

PENERAPAN ALGORITMA SIMETRI RC 5 UNTUK MENGENKRIPSI FILE TRANSAKSI PENJUALAN BERBASIS WEB

Choiril Akhlar^{1*}, Subandi²

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

Email: ^{1*}1911501128@student.budiluhur.ac.id, ²subandi@budiluhur.ac.id

(* : corresponding author)

Abstrak-Kriptografi adalah sektor pengetahuan untuk mengamankan pesan (*message*). Kriptografi sering kali diterapkan di banyak hal. *Mobile Phone, pay TV, Anjungan Tunai Mandiri (ATM)*, Komputer dan *Smart Card* termasuk contoh berupa barang teknologi yang memakai teknik kriptografi untuk keamanan datanya. Cara kerjanya yaitu dengan merubah pesan asli yang mudah dipahami atau dimengerti manusia (*plaintexts*) ke bentuk pesan lain yang tidak dapat dipahami atau dimengerti oleh manusia (*chiphertexts*). Langkah perubahan *plaintexts* menjadi *ciphertexts* disebut enkripsi. Sedangkan langkah perubahan pesan *chiphertexts* menjadi *plaintexts* disebut dekripsi. UB Link yang berdiri sejak tahun 2019 bergerak di bidang network provider (penyedia jaringan) dengan focus utamanya yaitu jaringan internet. Toko ini harus melindungi dan mengamankan dokumen perusahaan yang dimiliki untuk mencegah bocornya *file* transaksi penjualan ke perusahaan lain. Dengan menggunakan metode kriptografi simetri RC 5 adalah salah satu algoritma yang dapat digunakan untuk melakukan kriptografi pada suatu *file*. Algoritma simetri RC 5 merupakan salah satu algoritma kriptografi yang berfungsi untuk mengamankan sebuah *file*. Adapun beberapa tahapan enkripsi sebuah *file* yaitu *plaintexts*, langkah enkripsi data, enkripsi *plaintexts*, *public key* untuk mengenkripsi, *plaintexts* terenkripsi. Sedikit berbeda dengan tahapan enkripsi, tahapan dekripsi dimulai dengan *file* enkripsi, *private key* untuk mendekripsi, *plaintexts*. Aplikasi ini diciptakan menggunakan bahasa pemrograman PHP dan mysql untuk databasenya. Dengan penelitian yang mendapatkan hasil yaitu enkripsi dan dekripsi *file* telah berhasil dilakukan, mengubah ukuran *file* dan nama *file* serta *file* tidak bisa dibuka. Menghasilkan kesimpulan yaitu, algoritma kriptografi RC5 menghasilkan kunci dengan cara melakukan pembangkitan kunci yang panjang kuncinya diatur sesuai pada jumlah putaran blok enkripsi maupun dekripsi.

Kata Kunci: Kriptografi, Simetri RC5, *file*, PHP, mysql.

APPLICATION OF RC 5 SYMMETRY ALGORITHM FOR WEB-BASED SALES TRANSACTION FILE ENCRYPTION

Abstract-Cryptography is a knowledge sector for securing messages (*messages*). Cryptography is often applied in many ways. Cell phones, pay TV, Automated Teller Machines (ATMs), Computers and Smart Cards are examples of technological goods that use cryptographic techniques for data security. The way it works is by changing the original message that is easy for humans to understand or understand (*plaintext*) into another form of message that humans cannot understand or understand (*chiphertext*). The step of converting plain text into ciphers is called encryption. Meanwhile, the step of converting ciphertext messages into plaintext is called decryption. UB Link, which was established in 2019, is engaged in the field of network providers (network providers) with the main focus being internet networks. This store must protect and secure the company's documents to prevent the leakage of sales transaction files to other companies. Using the RC 5 symmetric cryptography method is one of the algorithms that can be used to perform cryptography on a file. The RC 5 symmetry algorithm is a cryptographic algorithm that functions to secure a file. The several stages of encrypting a file are *plaintext*, data encryption steps, *plaintext encryption*, *public key for encryption*, *encrypted plaintext*. Slightly different from the encryption stage, the decryption stage starts with *file encryption*, *private key for decryption*, *plaintext*. This application was created using the programming language PHP and mysql for the database. With research that gets results, namely encryption and decryption of files have been successfully carried out, changing file sizes and file names and files cannot be opened. The conclusion is that the RC5 cryptographic algorithm generates a key by generating a key whose key length is set according to the number of rounds of the encryption and decryption blocks.

Keywords: Cryptography, RC 5 Symmetry, *file*, PHP, mysql

1. PENDAHULUAN

Kriptografi adalah sektor pengetahuan untuk mengamankan pesan (*message*). Kriptografi sering kali diterapkan di banyak hal salah satunya yaitu dokumen perusahaan. Dokumen merupakan salah satu aset penting dari setiap perusahaan, dokumen yang ada di suatu perusahaan bisa berupa hardcopy maupun softcopy. Contoh

dokumen yang berupa salinan keras adalah surat, sertifikat, ijazah, dan lain-lain. Sedangkan dokumen yang berupa Salinan halus atau tidak terlihat yaitu yang disimpan di komputer, dapat berbagai macam format file seperti word, excel, powerpoint, jpeg, mov, dan lain-lain. Banyak aktifitas dalam komputer melibatkan pertukaran *file* perusahaan yang akan sangat riskan jika *file* ini tidak diamankan dengan baik. Seiring majunya teknologi komputer, maka semakin tinggi pula tingkat acaman yang dapat mengancam pengguna komputer. Dampak negatif didalam perkembangan komputer salah satunya adalah pencurian data. Seiring majunya teknologi komputer, maka semakin tinggi pula tingkat acaman yang dapat mengancam pengguna komputer. Dampak negatif didalam perkembangan komputer salah satunya adalah pencurian data.

UB Link merupakan perusahaan yang berdiri sejak tahun 2019 bergerak di bidang jasa dengan fokus utama yaitu jaringan internet. Perusahaan ini harus melindungi data penjualan atau data transaksi setiap kali ada pelanggan yang memakai jasa internet. Untuk melakukan hal tersebut, pemilik usaha membutuhkan aplikasi yang dapat melindungi data dengan aman agar tidak terjadi pencurian data. Penelitian yang pernah dilakukan terkait dengan penelitian yang saat ini dikerjakan adalah:

- a. Penelitian yang dilakukan Widodo Arif Prabowo, Annisa Fitri Harahap, dan Ridha Ismaidah (2018) dari STMIK Budidarma, Medan, dengan judul “Penyandian File Word Berdasarkan Algoritma Rivest Code 5 (RC5)”. Permasalahan yang diangkat penulis adalah masalah keamanan file word, melihat saat ini penggunaan file jenis word untuk menyimpan informasi rahasia ini semakin meningkat. Metode algoritma kriptografi yang digunakan dalam perancangan dan pembuatan perangkat lunak ini adalah algoritma RC-5 yang meliputi dua tahap utama, yaitu proses perluasan kunci (key expansion), proses dekripsi atau enkripsi. Proses yang digunakan dalam pengsandian file word ini adalah proses manual.
- b. Penelitian yang dilakukan oleh Yohanes Setiawan Japriadi dan Dian Novianto (2019) dari STMIK Atma Luhur, Bangka Belitung, Jurusan Teknik Informatika dengan judul “Penerapan RC 5 Untuk Pengamanan Nilai Mata Kuliah Mahasiswa Pada Kampus Atma Luhur”. Permasalahan pada penelitian ini adalah nilai data yang ada pada basis data belum mengalami proses enkripsi (masih dalam bentuk *plainteks*). Aplikasi yang dibuat dalam penelitian ini berbasis web dengan menggunakan Bahasa pemrograman PHP, jumlah basisdata MySQL yang dikumpulkan sebanyak 6.020 nilai dan metode yang digunakan adalah algoritma kriptografi RC 5.

Dari kedua penelitian yang telah dilakukan, perbedaan yang dilakukan dalam penelitian ini adalah pengumpulan data yang dilakukan program aplikasi ini adalah dengan mengambil file secara langsung dari pihak instansi dan dapat segera dilakukan proses enkripsi atau dekripsi. Proses enkripsi dan dekripsi dilakukan secara otomatis dengan memasukkan kode enkripsi dan dekripsi RC 5 dalam bahasa pemrogramannya serta berbasis web. Alasan pemilihan metode ini adalah karena kunci algoritma ini merupakan kunci simetris yang terparameterisasi. Artinya, melalui parameter yang diberikan dapat dihasilkan *ciphertext* yang memiliki tingkat keamanan berbeda-beda, selain itu metode ini juga dipilih karena waktu pemrosesan enkripsi atau dekripsinya yang cepat, yaitu dibawah 1 detik.

2. METODE PENELITIAN

2.1 Data Penelitian

Dalam penelitian yang dilakukan saat ini, yang digunakan adalah data berupa dokumen *file* yang masih berhubungan dengan transaksi penjualan UB Link baik berupa microsoft *word*, microsoft excel, pdf, dan lain-lain. Data ini didapatkan langsung dari salah satu karyawan UB Link dalam jangka tanggal 1 juni sampai dengan tanggal 30 juni 2023 dengan pemilihan data yang sesuai dengan topik tugas akhir.

2.2 Penerapan Metode Algoritma Kriptografi RC 5

Terdapat 3 langkah dalam Algoritma RC5, yaitu perluasan enkripsi, dekripsi dan perluasan kunci. Perluasan kunci adalah langkah pembangkitkan kunci internal dengan memanfaatkan komputasi rotasi kiri *regular shift* ($\ll\gg$), dengan panjang kunci tergantung dari jumlah putaran. Kunci internal lalu dipakai dalam langkah enkripsi dan dekripsi. Langkah enkripsi dibagi menjadi tiga, yaitu: XOR, rotasi dan penjumlahan integer. Untuk lebih jelasnya, diberikan penjelasan detail sebagai berikut:

a. Enkripsi

Diperkirakan terdapat dua buah blok input sebesar w bit, A dan B . Dan diperkirakan juga bahwa pembangkitan kunci internal telah dilakukan, sehingga array $S[0..t-1]$ yang telah dihitung. Sehingga pseudocode untuk langkah enkripsi terlihat seperti di bawah:

$$A \leftarrow A + KI [0]$$

```
B ← B + K2 [1]
For i ← 1 to r do
A ← ((A⊕B) <<<< B) + KI [2i]
B ← ((B⊕A) <<<< A) + KI [2i+1]
Endfor
```

b. Dekripsi

Algoritma pada langkah dekripsi adalah kebalikan dari algoritma langkah enkripsi. Jika sebelumnya digeser ke kiri, maka pada langkah dekripsi akan dilakukan dengan melakukan pergeseran ke kanan (*right regular shift*).

```
For i ← r downto 1 do
B ← ((B - KI [2i+1])>>>>A) ⊕ A
A ← ((A - KI [2i])>>>>B) ⊕ B
Endfor
B ← B - KI[1]
A ← A - KI[0]
```

Untuk mendekripsi *file* yang telah terenkripsi, diperlukan KI yang sama dengan KI saat mengenkripsi. Langkah pembangkitan kunci KI pada kedua langkah tersebut juga sama.

c. Pembangkitan Kunci Internal

K[0-1]...K[b] disalin ke tabel L[0- 1]...L[b] memakai aturan di-padding dengan karakter 0 sehingga ukuran L[i] menjadi w/2 bit. Seperti contoh:

```
K[0] = k    L[0] = k000
K[1] = k    L[1] = r000
K[2] = k    L[2] = i000
K[3] = k    L[3] = p000
K[4] = k    L[4] = t000
K[5] = k    L[5] = o000
```

Lalu, inialisasikan tabel kunci internal KI memakai ukuran $t = 2r + 2$ seperti berikut: $KI[0] \leftarrow P$

```
For i ← 1 to t - 1 do
KI[i] ← KI[i - 1]
Endfor
```

Algoritma pembangkitan kunci internal memakai konstanta Q dan P diperoleh dari fungsi yang mengkaitkan bilangan irasional sebagai berikut :

```
P=odd[(e-2)2w]
Q=odd[(f-1)2w]
```

Keterangan:

E = 2.718281828459..... F = 1.618033988749.....

Lalu L dan S dicampurkan dengan algoritma berikut:

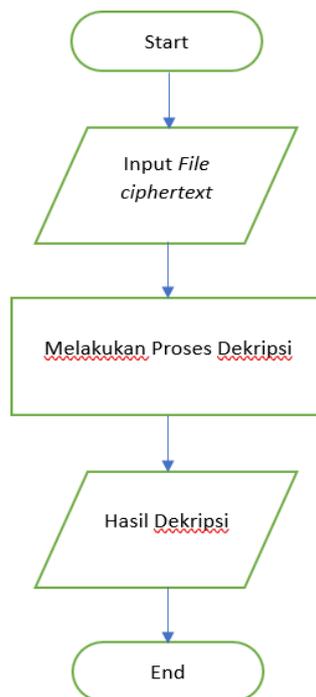
```
i ← 0
j ← 0
x ← 0
y ← 0
n ← 3*max (r,c)
For k ← 1 to n do
KI[i] ← (KI[i] + X + Y) <<<< 3 X ← KI[i]
i ← (i + 1) mod t
L[j] ← (L[j] + X + Y) <<<< 3
Y ← L[j]
j ← (j + 1) mod c
Endfor
```

Keterangan:

Maksimal (r,c) merupakan fungsi untuk memilih bilangan terbesar diantara r dan c. c merupakan nilai maksimal dari Panjang kunci b yang dibagi dengan angka 4. Berikut dibawah ini *flowchart* yang digambarkan untuk menelusuri langkah alur sistem pada program Kriptografi algoritma RC5 untuk keamanan pada file dokumen docx, xlsx dan pdf, seperti terlihat pada Gambar 1 dan Gambar 2.



Gambar 1. Proses Enkripsi



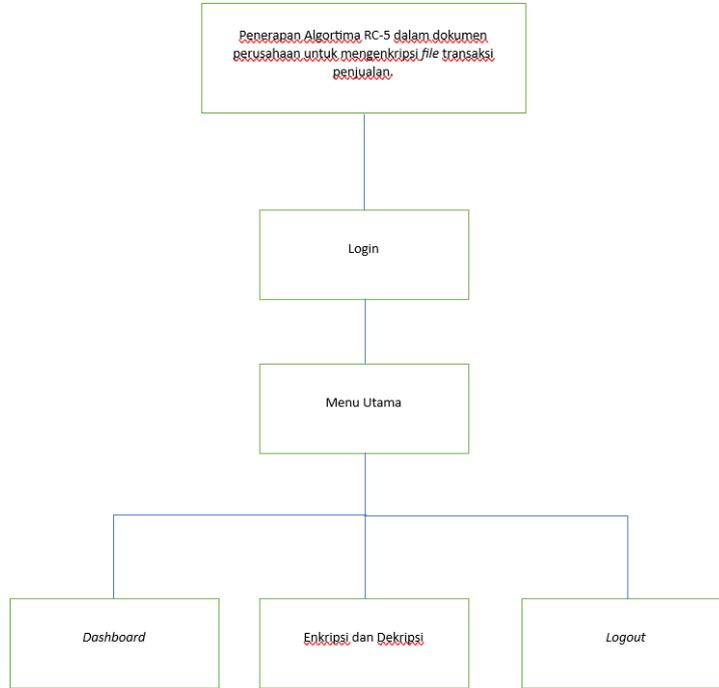
Gambar 2. Proses Dekripsi

2.3 Rancangan Pengujian

Dalam pembuatan sistem enkripsi dan dekripsi RC5 ini dibutuhkan basis data untuk menyimpan data enkripsi, data dekripsi, dan akun *login*.

2.4 Rancangan Menu Web

Program yang akan dibuat terdiri dari 4 buah relasi *menu web*, yaitu terdiri dari *dashboard*, Enkripsi dan Dekripsi, tentang aplikasi, *Logout*. Aplikasi ini hanya ada di *mode admin*, dapat dilihat pada Gambar 3.

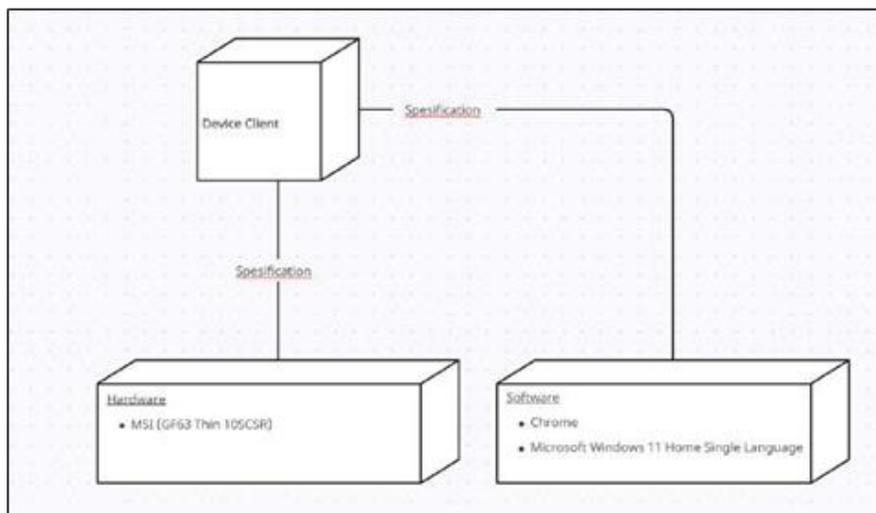


Gambar 3. Rancangan Menu Web

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

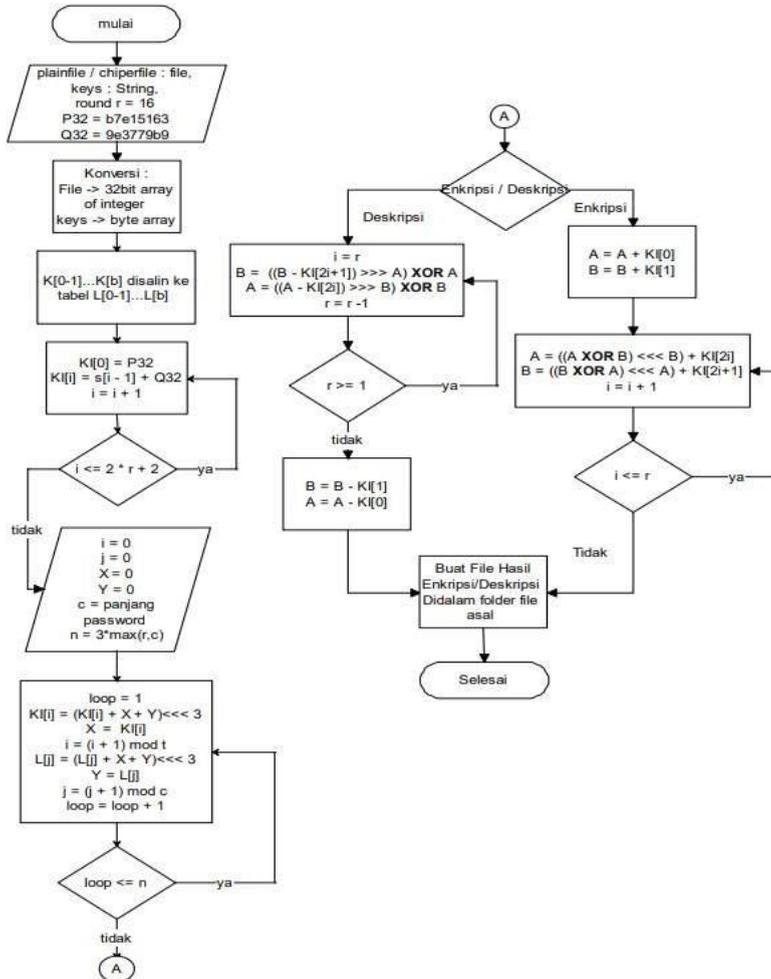
Dalam melakukan pengujian *software* tentu saja diperlukan sebuah *device* untuk menguji aplikasi yang telah dibuat, berikut adalah spesifikasi *hardware* dan *software* yang akan digambarkan dalam *Deployment Diagram*, terlihat pada gambar 4.



Gambar 4. Spesifikasi Hardware dan Software

3.2 Implementasi Metode

Implementasi metode algoritma kriptografi didalam sistem aplikasi akan di jelaskan melalui flowchart, berikut Gambar 5.



Gambar 5. Flowchart Langkah Penerapan Algoritma RC5

Pada gambar 3.2, langkah enkripsi dan dekripsi dilakukan memakai dua blok inputan yaitu A dan B sebagai *word* sebesar 32 bit yang dihasilkan dari langkah konversi pada *file*. Selanjutnya, langkah enkripsi akan dilakukan seperti algoritma berikut:

$$A \leftarrow A + KI [0] \quad B \leftarrow B + K2 [1]$$

For $i \leftarrow 1$ **to** r **do**

$$A \leftarrow ((A \oplus B) \lll B) + KI [2i]$$

$$B \leftarrow ((B \oplus A) \lll A) + KI [2i+1]$$

Endfor

Sedangkan langkah dekripsi dilakukan seperti algoritma berikut:

For $i \leftarrow r$ **downto** 1 **do**

$$B \leftarrow ((B - KI [2i+1]) \ggg A) \oplus A$$

$$A \leftarrow ((A - KI [2i]) \ggg B) \oplus B$$

Endfor

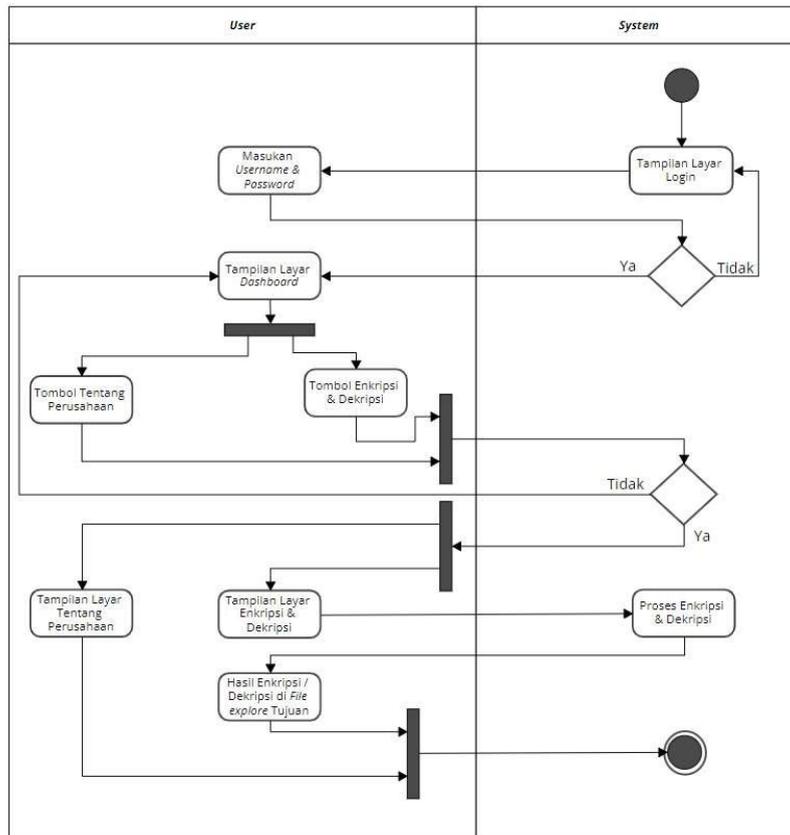
$$B \leftarrow B - KI[1]$$

$A \leftarrow A - KI[0]$

Setelah dua buah blok inputan tersebut selesai diproses, lalu sistem akan melakukan kembali penggabungan dan menuliskan hasil dekripsi dan enkripsi kedalam sebuah *file* baru dengan hasil nama *file* yang baru.

3.3 Rancangan Diagram Aktivitas (Activity Diagram)

Activity Diagram adalah aliran rancangan aktivitas atau alur kerja dalam sistem yang sedang berjalan. *Activity Diagram* dapat digunakan untuk mengelompokkan atau mendefinisikan alur tampilan sistem. Alur kegiatan dalam program digambarkan dalam *Activity Diagram* di bawah ini, terlihat pada Gambar 6.



Gambar 6. Activity Diagram

3.4 Tabel Pengujian dan Analisa Program

Dalam pengujian penelitian saat ini, akan dibahas perbandingan antara proses enkripsi dan dekripsi *file*. Pengujiannya yaitu antara lain ukuran *file*, waktu proses enkripsi, waktu proses dekripsi hingga hasil yang dicapai dalam proses enkripsi maupun dekripsi. Dapat dilihat pada tabel 1 dan 2.

Tabel 1. Hasil Pengujian Enkripsi

Nama File Awal	Ukuran File (KB)	Waktu Enkripsi (Seconds)	Ukuran Hasil Enkripsi (KB)	Nama File Hasil Enkripsi
InvoiceAbdul..	78	50 ns	104	enkripsi_Invoice..
Logo-Ub Link	14	28 ns	19	enkripsi_Logo..
Invoice-Adin..	78	50 ns	104	enkripsi_Invoice..
Surat Keterangan..	30	35 ns	40	enkripsi_Surat..
Tagihan Inter..	123	67 ns	164	enkripsi_Tagihan..

Tabel 2. Hasil Pengujian Dekripsi

Nama File Awal	Ukuran File (KB)	Waktu Dekripsi (Seconds)	Ukuran Hasil Dekripsi (KB)	Nama File Hasil Dekripsi
enkripsi_Invoice..	104	42 ns	78	dekripsi_enkrip..
enkripsi_Logo..	19	18 ns	14	dekripsi_enkrip..
enkripsi_Invoice..	104	42 ns	78	dekripsi_enkrip..
enkripsi_Surat..	40	27 ns	30	dekripsi_enkrip..
enkripsi_Tagihan..	164	55 ns	123	dekripsi_enkrip..

Berdasarkan pengujian aplikasi dekripsi dan enkripsi yang telah dilakukan, baik itu berupa *file* dokumen DOCX, XLSX maupun *file* PDF. Dari hasil pengujian program yang telah dilakukan, disimpulkan beberapa analisa kekurangan dan kelebihan program ini yaitu:

- Rata – rata waktu kecepatan aplikasi dalam mengenkripsi dan mendekripsi *file* berada di bawah satu detik.
- Kecepatan dekripsi lebih unggul dibandingkan kecepatan mengenkripsi *file*.
- Semakin besar ukuran *file* yang akan didekripsi ataupun dienkripsi maka akan membutuhkan waktu enkripsi atau dekripsi yang lebih lama.
- Hasil dari inputan *file* yang telah dienkripsi maupun didekripsi akan memiliki nama *file* yang berbeda.
- File* yang telah dienkripsi tidak dapat dikembalikan atau dibuka seperti semula tanpa proses dekripsi.

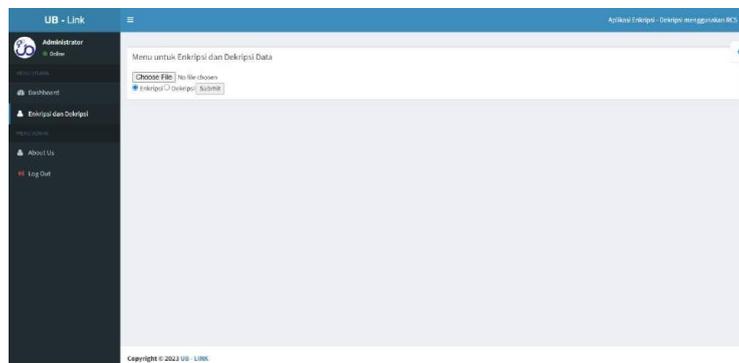
3.5 Tampilan Layar Aplikasi

Tampilan layar aplikasi adalah hasil tampilan dari rancangan layar yang di telah buat . Tampilan layar terdiri dari halaman layar login, halaman layar *Dashboard*, halaman layar enkripsi dan dekripsi, dan halaman layar *About Us*. Terlihat pada gambar 7 dan 8.



Gambar 7. Tampilan Layar Login

Tampilan Layar *login* menampilkan halaman untuk masuk kedalam aplikasi berbasis *web*. Akun yang sudah dibuat oleh *admin* dapat masuk ke halaman *dashboard*. Jika akun tidak terdaftar maka sistem akan menolak untuk *login*.



Gambar 8. Tampilan Halaman Layar Menu Enkripsi dan Dekripsi

Tampilan Layar *Menu* Enkripsi dan Dekripsi menampilkan halaman untuk melakukan enkripsi maupun dekripsi. Berisi dua panel tombol untuk memilih proses apa yang ingin *user* lakukan.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian yang telah dilakukan adalah :

- a. Cara mengamankan data berupa dokumen *file* transaksi dan dokumen penjualan yang didapat pada UB Link adalah dengan membuat program aplikasi kriptografi dengan menginput *file* transaksi penjualan ke dalam aplikasi berbasis *web* dan membuat *file* dikunci, sehingga pihak yang tidak berwenang tidak bisa sembarangan mengakses *file* transaksi penjualan milik UB Link.
- b. Algoritma kriptografi RC5 menghasilkan kunci dengan cara melakukan pembangkitan kunci (*set up key*) yang panjang kuncinya diatur sesuai pada jumlah putaran blok enkripsi maupun dekripsi.
- c. Hasil pengujian yang telah dilakukan pada aplikasi adalah rata – rata waktu kecepatan aplikasi dalam mengenkripsi dan mendekripsi *file* berada di bawah satu detik, Kecepatan dekripsi lebih unggul dibandingkan kecepatan mengenkripsi *file*, Semakin besar ukuran *file* yang akan didekripsi atau dienkripsi maka akan membutuhkan waktu enkripsi atau dekripsi yang lebih lama, Hasil dari masukan *file* yang telah dienkripsi maupun didekripsi akan memiliki nama *file* yang berbeda. *File* yang telah dienkripsi tidak dapat dikembalikan atau dibuka seperti semula tanpa proses dekripsi.

DAFTAR PUSTAKA

- [1] Widodo, A.P., Annisa F., & Ridha, I. (2018). Penyandian *File Word* Berdasarkan Algoritma Rivest Code 5 (RC5). *Jurnal Sains & Informatika (J-SAKTI)*.
- [2] Indra, N.A., Dewi, K., & Mohammad, A. (2018). Aplikasi Enkripsi *File* Dokumen Menggunakan Algoritma AES (Advance Encryption Standard) Dan OTP (One Time Pad) Berbasis Web Pada PT. MNC SKY VISION. *Jurnal Telematika MKOM*.
- [3] Yohanes, S.J., & Dian, N. (2019). Penerapan RC5 Untuk Pengamanan Nilai Mata Kuliah Mahasiswa Pada Kampus Atma Luhur. *Jurnal Algoritma, Logika dan Komputasi*.
- [4] Sastya, H.W., & Diana. (Maret 2023). Analisis Dan Implementasi Algoritma *Rivest Code-5* Pada Keamanan Data. *Jurnal Penelitian Teknologi Informasi Dan Sains (JPTIS)*. Vol 1. No 1. e-ISSN: 2 2985-7635. Hal 09-21.
- [5] Karina, A., & Herawan, B. (2022). Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (RSA) Pada Toko Baju Family. *Journal of Science and Social Research*. V (3). 664 – 670.
- [6] Saputra, D.N. (2022). Perancangan Aplikasi Enkripsi Dan Dekripsi Dengan Algoritma Kriptografi Berbasis *Web*. *Jurnal Nasional Komputasi dan Teknologi Informasi*. Vol 5. No 4. E-ISSN 2621 – 3052.
- [7] Yusna, W.H., Isnarto, Rahayu, B. (2022). Perancangan dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode ASCII. *UNNES Journal of Mathematics*.
- [8] Aditya, U., & Fanry R.S. (2021). Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada *Easy Tronik Metode RC-5* *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*.
- [9] Harni, K., Satya, D., & Raka, Y. (2018). Penerapan Algoritma *Rivest Code 4 (RC4)* Pada Aplikasi Kriptografi Dokumen. *Jurnal Petir* Vol 11. No 1.
- [10] Ilham, M.G., & Utomo, B. (2022). Algoritma FP-Growth Untuk Mengkaji Pola Belanja Konsumen pada *Baby Shop By Netti*. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*.
- [11] Surya, A.G. (2020). Kriptografi Pengamanan Data *File* Berupa Gambar Menggunakan Metode RSA dan *Digital Signature*. *Jurnal Teknik Informatika Universitas Muhammadiyah Gresik*.
- [12] I Nyoman, P. (2019). Implementasi Algoritma Enkripsi RC5 Untuk Mengamankan Gambar Pada Perangkat Android. *Jurnal Informatika & Rekayasa Elektronika (JIRE)* Vol 2. No 2.
- [13] Jonas, S., Muhammad, I., Sri, N. (2018). Penyandian Pesan Berdasarkan Algoritma RC5 dan El-Gamal. *Jurnal Penelitian Teknik Informatika*. Vol 2. No 2. E-ISSN: 2541-2019.
- [14] Rozali, T., & Ardi, W. (2018). Analisis Perbandingan Algoritma Simetris *Rivest Code 5* dengan Algoritma *Rivest Code 6*. *Jurnal Informatika UPGRIS* Vol 4. No 2. E-ISSN: 2460-4801.
- [15] Galih, Y., Asep, I., Puspita, N. (2022). Kriptografi Untuk Enkripsi Ganda Pada Gambar Menggunakan Algoritma AES (*Advance Encryption Standard*) Dan RC5 (*Rivest Code 5*). *Journal of Informatic and Digital Expert*. Vol 4. No 1.