

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD 128* (AES 128) BERBASIS WEB PADA KEDAI KOPI NGOPIYUKA!

Muhammad Hadin Ibrahim¹, Sri Mulyati^{2*}, Joko Christian Chandra³, Dolly Virgianshaka Yudha Sakti⁴

^{1,2,3,4} Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: ¹hadinibrahim2803@gmail.com, ^{2*}sri.mulyati@budiluhur.ac.id, ³joko.chiritian@budiluhur.ac.id, ⁴dolly.virgianshaka@budiluhur.ac.id

Abstrak-Data sensitif seperti data keuangan, resep, penjualan dan *inventory* merupakan hal penting yang harus dilindungi dari pihak yang tidak berwenang. Dalam hal ini, kedai kopi membutuhkan sistem keamanan yang handal untuk melindungi data sensitif tersebut. Lalu bagaimana cara mengamankan data tersebut dari pencurian data? Dan bagaimana cara mengembalikan data yang telah di enkripsi menjadi data yang asli tanpa mengalami perubahan data tersebut ?. Algoritma kriptografi *Advanced Encryption Standard* (AES) 128 mendekripsi data asliyang sudah terenkripsi membantu agar tidak adanya pencurian/ kebocoran file. Algoritma Kriptografi *Advanced Encryption Standard* (AES) 128 menjadi solusi yang tepat karena memiliki kemampuan untuk melindungi data dengan baik dan memenuhi standar keamanan yang tinggi. Dokumen .doc, .docx, .xls, .xlsx, .ppt, .pptx dan.pdf adalah jenis-jenis dokumen yang dapat digunakan untuk melakukan proses enkripsi dan dekripsi, sistem yang dikembangkan memastikan bahwa data tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang. Metodologi penelitian menggunakan sistem dan analisis keamanan sistem, serta uji coba untuk memvalidasi hasilimplementasi. Kesimpulan dari penelitian ini bertujuan untuk mengimplementasikan AES 128 pada kedai kopi NgopiYuka! untuk melindungi data sensitif dengan baik dan memenuhi standar keamanan yang tinggi, dan dengan adanya aplikasi pengamanan *file*, penyimpanan data keuangan, transaksi dan resep khususnya dalam bentuk dokumen menjadi lebih aman. Lalu aplikasi pengamanan *file* ini dapat menjamin keutuhan *file* pada saat enkripsi maupun dekripsi tanpa mengalami kerusakan atau perubahan data. Implementasi ini merupakan solusi yang baik untuk memastikan data sensitif pada kedai kopi.

Kata Kunci: Algoritma Kriptografi, *Advanced Encryption Standard*, Keamanan Data.

WEB-BASED IMPLEMENTATION OF *ADVANCED ENCRYPTION STANDARD 128* (AES 128) ALGORITHM AT NGOPIYUKA COFFEE SHOP!

Abstract-Sensitive data such as financial data, recipes, sales and inventory are important things that must be protected from unauthorized parties. In this case, coffee shops need a reliable security system to protect sensitive data. Then how do you secure the data from data theft? And how do you restore encrypted data to original data without changing the data? The *Advanced Encryption Standard* (AES) 128 cryptographic algorithm decrypts the original encrypted data to help prevent file theft/leakage. The *Advanced Encryption Standard* (AES) 128 Cryptographic Algorithm is the right solution because it has the ability to protect data properly and meets high security standards. Documents .doc, .docx, .xls, .xlsx, .ppt, .pptx and .pdf are types of documents that can be used to carry out the encryption and decryption process, the system developed ensures that data cannot be read or modified by unauthorized parties. not authorized. The research methodology uses system and system security analysis, as well as trials to validate implementation results. The conclusion of this study aims to implement AES 128 at the NgopiYuka! coffee shop. to properly protect sensitive data and meet high security standards, and with file security applications, financial data storage, transactions and recipes, especially in document form, are safer. Then this file security application can guarantee file integrity during encryption and decryption without experiencing data damage or changes. This implementation is a good solution for ensuring sensitive data on coffee shops.

Keywords: Cryptographic Algorithms, *Advanced Encryption Standard*, Data Security

1. PENDAHULUAN

Keamanan data merupakan pertimbangan penting saat mengirim data melalui internet. Untuk menjaga keamanan dan kerahasiaan informasi dan data, diperlukan salah satu teknik enkripsi dan dekripsi. Teknik ini berguna untuk membuat pesan atau data yang masuk tidak terbaca oleh pihak yang tidak bertanggung jawab. Teknik enkripsi dan dekripsi ini dikenal dan dipelajari dalam kriptografi. Keamanan penyimpanan data sangat penting dan tidak dapat diabaikan. Salah satu dampak negatif dari perkembangan teknologi adalah pencurian data dokumen, dan terkait dengan pencurian data dokumen, aspek keamanan informasi dalam pertukaran data dan penyimpanan data dianggap sangat penting.

NgopiYuka! Merupakan UMKM dibidang kuliner, lebih tepatnya menjual minuman berbentuk kopi dan the dalam bentuk botol, baik untuk kebutuhan perseorangan ataupun kelompok. Dikarekanakan banyaknya data penting bagi NgopiYuka! yang akan merugikan apabila data tersebut jatuh kepada pihak lain, maka digunakanlah metode algoritma *Advanced Encryption Standard* (AES) 128 untuk proses enkripsi dan dekripsi sebagai bentuk pengamanannya. Proses enkripsi dan dekripsi akan melakukan perlindungan terhadap data dan informasi dengan menggunakan algoritma yang sudah ditetapkan sebelumnya. Dapat diartikan bahwa proses enkripsi ialah sebuah proses merubah pesan asli (*plain text*) menjadi suatu pesan yang tersandi (*chiper text*), sedangkan proses dekripsi ialah proses mengembalikan pesan yang tersandi menjadi pesan data asli kembali [1].

Algoritma kriptografi yang digunakan saat mengenkripsi data atau informasi apa pun yang terkait dengan masalah ini adalah *Advanced Encryption Standard* (AES). Algoritma ini tidak harus menunggu sejumlah data input, pesan atau data tertentu sebelum memproses atau menambahkan lebih banyak byte untuk enkripsi. Algoritma AES adalah algoritma enkripsi blok yang menggunakan teknik substitusi, mutasi dan putaran ganda dari setiap blok selama enkripsi dan dekripsi [2]. Pada penelitian ini, proses enkripsi dan dekripsi menggunakan algoritma enkripsi AES-128 untuk melindungi data. Perlindungan data yang menggunakan algoritma ini menggunakan dokumen dengan ekstensi .doc, .docx, .xls, .xlsx, .ppt, .pptx dan .pdf. Algoritma AES (*Advanced Encryption Standard*) dipilih karena memiliki tingkat keamanan yang tinggi dan kebal terhadap berbagai serangan juga karena kesederhanaan desain, kekompakan kode dan kecepatan enkripsi dan deskripsi semua data [2].

2. METODE PENELITIAN

2.1 Keamanan Data

Keamanan adalah keadaan yang menunjukkan keadaan bebas dari bahaya atau ancaman. Masalah keamanan informasi sering diabaikan oleh para perancang dan pengelola sistem informasi, masalah kinerja aplikasi sering mendapat perhatian lebih dari keamanan informasi, oleh karena itu masalah keamanan informasi dianggap kurang penting dibandingkan masalah lainnya. Istilah keamanan dan perlindungan sering digunakan secara bergantian. Istilah keamanan lebih berfokus pada semua masalah keamanan informasi sedangkan istilah mekanisme keamanan berfokus pada mekanisme sistem yang digunakan untuk melindungi data dalam sistem komputer. [3].

2.2 Kriptografi

Kriptografi adalah ilmu menjaga kerahasiaan pesan dengan mengenkripsinya dalam bentuk yang tidak dapat lagi dipahami. Enkripsi memiliki dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut teks biasa karena siapa pun dapat dengan mudah membaca dan memahami informasi ini. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi teks biasa melibatkan penggunaan beberapa jenis kunci [4]. Menurut [5] kriptografi memiliki 4 aspek yang merupakan dari fundamental pada sistem kriptografi, yaitu

- a. Kerahasiaan (*Confidentiality*)
Kerahasiaan dipakai untuk menjaga suatu informasi agar tidak bisa diakses oleh pihak yang tidak bertanggung jawab.
- b. Integritas Data (*Data Integrity*)
Integritas data berfungsi untuk mencegah perubahan informasi oleh pihak yang tidak bertanggung jawab. Integritas data harus di pastikan keasliannya supaya mampu mendeteksi manipulasi data yang terjadi pada sistem informasi. Yang dimaksud dengan manipulasi data di sini ialah perubahan dan penghapusan pada data.
- c. Autentikasi (*Authentication*)
Autentikasi ialah mengidentifikasi pihak-pihak yang berusaha untuk mengakses sistem informasi ataupun keaslian data dari sistem informasi tersebut.
- d. Ketiadaan Penyangkalan (*nonrepudiation*)
Ketiadaan penyangkalan berguna untuk mencegah suatu penyangkalan terhadap satu aksi yang dilakukan oleh pelaku sistem informasi.

Menurut [6] terdapat 4 elemen utama di dalam kriptografi yang saling berkaitan, yaitu:

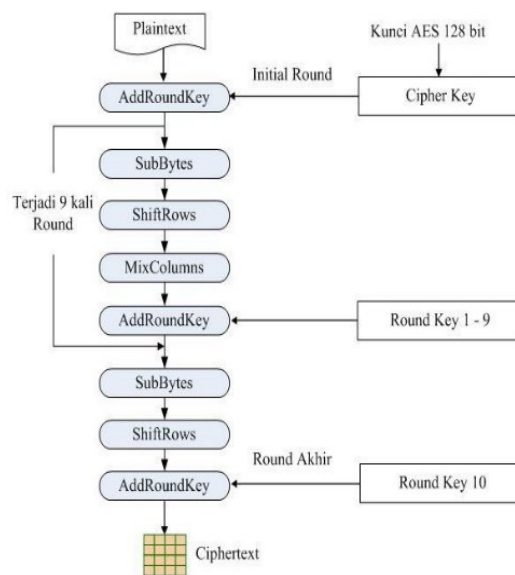
- a. *Plain Text* ialah pesan asli pada dokumen yang dikirim saat proses komunikasi. Nantinya *plain text* ini yang akan dipakai saat proses enkripsi dan dekripsi.
- b. *Cipher Text* ialah pesan yang sudah disembunyikan, atau dengan kata lain *chiper text* adalah pesan asli (*plain text*) yang sudah di enkripsi. *Cipher text* dapat diubah menjadi bentuk aslinya (*plain text*) dengan memanfaatkan *key* yang disediakan.
- c. *Cryptography Key* adalah kunci yang digunakan dalam proses enkripsi dan dekripsi dalam kriptografi. Proses enkripsi dan dekripsi tidak dapat dilakukan dengan benar jika tidak ada kunci (*key*) yang tepat. Kunci (*key*) adalah informasi yang dapat mengontrol proses enkripsi.
- d. *Encryption Decryption Algorithm* merupakan algoritma yang tidak kalah pentingnya pada proses kriptografi saat melakukan enkripsi dan dekripsi.

2.3 Advanced Encryption Standard (AES)

Sebuah agen dari Departemen Perdagangan AS percaya bahwa DES tidak lagi aman, sehingga pada tahun 1988 *National Institute of Standards and Technology*, atau yang sering disebut *National Bureau of Standards*, mengusulkan kepada pemerintah federal AS desain baru teknologi enkripsi tunggal secara *default*. NIST kemudian mengadakan kompetisi terbuka untuk membuat standar algoritma baru untuk menghindari konflik atas standar baru, seperti saat membuat DES. [7]. Standar algoritma kriptografi yang ditemukan untuk mengganti *Data Encryption Standard* (DES) adalah algoritma *Advanced Encryption Standard* (AES) yang ditemukan oleh Vincent Rijmen dan Joan Daeman. Algoritma AES 128 sendiri memiliki panjang blok berjumlah 128 bit dan panjang kuncinya memiliki jumlah yang berbeda-beda. Proses pengulanagankunci AES 128 atau bisa disebut dengan *round* dilakukan sebanyak 10 kali putaran dan menggunakan pola *matriks*4x4, dimana untuk melakukan enkripsi dan dekripsi terdiri dari 1 *byte* atau 8 bit [8]. Menurut [8] ada beberapa tahapan enkripsi dalam algoritma *Advanced Encryption Standard* (AES) pada panjang 128-bit, yaitu

- a. *AddRoundKey*: yang merupakan *initial round* dan melakukan XOR antara *plaintext* dengan *chipper key*.
- b. *Round* : Putaran sebanyak $N_r - 1$ kali. Proses yang dilakukan pada setiap putaran adalah :
 1. *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (S-box).
 2. *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
- c. *MixColumns*: mengacak data pada masing-masing kolom *array state* dengan persamaan sebagai berikut

$$A(x) = \{03\}x^2 + \{01\}x^2 + \{01\}x^2 + \{02\}$$
- d. *AddRoundKey* : melakukan XOR antara *state* sekarang *round key*.
- e. *Final Round* : proses untuk putaran terakhir antara lain :
 1. *SubBytes*
 2. *ShiftRows*
 3. *AddRoundKey*



Gambar 1. Tahapan-Tahapan Enkripsi Metode AES

2.4 Black Box Testing

Black box testing merupakan metode yang mudah digunakan karena hanya membutuhkan batas bawah dan atas pada data yang diharapkan. Jumlah data uji yang dapat dihitung dari jumlah bidang entri data yang akan diuji dan yang harus mengisi kasus data atas dan bawah. Dengan menggunakan cara ini untuk mengetahui apakah fungsi masih dapat menerima data masuk yang tidak terduga dan apakah data yang disimpan kurang valid atau tidak [9].

2.5 Rancangan Pengujian

Rancangan pengujian ini akan menggunakan aplikasi berbasis *web* yang memiliki menu *login* untuk menggunakan aplikasi, *user* atau *admin* diharuskan untuk memasukkan *username* dan *password*. Setelah *login*, *user* atau *admin* akan langsung diarahkan pada menu *dashboard*. Didalam halaman *dashboard* terdapat beberapa

sub menu seperti menu enkripsi dan dekripsi jika masuk sebagai *user*, lalu jika masuk sebagai *admin* maka akan ada menu *file master* dan *list user*. Lalu pada menu *dashboard* terdapat juga submenu *logout* jika sudah melakukan enkripsi dan dekripsi *file*.

Tabel 1. Rancangan Pengujian

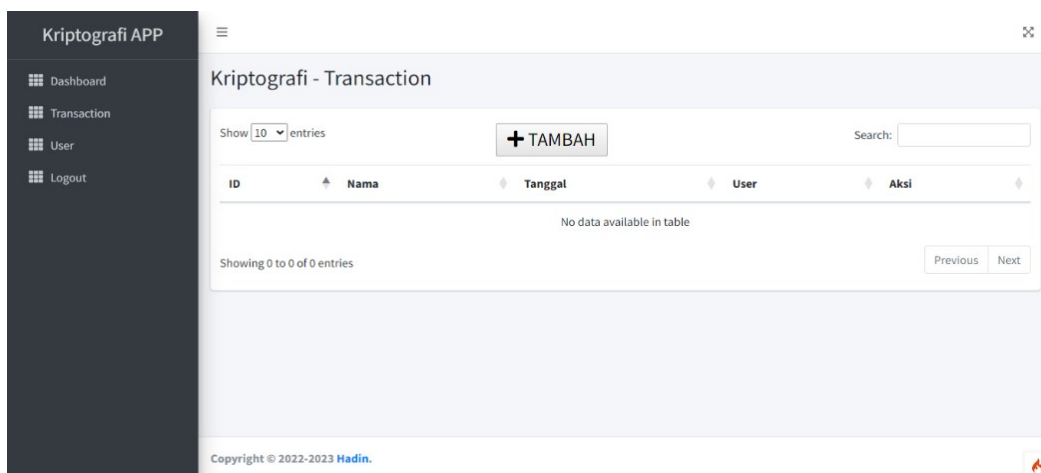
No	Skenario Pengujian	Hasil Yang Diharapkan
1.	<i>User</i> atau <i>admin</i> mengisi <i>form login</i> sesuai dengan role	Tampil halaman menu home
2.	<i>User</i> memilih menu <i>Transaction</i>	Tampil halaman menu <i>encrypt</i> atau <i>decrypt</i>
3.	Pilih <i>file</i> kemudian masukkan <i>password</i> dan klik tombol <i>encrypt</i> atau <i>decrypt</i> untuk <i>file</i> yang akan dienkripsi atau didekripsi	Tampil halaman hasil proses enkripsi atau dekripsi
4.	Men- <i>download file</i> yang sudah terenkripsi dan terdekripsi	Berhasil men- <i>download file</i>
5.	<i>User</i> atau <i>admin</i> menekan tombol <i>logout</i>	Kembali kehalaman <i>login</i>
6.	<i>Admin</i> memilih menu <i>list user</i>	Tampil halaman menu <i>list user</i>
7.	<i>Admin</i> menghapus pada <i>user</i> yang terdaftar	Berhasil menghapus <i>user</i>
8.	<i>Admin</i> memilih menu <i>list file</i>	Tampil halaman menu <i>list file</i>
9.	<i>Admin</i> menghapus dan <i>download</i> data pada <i>list file</i>	Berhasil menghapus dan men- <i>download</i> data

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Metode

a. Proses Enkripsi

Pada proses enkripsi ini, *user* harus masuk terlebih dahulu ke menu form enkripsi yang terletak di bagian sub menu *transaction*. Kemudian *user* harus mengklik tombol tambah lalu memilih file yang ingin di enkripsi, setelah memilih file, *user* harus memasukkan *password* yang sesuai.



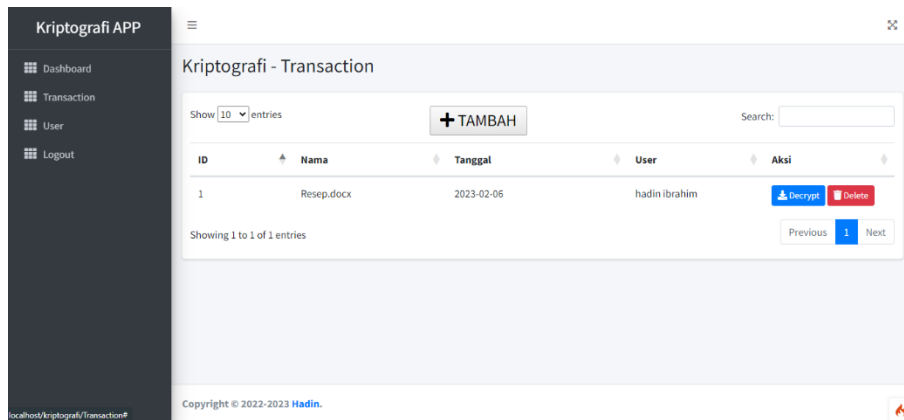
Gambar 2. Sub menu *transaction*



Gambar 3. Proses Enkripsi

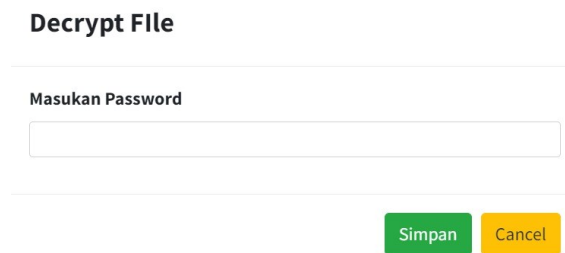
b. Proses Dekripsi

Untuk memulai proses dekripsi, *user* hanya perlu memilih file yang ingin di dekripsi yang berada di sub menu *transaction*, kemudian *user* dapat memilih berkas yang ingin didekripsi dengan menekan tombol dekripsi berkas.



Gambar 4. Submenu *Transaction* Saat Dekripsi

Setelah *user* memilih file yang ingin di dekripsi, *users* diminta untuk memasukkan *password* yang sama saat melakukan proses enkripsi



Gambar 5. Proses Dekripsi

3.2 Hasil Proses Enkripsi dan Dekripsi

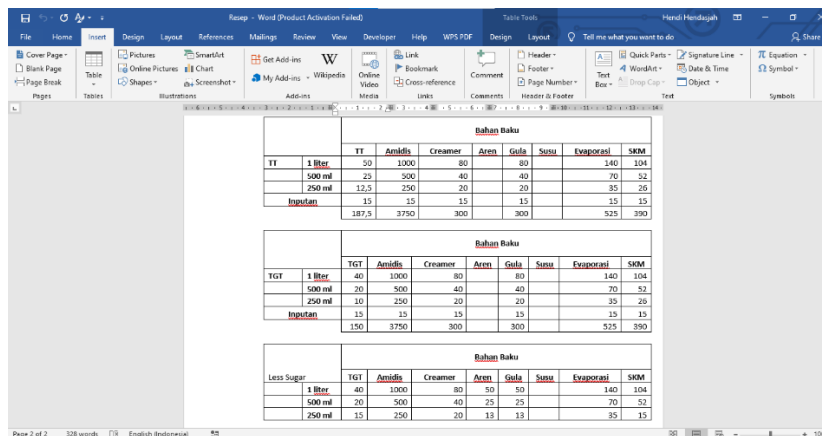
a. Enkripsi

Proses enkripsi file dibuat menjadi tabel untuk melihat nama asli file sebelum di enkripsi dan setelah di enkripsi, serta melihat ukuran file saat sebelum dan setelah di enkripsi.

Tabel 2. Proses Enkripsi *File*

No.	Nama Asli File	Ukuran File Asli Per (KB)	Nama File Setelah di-Enkripsi	Ukuran File Setelah di Enkripsi Per (KB)	Waktu per (Detik)
1.	Data keuangan.xlsx	39 KB	10912-data-keuangan.rda	39 KB	2 detik
2.	Resep.docx	27 KB	15823-resep.rda	27 KB	1 detik
3.	Penjualan.xlsx	58 KB	53337-penjualan.rda	58 KB	2 detik
4.	Data <i>inventory</i> .pdf	212 KB	54930-data- <i>inventory</i> .rda	212 KB	6 detik

Pengujian enkripsi file ber ekstensi .doc, .docx, .xls, .xlsx, dan .pdf, data yang ada masih berupa data asli dan belum ter enkripsi.



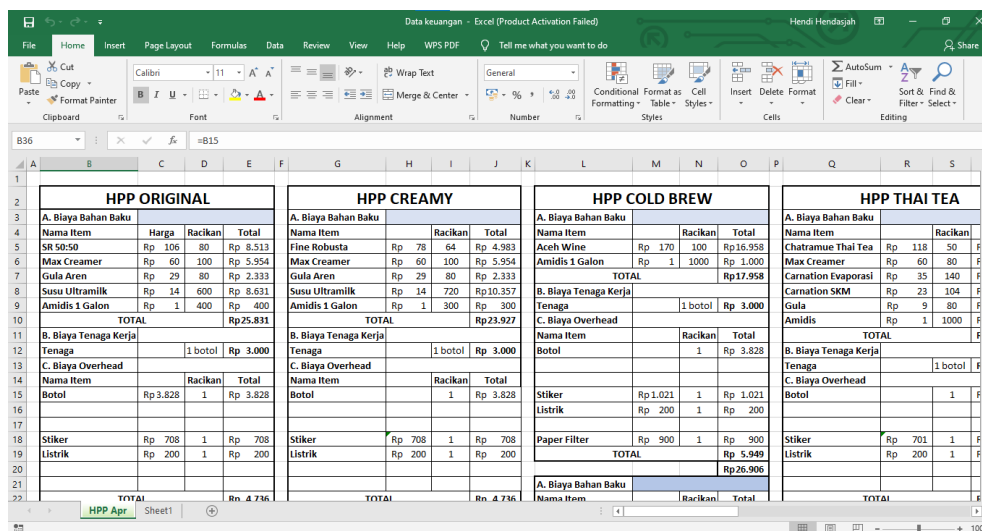
The image shows a Microsoft Word document with three tables, each titled "Bahan Baku". Each table lists ingredients and their quantities for different product variants.

	TT	Amidis	Creamer	Aren	Gula	Susu	Evaporasi	SKM
1 liter	20	1000	80		80			140
500 ml	25	500	40		40			70
250 ml	12,5	250	20		20			35
Inputan	187,5	3750	300		300			525

	TGT	Amidis	Creamer	Aren	Gula	Susu	Evaporasi	SKM
1 liter	40	1000	80		80			140
500 ml	20	500	40		40			70
250 ml	10	250	20		20			35
Inputan	150	3750	300		300			525

	TGT	Amidis	Creamer	Aren	Gula	Susu	Evaporasi	SKM
1 liter	40	1000	80	50	50			140
500 ml	20	500	40	25	25			70
250 ml	15	250	20	13	13			35

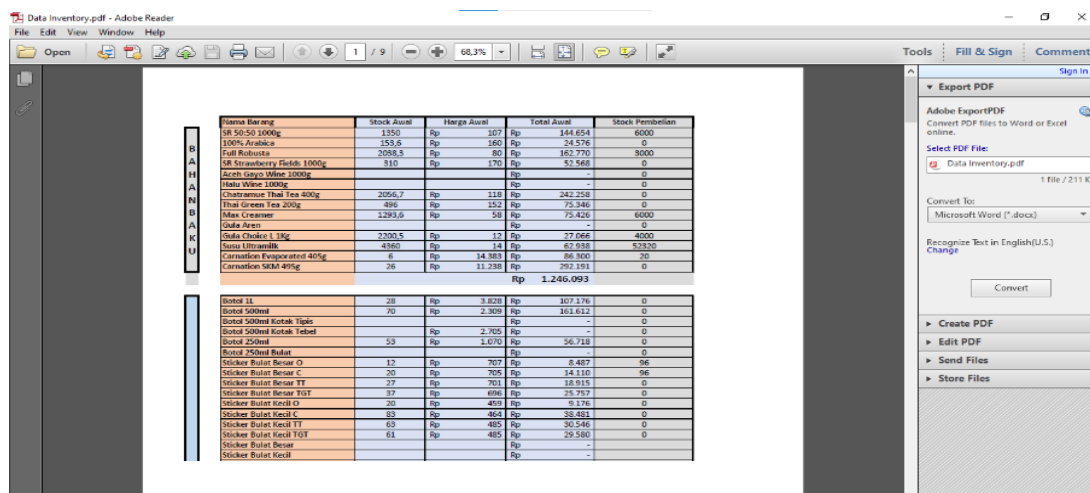
Gambar 9. Proses Enkripsi File. Doc



The image shows an Excel spreadsheet with four main sections: HPP ORIGINAL, HPP CREAMY, HPP COLD BREW, and HPP THAI TEA. Each section contains a table of items, their prices, and quantities.

HPP ORIGINAL				HPP CREAMY				HPP COLD BREW				HPP THAI TEA			
A. Biaya Bahan Baku				A. Biaya Bahan Baku				A. Biaya Bahan Baku				A. Biaya Bahan Baku			
Nama Item	Harga	Racikan	Total	Nama Item	Harga	Racikan	Total	Nama Item	Harga	Racikan	Total	Nama Item	Harga	Racikan	Total
SR 50:50	Rp 106	80	Rp 8.513	Fine Robusta	Rp 78	64	Rp 4.983	Aceh Wine	Rp 170	100	Rp 16.938	Chatramue Thai Tea	Rp 118	50	F
Max Creamer	Rp 60	100	Rp 5.954	Max Creamer	Rp 60	100	Rp 5.954	Amidis 1 Galon	Rp 1	1000	Rp 1.000	Max Creamer	Rp 60	80	F
Gula Aren	Rp 29	80	Rp 2.333	Gula Aren	Rp 29	80	Rp 2.333	TOTAL			Rp 17.938	Carnation Evaporasi	Rp 35	140	F
Susu Ultramilk	Rp 14	600	Rp 8.531	Susu Ultramilk	Rp 14	720	Rp 10.357	B. Biaya Tenaga Kerja				Carnation Evaporasi	Rp 23	104	F
Amidis 1 Galon	Rp 1	400	Rp 400	Amidis 1 Galon	Rp 1	300	Rp 300	Tenaga		1	Rp 3.000	Gula	Rp 9	80	F
TOTAL			Rp 25.831	TOTAL			Rp 23.927	C. Biaya Overhead				Amidis	Rp 1	1000	F
B. Biaya Tenaga Kerja				B. Biaya Tenaga Kerja				Botol		1	Rp 3.828	TOTAL			Rp 1.000
Tenaga		1	Rp 3.000	Tenaga		1	Rp 3.000	Botol		1	Rp 3.828	B. Biaya Tenaga Kerja			
C. Biaya Overhead				C. Biaya Overhead				Stiker	Rp 1.021	1	Rp 1.021	Tenaga		1	Rp 3.000
Nama Item		Racikan	Total	Nama Item		Racikan	Total	Listrik	Rp 200	1	Rp 200	C. Biaya Overhead			
Botol		Rp 3.828	1	Botol		1	Rp 3.828	Paper Filter	Rp 900	1	Rp 900	Botol		1	Rp 3.828
Stiker	Rp 708	1	Rp 708	Stiker	Rp 708	1	Rp 708	TOTAL			Rp 5.949	Stiker	Rp 701	1	F
Listrik	Rp 200	1	Rp 200	Listrik	Rp 200	1	Rp 200	A. Biaya Bahan Baku			Rp 26.906	Listrik	Rp 200	1	F
TOTAL			Rp 4.736	TOTAL			Rp 4.736	Nama Item				TOTAL			

Gambar 10. Proses Enkripsi File.xls



The image shows a PDF document with a table titled "Data Inventory.pdf". The table lists various items, their stock, and prices.

Plasma Barang	Stock Awal	Harga Awal	Total Awal	Stock Pembelian
SR 50:50 1000g	1350	Rp 107	Rp 144.654	6000
100% Arabica	153,6	Rp 160	Rp 24.576	0
Fall Robusta	2058,3	Rp 80	Rp 164.770	3000
SR Strawberry Fields 1000g	310	Rp 170	Rp 52.700	0
Aceh Gayo Wine 1000g		Rp		0
Hulu Wine 1000g		Rp		0
Chatramue Thai Tea 400g	2056,7	Rp 118	Rp 242.256	0
Thai Green Tea 200g	496	Rp 152	Rp 75.348	0
Max Creamer	1293,6	Rp 58	Rp 75.426	6000
Gula Aren		Rp		0
Susu Chiken 1.1kg	2000,5	Rp 12	Rp 27.666	4000
Susu Ultramilk	4566	Rp 14	Rp 63.924	93300
Carnation Evaporasi 400g	6	Rp 14.383	Rp 86.300	20
Carnation SKM 400g	26	Rp 11.238	Rp 292.191	0
			Rp 1.246.093	
Botol 1l	28	Rp 3.828	Rp 107.176	0
Botol 500ml	70	Rp 2.369	Rp 165.812	0
Botol 500ml Kotak Tisip		Rp		0
Botol 500ml Kotak Tebel		Rp 2.705	Rp 0	0
Botol 250ml	53	Rp 1.070	Rp 56.718	0
Botol 250ml Bulat		Rp		0
Sticker Bulat Besar C	12	Rp 707	Rp 8.487	96
Sticker Bulat Besar C	20	Rp 705	Rp 14.100	96
Sticker Bulat Besar TT	27	Rp 701	Rp 18.915	0
Sticker Bulat Besar TGT	37	Rp 496	Rp 28.737	0
Sticker Bulat Kecil C	20	Rp 459	Rp 9.176	0
Sticker Bulat Kecil C	85	Rp 464	Rp 39.453	0
Sticker Bulat Kecil TT	63	Rp 485	Rp 30.546	0
Sticker Bulat Kecil TGT	61	Rp 485	Rp 29.585	0
Sticker Bulat Besar		Rp		0
Sticker Bulat Kecil		Rp		0

Gambar 11. Proses Enkripsi File.Pdf

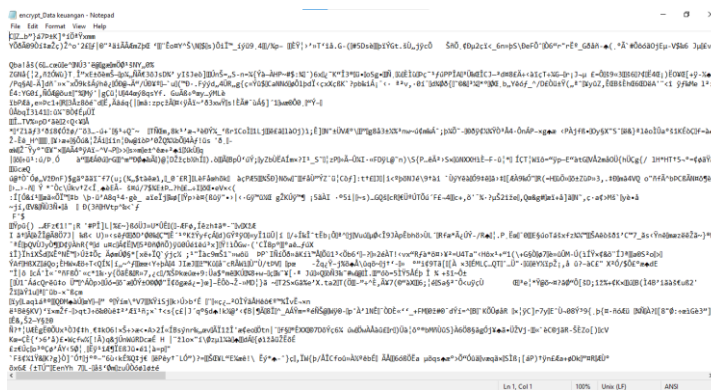
b. Dekripsi

Proses dekripsi file dibuat menjadi tabel untuk melihat nama asli file setelah didekripsi dan sebelum didekripsi, serta melihat ukuran file saat sebelum dan setelah didekripsi

Tabel 3. Proses dekripsi file

No.	Nama File Enkripsi	Ukuran Setelah Di Enkripsi Per (KB)	Nama File Setelah di-Dekripsi	Ukuran File Setelah di-Dekripsi per (KB)	Waktu per (detik)
1.	10912-data-keuangan.rda	39 KB	Data keuangan.xlsx	39 KB	2
2.	15823-resep.rda	27 KB	Resep.docx	27 KB	1
3.	53337-penjualan.rda	58 KB	Penjualan.xlsx	58 KB	2
4.	54930-data-inventory.rda	212 KB	Data <i>inventory</i> .pdf	212 KB	6

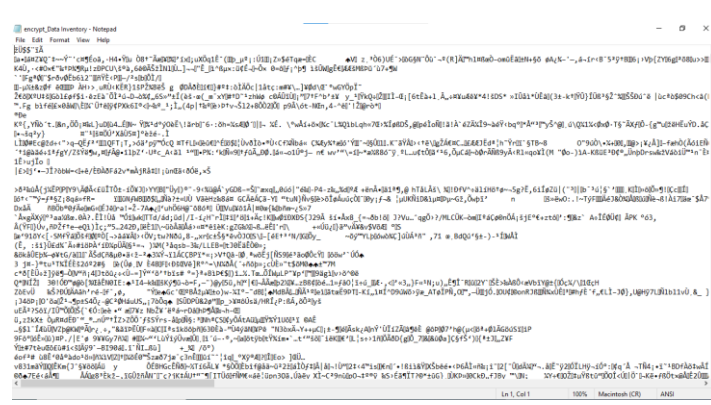
Pengujian dekripsi file ber ekstensi .doc, .docx, .xls, .xlsx, dan .pdf yang isi datanya sudah berubah tidak sama seperti data dari file asli.



Gambar 12. Hasil Dekripsi File.xls



Gambar 13. Hasil Dekripsi File.doc



Gambar 14. Hasil dekripsi file .pdf

4. KESIMPULAN

Setelah selesainya dilakukan analisis pada penelitian diatas, maka dapat ditarik kesimpulan bahwa dengan adanya aplikasi pengamanan *file* ini, penyimpanan data atau informasi keuangan, transaksi dan resep khususnya dalam bentuk dokumen data menjadi lebih aman. Dengan adanya aplikasi pengamanan *file* ini dapat menerapkan dan melakukan proses enkripsi atau dekripsi algoritma *Advances Encryption Standard* 128 (AES 128) dengan baik dan dikhususkan untuk mengamankan *file* dalam bentuk format *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, dan *.pdf saja. Waktu yang dibutuhkan untuk melakukakn proses enkripsi dan dekripsi sebanding dengan ukuran *file* yang diproses (semakin kecil ukuran *file* yang diproses, semakin cepat proses enkripsi dan dekripsi. Semakin besar ukuran *file*, semakin lama waktu untuk enkripsi dan dekripsinya). Aplikasi pengamanan *file* ini dapat terjamin keutuhan *file* pada saat enkripsi maupun didekripsikan tanpa mengalami kerusakan atau perubahan data ketika di dekripsi.

DAFTAR PUSTAKA

- [1] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.
- [2] 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>
- [3] L. Silalahi and A. Sindar, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 182–186, 2020, doi: 10.32672/jnkti.v3i2.2413.
- [4] 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.
- [5] B. Purba, F. A. Gulo, N. I. Utami, and ..., "Pengamanan File Teks Menggunakan Algoritma RC4," ... *Teknol. Komput. ...*, pp. 38–42, 2020, [Online]. Available: <http://seminar-id.com/prosiding/index.php/sainteks/article/view/473>
- [6] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encryption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.
- [7] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 54–60, 2020.
- [8] H. Wijaya, "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection," *Akad. J.*, vol. 17, no. 1, pp. 8–13, 2020.
- [9] W. N. Cholifah, Y. Yulianingsih, and S. M. Sagita, "Pengujian Black Box Testing pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 3, no. 2, p. 206, 2018, doi: 10.30998/string.v3i2.3048.