3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

# IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITME ADVANCED ENCRYPTION STANDART(AES-128) MENGAMANKAN DATA CUSTOMER PT.SARANA TEKNIK INTERNUSA

**Muhammad Ridho[1*], Dewi Kusumaningish[2]**

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]11911502266@student.budi.luhur.ac.id, [2]Dewi.Kusumaningsh@budiluhur.ac.id
(* : corresponding author)

**Abstrak-**PT. Sarana Teknik Internusa memiliki masalah untuk meyimpan data penting yang rapih dan aman.PT. Sarana Teknik Internusa adalah perusahaan dalam bidang penjualan filter udara cukup lama berdiri. Untuk menyimpan data penjualan dan lainya harus memiliki suatu aplikasi pengamanan data. Supaya tidak terjadi kehilangan atau kebocoran data pada PT. Sarana Teknik Internusa dibutuhkan suatu aplikasi atau web untuk mengamankan datanya. Kriptografi adalah teknik pengamanan informasi yang melibatkan pengolahan informasi awal *(plaintext*) menggunakan sebuah kunci dalam proses enkripsi. Hal tersebut dapat menghasilkan pesan baru yang disebut *chipertext*, yang untuk membacanya tidak dapat secara langsung. Untuk mengembalikan chipertext menjadi informasi awal, diperlukan proses deskripsi yang menggunakan kunci yang sama. Dengan demikian, kriptografi memungkinkan pengamanan informasi melalui proses enkripsi dan deskripsi. Dengan kriptografi bisa menjaga kerahasiaan file penting PT Sarana Internusa. Kriptografi yang digunakan akan memakai metode "*Advanced Encryption Standard*" (AES-128) adalah sebuah algoritme kriptografi simetris yang secara luas digunakan untuk melindungi keamanan data dalam berbagai aplikasi dan protokol. Penerapan kriptografi memungkinkan PT Sarana Internusa untuk menjaga kerahasiaan file-file penting mereka. Dalam konteks ini, kriptografi yang akan digunakan adalah metode "*Advanced Encryption Standard* (AES-128)", yang merupakan sebuah algoritme kriptografi simetris yang telah terbukti secara luas digunakan untuk melindungi keamanan data dalam berbagai aplikasi.

Kata kunci : PT. Sarana Teknik Internusa, Kriptografi, *Advanced Encryption Standard* (AES-128), *Plaintext*, *Chipertext*, Enkripsi dan Dekripsi.

# *IMPLEMENTATION OF CRYPTOGRAPHY USING ADVANCED ENCRYPTION STANDARD (AES-128) TO SECURE CUSTOMER DATA AT PT. SARANA TEKNIK INTERNUSA*

**Abstract**-*PT. Sarana Teknik Internusa has problems keeping important data neat and secure.PT. Sarana Teknik Internusa is a company in the field of air filter sales that has been around for a long time. To store sales data and others, you must have a data security application. So that data loss or leakage does not occur at PT. Sarana Teknik Internus requires an application or web to secure its data. Cryptography is an information security technique that involves processing initial information (plaintext) using a key in the encryption process. This can generate a new message called ciphertext, which cannot be read directly. To return the ciphertext to the initial information, a description process is required that uses the same key. Thus, cryptography allows information security through the process of encryption and description. With cryptography, PT Sarana Internusa can maintain the confidentiality of important files. The cryptography used will use the "Advanced Encryption Standard" (AES-128) method, which is a symmetric cryptographic algorithm that is widely used to protect data security in various applications and protocols. The application of cryptography allows PT Sarana Internusa to maintain the confidentiality of their important files. In this context, the cryptography that will be used is the "Advanced Encryption Standard (AES-128)" method, which is a symmetric cryptographic algorithm that has been proven to be widely used to protect data security in various applications.*

***Keywords****: PT. Sarana Teknik Internusa, Kriptografi, Advanced Encryption Standard (AES-128), Plaintext, Chipertext, Enkripsi dan Dekripsi.*

## 1. PENDAHULUAN

PT. Sarana Teknik Internusa merupakan perusahaan yang berada dipenjualan air filter dengan bermacam jenis yang memiliki kualitas terbaik. PT.Sarana Teknik Internusa menyediakan produk dan layanan yang berhubungan

dengaan air filter [1]. Sebagai perusahaan yang bergerak di indutri PT. Sarana Teknik Internusa memiliki banyak *customer* dari penjualan dan layanan produknya. tentu keamanan data sangat dibutuhkan oleh PT. Sarana Teknik Internusa dalam upaya melingduingi dan menjaga data *customer* yang dimilikinya. Dengan adanya salah satu visi dari PT. Sarana Teknik Internusa yaitu meningkatakna kualitas pelayanan dan komitmen untuk mempertahankan kepercayaan *customer* [2].

Seiring perkembangan teknologi dan pentingnya keamanan data pribadi. PT.Sarana Teknik Internusa menjaga data *customer* yang bisa bocor saat *file-file* dikirim dengan tidak adanya keamanan. Walaupun belum ada data yang bocor, oleh karna itu untuk menjaganya dengan ini PT. Sarana Teknik Internusa telah mengambil langkah-langkah untuk memastikan bahwa data para *customer* yang diterima aman[3]. Langkah-langkah yang diambil untuk meningkatkan keamanan data pelanggan, PT.Sarana Teknik Internusa akan membuat keamanan kriptografi untuk mengenkripsi data dan mencegah akses yang tidak sah[4].

Kriptografi merupakan ilmu yang bertujuan untuk menjaga keamanan informasi dengan mengubah pesan asli agar tidak dapat dipahami atau dibaca oleh pihak yang tidak berwenang. Fokus utama dari kriptografi adalah melindungi kerahasiaan, integritas, dan otentikasi data[5]. Dalam kriptografi, pesan asli yang belum diubah disebut sebagai plaintext, sedangkan pesan yang telah diubah menjadi bentuk yang tidak dapat dimengerti disebut *ciphertext.* Kriptografi melibatkan penggunaan algoritme matematis dan kunci enkripsi untuk melakukan proses enkripsi dan dekripsi[6].

Salah satu metode kriptografi yang populer adalah *Advanced Encryption Standard* (AES). AES terdiri dari tiga varian blok enkripsi, yaitu AES-128, AES-192, dan AES-256. Pada topik tugas akhir ini, metode yang digunakan adalah AES-128[7]. AES-128 adalah salah satu algoritme kriptografi simetris yang paling umum digunakan. Algoritme ini menggunakan kunci 128 bit untuk melakukan proses enkripsi dan dekripsi data. AES-128 menggantikan standar enkripsi sebelumnya, yaitu *Data Encryption Standard* (DES), dengan tingkat keamanan dan kecepatan yang lebih baik[8]. AES-128 telah terbukti kuat dan aman dalam menjaga keamanan data. Meskipun menggunakan kunci 128 bit, algoritme ini mampu memberikan tingkat keamanan yang tinggi dalam proses enkripsi dan dekripsi data dan informasi.Penelitian sebelumnya yaitu "Pengamanan Data Pelanggan dan Penjual Menggunakan Implementasi Algoritme RSA" yang mengimplementasikan aplikasi berbasis web, sedangkan pada penelitian kali ini berbasis web untuk mengamankan data penjualan dan pembelian dengan menggunakan metode AES-128[9].

# 2. METODE PENELITIAN

## 2.1. Studi Literatur

Pada Tahap Literature Review Dilakukan Review Terhadap Berbagai Penelitian Sebelumnya, Khususnya Sistem Keamanan Database Menggunakan Advanced Economic Standar (AES-128).Red Avenue Indonesia, Aplikasi Keamanan Data Menggunakan Discrete Cosine Transform dan Algoritma 128-Bit AES Cipher Hide Di SMK PGRI 15 Jakarta, Aplikasi Chat Security Android Menggunakan Kriptografi Menggunakan Metode Kode Advanced Standar (AES) 128 Di PT. Selamat Medina Indonesia, Polda Timur Nusa Tenggara Penyimpanan Dokumen Penting Keamanan Website Dengan Alternatif AES-128, Implementasi dan Analisis Alternatif AES (Advanced Encryption Standard) Pada File Multifungsi Ketiga, Kriptografi Untuk Keamanan Data, Implementasi Classic C Ryptography In Com- Berbasis Unication Text, Mengamankan Data Informasi Dengan Kriptografi Klasik, Implementasi Algoritma Enkripsi RSA Untuk Enkripsi dan Dekripsi Email, Implementasi Data Safe Code Pada Pesan Teks dan Isi Dokumen Dan File Dokumen Menggunakan Standard Advanced Engine.

## 2.2. Tahapan Pengumpulan Data

Wawancara (*Interview*), wawancara dengan pihak terkait yang bertujuan agar dapat mengantisipasi permasalahan yang sudah ada sehingga dapat menghasilkan sebuah perancangan sistem yang dapat menyelesaikan masalah tersebut. Observasi (*Observation*), pada PT. Sarana Teknik Internusa untuk mengetahui keadaansebenarnya dari objek penelitian. Tujuannya adalah untuk memperoleh penjelasan tentang informasi dan data yang diperlukan untuk penelitian.

## 2.3. Analisis Sistem

### 2.3.1. Analisis Data

Salah satu langkah untuk mengatasi masalah keamanan ini, dalam analisis data, adalahmengumpulkan file-file yang digunakan untuk mendapatkan informasi yang dibutuhkan untuk merancangprogram. Kumpulan file menurut jenisnya. Dekripsi File menentukan langkah-langkah yang digunaka untuk membuat aplikasi yang mudah dipahami.

### 2.3.2. Analisis implementasi algoritma

Setelah tahap pengumpulan data dan memantau pengoperasian sistem. Selanjutnya, implementasi alias dari algoritma dilakukan. Analisis Aplikasi Algoritmik menjelaskan langkah-langkah penerapan enkripsi AES (Advanced Encryption Standard) untuk melindungi data penting. Jadi tentukan kunci yang digunakan untuk mengenkripsi dan mendekripsi file. Proses mengenkripsi file dengan kunci enkripsi, khususnya proses mengubah file terenkripsi menjadi ciphertext dengan menggunakan kunci enkripsi. Dengan Proses dekripsi ciphertext menggunakan kunci yang sama dengan kunci enkripsi, yaitu proses mengubah ciphertext menjadi pesan yang dapat dibaca (plaintext).

### 2.3.3. Analisis System

Pengamanan yang digunakan pada sistem adalah proses enkripsi isi file. Enkripsi dilakukan untuk mengamankan isi file rahasia (hanya pihak yang berwenang yang dapat mengaksesnya). Karena membutuhkan modul untuk mengenkripsi data. Modul enkripsi yang ditempatkan di aplikasi akan dipanggil saat pengguna mengamankan konten file. Selama ini, modul dekripsi dipanggil ketika pengguna ingin melihat isi file.

### 2.3.4. Desain Perangkat Lunak

Pada tahap perancangan sesuai hasil analisis sistem khususnya pada perancangan enkripsi dan dekripsi. Selain itu, dukungan tambahan dibangun ke dalam desain aplikasi dan antarmuka pengguna. Pengembangan sistem ini menggunakan metode waterfall, model harus diselesaikan satu per satu sebelum melanjutkan ke langkah selanjutnya, dan hasil setiap langkah harus dicatat secara akurat.

### 2.3.5. Implementasi

Dalam implementasi ini, apa yang dikandung pada tahap desain diwujudkan dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi ini perangkat lunak yang digunakan untuk melakukan pengamanan file data menggunakan bahasa pemrograman PHP dan phpMyAdmin sebagai databasenya. Hardware yang digunakan adalah MSI Modern 14 BSM, CPU AMD Ryzen 5 5500U, RAM 16GB DDR4, SSD 512GB.

### 2.3.6. Pemeriksaan Sistem

Metode pengujian berupa kotak hitam yang digunakan untuk memeriksa kesalahan dan ketika dieksekusi, aplikasi akan menunjukkan apakah data yang dimasukkan benar atau tidak dan hasil yang diperoleh benar atau tidak.

### 2.3.7. Kesimpulan

Langkah terakhir ini menyimpulkan bahwa adopsi kriptografi Advanced Encryption Standard (AES) 128 bekerja dengan baik dan dapat mengamankan file data yang dibeli dan dijual di Galeri Baroqah Mobil dan saat ini ada proposal untuk pengembangan di area ini. sistem

## 2.4. *Advanced Encryption Standard* 128

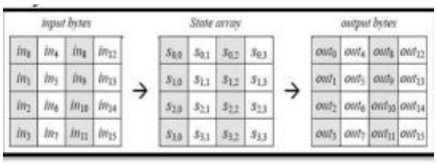
Pada tahun 1997, kontes seleksi standar Sebuah algoritma kriptografi baru untuk menggantikan DES diperkenalkan dan dengan dihadiri oleh 21 peserta dari seluruh dunia.Setelah melalui seleksi yang ketat,pada tahun 1999 hanya ada 5 kandidat yaitu algoritma Ular (Universitas Ross Anderson-Cambridge, Eli Biham-Technion, Universitas Lars Knudsen California San Diego), MARS (IBM USA), Twofish (Bruce Schneier, John Kelsey dan Niels Ferguson-Counterpane Internet Security Inc, Doug kunci Encoding dalam Decoding Jelas teks sandi Hapus teks Majalah Komputer Mulawarman Vol. 10 Tidak. 1 Februari 2015 23 Whiting-Hi/fn Inc., David Wagner-Universitas California Berkeley, Chris Hall-Princeton Universitas), Rijndael (Dr. Vincent RijmenKatholieke Universiteit Leuven dan Dr. Joan Daemen-Proton World International) dan RC6 (RSA AS). Setahun kemudian pada tahun 2000, algoritma Rijndael dipilih sebagai algoritma kriptografi Selain aman, juga efektif dalam kinerja dan memahkotai AES. Nama asli Rijndael berasal dari gabungan nama penemunya.

## 2.5. Proses Enkripsi

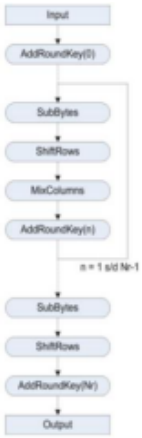
Berikut Gambar 1 adalah perbandingan jumlah proses panjang kunci yang ditransfer per bit masukan [10]. Algoritma AES adalah cipher simetris dan cipher blok. Algoritma ini menggunakan kunci yang sama untuk enkripsi dan dekripsi, input dan output dalam bentuk blok dan kunci yang digunakan seperti Gmabar 2. AES memiliki blok tetap dan ukuran kunci 128, 192, 256 bit.

| Tipe | Jumlah key (Nk) | Besar Blok (Nb) | Jumlah Round (Nr) |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

Gambar 1 Tipe AES




Gambar 2 Input dan Output




Gambar 3. Algoritma Enkripsi AES

Operasi AES dilakukan terhadap array of byte dua dimensi (state). State memiliki ukuran NROWS X NCOLS. Pada saat awal enkripsi, data yang berupa in0, in2, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin kedalam array state. State ini yang nantinya dilakukan enkripsi/dekripsi. Kemudian keluarannya akan ditampung kedalam array out..

Masing-masing menggunakan kunci internal yang berbeda, yaitu kunci menara untuk setiap proses menara. Proses putaran enkripsi AES-128 dilakukan dalam 10 putaran sebagai Gamabar 3 berikut.

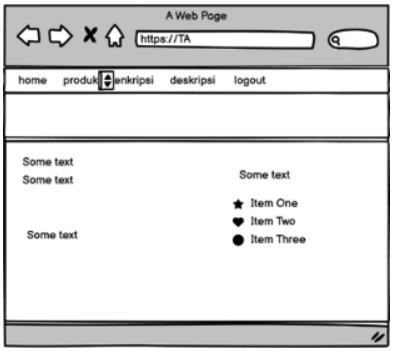
a. Kunci pelengkap, XOR antara data asli (jelas) dan kunci enkripsi. Langkah ini disebut putara awal.
b. Lakukan sebanyak 9 kali putaran, proses yang dilakukan pada setiap putaran adalah Studi kasus pada sistem keamanan basis data menggunakan algoritma standar enkripsi canggih 824 (AES-128): Jalan Merah Indonesia SubByte, ShiftRows, MixColumns, dan AddRoundKey.
c. Babak Final, yaitu proses babak ke 10.

## 2.6. Proses Dekripsi

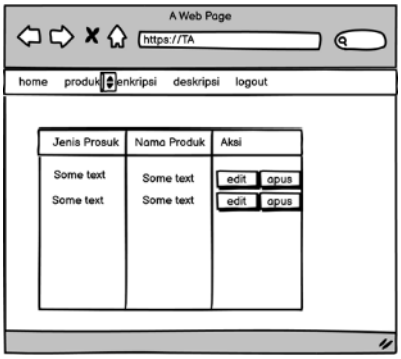
Transformasi chipper dapat dibalikan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse chipper yang mudah dipahami untuk algoritma AES. Transformasi byte ysng digunakan pada inverse chipper pada proses dekripsi AES adalah InvShiftRows,InvSubytes, InvMixColumns, dan AddRoundkey.

## 2.7. Rancangan Layar

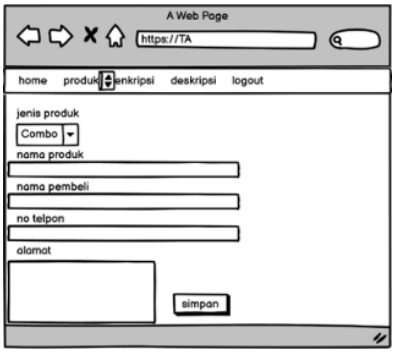
Dalam pembuatan suatu aplikasi, sangat diperlukan tahap perancangan layar sebagai bentuk dasar dalam membuat desain aplikasi yang diinginkan. Rancangan layar harus mudah dimengerti, tujuannya agar pengguna dapat merasa nyaman dan tidak bingung dalam menggunakan aplikasi ini [10]. Dapat dilihat pada gambar 4-9.



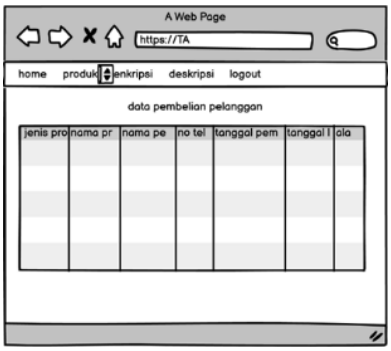

Gambar 4. Rancangan *Home*



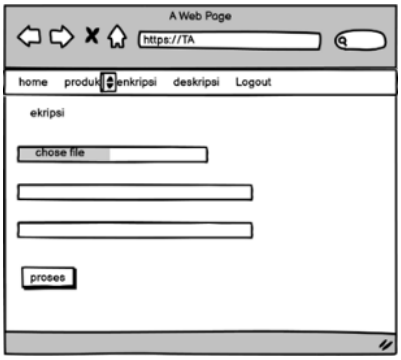

Gambar 5 Rancangan Data Produk



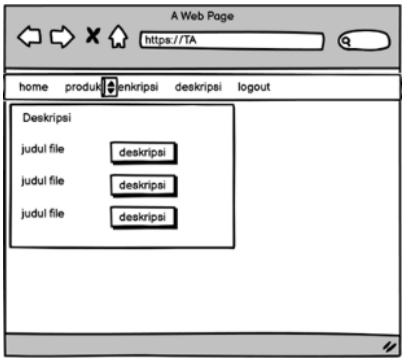

Gambar 6 Rancangan Form Pembelian




Gambar 7 Rancangan Data Pembelian




Gambar 8 Rancangan Enkripsi




Gambar 9. Rancangan Dekripsi

## 3. HASIL DAN PEMBAHASAN

Pada bagian ini adalah penjelasan dari implementasi algoritme AES-128 untuk enkripsi dan dekripsi data PT. Sarana Teknik Internusa. Bagian ini menjelaskan tentang *flowchart*, algoritme, proses, hasil enkripsi dan dekripsi dokumen dalam sebuah aplikasi.

### 3.1 *Flowchart* Enkripsi

Pada gambar 10. merupakan *flowchart* dari halaman form enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi file admin harus memasukkan password, setelah itu program akan memproses enkripsi.

Gambar 10. *Flowchart* Enkripsi

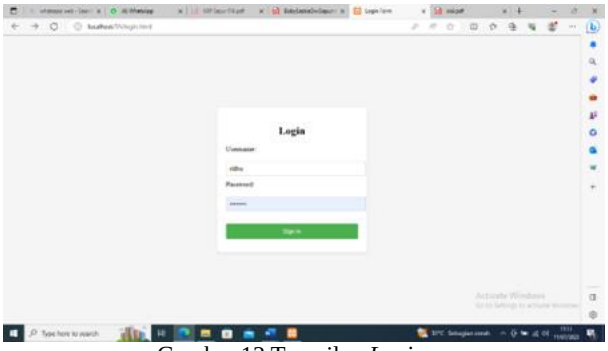
### 3.2 *Flowchart* Dekripsi

Pada gambar 11 merupakan *flowchart* dari halaman dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan dekripsi file. Dalam dekripsi file admin harus memasukkan password yang sesuai dengan enkripsi, setelah itu program akan memproses dekripsi.

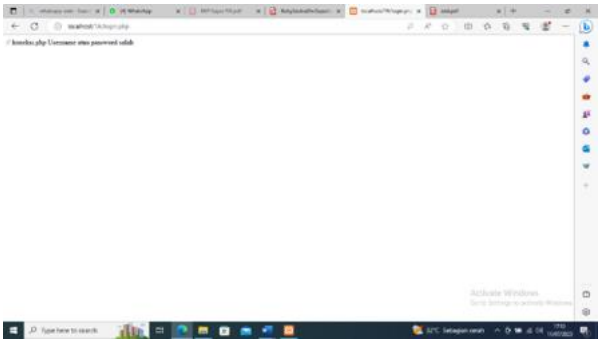
Gambar 11. Flowchar Dekripsi

### 3.3 Tampilan Layar

Pada tampilan layar Gambar 12-19, terdiri beberapa tampilan seperti tampilan login, tampilan home, tampilan listproduk, tampilan form, tampilan data pembelia, tampilan enkripsi, dan tampilan dekripsi.

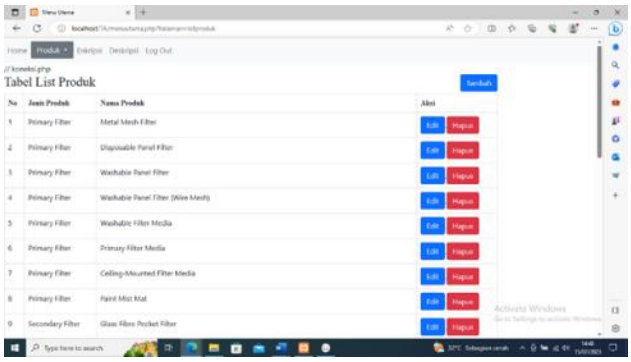



Gambar 12 Tampilan *Login*

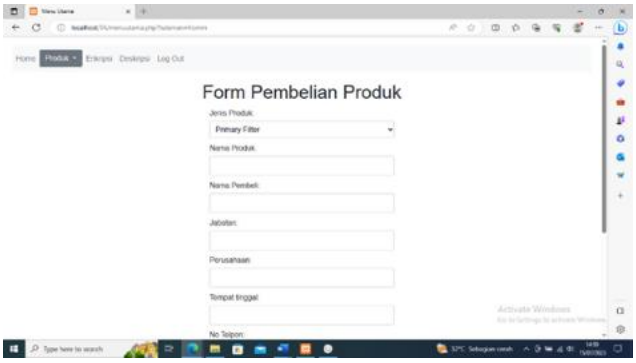


Gambar 13 Tampilan Gagal Login

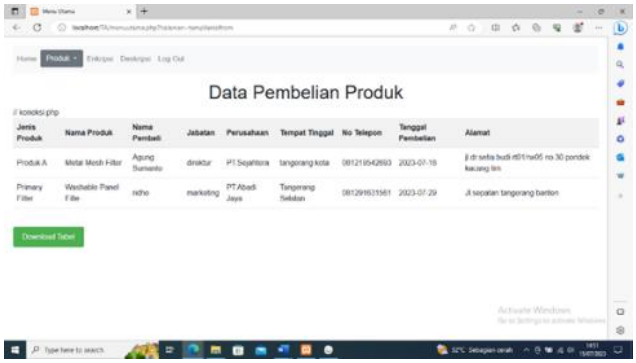

Gambar 14 Tampilan Home



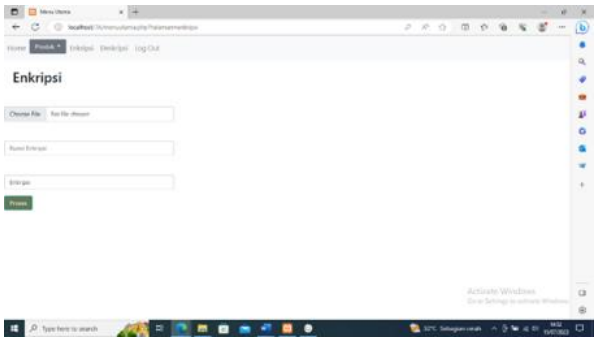

Gambar 15 Tampilan Tabel Produk



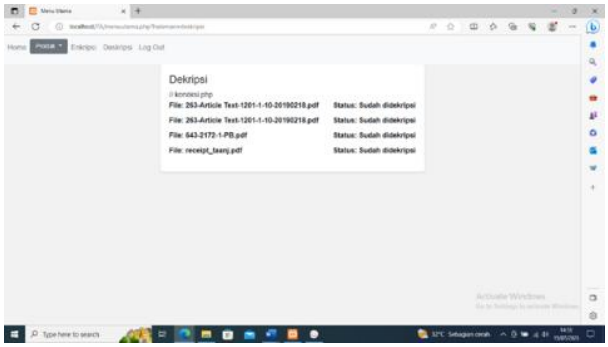

Gambar 16 Tampilan Form Produk




Gambar 17 Tampilan Data Pembelian Produk




Gambar 18 Tampilan Enkripsi




Gambar 19. Tampilan Dekripsi

### 3.4 Pengujian File

Dari pengujian yang telah dilakukan terdapat sisi kecepatan dan hasil enkripsi yang berupa file tidak bisa dibuka dan beberapa ukuran data sebelum dan sesudah dienkripsi menggunakan algoritme kriptografi AES-128. Tabel 1 menunjukan hasil pengujian yang dilakukan.

**Tabel 1**. Pengujian File

| Nama *File* | Ukuran *File* (*Kilobyte*) | | | Waktu (Detik) | |
|---|---|---|---|---|---|
| | Asli | Enkripsi | Dekripsi | Enkripsi | Dekripsi |
| PO MASUK STI 2023 | 105 KB | 141 KB | 105 KB | 0,457 | 0,600 |

## 4. KESIMPULAN

Kriptografi dengan metode AES-128 dapat mengamankan file penting pada PT. Sarana Teknik Internusa dengan cepat dan aman. Aplikasi ini dapat digunakan untuk menginput data penjualan dan pembelian serta untuk mengamankan file data penjualan dan pembelian pada PT. Sarana Teknik Internusa. Dengan memodifikasi proses enkripsi khususnya pada random key, aplikasi ini memiliki tingkat keamanan yang tinggi. Aplikasi ini bisa mengamankan file dengan format .pdf. Diharapkan untuk dikembangkan lagi untuk program enkripsi dan dekripsi file ini dengan memodifikasi ataupu mengkombinasikan metode AES-128 dengan metode yang lain supaya sistem semakin sulit untuk diretas. Diharapkan untuk dikembangkan lagi aplikasi ini supaya fleksibilitas dengan membuat versi mobile dari aplikasi ini.

# DAFTAR PUSTAKA

[1] Akbar, F., & Waluyo, S. (2018). Sistem Keamanan Database Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus: Red Avenue Indonesia. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *1*(2), 821-828.

[2] Rahmawati, R., & Rahardjo, D. (2016). Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi AES 128 BIT pada SMK PGRI 15 Jakarta. *Jurnal Teknik Informatika dan Sistem Informasi*, *2*(1).

[3] Hadi, W. K., & Mulyati, S., "Pengamanan Aplikasi Chatting Pada Perangkat Android Menggunakan Kriptografi Dengan Metode Advanced Encryption Standard (AES) 128 Pada PT. Salam Medina Indonesia", *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, *14*(2), 2017.

[4] Gadja, A. L., & Belutowe, Y. S., "Pengamanan Website Pengarsipan Dokumen Penting Di Polda Nusa Tenggara Timur Dengan Algoritma AES-128", In *Seminar Nasional & Konferensi Ilmiah Sistem Informasi, Informatika & Komunikasi* (pp. 636-641), 2018, November.

[5] Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W., "Implementasi Dan Analisis Algoritma Advanced Encryption Standard (AES) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia". *Transient: Jurnal Ilmiah Teknik Elektro*, *4*(4), 1008-10112, 2016.

[6] Mukhtar, H. *Kriptografi untuk Keamanan Data*. Deepublish. 2018.

[7] Amin, M. M. Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Pseudocode*, *3*(2), 129-136. 2016.

[8] Sasongko, J. Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Dinamik*, *10*(3). 2005.

[9] Ginting, A., Isnanto, R. R., & Windasari, I. P., "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email". *Jurnal Teknologi dan Sistem Komputer*, *3*(2), 253-258, 2015.

[10] Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H., "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard". *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20-31, 2016.