

IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK ENKRIPSI DAN DEKRIPSI FILE

Aji Teguh Utomo^{1*}, Rizky Pradana^{2*}

^{1,2}Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*}ajiteguhutomo@yahoo.com, ²rizky.pradana@budiluhur.ac.id

(* : corresponding author)

Abstrak-Pada era industri 4.0 yang menggambarkan tren yang berkembang saat ini tentang transformasi digital, dan kemajuan sistem informasi. Keamanan data dan informasi sangat penting bagi pengguna internet saat ini. Kasus penyadapan pesan atau informasi adalah salah satu kasus yang paling merusak, dan keamanan harus diperkuat karena hal ini dapat terjadi. Hal tersebut merupakan latar belakang dibuatnya aplikasi ini. Pada hal ini saya akan coba untuk melakukan penerapan pada perusahaan tempat saya berkerja PT. Supra Primatama Nusantara (Biznet Networks), tepatnya di Biznet Network Head Office (Jakarta Pusat). PT. Supra Primatama Nusantara, lebih dikenal sebagai Biznet Networks, adalah perusahaan infrastruktur digital terintegrasi Indonesia yang menyediakan layanan internet, data center, cloud computing dan IPTV. Berdasarkan analisa masalah yang akan dilakukan oleh peneliti adalah terkait keamanan data file. Baik itu data pelanggan, data teknis pembangunan, data maintenance jaringan, dll. Salah satu cara untuk meningkatkan keamanan data atau file anda adalah dengan menggunakan metode enkripsi dengan metode yang diusulkan yaitu kriptografi dengan algoritma AES-128. Saat ini keamanan informasi ini memerlukan perhatian khusus, sehingga penelitian ini akan menjadi implementasi kriptografi dari algoritma AES-128 untuk enkripsi dan dekripsi data dalam format file. Penelitian ini di implementasikan dalam bentuk aplikasi berbasis web dengan menggunakan bahasa pemrograman PHP dan database MySQL. Memungkinkan pengguna untuk melindungi file data sensitif di mana data dienkripsi dan hanya data terenkripsi yang dapat didekripsi atau dibuka kembali oleh staff Biznet. Beberapa hasil pengujian pada aplikasi ini berhasil melakukan enkripsi dan dekripsi berbagai file contohnya dengan ekstensi .txt, .docx, .xls, .ppt, .jpg, dan lain-lain. Tujuan aplikasi ini di buat agar dapat memberikan keamanan lebih terhadap isi data file yang bersifat rahasia tanpa takut adanya pihak lain yang tidak bertanggung jawab. Uji coba aplikasi dilakukan dengan melakukan enkripsi dan dekripsi file dengan format .txt, .docx, .doc, .xlsx dengan penjian waktu enkripsi dan dekripsi menggunakan fungsi microtime. Hasil dari enkripsi file .txt (size 1KB) 0.02 Detik, .doc (size 53KB) 4.01 Detik, .docx (size 77KB) 5.66 Detik, .xlsx (size 232KB) 16.98 Detik. Sedangkan untuk dekripsi file .txt (size 1KB) 0.02 Detik, .doc (size 53KB) 3.92 Detik, .docx (size 77KB) 5.64 Detik, .xlsx (size 232KB) 16.98 Detik. Kesimpulan dari enkripsi dan dekripsi file AES-128 yaitu semakin besar file yang di enkripsi dan di dekripsi maka akan semakin lama proses.

Kata Kunci: kriptografi, advance encryption standard, keamanan, enkripsi file, dekripsi file

IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM FOR FILE ENCRYPTION AND DECRYPTION

Abstract-In the industrial era 4.0 which describes the current developing trends regarding digital transformation, and the advancement of information systems. Data and information security is very important for today's internet users. The case of eavesdropping on messages or information is one of the most damaging cases, and security must be strengthened because this can happen. This is the background for making this application. In this case, I will try to apply it to the company where I work, PT. Supra Primatama Nusantara (Biznet Networks), to be precise at Biznet Network Head Office (Central Jakarta). PT. Supra Primatama Nusantara, better known as Biznet Networks, is an Indonesian integrated digital infrastructure company that provides internet, data center, cloud computing and IPTV services. Based on the analysis of the problem that will be carried out by the researcher is related to the security of the data file. Be it customer data, technical development data, network maintenance data, etc. One way to increase the security of your data or files is to use the encryption method with the proposed method, namely cryptography with the AES-128 algorithm. Currently this information security requires special attention, so this research will be a cryptographic implementation of the AES-128 algorithm for encryption and decryption of data in file format. This research is implemented in the form of a web-based application using the PHP programming language and MySQL database. Allows users to protect sensitive data files where data is encrypted and only encrypted data can be decrypted or reopened by Biznet staff. Some test results on this application successfully encrypt and decrypt various files, for example with the extension .txt, .docx, .xls, .ppt, .jpg, and others. The purpose of this application is to be able to provide more security for the contents of confidential data files without fear of other parties who are not responsible. Application testing is done by encrypting and decrypting files in .txt, .docx, .doc, .xlsx formats with encryption and decryption time assessment using the microtime function. The result of file encryption is .txt (size 1KB) 0.02 Seconds, .doc (size 53KB) 4.01 Seconds, .docx (size 77KB) 5.66 Seconds, .xlsx (size 232KB) 16.98 Seconds. As for the decryption of .txt files (size 1KB) 0.02 seconds, .doc (size 53KB) 3.92 seconds, .docx (size 77KB) 5.64 seconds, .xlsx (size 232KB) 16.98 seconds. The conclusion of AES-128 file encryption and decryption is that the larger the encrypted and decrypted file, the longer the process.

Keywords : cryptography, advanced encryption standard, security, file encryption, file decryption

1. PENDAHULUAN

Keamanan data dan informasi sangat penting bagi pengguna internet saat ini. Kasus penyadapan pesan atau informasi adalah salah satu kasus yang paling merusak, dan keamanan harus diperkuat karena hal ini dapat terjadi.

Beberapa permasalahan yang menarik seperti keamanan data file menjadi fokus utama dalam penelitian ini. Seperti misalnya data informasi pelanggan biznet, data teknis pembangunan jaringan biznet, dan data lainnya bisa terjaga keamanannya agar kedepannya tidak ada pihak yang bertanggung jawab atas penyertaan atau modifikasi data. Untuk menangani masalah ini perlu adanya suatu sistem keamanan yang bisa membantu untuk meng-enkripsi dan men-dekripsi data file.

Salah satu cara untuk meningkatkan keamanan data atau file Anda yaitu menggunakan metode enkripsi. Kriptografi adalah ilmu yang mempelajari teknik kriptografi di mana *plaintext* (naskah asli) diacak dengan kunci enkripsi, sehingga mengubah naskah menjadi *ciphertext* (naskah teracak) yang sulit dibaca oleh orang lain tanpa kunci dekripsi. Cipher dibagi menjadi dua jenis: klasik dan modern. Kriptografi klasik bekerja dalam mode karakter, menggunakan abjad (A-Z), dan algoritma yang digunakan sederhana untuk memecahkan ciphertext dengan mudah, sedangkan algoritma modern bekerja pada bit biner (0 dan 1) yang terbentuk dari *ASCII* (*American Standard Code for Information Interchange*) membuat kunci sangat kompleks sehingga menjadi sulit untuk mendapatkan ciphertext tanpa mengetahui kuncinya.

Kunci kriptografi dibagi menjadi kunci simetris dan asimetris. Algoritma enkripsi simetris menggunakan kunci yang sama untuk melakukan fungsi enkripsi dan dekripsi. Algoritma enkripsi asimetris, di sisi lain, menggunakan satu kunci untuk mengenkripsi data dan kunci lain untuk mendekripsi data. Salah satu skema kunci simetris adalah *Advanced Encryption Standard (AES)*, atau disebut Rijndael. *AES* merupakan algoritma enkripsi yang aman untuk melindungi data atau file dengan berbagai teknik enkripsi dan dekripsi. panjang kunci *AES* yaitu 128bit, 192bit, dan 256bit.

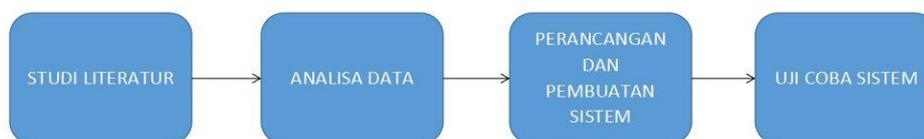
Dari uraian diatas, penulis membuat aplikasi kriptografi dengan menggunakan algoritma kriptografi *Advanced Encryption Standard (AES)* 128bit. Bahasa pemrograman yang digunakan yaitu PHP dengan output aplikasi web dan MySQL sebagai database. File yang di unggah untuk di enkripsi disimpan kedalam database. Dengan adanya aplikasi ini diharapkan dapat membantu pihak manajemen Biznet untuk menjaga keamanan data file.

Penelitian sebelumnya oleh Binanda Wicaksana1*, Ma'mun Setiawan2 [7], yang berjudul "Penerapan Algoritma *Advanced Encryption Standard (AES)* untuk Pengamanan Berkas Soal Ujian" dengan menggunakan algoritma *AES-128* berbasis desktop, sehingga dibuatlah aplikasi kriptografi *AES-128* berbasis web.

2. METODE PENELITIAN

2.1 Metode Penelitian

Langkah yang dilakukan dalam penelitian diawali dengan studi literatur tentang kriptografi, khususnya algoritma *AES*. Langkah selanjutnya adalah menganalisis data dan mempelajari apa yang dilakukan untuk keamanan data. Selanjutnya membuat rancangan aplikasi berdasarkan literature review dan analisis data untuk membuat aplikasi keamanan data berbasis web. Setelah aplikasi dibuat, sistem akan diuji. Fase-fase ini ditunjukkan pada Gambar 1.



Gambar 1. Metode Penelitian

2.2 Data Penelitian

Data yang digunakan dalam Implementasi Kriptografi merupakan data-data yang didapat dari tempat riset yaitu, data pelanggan internet biznet, data maintenance jaringan, data teknis pembangunan jaringan dan lainnya. Data ini merupakan data yang akan digunakan dalam pengujian implementasi kriptografi *AES-128*. Disini penulis merangkum data pelanggan, data maintenance, data pembangunan jaringan, dalam beberapa bentuk ekstensi file, Portable Document Format (.pdf), Text (.txt), Document (.docx), Gambar (.jpg), Powerpoint (.ppt), dan , Excel (.xls) untuk melakukan uji coba kriptografi *AES-128*.

2.3 Algoritma AES (*Advanced Encryption Standard*)

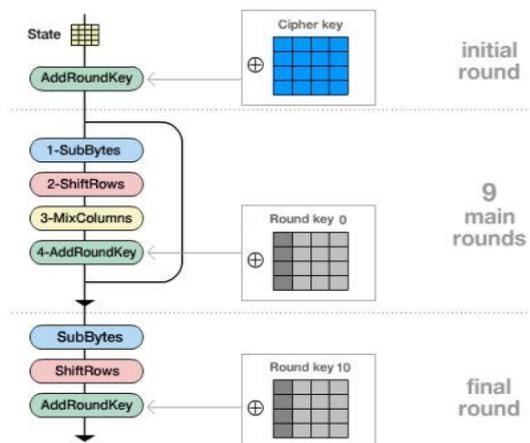
- a. *Advanced Encryption Standard (AES)* merupakan block cipher simetris. *AES* diterbitkan oleh Institut Standar dan Teknologi Nasional AS pada tahun 2001. *AES* diperkenalkan untuk menggantikan *DES* karena *DES* menggunakan kunci enkripsi yang sangat kecil dan algoritmanya lambat. Algoritma *AES* menggunakan plaintext 128bit dan kunci privat 128bit, yang bersama-sama membentuk blok 128bit yang digambarkan sebagai matriks persegi 4x4. Matriks persegi 4x4 ini adalah konversi pertama yang diterima. Langkah ini diikuti oleh 10 putaran. Diantaranya, 9 putaran meliputi tahapan sebagai berikut:
 - b. *Subbytes* : Gunakan S-Box untuk melakukan permutasi byte untuk seluruh blok matriks.
 - c. *Shift Rows* : Menggeser baris matriks.
 - d. *Mix Column* : Kolom matriks diacak dari kanan ke kiri.
 - e. *Add Round Key* : Di sini blok saat ini di-XOR dengan kunci yang diperluas.

10 putaran terakhir hanya berisi *subbyte*, menggeser baris dan menambahkan tahap kunci untuk menghasilkan 16 byte (128bit) *ciphertext*.

2.3.1 Proses Enkripsi AES-128

Berikut adalah ringkasan dari algoritma AES yang bekerja di blok 128bit menggunakan kunci 128bit (selain proses pembuatan round kunci).

1. *AddRoundKey* : XOR state awal (*plaintexts*) dengan *cipherkey*. Langkah ini disebut *initial round*.
2. Putaran sebanyak $N_r - 1$ kali. Langkah yang dilakukan dalam setiap putaran adalah :
 - a. *SubBytes* : Substitusi byte dengan S- box (tabel substitusi).
 - b. *ShiftRows* : Memindahkan baris *array state* dengan *wrapping*.
 - c. *MixColumns* : Acak data pada setiap kolom *state array*.
 - d. *AddRoundKey* : Melakukan XOR antara state saat ini dengan *round key*.
3. *Final round* : langkah putaran terakhir:
 - a. *SubBytes*
 - b. *ShiftRows*
 - c. *AddRoundKey*



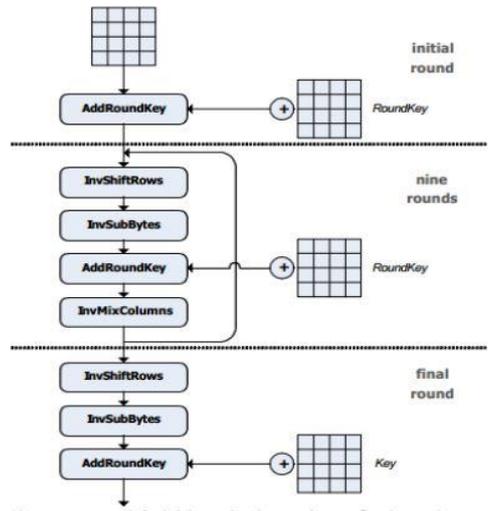
Gambar 2. Proses Enkripsi AES-128

2.3.2 Proses Dekripsi AES-128

Langkah dekripsi *AES*, juga dikenal sebagai *Invers Cipher* dari algoritma Rijndael, yang beroperasi blok 128bit dengan kunci 128bit, adalah :

- a. *InitialRound* : Tahap *AddRoundKey* yang melakukan XOR antara state awal (*ciphertext*) dan kunci enkripsi. Langkah ini juga disebut *InitialRound*.
- b. Putaran sebanyak $N_r - 1$ kali. Proses yang terjadi pada setiap putaran yaitu :
 - 1) *InvShiftRow* : Memindahkan baris *state array* dengan *wrapping*.
 - 2) *InvByteSub* : Substitusi byte dengan tabel substitusi kebalikan (*inverse S-box*).
 - 3) *AddRoundKey* : Yaitu XOR antara state saat ini dengan *round key*.

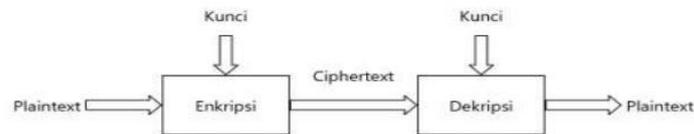
- 4) *InvMixColumn*: Acak data di setiap kolom *state array*.
- c. *Final Round* : Langkah untuk putaran terakhir :
 - 1) *InvShiftRow*,
 - 2) *InvByteSub*,
 - 3) *AddRoundKey*



Gambar 3. Proses Dekripsi AES-128

2.4 Skema Enkripsi dan Dekripsi

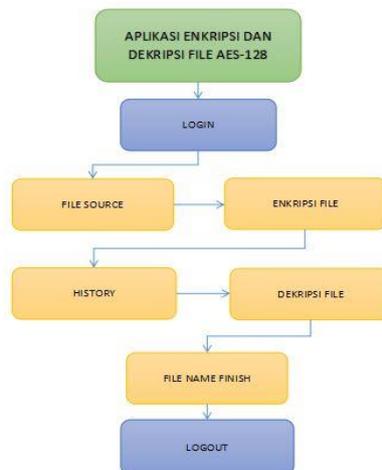
Berikut adalah gambaran dari proses enkripsi dan dekripsi.



Gambar 4. Skema Enkripsi dan Dekripsi AES-128

2.5 Rancangan Menu

Desain menu aplikasi Enkripsi dan Dekripsi File digunakan untuk memberikan deskripsi spesifik tentang alur proses yang dilalui pengguna dalam mengenkripsi, melihat riwayat, dan mendekripsi file. Desain menu untuk aplikasi dapat dilihat pada gambar desain menu yang dibuat di bawah ini.



Gambar 5. Rancangan Menu

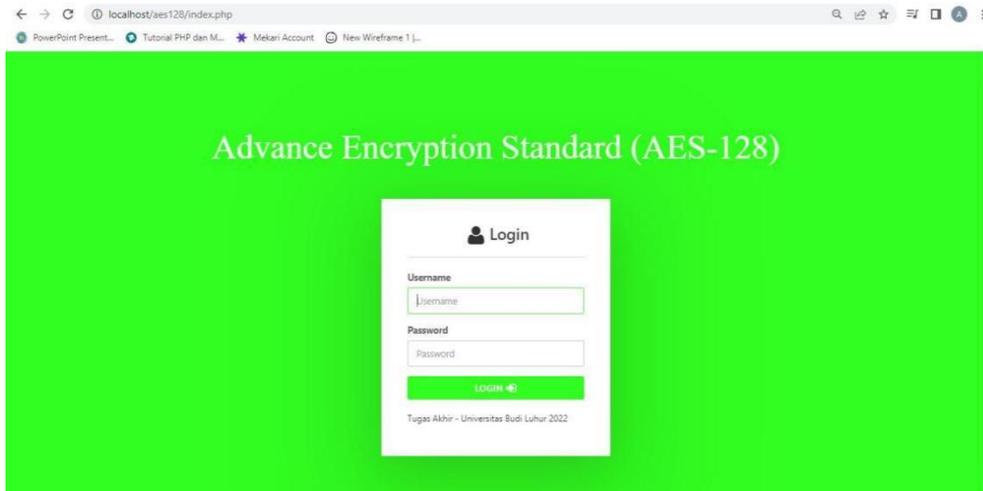
3. HASIL DAN PEMBAHASAN

Bagian ini berisi analisis, hasil implementasi, uji coba dan pembahasan topik penelitian. Bagian ini juga berisi uraian yang berupa uraian, gambar, tabel, dll.

3.1 Tampilan Layar

a. Tampilan Layar Login

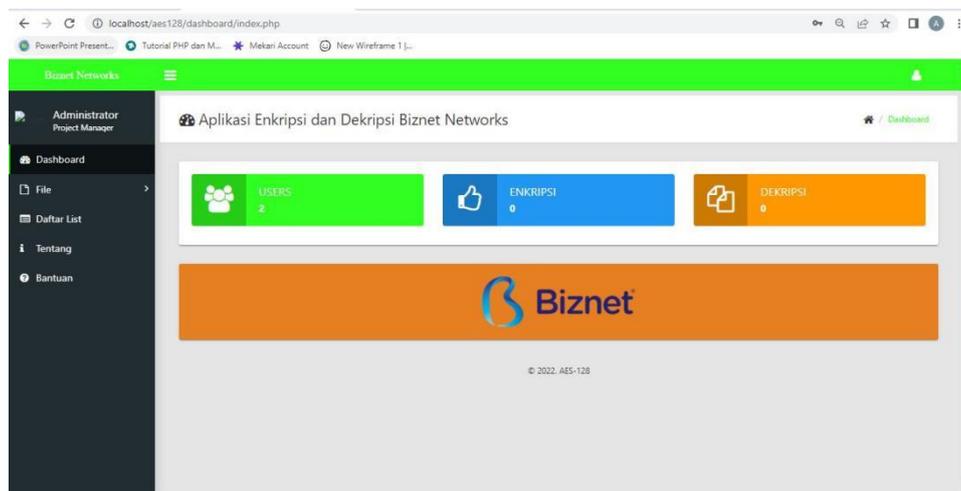
Pada tampilan layar login terdapat dua kolom yang berisi username dan password. Tampilan layar login seperti pada gambar di bawah ini.



Gambar 6. Tampilan Layar Login

b. Tampilan Layar Dashboard

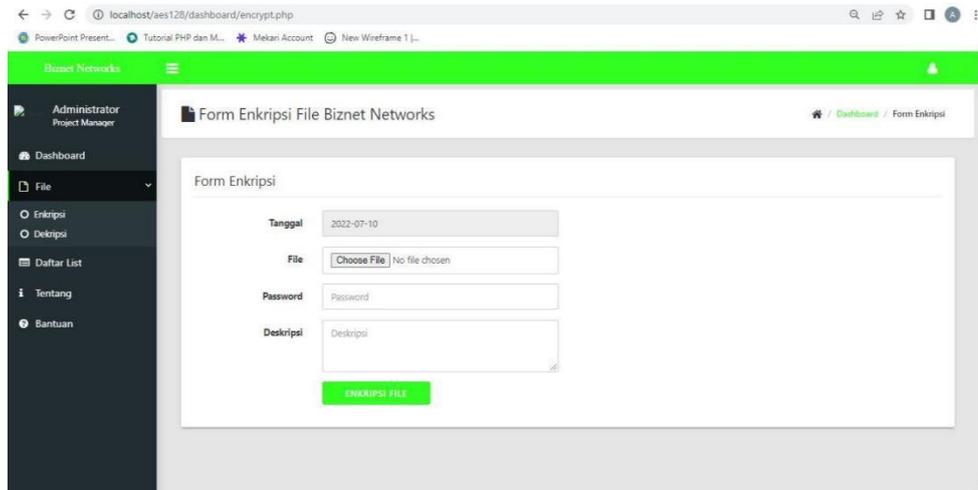
Pada tampilan layar dashboard terdapat beberapa menu yang ada di bagian kiri, yaitu file, enkripsi, dekripsi, daftar list, tentang dan bantuan. Tampilan layar dashboard seperti pada gambar di bawah ini.



Gambar 7. Tampilan Layar Dashboard

c. Tampilan Layar Enkripsi File

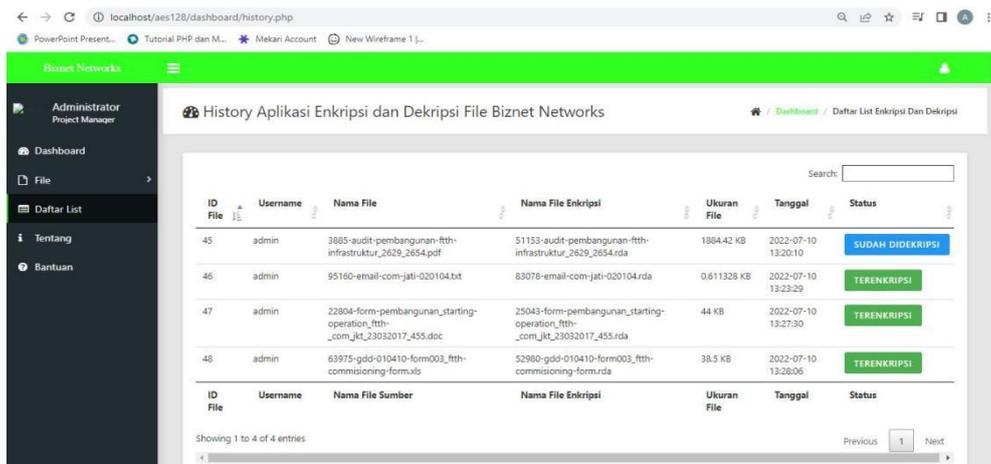
Pada tampilan layar enkripsi terdapat kolom yaitu tanggal, file, password dan deskripsi. Tampilan layar enkripsi seperti pada gambar di bawah ini.



Gambar 8. Tampilan Layar Enkripsi File

d. Tampilan Layar Daftar List / History

Tampilan layar history akan menampilkan daftar list file yang sudah di dekripsi dan yang belum di dekripsi. Tampilan layar History seperti pada gambar di bawah ini.



Gambar 9. Tampilan Layar Daftar List

3.2 Implementasi

a. Enkripsi File

Uji coba yang pertama yaitu melakukan enkripsi file, dengan file text document berekstensi .txt.

File : “Data Pelanggan-Aji Teguh Utomo.txt”

Password : 1234

Deskripsi : Data Pelanggan (1234)

Isi Teks File :

```
Data Pelanggan-Aji Teguh Utomo.txt - Notepad
File Edit Format View Help
Nama Pelanggan      : Aji Teguh Utomo
Alamat Instalasi    : Jl. Kebon Kacang 43 No. 1b, Kebon Kacang, Tanah Abang, Kota Jakarta Pusat, DKI Jakarta
Paket               : Biznet Home Internet 1B
Serial Number Modem : 48575443E7FEC9A4
```

Gambar 10. Tampilan Isi File “Data Pelanggan-Aji Teguh Utomo.txt”

b. Isi File Setelah di Enkripsi

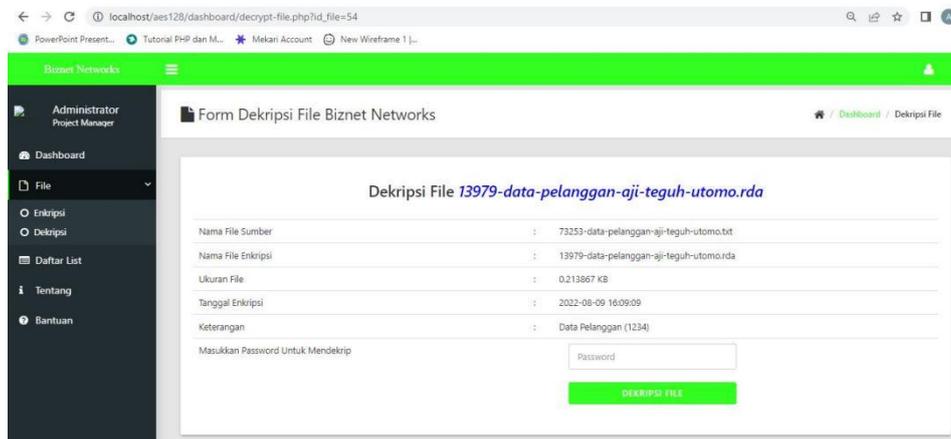
Setelah dilakukan proses enkripsi, lalu kemudian kita coba buka file yang di enkripsi tersebut. Maka hasilnya seperti dibawah ini.



Gambar 11. Tampilan Isi File “Data Pelanggan-Aji Teguh Utomo.txt.rda” setelah di enkripsi

c. Dekripsi File

Setelah dilakukan proses enkripsi, lalu kemudian kita coba untuk melakukan dekripsi file. Masuk ke menu enkripsi, lalu klik pada enkripsi file, kemudian masukkan password pada saat pertama kali enkripsi. Maka akan tampil pada gambar dibawah ini.



Gambar 12. Dekripsi file

d. Buka File yang sudah di dekripsi

Setelah dilakukan proses dekripsi, lalu kemudian kita coba membuka kembali file yang berhasil di dekripsi. File yang udah di dekripsi dibuka kembali, file telah kembali ke isi file semula. seperti gambar dibawah ini.



Gambar 13. Isi File Setelah Selesai di Dekripsi

3.3 Testing Waktu Enkripsi dan Dekripsi AES-128

Untuk pengujian eksekusi waktu disini terdapat 7 file yang akan di uji kan, dengan ukuran file dan ekstensi yang berbeda. List file yang akan di uji kan dapat dilihat pada tabel berikut.

Tabel 1. File Testing Upload Enkripsi dan Dekripsi

| No | Nama File | Size | Tipe File | Ekstensi |
|----|-------------------------------------|-------|---------------|----------|
| 1 | Data Pelanggan-Aji Teguh Utomo.txt | 1 KB | Text Document | .txt |
| 2 | Pembangunan Aktifasi GDD 010410.doc | 53 KB | DOC Document | .doc |

| | | | | |
|---|-----------------------------------------|--------|-------------------|-------|
| 3 | SPK Menteng.docx | 77 KB | DOCX Document | .docx |
| 4 | DATA MAINTENANCE JARINGAN JKT 2020.xlsx | 232 KB | XLSX Worksheet | .xlsx |
| 5 | Audit Pembangunan_JKT_20170410_482.pdf | 457 KB | PDF Document | .pdf |
| 6 | presentasi sidang TA.pptx | 875 KB | PPTX Presentation | .pptx |
| 7 | DRT 010203_170824_0005.jpg | 907 KB | Image / JPG File | .jpg |

Uji waktu enkripsi dan dekripsi dengan Microtime. Seperti hasil pemeriksaan waktu enkripsi dan dekripsi pada tabel berikut.

Tabel 2. Hasil Pengujian Waktu Enkripsi dan Dekripsi File

| No. | Nama File | Size | Waktu Enkripsi AES-128 (Dalam Satuan Detik / Second) | Waktu Eksekusi Dekripsi AES-128 (Dalam Satuan Detik / Second) |
|-----|-----------------------------------------|--------|------------------------------------------------------|---------------------------------------------------------------|
| 1 | Data Pelanggan-Aji Teguh Utomo.txt | 1 KB | 0.02 | 0.02 |
| 2 | Pembangunan Aktifasi GDD 010410.doc | 53 KB | 4.01 | 3.92 |
| 3 | SPK Menteng.docx | 77 KB | 5.66 | 5.64 |
| 4 | DATA MAINTENANCE JARINGAN JKT 2020.xlsx | 232 KB | 16.98 | 16.98 |
| 5 | Audit Pembangunan_JKT_20170410_482.pdf | 457 KB | 33.62 | 33.5 |
| 6 | presentasi sidang TA.pptx | 875 KB | 66.41 | 63.91 |
| 7 | DRT 010203_170824_0005.jpg | 907 KB | 66.83 | 65.97 |

4. KESIMPULAN

Dari hasil aplikasi enkripsi dan dekripsi file yang telah dibuat terdapat beberapa kesimpulan sebagai berikut:

- Dengan adanya dan digunakannya aplikasi enkripsi dan dekripsi file diharapkan dapat membantu mengamankan file-file penting yang bersifat rahasia.
- Dapat mengimplementasikan metode *Advanced Encryption Standard (AES-128)*.
- Penelitian ini berhasil melakukan enkripsi dan dekripsi pada file berbagai format file.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu menyelesaikan penelitian ini hingga terciptanya jurnal SENAFI. Khususnya kepada Bpk. Rizky Pradhana, S.Kom dan M.Kom selaku pembimbing yang telah membimbing dari awal penelitian hingga pembuatan jurnal SENAFI.

DAFTAR PUSTAKA

- [1] Andi Inayah Auliyah, Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document, "*Indonesian Journal of Data and Science (IJODAS)*", vol 1, no 1, pp. 23-28, 2020.
- [2] Asri Prameshwari¹, Nyoman Putra Sastra², Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen, "*Jurnal Eksplorasi Informatika*", Vol.8, No.1, pp. 52-58, September 2018
- [3] Natanael Sijabat¹, Nurul Hayaty², Eka Suswaini³, Implementasi Kriptografi Hybrid Menggunakan Algoritma AES-128 DAN Algoritma Rabin Untuk Mengamankan Data Dalam Database, "*Student Online Jurnal*", vol.3, no.1, pp. 178-183, 2022.
- [4] Niolinda Cristy¹, Fristi Riandari², Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan, "*Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*", vol.4, no.2, pp. 75-85, 2021.

- [5] Muhammad Azhari¹, Dadang Iskandar Mulyana², Faizal Joko Perwitosari³, Firhan Ali⁴, Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES), *“Jurnal Pendidikan Sains dan Komputer”*, vol. 2, no. 1, pp.163-171, 2022.
- [6] Megawati¹, Muhammad Fitra Hamidy², Sasqia Ismi Aulia³, Yuhendri Putra⁴, Mhd Arief Hasan, M. Kom⁵, Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python, *“Sains dan Teknologi Informasi (SATIN)”*, vol. 07, no. 01, pp. 102-111, 2021.
- [7] Binanda Wicaksana^{1*}, Ma'mun Setiawan², Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Berkas Soal Ujian, *“Jurnal Ilmiah Teknologi Informasi & Sains (TEKNOIS)”*, vol. 10, no. 1, pp. 25-34, 2020.
- [8] Arther Ignasius Suranta¹, Dolly Virgian Shaka Yudha Sakti^{2*}, Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi, *“Sistem Komputer dan Teknik Informatika (SKANIKA)”*, vol. 5, no. 1, pp. 1-10, 2022.
- [9] Imelda Asih Rohani Simbolon^{1*}, Indra Gunawan¹, Ika Okta Kirana¹, Rafiq Dew², S. Solikhun², Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar, *“Journal of Computer System and Informatics (JoSYC)”*, vol. 1, no. 2, pp. 54-60, 2020.
- [10] Nayuni Dwitri¹, Sukma Sindi², Irma Agustika Sihombing³, Indra Gunawan⁴, Pengamanan Data File Document Menggunakan Kriptografi Encryption System (DES), *“Journal of Information System, Informatics and Computing (JISICOM)”*, vol.4, no.1, pp. 40-45, 2020.