EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i2.2178

Aplikasi Pengamanan Data Inventaris Menggunakan Algoritma Kriptografi Tripple DES dan RC4

Simon Ricardo Valentino Hutauruk [1*], Mufida Khairani[2]
[1*,2] Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia
[1*]simonricardo190@gmail.com, [2]mufidakhairani1219@gmail.com
[*)] simonricardo190@gmail.com

Abstrak-Keamanan data merupakan aspek penting dalam pengelolaan informasi, khususnya data inventaris yang meliputi aset, persediaan, dan logistik. Jika data ini disalahgunakan, dapat menyebabkan kerugian finansial dan operasional. Penelitian ini membangun sistem keamanan data inventaris yang memanfaatkan algoritma kriptografi Triple Data Encryption Standard (Triple DES) dan Rivest Cipher 4 (RC4). Sistem ini mampu melindungi kolom nama barang dan harga dalam inventaris serta menyediakan fitur dekripsi data yang telah terenkripsi. Selain itu, keamanan aplikasi diperkuat melalui autentikasi pengguna. Kombinasi kedua algoritma kriptografi ini mampu memberikan solusi keamanan yang optimal, dengan mempertimbangkan performa dan kecepatan sistem tanpa mengganggu operasional harian.

Kata Kunci*: Inventaris, Kriptografi, RC4Data, TripleDES*

Abstract−Data security is an essential aspect of information management, particularly inventory data, which includes assets, supplies, and logistics. If this data is misused, it can lead to financial and operational losses. This research develops an inventory data security system that utilizes the Triple Data Encryption Standard (Triple DES) and Rivest Cipher 4 (RC4) cryptographic algorithms. The systemis capable of protecting the item name and price columns in the inventory, as well as providing a decryption feature for encrypted data. Additionally, the security of the application is strengthened through user authentication. Combining these two cryptographic algorithms offers an optimal security solution, considering system performance and speed without disrupting daily operations.

Keywords: *Inventory, Cryptographic, RC4Data, Triple DES*

1. PENDAHULUAN

Keamanan data merupakan salah satu aspek yang sangat penting dalam pengelolaan informasi di berbagai organisasi. Data inventaris, yang mencakup informasi mengenai aset, persediaan, dan logistik, memegang peranan krusial dalam operasional sehari-hari. Jika data ini jatuh ke tangan yang tidak berwenang, dapat menyebabkan kerugian finansial, gangguan operasional, dan risiko keamanan yang signifikan. Oleh karena itu, diperlukan metode yang efektif untuk melindungi data inventaris dari ancaman seperti pencurian data, pemalsuan, dan akses yang tidak sah.

Dalam upaya meningkatkan keamanan data, kriptografi telah menjadi salah satu pendekatan utama yang digunakan. Kriptografi melibatkan teknik-teknik untuk mengubah informasi menjadi bentuk yang tidak dapat dipahami. Dua algoritma kriptografi yang dikenal luas adalah Triple Data Encryption Standard (Triple DES) dan Rivest Cipher 4 (RC4). Triple DES merupakan pengembangan dari DES yang dirancang untuk mengatasi kelemahan keamanan pada sesi panjang kunci algoritma DES. Dengan melakukan enkripsi data sebanyak tiga kali menggunakan kunci yang berbeda, Triple DES mampu memberikan tingkat keamanan yang lebih tinggi dibandingkan DES, meskipun dengan biaya kinerja yang lebih [1]. Di sisi lain, RC4 merupakan stream cipher yang terkenal karena kecepatannya dalam proses enkripsi dan dekripsi [2]. RC4 banyak digunakan dalam berbagai aplikasi seperti protokol jaringan, dan pengamanan teks, RC4 sering digunakan karena efisiensinya [3].

Dengan menggabungkan kedua algoritma ini, aplikasi pengamanan data inventaris diharapkan dapat memanfaatkan kekuatan masing-masing algoritma, yaitu keamanan tinggi dari Triple DES dan kecepatan dari RC4. Kombinasi ini bertujuan untuk menyediakan solusi enkripsi yang tidak hanya aman tetapi juga efisien dalam hal kinerja, sehingga tidak menghambat operasional sehari-hari. Pada file berukuran 58 KB dibutuhkan waktu 5 detik dan pada file berukuran 214 KB dibutuhkan waktu 13 detik[4].

Keamanan data merupakan salah satu aspek yang sangat penting dalam pengelolaan informasi di berbagai organisasi. Data inventaris, yang mencakup informasi mengenai aset, persediaan, dan logistik, memegang peranan krusial dalam operasional sehari-hari. Jika data ini jatuh ke tangan yang tidak berwenang, dapat menyebabkan kerugian finansial, gangguan operasional, dan risiko keamanan yang signifikan. Oleh karena itu, diperlukan metode yang efektif untuk melindungi data inventaris dari ancaman seperti pencurian data,

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i2.2178

pemalsuan, dan akses yang tidak sah. Dalam upaya meningkatkan keamanan data, kriptografi telah menjadi salah satu pendekatan utama yang digunakan. Kriptografi melibatkan teknik-teknik untuk mengubah informasi menjadi bentuk yang tidak dapat dipahami. Dua algoritma kriptografi yang dikenal luas adalah Triple Data Encryption Standard (Triple DES) dan Rivest Cipher 4 (RC4). Triple DES merupakan pengembangan dari DES yang dirancang untuk mengatasi kelemahan keamanan pada sesi panjang kunci algoritma DES. Dengan melakukan enkripsi data sebanyak tiga kali menggunakan kunci yang berbeda, Triple DES mampu memberikan tingkat keamanan yang lebih tinggi dibandingkan DES, meskipun dengan biaya kinerja yang lebih [1]. Di sisi lain, RC4 merupakan stream cipher yang terkenal karena kecepatannya dalam proses enkripsi dan dekripsi [2]. RC4 banyak digunakan dalam berbagai aplikasi seperti protokol jaringan, dan pengamanan teks, RC4 sering digunakan karena efisiensinya [3]. Dengan menggabungkan kedua algoritma ini, aplikasi pengamanan data inventaris dapat memanfaatkan kekuatan masing-masing algoritma, yaitu keamanan tinggi dari Triple DES dan kecepatan dari RC4. Kombinasi ini bertujuan untuk menyediakan solusi enkripsi yang tidak hanya aman tetapi juga efisien dalam hal kinerja, sehingga tidak menghambat operasional sehari-hari.

2. METODE PENELITIAN

2.1 Data

Data merupakan sekumpulan keterangan ataupun fakta yang dibuat dengan kata-kata, kalimat, simbol, angka dan lainnya. Data dapat diperoleh melalui sebuah proses pencarian dan juga pengamatan berdasarkan sumber-sumber yang ada [5]. Data dapat dikelompokkan menjadi beberapa jenis berdasarkan sifat, sumber, cara mendapatkanya serta waktu pengumpulan data tersebut[6]. Adapun rinciannya sebagai berikut:

a. Data menurut sifatnya.
   Terbagi atas data kualitatif dan data kuantitatif. Data kualitatif merupakan data yang tidak berbentuk angka, biasanya berisi analisa kondisi saat ini pada suatu organisasi, sehingga membantu peneliti dalam menentukan permasalahan, seperti data observasi atau catatan permasalah yang pernah dihadapi. Data kuantitatif merupakan data berbentuk angka dapat berupa data dengan nilai yang terbatas pada bilangan bulat (diskrit) dan data yang nilainya dapat berubah secara terus menerus (kontinu).
b. Data menurut sumbernya.
   Terbagi atas data internal dan data eksternal. Data internal merupakan data yang didapatkan dari dalam organisasi, perusahaan atau tempat dilakukannya penelitian, seperti data keuangan, produksi dan hasil penjualan. Data eksternal merupakan data yang diperoleh dari luar perusahaan atau organisasi, seperti data inflasi, pendapatan masyarakat dan lainnya.
c. Data menurut cara mendapatkannya.
   Terbagi atas data primer dan sekunder. Data primer adalah data yang dikumpulkan langsung untuk maksud yang diketahui atau diteliti, seperti data yang didapatkan melalui kuisioner. Data sekunder merupakan data yang dikumpulkan untuk maksud selain menyelesaikan masalah yang dihadapi. Data ini didapatkan melalui internet atausumber lain seperti jurnal yang biasanya digunakan sebagai pelengkap teori dari suatupenelitian.
d. Data menurut waktu pengumpulannya
   Terbagi atas data *cross section* dan *time series*. Data *cross section* merupakan data yang dikumpulkan dalam waktu tertentu yang dapat menggambarkan keadaan/kegiatan pada waktu tersebut, seperti data sensus penduduk, kuisoner pelanggan pada waktu tertentu dan lainnya. Data *time series* merupakan data dari satu periode ke periode lainnya. Data ini memberikan gambaran tentang perkembangan suatu kegiatan dari waktu ke waktu, seperti data perkembangan ekonomi, data perkembangan jumlah mahasiswa
   Data dapat dikumpulkan dan diolah, sehingga menghasilkan suatu informasi. Data yang baik harus sesuai dengan kebenaran, akurat, tepat waktu dan mencakup ruang lingkup yang luas. Data yang relevan dan diolah dengan baik dapat memberikan beberapa manfaat, seperti membantu dalam pengambilan keputusan, sebagai dasar dalam perencanaan lanjut, bahan acuan atau implementasi suatu kegiatan dan sebagai bahan evaluasi [7].

2.2 Kriptografi

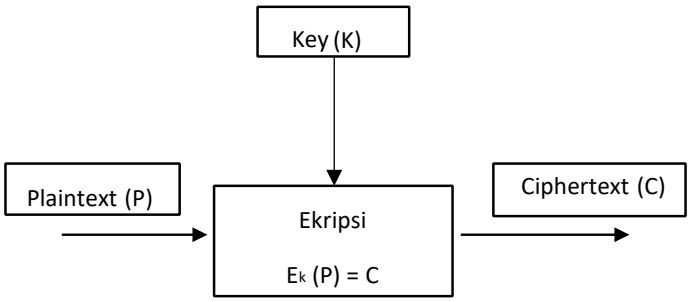
Kriptografi berasal dari bahasa Yunani, yaitu cryptos yang berarti rahasia dan graphein yang berarti tulisan. Secara terminologi kriptografi diartikan sebagai ilmu dan seni yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga [8]

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i2.2178

Pada penerapannya, kriptografi menggunakan teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data[9]. Kriptografi melibatkan dua proses utama, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses untuk mengamankan data yang disebut *plaintext* menjadi data yang tersembunyi atau *ciphertext*. *Plaintext* merupakan data atau pesan yang mudah dibaca, sedangkan *ciphertext* merupakan data atau pesan yang tidak dapat dimengerti. Dekripsi merupakan proses mengembalikan *ciphertext* menjadi *plaintext* [10].

2.2.2 Klafikasi Kriptografi

Berdasarkan kunci yang dipakai, kriptografi dibagi menjadi dua bagian, yaitu kriptografi simetris dan asimetris. Kriptografi simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini dibagi menjadi dua kategori, yaitu algoritma aliran (stream cipher) dan algoritma blok (block cipher). Pada algoritma *stream cipher* proses penyandiannya akan beriorientasi pada satu *bit/byte* data, sedangkan pada algoritma *block cipher*, proses penyandiannya berorientasi pada sekumpulan *bit/byte* data (per blok) [11]. Penggunaan kriptografi asimetris dimulai pada tahun 70an setelah teknik ini dipublikasikan oleh Whitfield Diffie dan Martin Hellman [12].



Gambar 1. Proses Enkripsi Kriptografi Simetris [13]

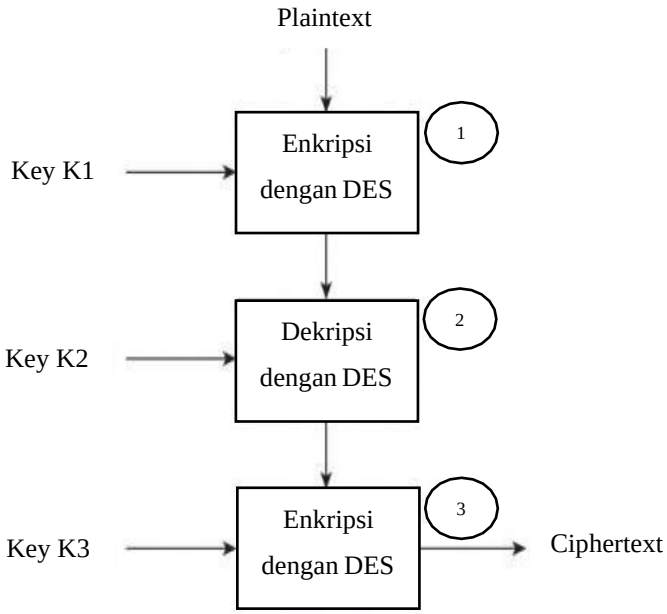
2.2.3 Algoritma Triple DES

Algoritma Triple DES merupakan algoritma simetris hasil dari pengembangan algoritma DES yang telah dienkripsi sebanyak tiga kali. Triple DES menggunakan tiga kunci dengan panjang 168 bit. Triple DES mempunyai tiga tahap yang merupakan hasil dari implementasi algortima DES [14]. Adapun tahapannya sebagai berikut:

a. Tahap pertama, plaintext yang dioperasikan dengan kunci eksternal pertama (K1) dan dienkripsi dengan menggunakan algoritma DES
b. Tahap kedua, hasil dari enkripsi pada tahap pertama kemudian dioperasikan dengan menggunakan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses dekripsi. Jika dilakukan enkripsi, maka Triple DES ini menggunakan jenis enkripsiCiphertext (C) Plaintext (P) Key (K1) Enkripsi Ek (P) = C Dekripsi Dk (C) = P Plaintext (P) Key (K2) 11 enkripsi-enkripsi (EEE). Jika pada tahap kedua menggunakan proses dekripsi, maka jenis Triple DES yang digunakan adalah enkripsi-dekripsi-enkripsi (EDE).
c. Tahap ketiga, ciphertext yang dihasilkan pada tahap kedua dioperasikan dengan menggunakan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan ciphertext.

Pemilihan kunci pada algoritma Triple DES dapat menggunakan dua ketentuan. Ketentuan pertama ketiga kunci bersifat saling bebas, dimana K1≠ K2≠ K3≠ K1. Ketentuan kedua menggunakan kunci yang saling bebas pada K1 dan K2 dan terikat pada K3 dan K1, dimana K1≠ K2 dan K3 = K1. Penggunaan jenis kunci pada ketentuan kedua ini biasanya digunakan pada model EEE algoritma Triple DES [16]. Untuk proses dekripsi menggunakan langkah yang sama DED ataupun DDD dengan urutan kunci dimulai dari K3. Triple DES merupakan pengembangan dari algoritma DES yang memiliki kelebihan dalam hal mudah untuk diimplementasikan tanpa harus mengubah infrastruktur secara masif. Jika dibandingkan dengan algoritma AES, Triple DES memiliki kecepatan yang lebih lambat dikarenakan Triple DES melakukan tiga kali proses enkripsi dekripsi.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i2.2178



Gambar 2. Tahapan Enkripsi Triple DES [15]

Rumus yang digunakan untuk melakukan enkripsi dengan algoritma Triple DES sebagai berikut:

$$C = EK3(DK2(EK1(P))) \quad (1)$$

Keterangan:

C = Ciphertext.
E = Enkripsi.
P = Plaintext.
K = Kunci.

Sedangkan untuk pembaruan variabel pada Triple Des dapat dilakukan dengan rumus sebagai berikut.

$$Ri+i = Li \oplus F(Ri, Ki) \quad (2)$$

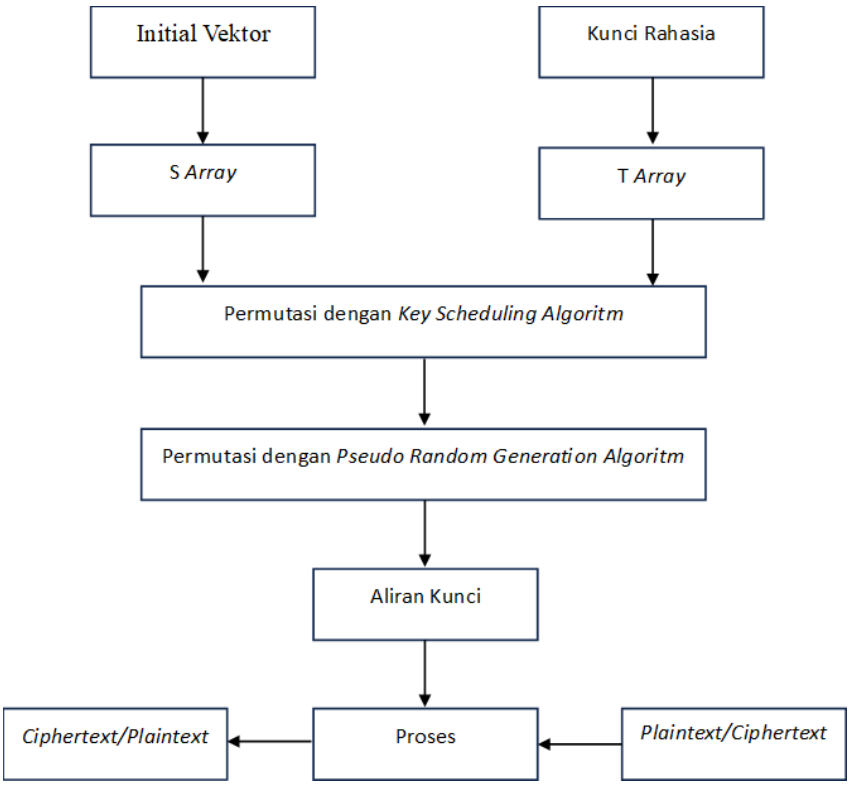
Keterangan:

Li = plaintext kiri iterasi ke-i
F (Ri, Ki) = Hasil dari fungsi permutasi
Ri = plaintext kanan ke-i

Algoritma *Rivest Cipher* 4 (RC4) merupakan jenis algoritma aliran (*stream cipher*) yang menggunakan operasi biner (XOR). Ditemukan oleh Ronald Rivest pada tahun 1987. RC4memiliki kunci dengan panjang 2048 *bit* (256 *byte*) [17]. RC4 biasanya digunakan untuk pengamanan pada *Secure Socket Layer/Transport Layer Security* (SSL/TLS), *Wifi Protected Access – Temporal Key Integrity Protocol* (WPA-TKIP). RC4 merupakan algoritma kriptografi yang terbentuk dari dua algoritma dasar, yaitu *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generator Algorithm* (PGRA). KSA menginisialisasi *state array* menggunakan kunci simetris. *State array* adalah permutasi dari angka 0 hingga 255, PRGA menggunakan state array yang telah dipermutasi untuk menghasilkan stream kunci (*keystream*). RC4 menggunakan keystream yang dihasilkan oleh PRGA untuk melakukan enkripsi dan dekripsi dengan operasi XOR [18]. Adapun langkah-langkah yang harus dilakukan agar pesan dapat terenkripsi dengan algoritma RC4 sebagai berikut:

a. Melakukan inisialisasi larik yang berada di dalam *S-box*, larik berjumlah 256 kotak dimulai dari larik 0 hingga 255.
b. Menentukan nilai kunci, jika panjang kunci < 256, maka dilakukan *padding* dengan cara mengulangi kunci yang ada hingga panjang kunci menjadi 256 *byte*.
c. Melakukan permutasi nilai-nilai di dalam larik *S-Box*, proses ini dinamakan *Key Schedulling Algorithm* (KSA).
d. Melakukan pembangkitan kunci, proses ini dinamakan *Pseudo Random GenerationAlgorithm* (PRGA) dan enkripsi pesan.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i2.2178



Gambar 3. Tahapan Enkripsi RC4 [19]

Penggunaan kunci pada algoritma RC4 biasanya hanya sepanjang 40 hingga 128 *bit*, sisanya digunakan untuk perulangan kunci yang dipakai, hingga panjang kunci mencapai 255 *byte*.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Database

Database yang dibuat memiliki tiga tabel, yaitu tb_inventaris, tb_kunci, dan tb_pengguna. Gambar 4 merupakan tabel tb_inventaris digunakan untuk menyimpan data inventaris barang yang memiliki beberapa kolom, yaitu kolom ID, barang, satuan, jumlah, harga, dan status.

tb_inventaris

Field Name	Data Type
ID	AutoNumber
barang	Short Text
satuan	Short Text
jumlah	Short Text
harga	Short Text
status	Short Text

Gambar 4. Tampilan tb_inventaris

Gambar 5 adalah rancangan tabel tb_kunci yang berfungsi untuk menampung data kunci. Tabel ini terdiri dari *field* k1, k2 dan k3 untuk menampung data kunci *Triple* DES, *field* k4 untuk menampung data kunci RC4.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i2.2178

Field Name	Data Type
k1	Long Text
k2	Long Text
k3	Long Text
k4	Long Text

Gambar 5. Tampilan tb_kunci

Gambar 6 adalah rancangan tabel tb_pengguna yang berfungsi untuk menampung data akses pengguna kedalam aplikasi. Tabel ini terdiri dari tiga *field*, yaitu ID untuk data id pengguna, idu untuk data *username* pengguna dan *field* pass untuk data password pengguna.

Field Name	Data Type
ID	AutoNumber
idu	Short Text
pass	Short Text

Gambar 6. Tampilan tb_pengguna

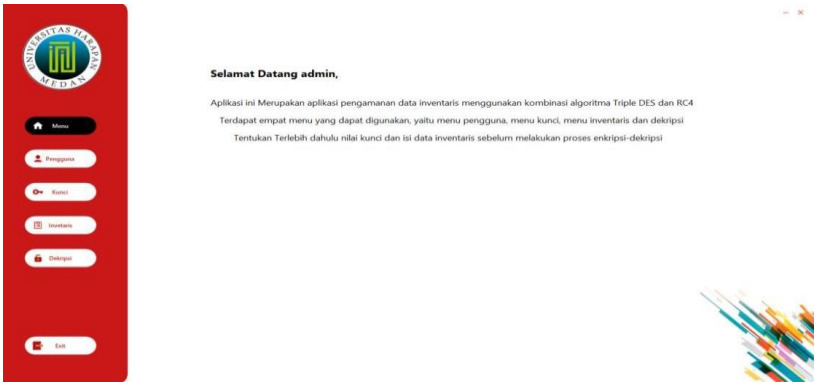
3.3 Pengujian Sistem

Pengujian sistem merupakan tahap krusial dalam evaluasi kinerja aplikasi, bertujuan untuk memastikan bahwa sistem dapat melakukan login ke dalam aplikasi, melakukan modifikasi pada data pengguna dan data inventaris, serta melaksanakan enkripsi dan dekripsi data inventaris sesuai dengan algoritma yang diterapkan, yaitu *Triple* DES dan RC4. Sebagai langkah awal dalam pengujian, fungsi login aplikasi diuji secara mendalam. Apabila terdapat ketidaksesuaian antara *username* atau *password* yang dimasukkan dengan data yang tersimpan dalam sistem, maka sistem akan menampilkan pesan peringatan, yaitu “Username atau password Anda salah.

Gambar 7. Tampilan Gagal Login

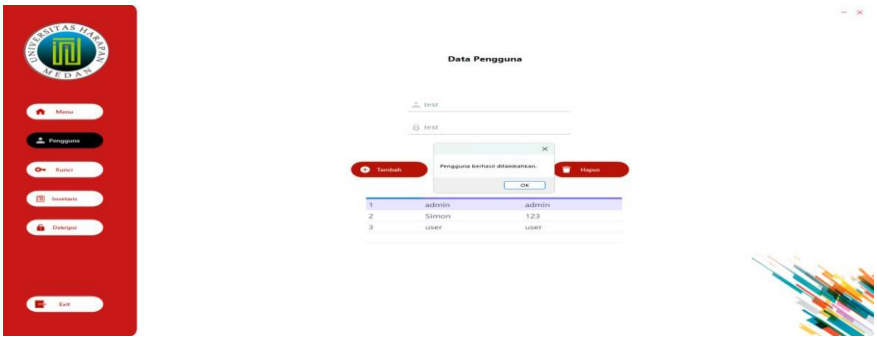
Pengujian ini tidak hanya berfokus pada keberhasilan proses login, tetapi juga menekankan pentingnya keamanan dan kontrol akses dalam sistem, yang merupakan aspek fundamental dalam pengelolaan data yang sensitif.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i2.2178



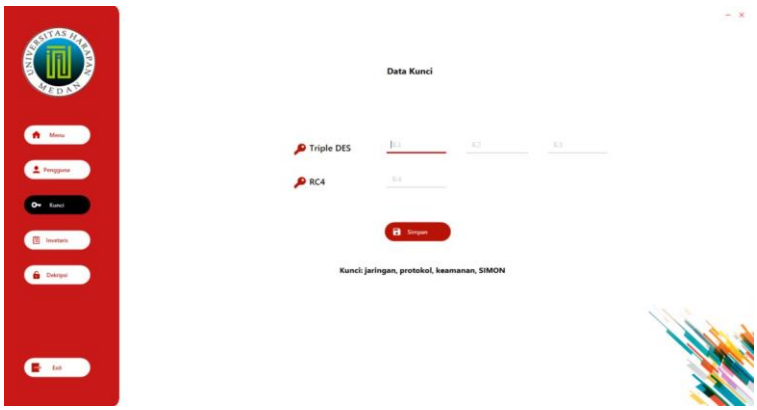
Gambar 8. Tampilan Menu Utama Setelah Berhasil Login

Gambar 8 adalah halaman utama aplikasi, pengguna akan disambut dengan pesan selamat datang yang disertai dengan nama pengguna yang sedang aktif. Laman ini dilengkapi dengan tiga fitur utama, di mana fitur pertama berfungsi untuk menambahkan pengguna baru ke dalam basis data. Sebelum fitur ini dapat digunakan, pengguna diwajibkan untuk mengisi informasi yang diperlukan pada kolom *username* dan *password*.



Gambar 9. Tampilan Pengguna

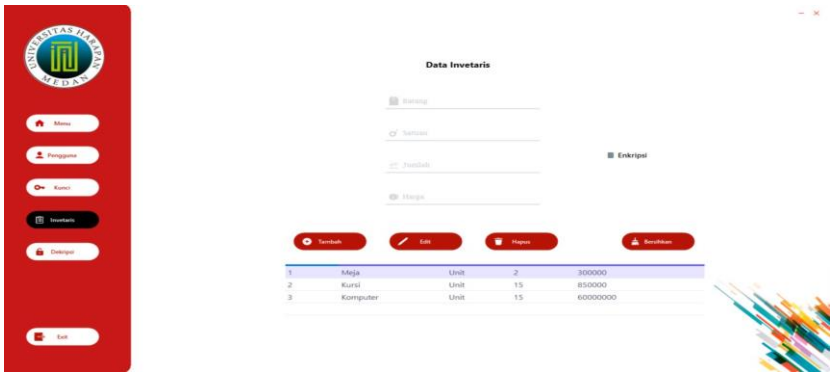
Jika proses penyimpanan berhasil maka sistem akan menampilkan pesan konfirmasi seperti gamabar 9 yang menyatakan "Pengguna berhasil ditambahkan". Setelah data berhasil ditambahkan, akan muncul *record*. Fitur kedua dalam aplikasi ini adalah fitur *edit*, yang memungkinkan pengguna untuk melakukan perubahan terhadap data pengguna yang tersimpan dalam basis data. Untuk memanfaatkan fitur ini, pengguna perlu terlebih dahulu memilih data yang ingin diubah dari tabel yang tersedia.



Gambar 10. Tampilan Kunci

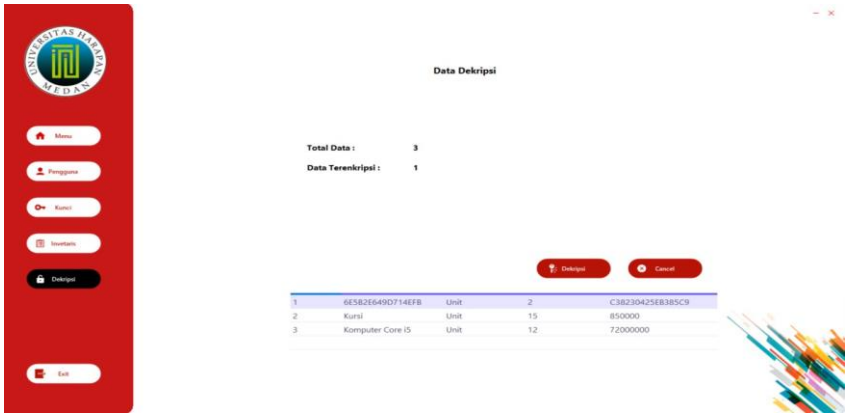
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i2.2178

Pengujian selanjutnya pada gambar 10 adalah pengujian menu kunci. Pada menu ini pengguna dapat memasukkan kunci k1 hingga k4. Kunci k1 sampai k3 digunakan untuk algoritma *Triple* DES, sedangkan k4 digunakan untuk algoritma RC4. Kunci yang digunakan pada *Triple* des harus memiliki panjang 8 karakter jika tidak sesuai, maka akan muncul pesan "Panjang kunci k1, k2 dan k3 harus tepat 8 karakter". Hal ini dilakukan sesuai dengan ketentuan kunci yang digunakan untuk enkripsi dan dekripsi *plaintext* pada algoritma *Triple* DES. Jika kunci belum diisi dan langsung menekan tombol simpan, maka akan muncul pesan "Harap isi semua kunci k1, k2, k3, k4 terlebih dahulu".



Gambar 11. Tampilan Data Inventaris

Pengujian berikutnya difokuskan pada menu inventaris seperti pada gambar 11, di mana pengguna dapat melakukan penambahan data inventaris. Proses ini dimulai dengan memasukkan rincian data ke dalam kolom input yang disediakan. Setelah semua informasi diisi, pengguna perlu menekan tombol tambah untuk mengonfirmasi penyimpanan data tersebut. Fitur *edit* memungkinkan pengguna untuk melakukan perubahan terhadap data yang telah disimpan dalam database. Data yang sudah dienkripsi tidak dapat diubah melalui fitur *edit* ataupun tambah. Tombol tambah dan *edit* akan menjadi *disable* ditandai dengan perubahan warna tombol menjadi abu-abu.



Gambar 12. Tampilan Dekripsi

Pengujian terakhir adalah pengujian fungsi dekripsi pada gamabar 12 yang dapat dilakukan pada menu dekripsi di aplikasi. fitur yang dapat digunakan pada menu ini adalah fitur dekripsi dan *cancel*. Fitur dekripsi berfungsi untuk mengembalikan data yang sudah dienkripsi menjadi seperti keadaan awal dan menyalin data tersebut kembali kedalam *database*, sedangkan fitur *cancel* berfungsi untuk membatalkan hasil dekripsi pada data.
Sedangkan untuk melihat hasil pengujian *blackbox testing* dapat dilihat pada tabel 1.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i2.2178

Tabel 1. Hasil Pengujian

No.	Sekenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Keterangan
1	Menambahkan, mengubah dan menghapus data pengguna	Data pengguna berkurang/bertambah/ berubah pada *database*	Data pengguna berkurang/bertambah/ berubah pada *database*	Valid
2	Menambahkan, mengubah dan menghapus data inventaris	Data inventaris berkurang/bertambah/ berubah pada *database*	Data inventaris berkurang/bertambah/ berubah pada *database*	Valid
3	Memasukkan Nilai Kunci	Nilai Kunci Tersimpan	Nilai Kunci Tersimpan	Valid
4	Enkripsi data inventaris	Data terenkripsi sesuai dengan *Triple* DES dan RC4	Data terenkripsi sesuai dengan *Triple* DES dan RC4	Valid
5	Dekripsi data inventaris	Data terdekripsi sesuai dengan a *Triple* DES dan RC4	Data terdekripsi sesuai dengan *Triple* DES dan RC4	Valid
6	Menu exit	Menutup aplikasi	Menutup aplikasi	Valid
7	Tombol Minimize	Mengecilkan layar aplikasi	Mengecilkan layar aplikasi	Valid

4. KESIMPULAN

Berdasarkan Hasil Pembahasan dan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai Sistem yang dibangun dapat mengamankan data inventaris berupa kolom nama barang dan harga.Sistem dapat melakukan dekripsi kembali data yang sudah diamankan dengan baik. Sistem dapat mengamankan aplikasi melalui proses autentikasi pengguna. Penggunaan kombinasi dengan algoritma tertentu mempengaruhi tingkat keamanan data.

REFERENSI

[1] M. Siahaan dan J. Manurung, "Perancangan Aplikasi Penyandian Teks Menggunakan Algoritma Triple DES," *J. Ilmu Komput. dan Sist. ...*, vol. 3, no. 3, hal. 197–201, 2021, [Daring]. Tersedia pada: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/116

[2] A. Davy Wiranata dan R. Tamara Aldisa, "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 5, no. 3, hal. 4–8, 2021, [Daring]. Tersedia pada: http://journal.lembagakita.org/index.php/jtik/article/view/219/pdf

[3] B. Noviansyah, "Modifikasi Pembentukan Algoritma Rc4 Cipher Dengan Metode Acak Mid-Square Technique Untuk Pengamanan Voice Chat," *J. Sains dan Teknol. Inf.*, vol. 2, no. 1, hal. 26–30, 2022, doi: 10.47065/jussi.v2i1.3179.

[4] Z. Basim dan Painem, "Implementasi Kriptografi Algoritma Rc4 Dan 3Des Dan Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As-Su'Udiyyah," *Skanika*, vol. 3, no. 4, hal. 54–60, 2020.

[5] A. T. A. P. Rukmana, Y. A., Rahman, R., Afriyadi, H., Moeis, D., Setiawan, Z., Subchan, N., Magdalena, L., Singadji, M., Rayeb, E. A., & Kusuma, *No TitlePengantar Sistem Informasi: Panduan Praktis Pengenalan Sistem Informasi & Penerapannya*. PT. Sonpedia Publishing Indonesia, 2023.

[6] N. Wijaya, E., Indriyati, R., Rinawati, R., Utami, R. N., Negsih, A. T., Suharyanto, S., Hermawan, E., Deseria, R., & Aziza, *Pengantar Statistika: Konsep Dasar untuk Analisis Data*. PT. Sonpedia Publishing

Indonesia, 2024.
[7] M. K. Dedy Rahman Prehanto, S.Kom., *Buku Ajar Konsep Sistem Informasi*. SCOPINDO MEDIA PUSTAKA, 2020.
[8] A. Z. F. Rangkuti dan H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, hal. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.
[9] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. A. S. A, dan S. A. F, "Penerapan kriptografi," vol. 2, no. 3, hal. 35–41, 2023.
[10] S. P. Lestari, H. N. Fadlan, R. Angelia Purba, dan I. Gunawan, "Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp," *J. Media Inform.*, vol. 4, no. 1, hal. 1–8, 2022, doi: 10.55338/jumin.v4i1.423.
[11] T. H. Saputro, N. H. Hidayati, dan E. I. H. Ujianto, "Survei Tentang Algoritma Kriptografi Asimetris," *J. Inform. Polinema*, vol. 6, no. 2, hal. 67–72, 2020, doi: 10.33795/jip.v6i2.345.
[12] G. A. J. Rahman, R., Ariantini, M. S., Hadi, A., Hayati, N., Gunawan, P. W., Mandowen, S. A., Widiyasono, N., & Saskara, *Buku Ajar Keamanan Jaringan Komputer*. PT. Sonpedia Publishing Indonesia., 2024.
[13] G. A. J. Rahman, R., Ariantini, M. S., Hadi, A., Hayati, N., Gunawan, P. W., Mandowen, S. A., Widiyasono, N., & Saskara, *Buku Ajar Keamanan Jaringan Komputer*. PT. Sonpedia Publishing Indonesia, 2024.
[14] M. Adik Putra, D. I. Mulyana, R. A. Amalia, dan M. Mirsandi, "Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen Dengan Algoritma Triple DES Berbasis Web," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, hal. 57–69, 2022, doi: 10.47709/jpsk.v2i01.1354.
[15] K. Martin, *Everyday Cryptography Fundamental Principles and Applications*. OUP Oxford, 2017.
[16] M. Stamp, *Information Security Principles and Practice*. Wiley, 2021.
[17] I. Zufria, A. H. Hasugian, dan S. Oktawijaya, "Sistem Keamanan Folder Dengan Menggunakan Algoritma Rivest Code 4," *J. Multimed. dan Teknol. Inf.*, vol. 5, no. 2, hal. 45–52, 2023.
[18] G. Susilo, W., & Yang, *Information Security and Privacy 23rd Australasian Conference*. Springer International Publishing, 2018.
[19] B. A. Iswara, J. Tarigan, S. Man, dan A. Candra, "Comparison AES and RC4 Algorithm for Secure Data Passed Through an URL," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 22, no. 2, hal. 357, 2023, doi: 10.53513/jis.v22i2.8400.