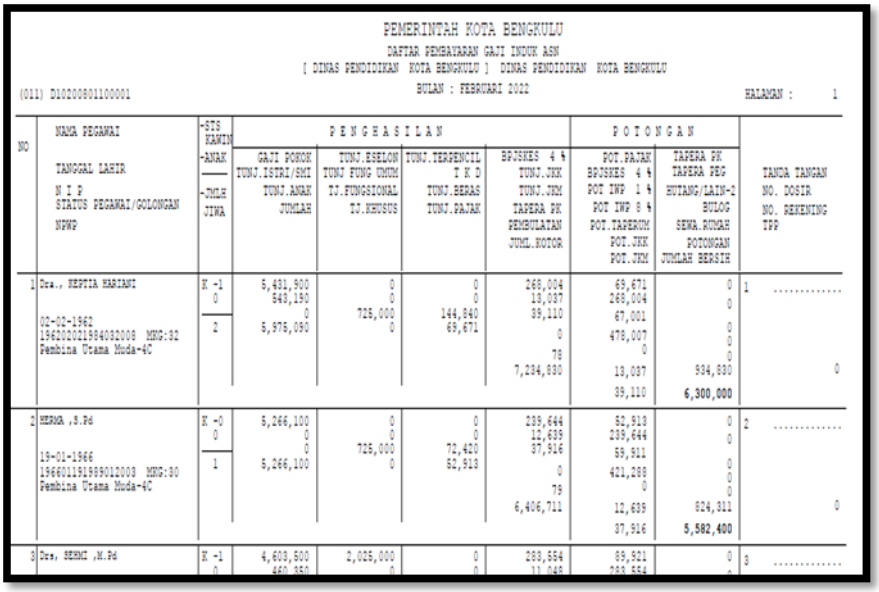


Gambar 7. Memilih Tempat File Baru

f) Setelah berhasil melakukan proses dekripsi, maka akan tampil informasi berupa waktu proses dan ukuran file setelah dekripsi seperti Gambar 8

Gambar 8. Informasi Waktu Proses dan Ukuran File Setelah Dekripsi

g) Adapun hasil file dokumen yang telah di enkripsi ketika dibuka, akan tampil seperti Gambar 9


PEMERINTAH KOTA BENGKULU

DAFTAR PEMBAYARAN GAJI INDUK ASN

[DINAS PENDIDIKAN KOTA BENGKULU] DINAS PENDIDIKAN KOTA BENGKULU

BULAN : FEBRUARI 2022

(011) D1020000100001 HALAMAN : 1

NO	NAMA PEGAWAI / TANGGAL LAHIR / N I P / STATUS PEGAWAI/GOLONGAN / NPWP	STS KAWIN -ANAK -JMLH JIWA	PENGHASILAN: GAJI POKOK TUNJ.ISTRI/SUI TUNJ.ANAK JUMLAH	TUNJ.ESELON TUNJ FUNG UMUM TJ.FUNGSIONAL TJ.KHUSUS	TUNJ.TERPENCIL T K D TUNJ.BERAS TUNJ.PAJAK	BPJSKES 4 % TUNJ.JKK TUNJ.JKM TAPERA PK PEMULATAN JUML.KOTOR	POTONGAN: POT.PAJAK BPJSKES 4 % POT JHT 2 % POT JHT 8 % POT.TAPERUM POT.JKK POT.JKM	TAPERA PK TAPERA PEG HUTANG/LAIN-2 BULOG SEWA.RUMAH POTONGAN JUMLAH BERSIH	TANDA TANGAN NO. DOSIR NO. REKENING TPP
1	Dra., HEPTIA HARIANI 02-02-1962 196202021984032008 MKG:32 Pembina Utama Muda-4C	K -1 0 2	5,401,800 948,190 0 6,976,090	0 0 725,000 0	0 0 144,840 69,671	268,004 13,087 39,110 0 78 7,234,830	69,671 268,004 67,001 478,007 0 13,087 39,110	0 0 0 0 0 934,830 **6,300,000**	1 0
2	HERWA ,S.Pd 19-01-1966 196601191989012003 MKG:30 Pembina Utama Muda-4C	K -0 0 1	5,266,100 0 0 5,266,100	0 0 725,000 0	0 0 72,420 62,913	239,644 12,639 37,916 0 79 6,406,711	62,913 239,644 69,911 421,288 0 12,639 37,916	0 0 0 0 0 824,311 **5,582,400**	2 0
3	Drs, SEKMI ,M.Pd	K -1 0	4,603,800 460,380	2,025,000 0	0 0	283,654 11,048	69,921 283,654	0 0	3 .....

Gambar 9. Hasil Dekripsi File Dokumen

Pengujian Sistem

Pengujian aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu menggunakan metode black box. Adapun hasil pengujian metode black box, seperti Tabel 4.6.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Tabel 1 Hasil Pengujian Metode Black Box

No.	Komponen Yang Diuji	Skenario Pengujian	Hasil Pengujian
1.	Form Enkripsi	Melakukan proses enkripsi menggunakan algoritma DES	Sistem berhasil melakukan proses enkripsi menggunakan algoritma DES
		Melakukan proses enkripsi menggunakan algoritma AES	Sistem berhasil melakukan proses enkripsi menggunakan algoritma AES
2.	Form Deskripsi	Melakukan proses dekripsi menggunakan algoritma DES	Sistem berhasil melakukan proses dekripsi menggunakan algoritma DES
		Melakukan proses dekripsi menggunakan algoritma AES	Sistem berhasil melakukan proses dekripsi menggunakan algoritma AES

Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu mampu melakukan proses enkripsi dan dekripsi file dokumen dan fungsional dari aplikasi telah berjalan sesuai harapan. Selain itu, dari data uji yang telah dilakukan proses enkripsi dan dekripsi didapatkan hasil :

a) Berdasarkan waktu proses enkripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES
b) Berdasarkan waktu proses dekripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES
c) Berdasarkan ukuran file setelah proses enkripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama
d) Berdasarkan ukuran file setelah proses dekripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama

KESIMPULAN DAN SARAN

Kesimpulan

1. Aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu dibuat menggunakan bahasa pemrograman Visual Basic .Net. Pada aplikasi tersebut telah diterapkan 2 algoritma kriptografi yang dapat digunakan dalam mengamankan file dokumen khususnya file daftar pembayaran gaji pegawai yaitu algoritma DES dan algoritma AES.
2. Selain itu pada aplikasi ini juga telah ditanamkan proses untuk menganalisis perbandingan algoritma DES dan AES, agar dapat diketahui algoritma mana yang lebih baik untuk digunakan. Adapun aspek perbandingan terdiri dari 2 aspek yaitu waktu proses dan ukuran file setelah proses.
3. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi keamanan file dokumen di Dinas Pendidikan Kota Bengkulu mampu melakukan proses enkripsi dan dekripsi file dokumen dan fungsional dari aplikasi telah berjalan sesuai harapan.
4. Dari data uji yang telah dilakukan proses enkripsi dan dekripsi didapatkan hasil :
   a. Berdasarkan waktu proses enkripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES
   b. Berdasarkan waktu proses dekripsi didapatkan bahwa algoritma AES lebih cepat dibandingkan dengan algoritma DES
   c. Berdasarkan ukuran file setelah proses enkripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama

d. Berdasarkan ukuran file setelah proses dekripsi didapatkan bahwa algoritma DES dan algoritma AES memiliki ukuran file yang sama

Saran

Berdasarkan kesimpulan, maka penulis menyarankan untuk memilih algoritma AES dalam proses enkripsi dan dekripsi karena memiliki waktu yang lebih cepat dibandingkan dengan algoritma DES

DAFTAR PUSTAKA

Adhar, D., 2019. Implementasi Algoritma DES (Data Encryption Satandard) Pada Enkripsi dan Dekripsi SMS Berbasis Android. Jurnal Teknik Informatika Kaputama (JTIK), Volume Vol.3 No.2 p-ISSN. 2548-9704.

Blazing, A., 2018. Pemrograman Windows Dengan Visual Basic .Net : Praktikum Pemrograman VB.Net. s.l.:Google Book.

Budiarto, E., 2017. Pembuatan Aplikasi Web Berbasis SMS Sebagai Media Penyalur Informasi dan Komunikasi Antara Sekolah Dengan Orang Tua Siswa. Junal Ilmiah Pendidikan Teknik Kejuruan (JIPTEK) Vol.X No.1 Januari 2017.

Handoyo, J. & Subakti, Y. M., 2020. Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal Sistem Informasi dan Teknologi (SITECH), Volume Vol. 3 No.2 e-ISSN:2622-2973.

Indrajani., 2017. Database Design Theory, Practice, and Case Study. Jakarta: PT. Elex Media Komputindo.

Jamaludin & Romindo, 2020. Kriptografi : Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA. Medan: Yayasan Kita Menulis.

Kirana, C. & Sugianto, E., 2019. Penerapan Algoritma AES dan Konversi SMS Ke Dalam Bahasa Khek Pada Aplikasi Enkripsi Berbasis Mobile Application. Jurnal Ilmu Komputer dan Informatika (Khazanah Informatika), Volume Vol.5 No.1 ISSN:2621-038X.

Lasminiasih, 2016. Perancangan Sistem Informasi Kredit Mikro Mahasiswa Berbasis Web. Jurnal Sistem Informasi (JSI) Vol.8 No.1 April 2016 ISSN : 2085-1588.

Mukhtar, H., 2018. Kriptografi Untuk Keamanan Data. Yogyakarta: Deepublish.

Purba, D. F. & Puspasari, R., 2020. Penerapan Algoritma Rail Fence Unutk Penghasil Pesan Rahasia Berbasis Android. Jurnal FTIK, Volume Vol.1 No.1.

Rusmala & Prasti, D., 2019. Implementasi Metode Rail Fence Chiper dan Row Transposition Chiper Pada Mata Kuliah Kriptografi. Jurnal Ilmiah d'Computare , Volume Vol.9.

Siahaan, V. & Sianipar, R. H., 2019. Database Dan Kriptografi Menggunakan Java/MySQL. Yogyakarta: Sparta Publishing.

Simbolon, I. A. R. et al., 2020. Penerapan Algoritma AES 128-bit Dalam Pengamanan Data Kependudukan Pada Dinas Dukcapil Kota Pematangsiantar. Journal Of Computer System and Informatics (JoSYC), Volume Vol.1 No.2 e-ISSN:2714-8912.