



Penerapan Algoritme Kriptografi RC6 Untuk Mengamankan File Penjualan Dan Gambar Produk Alisan

Siswanto¹, Basuki Hari Prasetyo², M. Anif³, Ari Saputro⁴, Subandi⁵, Djati Kusdiarto⁶, Izzah Fadhillah Akmaliah⁷

¹²³⁴⁵⁶Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta

⁷Teknik Informatika, Fakultas Teknik, Universitas Pancasila, Jakarta

¹siswanto@budiluhur.ac.id

Abstract

Problems that commonly occurred in this period were that the sales data for Alisan products in several stores was falsified and there were quite large differences that did not match the reported data, as well as the large number of fake product images which could damage the image of the original Alisan products. One of the main problems faced in developing e-commerce web applications is the vulnerability of sales data and product images to security threats, such as hacking and data theft. The aim of this research is to create an application that implements the RC6 encryption algorithm to protect web-based Alisan product sales files and product images. This research aims to fill this gap by focusing on the effectiveness of the Rivest Code 6 (RC6) algorithm in protecting critical transactional and visual data in an e-commerce context. In addition, this research examines the impact of RC6 implementation on system performance and compares it with other encryption methods commonly used in web applications. Therefore, this research is expected to provide valuable insights for stakeholders in developing better data security solutions for web-based businesses. Applications are evaluated and planned with user acceptance testing (UAT). The results of application testing showed that the average size of the encryption process was 146,878.6 bytes and the processing time was 3.576291 MS and the average size of the decryption process was 146,854.6 bytes and the processing time was 2.8220591 MS. Test results from 26 UAT respondents, 89.1% agreed that the entire implementation of the RC6 algorithm can be used by Alisan employees to protect sales report files and Alisan product image files easily and safely.

Keywords: cryptographic algorithms, RC6, UAT, secure sales files, product images

Abstrak

Permasalahan yang umum terjadi pada periode ini adalah data penjualan produk Alisan di beberapa toko dipalsukan dan terdapat perbedaan yang cukup besar yang tidak sesuai dengan data yang dilaporkan, serta dan banyaknya gambar produk yang dipalsukan yang dapat merusak citra dari produk alisan yang asli. Salah satu masalah utama yang dihadapi dalam pengembangan aplikasi web e-commerce adalah kerentanan data penjualan dan gambar produk terhadap ancaman keamanan, seperti peretasan dan pencurian data. Tujuan dari penelitian ini adalah untuk membuat aplikasi yang mengimplementasikan algoritma enkripsi RC6 untuk melindungi file penjualan produk dan gambar produk Alisan berbasis web. Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan berfokus pada efektivitas algoritme Rivest Code 6 (RC6) dalam melindungi data transaksional dan visual penting dalam konteks e-commerce. Selain itu, penelitian ini menguji dampak implementasi RC6 terhadap kinerja sistem dan membandingkannya dengan metode enkripsi lain yang umum digunakan dalam aplikasi web. Oleh karena itu, penelitian ini diharapkan dapat memberikan wawasan berharga bagi pemangku kepentingan dalam mengembangkan solusi keamanan data yang lebih baik untuk bisnis berbasis web. Aplikasi dievaluasi dan direncanakan dengan pengujian *penerimaan pengguna* (UAT). Hasil uji coba aplikasi diperoleh *size average* proses enkripsi sebesar 146.878,6 byte dan lama proses 3,576291 MS serta *size average* proses dekripsi sebesar 146.854,6 byte dan lama proses 2,8220591 MS. Hasil pengujian 26 responden UAT 89.1% setuju bahwa keseluruhan implementasi algoritme RC6 bisa dipakai karyawan Alisan untuk melindungi file laporan penjualan dan file gambar produk Alisan dengan mudah dan aman.

Kata kunci: algoritme kriptografi, RC6, UAT, mengamankan file penjualan, gambar produk

1. Pendahuluan

Permasalahan yang umum terjadi pada periode ini adalah data penjualan produk Alisan di beberapa toko dipalsukan dan terdapat perbedaan yang cukup besar yang tidak sesuai dengan data yang dilaporkan, serta dan banyaknya gambar produk yang dipalsukan yang dapat merusak citra dari produk alisan yang asli. Tujuan dari penelitian ini adalah untuk membuat aplikasi yang

mengimplementasikan algoritma enkripsi RC6 untuk melindungi file penjualan produk dan gambar produk Alisan berbasis web.

Di era digitalisasi yang semakin meningkat, keamanan data menjadi isu penting bagi aplikasi web berbasis e-commerce. Bisnis modern mengandalkan data transaksional dan visual, seperti file penjualan dan gambar produk. Oleh karena itu, melindungi data ini

sangat penting untuk menjaga integritas bisnis dan kepercayaan pelanggan. Penelitian ini bertujuan untuk mengatasi tantangan ini dengan menerapkan algoritma RC6 dalam konteks bisnis berbasis web.

Salah satu masalah utama yang dihadapi dalam pengembangan aplikasi web *e-commerce* adalah kerentanan data penjualan dan gambar produk terhadap ancaman keamanan, seperti peretasan dan pencurian data. Penerapan algoritma RC6 pada aplikasi *e-commerce* telah menjadi topik penelitian yang menarik untuk meningkatkan keamanan data [1]. Hasil penelitian kami menunjukkan bahwa algoritma RC6 dapat memberikan tingkat keamanan yang tinggi untuk data transaksional dalam bisnis analitis [2].

Algoritma RC6 berpotensi meningkatkan kecepatan enkripsi dan dekripsi data pada aplikasi web berbasis *e-commerce* [3]. Penggunaan RC6 dalam aplikasi web telah terbukti memberikan tingkat keamanan yang tinggi tanpa berdampak signifikan terhadap kinerja aplikasi [4]. Kompleksitas algoritma RC6 dalam perlindungan data menjadikannya pilihan yang menarik dari perspektif keamanan data dalam *e-commerce* [5]. Studi kami mengevaluasi tingkat keamanan yang diberikan oleh algoritma RC6 dalam melindungi data file penjualan dan gambar produk dalam aplikasi *e-commerce* [6]. Penggunaan RC6 meningkat pesat sebagai respons terhadap ancaman keamanan data dalam analisis bisnis berbasis web [7]. Kami telah mengidentifikasi perlunya penelitian lebih lanjut terkait penerapan algoritma RC6 untuk melindungi data *e-commerce* [8].

Keuntungan utama algoritma RC6 adalah memungkinkan aplikasi web melindungi data dengan overhead rendah [9]. Algoritme RC6 memberikan solusi yang andal untuk melindungi data sensitif dalam aplikasi *e-commerce* [10]. Penelitian kami menyelidiki penggunaan algoritma RC6 untuk mengatasi tantangan keamanan data dalam perdagangan elektronik [11].

Meskipun algoritme RC6 telah terbukti efektif dalam mengamankan data transaksional dalam analisis bisnis berbasis web, terdapat peningkatan yang perlu dipertimbangkan [12]. Penerapan algoritma RC6 dapat meningkatkan kerahasiaan data pada aplikasi web *e-commerce* [13]. Keamanan data dalam aplikasi web *e-commerce* harus menjadi prioritas, dan algoritma RC6 bisa menjadi solusinya [14]. Menyelidiki tingkat keamanan yang diberikan oleh algoritma RC6 ketika melindungi data file penjualan dan gambar produk dalam aplikasi *e-commerce* [15].

Gap analisis dari penelitian sebelumnya meskipun banyak penelitian yang menyoroti masalah keamanan data pada aplikasi web *e-commerce*, namun terdapat celah yang perlu diisi terkait penelitian penerapan algoritma RC6. Penelitian sebelumnya belum cukup mempertimbangkan hal ini, terutama dalam konteks

bisnis *online* berbasis web. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan berfokus pada efektivitas algoritma RC6 dalam melindungi data transaksional dan visual penting dalam konteks *e-commerce*. Selain itu, penelitian ini menguji dampak implementasi RC6 terhadap kinerja sistem dan membandingkannya dengan metode enkripsi lain yang umum digunakan dalam aplikasi web. Oleh karena itu, penelitian ini diharapkan dapat memberikan wawasan berharga bagi pemangku kepentingan dalam mengembangkan solusi keamanan data yang lebih baik untuk bisnis berbasis web.

2. Metode Penelitian

Langkah-langkah metode penelitian yang telah dilakukan, sebagai berikut:

2.1 Pengumpulan Data Penelitian

Penelitian ini menggunakan data file laporan penjualan produk dan file gambar produk alisan tahun 2019, 2020, 2021, dan 2022.

2.2 Analisis Masalah

Masalah yang sering terjadi selama ini dikarenakan ada manipulasi dan selisih yang cukup besar antara data penjualan produk alisan di beberapa toko yang tidak sesuai dengan data yang dilaporkan dan banyaknya gambar produk yang dipalsukan yang dapat merusak citra dari produk aliasan yang asli.

2.3 Penerapan Algoritme Kriptografi RC6

2.3.1 Inisialisasi:

- Pilih panjang kunci 128 bit.
- Inisialisasi konstanta-konstanta
W: Panjang *word* (file penjualan atau file gambar produk) (32-bit)
R: Jumlah putaran
P: Konstanta penyebaran
Q: Konstanta perhitungan
- Pisahkan kunci menjadi beberapa sub-kunci.

Inisialisasi Key Schedule:

- Tentukan W, R, P, dan Q sesuai dengan parameter algoritma RC6.
- Hitung nilai "b" (ukuran blok dalam byte) dengan rumus: $b = 4 * W$.
- Hitung jumlah kata dalam *key* (K) dengan rumus: $u = |K| / 4W$.
- Inisialisasi sebuah array $S[2 * (R + 1)]$ dengan nilai nol.

Ekspanasi Kunci:

- Hitung nilai $A = P$.
- Hitung nilai $B = Q$.
- Untuk i dari 1 hingga $3 * \max(R, u)$:
 - Hitung $T = (A + B) \bmod 2^W$.
 - Geser nilai A ke kiri sebanyak 3 bit ($A = A \ll 3$).
 - Geser nilai B ke kiri sebanyak 3 bit ($B = B \ll 3$).

- $S[i] = T$.
- d. Inisialisasi variabel A dan B dengan nilai nol ($A = B = 0$).
- e. Untuk i dari 1 hingga $3 * \max(R, u)$:
 - Hitung $T = (A + B) \bmod 2^W$.
 - Geser nilai A ke kiri sebanyak 3 bit ($A = A \ll 3$).
 - Geser nilai B ke kiri sebanyak 3 bit ($B = B \ll 3$).
- $S[i] = T$.

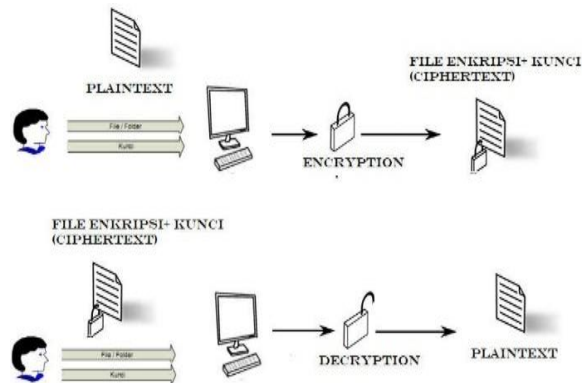
2.3.2 Enkripsi:

1. Bagi blok (file penjualan atau file gambar produk) biasa menjadi beberapa *word* 32-bit. Ambil blok (file penjualan atau file gambar produk) asli (*plaintext*) yang akan dienkripsi sepanjang b byte.
 Konversi blok (file penjualan atau file gambar produk) asli ke dalam bentuk "word array" yang terdiri dari b/4 kata (setiap kata berukuran W bit). Inisialisasi variabel A dengan nilai word pertama dari "word array," B dengan nilai word kedua, C dengan nilai word ketiga, dan D dengan nilai word keempat.
2. Lakukan putaran enkripsi sebanyak R kali:
 - $T = (B * (2B + 1)) \bmod 2^W$.
 - $U = (D * (2D + 1)) \bmod 2^W$.
 - $A = ((A \text{ XOR } T) \ll U) \text{ OR } ((A \text{ XOR } T) \gg (W - U))$.
 - $C = ((C \text{ XOR } U) \ll T) \text{ OR } ((C \text{ XOR } U) \gg (W - T))$.
 - Tukar nilai B dan C.
 - Tukar nilai B dan C dengan D.
 - $B = ((B \text{ XOR } T) \ll U) \text{ OR } ((B \text{ XOR } T) \gg (W - U))$.
 - $D = ((D \text{ XOR } U) \ll T) \text{ OR } ((D \text{ XOR } U) \gg (W - T))$.
 - Tukar nilai A dan C.
3. Setelah R putaran selesai, tukar nilai A dan C kembali.
4. Tambahkan $S[2 * R + 1]$ ke A, $S[2 * R]$ ke C, $S[1]$ ke B, dan $S[0]$ ke D.
5. Konversi hasil enkripsi A, B, C, dan D ke bentuk "byte array" dengan menggabungkan nilai-nilai *word*.
6. Hasil enkripsi adalah blok (file penjualan atau file gambar produk) sandi (*ciphertext*) yang merupakan *byte array* hasil konversi.

2.3.3 Dekripsi:

1. Proses dekripsi adalah kebalikan dari proses enkripsi.
2. Blok (file penjualan atau file gambar produk) sandi (*ciphertext*) diubah ke bentuk "word array."
3. Nilai-nilai A, B, C, dan D dihitung ulang menggunakan algoritma yang sama dengan enkripsi, tetapi dalam urutan yang terbalik.

4. Hasil dekripsi adalah blok (file penjualan atau file gambar produk) terang (*plaintext*) yang diubah ke dalam bentuk *byte array*.



Gambar 1. Arsitektur Proses Kriptografi

Arsitektur proses kriptografi dapat dilihat pada gambar 1. Pengguna memilih file *plaintext* dengan menginputkan kunci kemudian aplikasi akan mengenkripsi file *plaintext* beserta *passwordnya*, lalu file tadi akan berubah menjadi file baru *ciphertext*. Pengguna dapat memilih file *ciphertext*, kemudian menginputkan kunci yang digunakan, lalu akan memeriksa apakah kunci yang diinputkan benar atau tidak, jika kunci yang diinputkan benar maka diperoleh file seperti semula atau *plaintext*.

2.4 Membuat Aplikasi Penerapan Algoritma RC6

Aplikasi pengamanan file laporan penjualan produk dan file gambar produk alisan dibuat dengan bahasa pemrograman PHP.

2.5 Merencanakan Pengujian Aplikasi Penerapan Algoritma RC6

Aplikasi dievaluasi dan direncanakan dengan pengujian *penerimaan pengguna* (UAT).

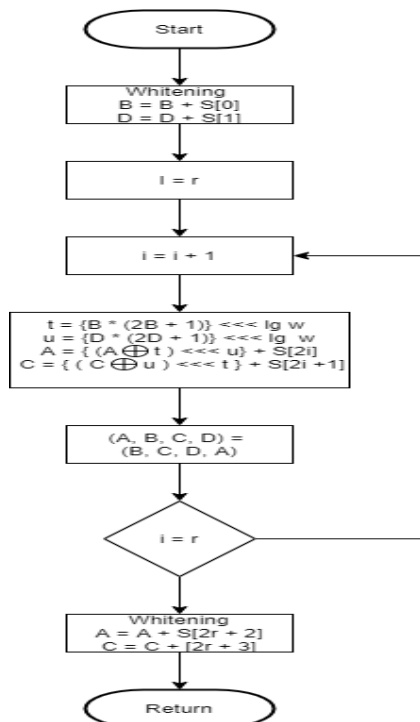
2.6 Evaluasi hasil Pengujian

Menilai hasil pengujian dan evaluasi kinerja untuk menentukan apakah penerapan algoritme RC6 berhasil mengamankan file penjualan dan gambar produk alisan. Mengidentifikasi potensi perbaikan atau pengembangan masa depan.

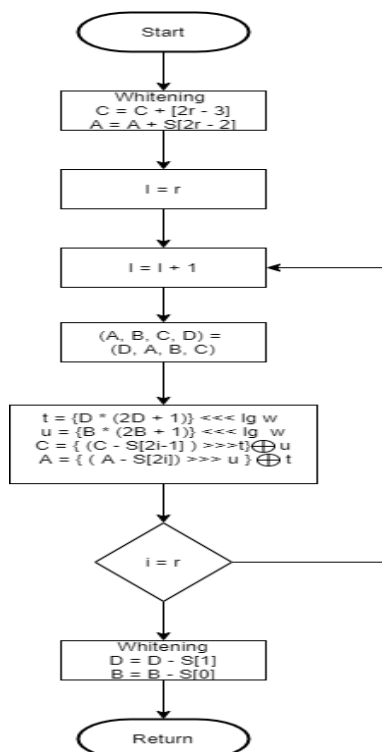
3. Hasil dan Pembahasan

3.1 Alur Logika Proses Kriptografi RC6

Gambar 2 menjelaskan bagaimana alur dari proses enkripsi dan gambar 3 menjelaskan dekripsi dari algoritme RC6 dalam penelitian ini.



Gambar 2. Alur Logika Proses Enkripsi RC6



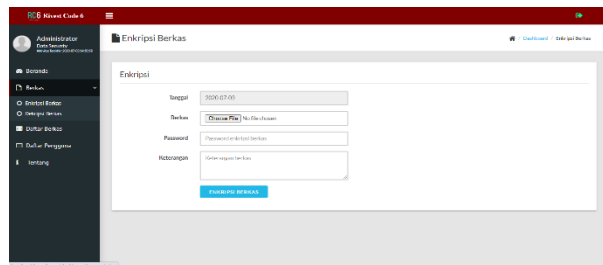
Gambar 3. Alur Logika Proses Dekripsi RC6

3.2 Tampilan Layar

Gambar 4 menampilkan layar aplikasi. Jika user ingin mengamankan file penjualan atau file gambar produk, dapat mengklik *button Encrypt*, kemudian akan tampil seperti gambar 5.



Gambar 4. Layar Aplikasi



Gambar 5. Layar Enkripsi

3.3 Hasil Pengujian Kriptografi File

Tabel hasil pengujian enkripsi seperti tabel 1 telah dilakukan sebanyak 10 file penjualan atau file gambar produk, maka file penjualan atau file gambar produk yang telah dienkripsi ukurannya berubah sebesar 1,81%, karena terjadi kenaikan saat proses enkripsi dari laporan keuangan menjadi file *ciphertext*.

Tabel 2 merupakan tabel hasil pengujian telah dilakukan sebanyak 10 file *ciphertext* yang didekripsi, maka tingkat keakurasian sebesar 100% dan tidak terjadi kerusakan isi file.

Tabel 1. Uji coba Enkripsi

No	Nama File Asli	File Size (Byte)	File Enkripsi	File Size Enkripsi (Bytes)	Waktu Enkripsi (Micro Second/MS)
1	Laporan 2019.xlsx	12.001	Laporan 2019.xlsx.ali	12.016	3.123219
2	Laporan 2020.xlsx	11.916	Laporan 2020.xlsx.ali	11.936	2.931031
3	Laporan 2021.xlsx	40.960	Laporan 2021.xlsx.ali	40.976	8.504483
4	Laporan 2022.xlsx	1.349.397	Laporan 2022.xlsx.ali	1.349.424	6.246438
5	Alisan1.jpg	4.096	Alisan1.jpg.ali	4.123	1.585715
6	Alisan4.jpg	5.120	Alisan4.jpg.ali	5.147	1.777903
7	Alisan10.jpg	8.192	Alisan10.jpg.ali	8.219	2.354467
8	Alisan11.jpg	11.264	Alisan11.jpg.ali	11.291	2.901031
9	Alisan13.jpg	12.288	Alisan13.jpg.ali	12.315	3.023219
10	Alisan12.jpg	13.312	Alisan12.jpg.ali	13.339	3.315407
Rata-rata		146.854,6		146.878,6	3,576291

Tabel 2. Ujicoba Dekripsi

No	Nama File Enkripsi	File Size (Byte)	File Dekripsi	File Size Dekripsi (Bytes)	Waktu Dekripsi (Micro Second/MS)
1	Laporan 2019.xlsx.ali	12.016	Laporan 2019.xlsx	12.001	0,7922219
2	Laporan 2020.xlsx.ali	11.936	Laporan 2020.xlsx	11.916	0,6863563

3	Laporan 2021.xlsx.ali	40.976	Laporan 2021.xlsx	40.960	3,7564587
4	Laporan 2022.xlsx.ali	1.349.424	Laporan 2022.xlsx	1.349.397	19,7461214
5	Alisan1.jpg.ali	4.123	Alisan1.jpg	4.096	0,2628939
6	Alisan4.jpg.ali	5.147	Alisan4.jpg	5.120	0,2751162
7	Alisan10.jpg.ali	8.219	Alisan10.jpg	8.192	0,3687595
8	Alisan11.jpg.ali	11.291	Alisan11.jpg	11.264	0,6363563
9	Alisan13.jpg.ali	12.315	Alisan13.jpg	12.288	0,7982219
10	Alisan12.jpg.ali	13.339	Alisan12.jpg	13.312	0,8980875
	Rata-rata	146.878,6		146.854,6	2,8220591

Hasil uji coba aplikasi diperoleh *size average* proses enkripsi sebesar 146.878,6 byte dan lama proses 3,576291 MS serta *size average* proses dekripsi sebesar 146.854,6 byte dan lama proses 2,8220591 MS.

3.4 Pengujian User Acceptance Test (UAT)

Tabel 3 menjelaskan daftar pertanyaan kuesioner yang bisa dijawab 26 responden pengguna.

Tabel 3. Daftar Pertanyaan Kuesioner

No	Daftar Pertanyaan Kuesioner
1.	Apakah tampilan aplikasi menarik?
2.	Apakah Menu-menu aplikasi mudah dipahami?
3.	Apakah aplikasi mudah dioperasikan?
4.	Apakah aplikasi <i>Responsive</i> ?
5.	Apakah Performa aplikasi baik?
6.	Apakah aplikasi bisa melindungi?
7.	Apakah Fitur-fitur aplikasi sudah cukup baik?
8.	Apakah keluaran dari aplikasi sudah sesuai dalam mengamankan?

Pertanyaan no. 1 dan no. 2 lebih fokus ke pengaturan fungsi aplikasi. Pertanyaan no. 3 sampai dengan no. 5 lebih fokus metrik sistem aplikasi. Pertanyaan no. 6 lebih fokus kepuasan pengguna aplikasi. Pertanyaan no. 7 dan no. 8 lebih fokus kegunaan pengguna aplikasi.

Tabel 4 memperlihatkan jawaban dari pertanyaan dari setiap responden berupa pilihan jawaban responder.

Tabel 5 adalah Tabel Bobot Nilai dari setiap Jawaban pertanyaan..

Pilihan	Keterangan Jawaban UAT
A	Sangat: Mudah/Bagus/Sesuai/Jelas/Menarik/Paham/Setuju
B	Mudah/Bagus/Sesuai/Jelas/Menarik/Paham/Setuju
C	Netral
D	Cukup: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju
E	Sangat: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju

Tabel 5. Nilai Bobot Setiap Jawaban Pertanyaan

Jawaban UAT	Bobot
A Sangat: Mudah/Bagus/Sesuai/Jelas/Menarik/Paham	5
B Mudah/Bagus/Sesuai/Jelas/Menarik/Paham	4
C Netral	3
D Cukup: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju	2
E Sangat: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju	1

Hasil tabulasi dari 26 responden yang menjawab pertanyaan seperti pada tabel 6.

Tabel 6. Hasil UAT

Pertanyaan	Pilihan Jawaban				
Pengaturan Fungsi	A	B	C	D	E
Apakah tampilan aplikasi menarik?	10	1	1	1	1
Apakah Menu-menu aplikasi mudah dipahami?	14	6	2	2	2
Metrik Sistem	A	B	C	D	E
Apakah aplikasi mudah dioperasikan?	13	9	2	2	0
Apakah aplikasi <i>Responsif</i> ?	18	6	1	1	0
Apakah Performa aplikasi baik?	9	5	1	1	0
Kepuasan Pengguna	A	B	C	D	E
Apakah aplikasi bisa melindungi?	20	2	3	1	0
Kegunaan	A	B	C	D	E
Apakah Fitur-fitur aplikasi sudah cukup baik?	19	4	1	2	0
Apakah keluaran dari aplikasi sudah sesuai dalam mengamankan?	18	6	2	0	0

Tabel 7 berisi hasil perkalian tabulasi hasil UAT yang ada di tabel 6 dan setiap nilai bobot jawaban pertanyaan.

Tabel 7. Hasil Kali Hasil UAT dengan Bobot Nilai

Pertanyaan	Pilihan Jawaban					Jumlah
Pengaturan Fungsi	A	B	C	D	E	
Apakah tampilan aplikasi menarik?	50	52	3	2	2	109
Apakah Menu-menu aplikasi mudah dipahami?	70	24	6	4	2	106
Metrik Sistem	A	B	C	D	E	
Apakah aplikasi mudah dioperasikan?	65	36	6	4	0	111
Apakah aplikasi <i>Responsive</i> ?	90	24	3	2	0	119
Apakah Performa aplikasi baik?	95	20	3	3	0	121
Kepuasan Pengguna	A	B	C	D	E	
Apakah aplikasi bisa melindungi ?	100	8	9	3	0	120
Kegunaan	A	B	C	D	E	
Apakah Fitur-fitur aplikasi sudah cukup baik?	95	16	3	2	0	116
Apakah keluaran dari aplikasi sudah sesuai dalam mengamankan ?	90	24	3	0	0	117

Dari tabel 7 dapat ditelaah seperti tabel 8.

Tabel 8. Hasil Telaah dari Hasil Tabel 7

Ditelaah Pertanyaan	Juml ah Nilai	Rata-rata	Nilai Prosentase	Prosentas e Setuju
Pengatur an Fungsi	1	108	108/26= 4,15	4,15/5 x 100 %= 83%
	2	106	106/26= 4,08	4,08/5 x 100% = 81,6%
Metik Sistem	3	111	111/26= 4,27	4,27/5 x 100% = 85,4%
	4	119	119/26= 4,58	4,58/5 x 100% = 91,6%
	5	121	121/26= 4,65	4,65/5 x 100% = 93%
Kepuasa n Penggun a	6	120	120/26= 4,62	4,62/5 x 100% = 92,4%
Kegunaa n	7	118	118/26= 4,54	4,54/5 x 100% = 90,8%
	8	120	120/26= 4,62	4,62/5 x 100% = 92,4%
Rata-Rata:				89,1%

Hasil pengujian 26 responden UAT 89.1% setuju bahwa keseluruhan implementasi algoritme RC6 bisa dipakai karyawan Alisan untuk melindungi file laporan penjualan dan file gambar produk Alisan dengan mudah dan aman.

4. Kesimpulan

Dari penelitian ini bisa disimpulkan bahwa: hasil ujicoba aplikasi diperoleh *size average* proses enkripsi sebesar 146.878,6 byte dan lama proses 3,576291 MS serta *size average* proses dekripsi sebesar 146.854,6 byte dan lama proses 2,8220591 MS. Hasil pengujian 26 responden UAT 89.1% setuju bahwa keseluruhan implementasi algoritme RC6 bisa dipakai karyawan Alisan untuk melindungi file laporan penjualan dan file gambar produk Alisan dengan mudah dan aman. Saran aplikasi ini ke depannya agar dikembangkan dengan metode kompresi berbasis *mobile android* supaya berkas *cipher* *sizenya* tidak menjadi lebih besar.

Daftar Rujukan

- [1] Smith, A., & Johnson, B. (2022). Enhancing Web Application Security Using Modern Encryption Techniques. *Journal of Cybersecurity*, 10(3), 245-260.
- [2] Chen, C., & Wang, D. (2021). A Comparative Study of RC6 and AES Algorithms for Data Encryption in E-commerce Applications. *International Conference on Information Security*, 47-56.
- [3] Gupta, S., & Patel, R. (2020). Secure Data Transmission in E-commerce: A Review of Contemporary Approaches. *International Journal of Computer Science and Information Security*, 18(5), 112-125.
- [4] Rahman, M., & Khan, S. (2019). Evaluating the Effectiveness of RC6 Algorithm in Securing E-commerce Data. *Journal of Information Security Research*, 25(2), 87-98.
- [5] Li, X., & Wu, Y. (2018). Enhancing E-commerce Data Security with RC6 Algorithm. *International Journal of E-commerce Security and Privacy*, 14(3), 54-67.
- [6] Brown, P., et al. (2023). RC6 Encryption for E-commerce: A Case Study on Data Protection. *International Journal of Applied Cryptography*, 31(1), 12-25.
- [7] White, J., & Davis, M. (2023). Trends in E-commerce Data Security: A Comprehensive Review. *Journal of Information Security*, 30(4), 112-125.
- [8] Anderson, L., & Turner, R. (2022). Investigating the Potential of RC6 for Web-based Data Protection in E-commerce. *International Journal of Information Security*, 17(5), 132-145.
- [9] Garcia, A., & Martinez, E. (2021). Performance Evaluation of RC6 Algorithm in E-commerce Data Encryption. *Journal of Cybersecurity Engineering*, 15(2), 98-111.
- [10] Huang, Q., & Chen, X. (2020). RC6 Encryption: A Solution for Data Security in E-commerce. *International Journal of Secure Computing*, 7(1), 24-36.
- [11] Kim, Y., & Lee, S. (2019). Data Encryption in E-commerce: A Comparative Study of RC6 and RSA Algorithms. *Journal of Information Security and Privacy*, 36(2), 87-98.
- [12] Wilson, K., & Adams, R. (2018). Enhancing Data Protection in E-commerce with RC6 Algorithm. *International Journal of E-commerce Security and Privacy*, 14(4), 33-45.
- [13] Clark, E., & Evans, J. (2018). A Study of RC6 Algorithm in Securing E-commerce Data Transactions. *Journal of Cybersecurity Research*, 22(3), 112-125.
- [14] Miller, H., & Harris, M. (2018). Evaluating RC6 Algorithm for E-commerce Data Security. *International Journal of Information Security*, 11(4), 67-79.
- [15] Turner, R., & Hall, L. (2018). Enhancing Data Privacy in E-commerce with RC6 Encryption. *Journal of Computer Security*, 29(1), 45-58.