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

IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITME ADVANCED ENCRYPTION STANDARD (AES-128) BERBASIS WEB UNTUK MENGAMANKAN FILE INVOICE PADA PT MUARA JUARA KREASI INDONESIA

Muhammad Adam Akmal[1], Purwanto[2*], Safrina Amini[3], Haris Munandar[4]

[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1]1911510707@student.budiluhur.ac.id, [2*]purwanto@budiluhur.ac.id, [3]safrina.amini@budiluhur.ac.id, [4]haris.munandar@budiluhur.ac.id
(* : corresponding author)

Abstrak- Pada era digital ini, teknologi informasi memainkan peran penting dalam mempermudah dan meningkatkan efisiensi proses bisnis. PT Muara Juara Kreasi Indonesia, sebagai entitas bisnis yang terlibat aktif dalam *sector* bisnis Food & Beverages atau sering disebut F&B, semakin tergantung pada sistem informasi berbasis web untuk mengelola dan menyimpan data transaksi, termasuk file *invoice* yang merupakan dokumen kunci dalam aktivitas bisnis F&B. Keberhasilan suatu perusahaan dalam mengelola transaksi bisnis dan informasi keuangan tidak hanya bergantung pada efisiensi operasionalnya, tetapi juga pada keamanan data yang diterapkan. Dengan meningkatnya ancaman terhadap keamanan di dunia maya, perlindungan terhadap informasi transaksi bisnis menjadi prioritas utama. Analisis ini ditujukan untuk menjalankan kriptografi memakai algoritme AES-128 berbasis web sebagai upaya strategis untuk pengamanan file *invoice* di PT Muara Juara Kreasi Indonesia, yang dimana sejauh ini menyimpan file *invoice* masih menggunakan flash disk dan dibuat arsip untuk disimpan dalam lemari. Dikarenakan file *invoice* merupakan file rahasia, jadi tidak ada jaminan keamanan pada file *invoice*. Oleh karena itu, algoritme AES-128 dipilih karena kemampuannya yang teruji dalam melindungi data dan efisiensinya dalam pengolahan informasi. Berdasarkan hasil dan pengujian, penerapan aplikasi pengamanan file *invoice* menggunakan AES-128 mampu mengamankan file *invoice* dengan terenkripsi yang mempunyai rata – rata dalam besaran file nya 100.9 KB dan rata – rata dalam waktu terenkripsi nya 1.2032 detik, serta dapat mengembalikan data pada file *invoice* seperti semula dengan terdekripsi yang mempunyai rata – rata dalam besaran file nya 100.9 KB dan rata – rata dalam waktu terdekripsi nya 3.1406 detik.

Kata Kunci : Teknologi Informasi, Food & Beverages, Keamanan Data, Arsip

IMPLEMENTATION OF CRYPTOGRAPHY USING A WEB-BASED ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM TO SECURE INVOICE FILES AT PT MUARA JUARA KREASI INDONESIA

Abstract- *In this digital era, information technology plays an important role in simplifying and increasing the efficiency of business processes. PT Muara Juara Kreasi Indonesia, as a business entity that is actively involved in the Food & Beverages business sector or often called F&B, is increasingly dependent on web-based information systems to manage and store transaction data, including invoice files which are key documents in F&B business activities. The success of a company in managing business transactions and financial information depends not only on its operational efficiency, but also on the data security implemented. With increasing threats to cyber security, protecting business transaction information has become a top priority. This analysis is aimed at carrying out cryptography using the web-based AES-128 algorithm as a strategic effort to secure invoice files at PT Muara Juara Kreasi Indonesia, which so far has been storing invoice files using flash disks and making archives to be stored in cupboards. Because the invoice file is a confidential file, there is no guarantee of security in the invoice file. Therefore, the AES-128 algorithm was chosen because of its proven ability to protect data and its efficiency in information processing. Based on the results and testing, the implementation of the invoice file security application using AES-128 is able to secure encrypted invoice files which have an average file size of 100.9 KB and an average encrypted time of 1.2032 seconds, and can restore data in invoice files such as initially decrypted which had an average file size of 100.9 KB and an average decryption time of 3.1406 seconds.*

Keywords*: Information Technology, Food & Beverages, Data Security, Archives*

1. PENDAHULUAN

Pada era digital ini, teknologi informasi memainkan peran penting dalam mempermudah dan meningkatkan efisiensi proses bisnis. PT Muara Juara Kreasi Indonesia, sebagai entitas bisnis yang terlibat

aktif dalam *sector* bisnis Food & Beverages atau sering disebut F&B, semakin tergantung pada sistem informasi berbasis web untuk mengelola dan menyimpan data transaksi, termasuk file *invoice* yang merupakan dokumen kunci dalam aktivitas bisnis F&B.

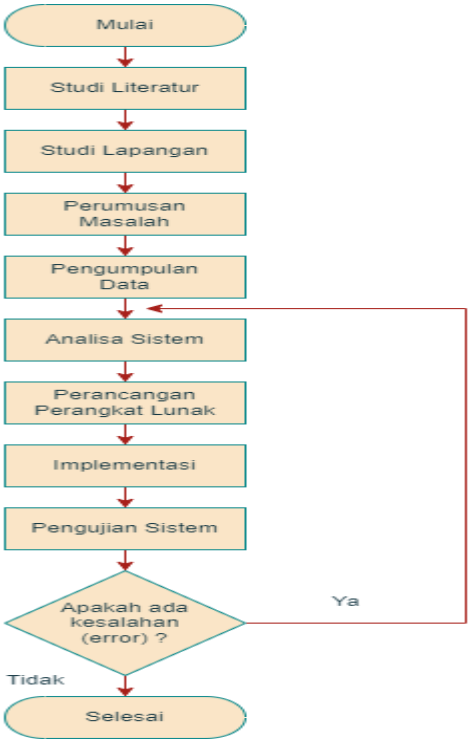
Menurut penelitian sebelumnya yang mengusung judul pengamanan file *invoice* pada PT Mitra Teknik menggunakan metode algoritma RC4.[1] Penelitian ini membuat aplikasi pengamanan file *invoice* dan file dokumen dengan format docx, pdf, xls, xlsx, txt, jpg pada PT Mitra Teknik menggunakan algoritma RC4 dan model waterfall. Hasil dari penelitian diperoleh setelah proses enkripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses enkripsi 9.250 millisecond serta setelah proses dekripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses dekripsi 9.250 millisecond. Dikutip dari Zaimah Panjaitan,[2] Algoritme RC4 termasuk kedalam golongan Stream Chiper (Chiper Aliran), serta yang mengenkripsi antara kombinasi plainteks dengan menggunakan bit-wise Xor (Exclusive-or). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari *pseudo random* yang menggunakan XOR dengan plainteks untuk menghasilkan *chipertext*. Masing – masing elemen dalam tabel saling ditukarkan minimal sekali. Dan Sedangkan menurut Sandeep Bhadari,[3] Algoritme AES menggambarkan sebagai algoritme kunci asimestris, yang berarti kunci yang sama digunakan untuk mendekripsi dan mengenkripsi data. AES juga dikenal dengan nama tradisional nya yaitu, Rijndael. Rijndael adalah keluarga sandi dengan ukuran blok dan kunci yang berbeda. Untuk AES, NIST memilih tiga anggota keluarga Rijndael, masing – masing dengan ukuran blok 128 – bit tetapi juga tiga Panjang kunci berbeda yaitu, 256, 192, dan 128 bit. Model ini dikenal sebagai AES 256 dengan 14 putaran, AES 192 dengan 12 putaran, dan AES 128 dengan 10 putaran.

Dua langkah utama kriptografi adalah enkripsi, yang melibatkan perubahan format data menjadi kode yang tidak dapat dipahami, dan dekripsi, yang melibatkan pemulihan data ke format aslinya.[4] Analisis ini ditujukan untuk mengaplikasikan kriptografi memakai algoritme AES-128 berbasis web sebagai tahapan strategis untuk pengamanan file *invoice* di PT Muara Juara Kreasi Indonesia, yang dimana sejauh ini menyimpan file *invoice* masih menggunakan flash disk dan dibuat arsip untuk disimpan dalam lemari. Dikarenakan file *invoice* merupakan file rahasia, jadi tidak ada jaminan keamanan pada file *invoice*. Oleh karena itu, algoritme AES-128 dipilih karena kemampuannya yang teruji dalam melindungi data dan efisiensinya dalam pengolahan informasi.

Analisis ini diinginkan bisa memberi partisipasi pada pengembangan solusi keamanan informasi berbasis web yang efektif, khususnya dalam konteks proteksi file *invoice* di PT Muara Juara Kreasi Indonesia. Dipilihnya algoritme Advanced Encryption Standard (AES) karena memberikan keamanan terbaik, tahan terhadap berbagai ancaman, mudah diterapkan, dan mengenkripsi serta mendekripsikan file dan data dengan cepat dan efisien.[5]

2. METODE PENELITIAN

2.1 Penerapan Metode



Gambar 1. Penerapan Metode

Di atas **gambar 1** pelaksanaan metode ialah rancangan tahapan atau proses yang dijalankan oleh peneliti dalam penerapan metode penelitian, yang dirancang dengan cermat untuk memastikan penelitian berjalan sistematis, terstruktur, dan memenuhi standar ilmiah dengan tujuan mencapai hasil yang diinginkan.

Berikut ini adalah langkah – langkah metode aplikasi yang dibuat oleh penulis :

a. Studi Literatur
Studi literatur berfungsi sebagai fondasi teoritis yang mendukung analisis masalah yang sedang diselidiki. Sumber – sumber yang dapat diakses dalam penelitian ini melibatkan internet, jurnal penelitian, buku – buku, artikel ilmiah yang berkenan dengan topik yang sedang dibicarakan ialah kriptografi, terutama algoritme *AES*. Hingga dapat mempermudah untuk menyelesaikan masalah yang sedang diselidiki.

b. Studi Lapangan
Dalam langkah ini dilakukannya analisis kasus terhadap file ditempat sebuah perusahaan swasta, yang mana lebih tepatnya di PT Muara Juara Kreasi Indonesia. Tujuannya adalah mengidentifikasi permasalahan yang ada dari file tersebut, sehingga dapat dirumuskan menjadi solusi yang tepat saat menangani permasalahannya.

c. Perumusan Masalah
Mengenai tahapan ini, dijalankan rumusan masalah yang telah di identifikasi dan akan diatasi di dalam perusahaan swasta, yaitu PT Muara Juara Kreasi Indonesia. Pendekatan yang digunakan melibatkan

metode kriptografi dengan menerapkan algoritme *AES* untuk memakai file *invoice* di perusahaan tersebut.

d. Pengumpulan Data
Untuk melakukan penelitian, penulis membutuhkan data yang terkait pada topik yang akan dibahas. Proses pengumpulan data dilaksanakan dengan tujuan memperoleh informasi yang diperlukan, yaitu :

1) Observasi
Observasi ini dilakukan dengan mengikuti kegiatan secara langsung di PT Muara Juara Kreasi Indonesia untuk memperhatikan masalah yang dihadapi oleh perusahaan. Dari temuan masalah tersebut, maka dirumuskan permasalahan serta strategi penyelesaiannya.
2) Wawancara
Wawancara adalah untuk memperoleh wawasan yang mendalam dan data yang relevan untuk penelitian, maka dilakukan wawancara secara langsung dengan pihak PT Muara Juara Kreasi Indonesia dengan pimpinan langsung dan assistant manajer keuangan yang menangani file *invoice*.
3) Studi Pustaka
Pada tahap ini, dilaksanakan lewat membaca jurnal, *e-book*, dan acuan terpaut untuk memahami ajaran kriptografi, keamanan file, *AES*, serta ajaran lain yang relevan dengan pengembangan kriptografi untuk pengamanan file *invoice*.

e. Analisis Sistem
Tahap ini ialah langkah identifikasi dan analisa kendala sistem yang diselaraskan berbarengan batasan yang terletak. Dalam proses menyoroti masalah, analisa dijalankan melalui beberapa tahapan, diantaranya termasuk analisis data, penerapan algoritme, dan analisis sistem, serta sebagai upaya mengatasi kendala dalam penelitian ini.

f. Perancangan Perangkat Lunak
Dalam langkah ini, temuan dari analisis sistem menginformasikan proses desain, dengan penekanan pada modul yang bertanggung jawab untuk enkripsi dan dekripsi serta segmen tambahan sekitar yang akan dimasukkan kedalam aplikasi. Selanjutnya, desain interface dilakukan untuk menjamin keselarasan sistem.

g. Implementasi
Dalam proses pelaksanaan ini, modul yang telah disusun pada langkah perancangan yang dijalankan dengan menggunakan bahasa penulisan kode khusus. Pada bagian konteks ini, aplikasi terpakai, yaitu :

1) Software yang dipakai dalam pelaksanaan pengaman data *file* memakai bahasa penulisan kode PHP dan DBMS yang dipakai ialah PHP MyAdmin.
2) Hardware yang dipakai ialah adalah *Prosesor Intel Core i5 8th Gen*, RAM 4GB, dan SSD 256 GB.

h. Pengujian Sistem
Tahap uji ini dijalankan dengan pendekatan metode *blackbox testing* untuk mengevaluasi keselarasan antara input dan output sistem yang menurut langkah – langkah yang sudah ditetapkan. Tujuan utamanya adalah mengidetifikasi potensi kesalahan yang dapat terjadi, dan mengevaluasi guna memperbaiki sistem.

2.2 Keamanan

Security atau keamanan adalah Teknik dan mekanisme yang digunakan untuk melindungi suatu hal data atau informasi pada sistem. Pada dasarnya, security ialah sistem yang dipakai untuk menjaga agar sistem dalam suatu

jaringan tetap terlindungi. Memastikan keamanan dan kerahasiaan data ialah komponen penting dari sistem informasi apapun. Informasi bagi pihak-pihak yang berkepentingan sangatlah penting dan hal ini berkaitan dengan hal tersebut. Informasi tersebut akan kehilangan keabsahannya jika diketahui atau dibajak oleh orang yang tidak berkepentigan.[6]

2.3 Kriptografi

Kriptografi adalah studi tentang metode komunikasi rahasia yang membuatnya tidak dapat dipahami oleh pihak yang tidak berwenang. Enkripsi dan dekripsi adalah dua langkah utama kriptografi. "Plaintext" menggambarkan komunikasi yang tidak terenkripsi. Alasan dinamakan demikian adalah karena semua orang dapat membaca dan memahaminya. Baik teknik enkripsi maupun dekripsi menggunakan kunci dalam satu atau lain cara. Ciphertext mengacu pada teks biasa yang menyertakan enkripsi. Kami sering menemukan beberapa frasa dalam pengkodean.[7]

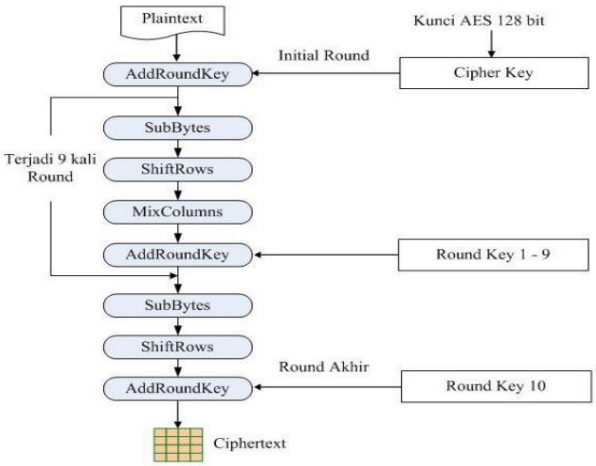
2.4 Algoritme Advanced Encryption Standard (AES)

Berbagai jenis data mungkin dilindungi oleh AES, sebuah teknik dalam kriptografi simetris. Algoritma ini dapat mengenkripsi dan mendekode data menggunakan formatnya, blok ciphertext simetris. Proses enkripsi dapat mengubah data jadi bentuk yang tidak bisa dipahami yang dikatakan ciphertext; sebaliknya, dekripsi digunakan untuk mengubah data ciphertext kembali ke bentuk aslinya yang disebut plaintext. Teknik AES mengenkripsi dan mendekripsi data dalam blok 128-bit memakai blok kunci kriptografi yang panjangnya 128, 192, dan 256 bit.[8]

Standar enkripsi baru, AES atau algoritma Rijindael, disosialisasikan pada November 2001 oleh NIST. Ini dikembangkan dengan algoritma DES melalui seleksi ketat dengan algoritma lain. Tim pemenang dalam kompetisi memilih algoritma pengganti DES, Vincent Rijmen dan Jian Daemen, mengembangkan metode ini, “alasan utama terpilihnya algoritme ini memiliki keseimbangan antara keamanan serta fleksibilitas dalam berbagai platform software dan hardware”.[9]

2.5 Proses Enkripsi AES

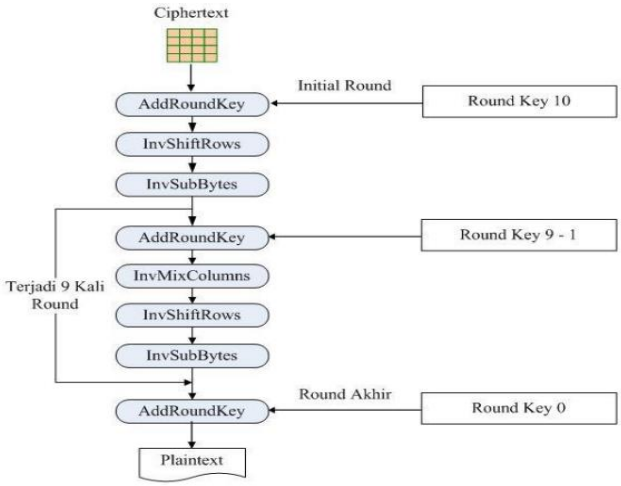
Tipe transformasi empat byte SubBytes, ShiftRows, MixColumns, dan AddRoundkey membentuk proses enkripsi algoritma AES-128. Perubahan byte AddRoundkey pada status (dimensi) akan dilakukan pada awal operasi enkripsi. Kemudian, hingga Nr (nilai bulat), status akan diubah menggunakan SubBytes, ShiftRows, MixColumns, dan AddRoundkey. Fungsi bulat menjelaskan prosedur ini. Putaran ketiga berbeda dari putaran kedua karena negara bagian tidak melalui transformasi MixColumn. Gambar 2 di bawah menunjukkan prosedur enkripsi AES [10] :



Gambar 2. Proses Enkripsi AES

2.6 Proses Dekripsi AES

Untuk melakukan dekripsi pada AES-128, dibutuhkan transformasi cipher yang terbalik untuk mendapatkan inverse cipher pada langkah ini ialah : InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Proses dekripsi AES bisa ditinjau pada **gambar 3.** dibawah ini [10] :



Gambar 3. Proses Dekripsi AES

2.7 *Blackbox Testing*

Aplikasi akan diuji dengan menggunakan *blackbox* testing sebab hanya membutuhkan batas bawah dan atas data yang diinginkan, jumlah kolom entri data yang akan diuji, aturan setiap kolom, dan kedua variable tersebut untuk menentukan berapa banyak data yang perlu diuji. Terisi dipangkalan, maka dapat menguji apakah fungsionalitas aplikasi masih dapat menangani input data yang tidak diinginkan menggunakan metode kotak hitam ini, sehingga mengurangi kebutuhan penyimpanan data. Untuk memperbaiki kesalahan yang ada, pengembangan sistem aplikasi harus ditingkatkan.[11]

3. HASIL DAN PEMBAHASAN

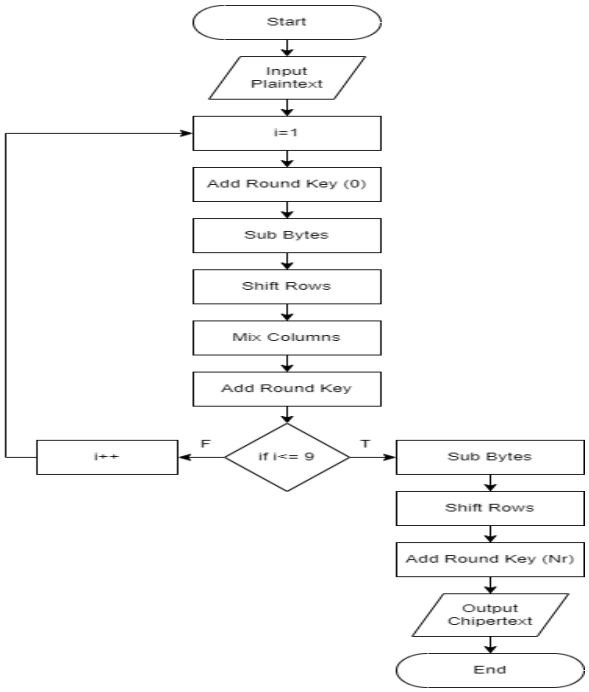
3.1 Lingkungan Percobaan

Sebelum mengimplementasikan dan menjalankan aplikasi enkripsi dan dekripsi, diperlukan spesifikasi *hardware* dan *software* tertentu guna aplikasi bisa terlaksana dengan baik. Pada penelitian ini, penulis memilih memakai bahasa pemrograman HTML dan PHP, serta dengan menggunakan *framework boostrap* untuk desain *website* guna meningkatkan estetika tampilan dari pemrograman sehingga dapat terlihat lebih menarik.

3.2 *Flowchart*

Flowchart adalah serangkaian *symbol* untuk mempresentasikan tahapan dan aliran logis dari suatu proses atau algoritme. *Symbol – symbol* ini diurutkan dan disambungkan dengan panah yang menyatakan aliran dari satu tahap ke tahap selanjutnya. Manfaat dari *flowchart* mencakup kemampuan untuk memahami, merancang, dan menganalisis proses atau algoritme secara visual. Selain itu, *flowchart* membantu menyusun dan menyajikan langkah – langkah, sehingga memudahkan penyampaian informasi kepada orang lain secara jelas dan terorganisir.

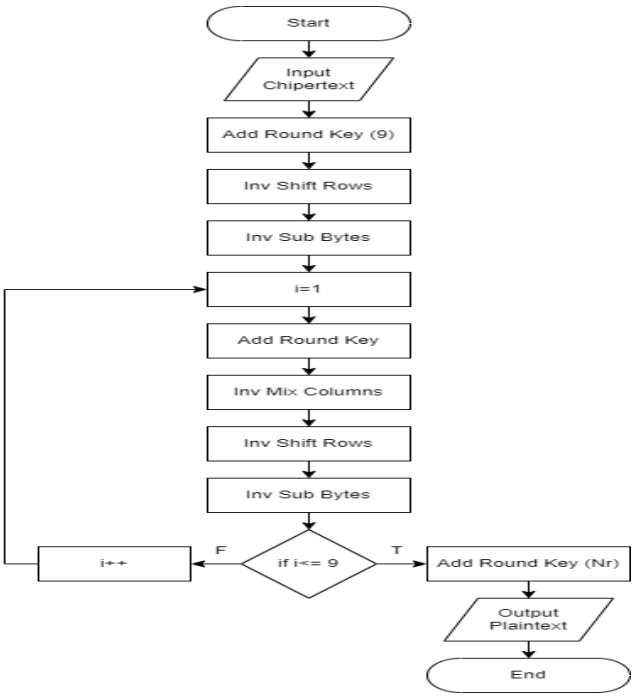
a. Flowchart Proses Enkripsi AES-128



Gambar 4. Flowchart Proses Enkripsi AES-128

Di **gambar 4.** *Flowchart* enkripsi AES-128 yang mendeskripsikan serangkain tahapan yang harus dilakukan atau ditetapkan untuk mengenkripsi blok data dengan memakai kunci enkripsi 128-bit. Proses ini melibatkan iterasi tahap – tahap SubBytes, ShiftRows, MixColumns, dan AddRoundKey sebanyak Sembilan kali dalam putaran pertama, diikuti oleh putaran terakhir yang memiliki sedikit berbeda. *Flowchart* tersebut memberikan gambaran visual tentang alur dan langkah – langkah dalam proses enkripsi AES-128.

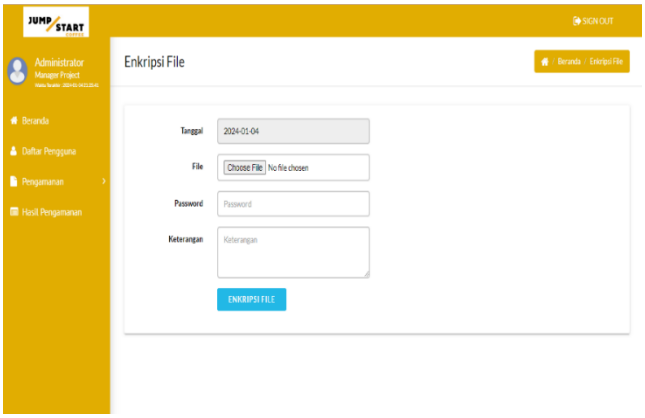
b. Flowchart Proses Dekripsi AES-128



Gambar 5. Flowchart Proses Dekripsi AES-128

Proses mendekripsi blok data terenkripsi menggunakan *flowchart* dekripsi yang benar ditunjukkan pada **gambar 5** diagram alur dekripsi AES-128**.** Dalam prosedur ini, loop utama mengulangi langkah InvShiftRows, InvSubBytes, AddRoundKey, dan Inv MixColumns sembilan kali, serta kemudian loop akhir yang sedikit dimodifikasi dijalankan. *Flowchart* ini menyajikan gambaran visual tentang alur dan langkah – langkah yang terlibat dalam proses dekripsi AES-128.

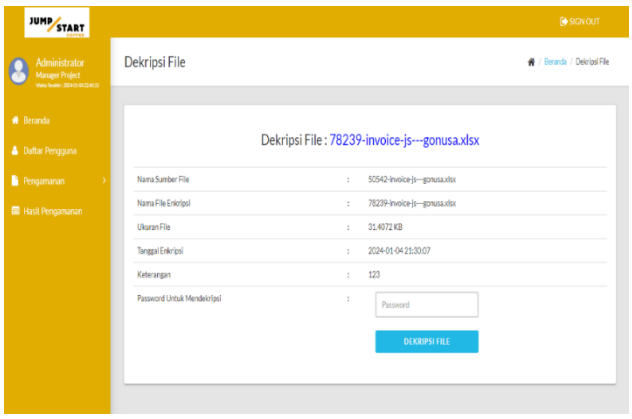
3.3 Tampilan Layar Halaman Enkripsi File



Gambar 6. Tampilan Layar Halaman Enkripsi File

Di **gambar 6.** di atas ini terdapat halaman tampilan layar enkripsi file. Pada halaman ini pengguna (admin maupun user) dapat melakukan proses enkripsi file dengan ekstensi tertentu, seperti (.docx, .pdf, dan .xlsx). Setelah itu pengguna dapat memasukkan file yang akan dienkripsi, *password (key)*, serta keterangan sebelum melakukan proses enkripsi dimulai dengan menekan tombol enkripsi file nya.

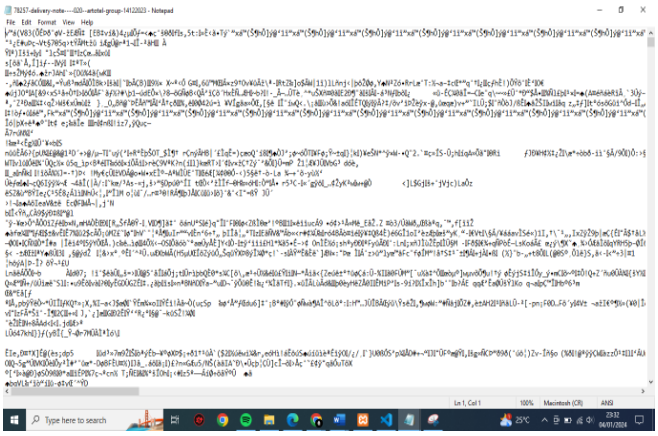
3.4 Tampilan Layar Halaman Dekripsi File



Gambar 7. Tampilan Layar Halaman Dekripsi File

Di **gambar 7.** di atas ini terdapat halaman tampilan layar proses dekripsi file. Pada halaman ini pengguna (admin maupun user) memiliki kemampuan untuk mendekripsi file dengan mengisi password yang sebelumnya sama dengan password yang digunakan untuk mengenkripsi file. Setelah itu, pengguna dapat menekan tombol dekripsi file untuk menjalan kan proses dekripsi nya.

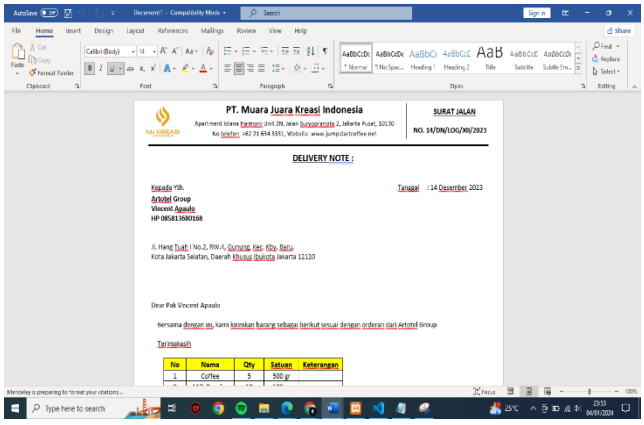
3.5 Tampilan File Terenkripsi



Gambar 8. Tampilan File Terenkripsi

Di **gambar 8.** Menampilkan file yang telah melalui proses enkripsi, penampilan file yang telah terenkripsi akan dipengaruhi oleh jenis algoritma enkripsi yang diterapkan. Enkripsi adalah langkah yang merubah data asli jadi bentuk yang tidak dapat dibaca, itu hanya bisa dikembalikan ke bentuk semula memakai kunci dekripsi yang sama.

3.6 Tampilan File Terdekripsi



Gambar 9. Tampilan File Terdekripsi

Pada **gambar 9.** file akan kembali ke tampilan awalnya sebelum proses enkripsi setelah melalui didekripsi. Tujuan dari dekripsi adalah mengembalikan data yang telah dienkripsi ke bentuk aslinya dengan memakai kunci dekripsi yang sesuai.

3.7 Uji Coba

Penulis melakukan dua tahap pengujian pada sistem aplikasi keamanan file *invoice* di PT Muara Juara Kreasi Indonesia, yang mencakup penelitian terhadap hasil proses enkripsi file dan dekripsi file memakai algoritme AES. Proses pengujian ini dirancang untuk mengumpulkan informasi yang berkaitan dengan kinerja sistem keamanan. Tabel pengujian berikut memberikan contoh hasil dari pengujian enkripsi dan dekripsi yang menggunakan program atau algoritme AES.

a. Uji Coba Hasil Enkripsi

Tabel 1. Tabel Uji Coba Hasil Enkripsi

No	Label file asli	Besaran file asli (/kb)	Label file terenkripsi	Besaran file terenkripsi	Waktu enkripsi (detik)	Posisi
1.	Invoice JS – ARTOTEL.xlsx	31.3 KB	34877-invoice-js---artotel.xlsx	31.3 KB	0.387 detik	Berhasil
2.	Invoice JS – POLA.xlsx	31.4 KB	84845-invoice-js---pola.xlsx	31.4 KB	0.383 detik	Berhasil
3.	Invoice JS – BLIBLI GANCIT1.pdf	125.7 KB	11598-invoice-js---blibli-gancit1.pdf	125.7 KB	1.537 detik	Berhasil
4.	Delivery Note - 020 Artotel Group 14122023.docx	188.9 KB	78257-delivery-note-----020--artotel-group-14122023.docx	188.9 KB	2.214 detik	Berhasil
5.	Invoice JS - RS GADING PLUIT1.pdf	127.2 KB	51309-invoice-js---rs-gading-pluit1.pdf	127.2 KB	1.495 detik	Berhasil
	Rata – rata			**100.9 KB**	**1.2032 detik**	

b. Uji Coba Hasil Dekripsi

Tabel 2. Tabel Uji Coba Hasil Dekripsi

No	Label file asli	Besaran file asli (/kb)	Nama file terdekripsi	Besaran file terdekripsi	Waktu dekripsi (detik)	Posisi
1.	34877-invoice-js---artotel.xlsx	31.3 KB	48986-invoice-js---artotel.xlsx	31.3 KB	1.154 detik	Berhasil
2.	84845-invoice-js---pola.xlsx	31.4 KB	10136-invoice-js---pola.xlsx	31.4 KB	1.092 detik	Berhasil
3.	11598-invoice-js---blibli-gancit1.pdf	125.7 KB	42281-invoice-js---blibli-gancit1.pdf	125.7 KB	3.852 detik	Berhasil
4.	78257-delivery-note----020--artotel-group-14122023.docx	188.9 KB	72804-delivery-note-----020--artotel-group-14122023.docx	188.9 KB	5.625 detik	Berhasil
5.	51309-invoice-js---rs-gading-pluit1.pdf	127.2 KB	7940-invoice-js---rs-gading-pluit1.pdf	127.2 KB	3.980 detik	Berhasil
	Rata – rata			**100.9 KB**	**3.1406 detik**	

4. KESIMPULAN

Kesimpulan dari penulis setelah membuat sistem aplikasi kriptografi adalah bahwa aplikasi ini memiliki beberapa keuntungan. Pertama, kehadiran sistem pengamanan file *invoice* meningkatkan keamanan data dan mencegah kebocoran informasi pada file yang sensitive. Kedua, aplikasi ini menjamin keutuhan file selama proses enkripsi dan dekripsi tanpa mengalami perubahan yang tidak diinginkan. Terakhir, waktu yang dibutuhkan untuk proses enkripsi dan dekripsi sesuai dengan ukuran file yang diproses, dimana file berukuran kecil akan diproses lebih cepat, sedangkan file berukuran besar memerlukan waktu lebih lama.

c. DAFTAR PUSTAKA

[1] F. T. Infirmasi, U. B. Luhur, and K. S. Restaurant, "Pengamanan File Invoice Pada Pt Mitra Teknik Menggunakan Metode Algoritma Rc4 Securing Invoice Files At Pt Mitra Teknik Using the Rc4 Algorithm Method," vol. 2, no. April, pp. 54–60, 2023.

[2] Zaimah Panjaitan M.Kom, "ALGORITMA RC4 (CONTOH PERHITUNGAN LENGKAP)," komputerkata.com. Accessed: Jan. 20, 2024. [Online]. Available: https://komputerkata.com/algoritma-rc4-contoh-perhitungan-lengkap/

[3] Sandeep Bhadari, "RC4 vs AES: Perbedaan dan Perbandingan," AskAnyDifference. Accessed: Jan. 20, 2024. [Online]. Available: https://askanydifference.com/id/difference-between-rc4-and-aes-with-table/#what-is-aes

[4] H. Linda, S. Sitorus, and U. Ristian, "Penerapan Algoritma Advanced Encryption Standard (Aes)-128 Bit Pada Keamanan Database Aplikasi Kepelangganan (Studi," *Komput. dan Apl.*, vol. 11, no. 01, pp. 128–136, 2023.

[5] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA

[6] S. N. Afifah and U. K. Indonesia, "Keamanan Informasi dengan Memanfaatkan Kriptografi," no. April, pp. 0–11, 2023, doi: 10.13140/RG.2.2.32685.15844.

[7] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[8] A. R. Ramadan, A. W. Prakoso, and G. Dwi C, "Implementasi Kriptografi AES untuk Keamanan Pengiriman Data Internet of Things Menggunakan Web Service Rest pada NodeMCU," *Syst. Inf. Syst. Informatics J.*, vol. 6, no. 1, pp. 1–6, 2021, doi: 10.29080/systemic.v6i1.752.

[9] D. Pratomo, N. Budi Nugroho, and R. I. Ginting, "Implementasi Kriptografi Untuk Mengamangkan Data Penjualanan Di Pt. Papparich Medan Menggunakan Metode Aes 128," *J. CyberTech*, vol. x. No.x, no. x, 2021, [Online]. Available: https://ojs.trigunadharma.ac.id/

[10] H. Wijaya, "Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection," *J. Akad.*, vol. 17, no. 1, pp. 8–13, 2020, [Online]. Available: https://www.ejournal.lppmunidayan.ac.id/index.php/akd

[11] A. S. Hardiansyah, Meri Hendayani, Ian Amukti Herlambang, Andhika Nove Rezki, "Implementasi Black Box Testing Pada Website," *J. Ilmu Komput. dan Sci.*, vol. 1, no. 01, pp. 135–148, 2022.