

# Android-Based Cryptography Applications Using The Rail Fence Cipher Algorithm

## Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Rail Fence Cipher

Raden Diky Zailani <sup>1)</sup>; Khairil <sup>2)</sup>; Abdussalam Al Akbar <sup>3)</sup>

<sup>1)</sup> Program Studi Informatika, Fakultas Ilmu computer, Universitas Dehasen Bengkulu

Email: <sup>1)</sup> [rdikyz@gmail.com](mailto:rdikyz@gmail.com)

### How to Cite :

Zailani, D.,R, Khairil, K., Akbar, A.,A. (2023). Aplikas Kriptografi Berbasis Android Menggunakan Algoritma Rail Fence Cipher. Jurnal Media Computer Science, 2(2).

### ARTICLE HISTORY

Received [01 Juni 2023]

Revised [29 Juni 2023]

Accepted [18 Juli 2023]

### KEYWORDS

Cryptography, Android,  
Rail Fence Cipher  
Algorithm

This is an open access  
article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/)  
license



### ABSTRAK

Aplikasi kriptografi berbasis android menggunakan algoritma rail fence cipher dibuat menggunakan bahasa pemrograman Java (AndroidStudio), bahasa pemrograman PHP (File web Service JSON) dan databaseMySQL. Aplikasi ini terdapat link url untuk menyimpan file PHP dan data pesan di database, adapun link url tersebut <http://railfencecipher.my.id/>. Aplikasi kriptografi berbasis android menggunakan algoritma rail fence cipher telah di upload ke google playstore dengan memasukkan kata kunci rail fence cipher. Aplikasi kriptografi berbasis android menggunakan algoritma rail fence cipher ini dapat digunakan untuk membantu komunikasi antara kedua belah pihak baik pengirim dan penerima pesan. Selain itu pada aplikasi ini telah diterapkan algoritma rail fence cipher yang digunakan untuk menjaga kerahasiaan pesan tersebut yang disimpan di dalam database dari aplikasi. Record pada kolom isi pesan di database dalam bentuk teracak, sehingga tidak dapat dibaca. Hal ini tentunya membuat aplikasi tersebut terjaga kerahasiaan pesan yang dikirim, karena terjadi proses pengacakan (enkripsi) pada pesan tersebut. Berdasarkan hasil pengujian yang telah dilakukan, fungsional dari aplikasi kriptografi berbasis android menggunakan algoritma rail fence cipher berjalan dengan baik sesuai yang diharapkan dan pesan yang dikirim antara penerima dan pengirim terjaga kerahasiaan keamanan pesan tersebut karena sudah teracak.

### ABSTRACT

Android-based cryptographic applications using the rail fence cipher algorithm are made using the Java programming language (AndroidStudio), the PHP programming language (JSON File Web Service) and the MySQL database. This application has a url link for storing PHP files and message data in the database, while the url link is <http://railfencecipher.my.id/>. An Android-based cryptographic application using the rail fence cipher algorithm has been uploaded to Google Playstore by entering the rail keyword fence cipher. An android-based cryptographic application using the rail fence cipher algorithm can be used to assist communication between the two parties, both the sender and the recipient of the message. In addition, this application has implemented a rail fence cipher algorithm that is used to maintain the confidentiality of the message stored in the application's database. The records in the message body column in the database are in random form, therefore they cannot be read. This of course makes the application maintain the confidentiality of the messages sent, because there is a process of scrambling (encryption) of the message. Based on the results of the tests that have been carried out, the functionality of the android-based cryptographic application using the rail fence cipher algorithm runs well as expected and the message sent between the recipient and the sender is kept confidential because the message is encrypted.

## PENDAHULUAN

Komunikasi merupakan salah satu kegiatan dasar dalam kehidupan manusia yang memungkinkan manusia saling dapat bertukar informasi. Pertukaran informasi jarak jauh ini menuntut keamanan terhadap kerahasiaan informasi yang dipertukarkan. Suatu informasi akan memiliki nilai tinggi apabila menyangkut tentang aspek keamanan, kepentingan umum dan kepentingan pribadi, sehingga informasi tersebut akan banyak diminati oleh pihak lain yang tidak berwenang untuk mendapatkan isi dari informasi tersebut. Salah satu cara dalam mengamankan informasi tersebut yaitu dengan melakukan keamanan terhadap informasi melalui kriptografi.

Kriptografi adalah bidang ilmu yang mempelajari tentang cara untuk menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu, dengan tujuan agar informasi dalam pesan tersebut tidak disalahgunakan oleh orang yang bukan penerima aslinya. Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti Caesar Cipher, Affine, Monoalphabetic, Polyalphabetic, Vigenere, Rail Fence Cipher, Transposisi, dan banyak lagi metode-metode dalam kriptografi ini.

Dalam penelitian ini dilakukan penerapan terhadap algoritma kriptografi ke bentuk aplikasi chatting. Aplikasi chatting yang berfungsi sebagai media berkomunikasi juga digunakan dalam kegiatan komunikasi untuk saling bertukar informasi. Pengiriman pesan melalui internet menggunakan aplikasi chatting bersifat realtime yang dilakukan dengan transaksi paket antara client dengan server.

Salah satu algoritma kriptografi yang diterapkan ke dalam aplikasi chatting untuk menjaga kerahasiaan informasi chat antara pengirim dan penerima yaitu algoritma rail fence cipher. Algoritma Rail Fence Cipher merupakan salah satu algoritma cipher transposisi yang mengacak urutan huruf-huruf pesan. Algoritma ini melibatkan penulisan plaintext ke bawah secara berturut turut yang memiliki baris atas dan baris bawah. Sedangkan ciphertext nya diperoleh dengan membaca huruf berdasarkan baris.

## LANDASAN TEORI

### Aplikasi Chatting

Aplikasi chatting adalah aplikasi yang digunakan untuk berkomunikasi dalam satu jaringan lokal atau internet yang saling terhubung satu sama lain untuk mempermudah percakapan. Aplikasi chatting yang saat ini banyak berkembang pesat antara lain WhatsApp, Line, dan Telegram aplikasi tersebut memiliki keunggulan dan fitur masing-masing, karena pada dasarnya aplikasi tersebut digunakan oleh umum dan diakses dari seluruh penjuru dunia (Prabowo & Pramusinto, 2018)

### Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani : "cryptos" artinya "secret"(rahasia), sedangkan "graphein" artinya "writing" (tulisan). Jadi, kriptografi berarti "secret writing" (tulisan rahasia) (Rosna, et al., 2019).

### Algoritma Rail Fence Cipher

Algoritma Rail Fence Cipher merupakan salah satu algoritma cipher transposisi yang mengacak urutan huruf-huruf pesan. Algoritma ini melibatkan penulisan plaintext ke bawah secara berturut turut yang memiliki baris atas dan baris bawah. Sedangkan ciphertext nya diperoleh

dengan membaca huruf berdasarkan baris. Algoritma Rail Fence Cipher menyusun plainteks secara ziq-zag dengan turun ke bawah dan naik ke atas sesuai ukuran kolom dan baris yang ditentukan oleh key (Purnamasari, 2021).

### **Android**

Android adalah sebuah sistem operasi perangkat mobile berbasis linux yang mencakup sistem operasi, middleware, dan aplikasi. Android adalah "sistem operasi berbasis linux yang di gunakan untuk telepon seluler (mobile) seperti telepon pintar (smartphone) dan komputer tablet (Safitri & Basuki, 2020).

### **Android Studio**

Android studio ini adalah lingkungan pengembangan baru dan terintegrasi dengan penuh, yang telah di rilis oleh google untuk sistem operasi Android dan di rancang untuk menjadi peralatan baru dalam pengembangan aplikasi dan memberi alternaif selain Eclips yang saat ini menjadi IDE yang banyak dipakai (Safitri & Basuki, 2020).

### **Bahasa Pemrograman Java**

Bahasa pemrograman java bersifat open source dan merupakan produk dari Sun Microsystem dan sekarang dipegang oleh Oracle. Bahasa java adalah bahasa modern yang telah diterima masyarakat komputasi dunia. Sifat dan jenis bahasa pemrograman java yaitu bahasa pemrograman multiplatform (dapat berjalan di berbagai macam sistem operasi) karena pada dasarnya java mempunyai JRE (Java Runtime Environment) atau sebagai mesin tersendiri untuk meneksekusi binary code hasil dari kompilasi program yang telah dibuat, berbeda dengan bahasa pemrograman visual basic, C++ yang memanfaatkan komponen sistem dalam windows untuk mengeksekusi binary code hasil kompilasi program (Efitra, 2021).

### **Bahasa Pemrograman PHP**

Hypertext Preprocessor atau lebih akrab dengan PHP merupakan bahasa pemrograman script server-side yang di desain untuk pengembangan web. PHP disebut bahasa pemrograman server-side karena diproses pada komputer server. Hal ini berbeda dengan bahasa pemrograman client-side seperti javascript yang diproses di dalam web browser. PHP dapat digunakan secara gratis dan bersifat open source. PHP dirilis dalam lisensi PHP License, sedikit berbeda dengan lisensi GNU (General Public License) yang biasa digunakan untuk proyek open source (Jannah, et al., 2019)

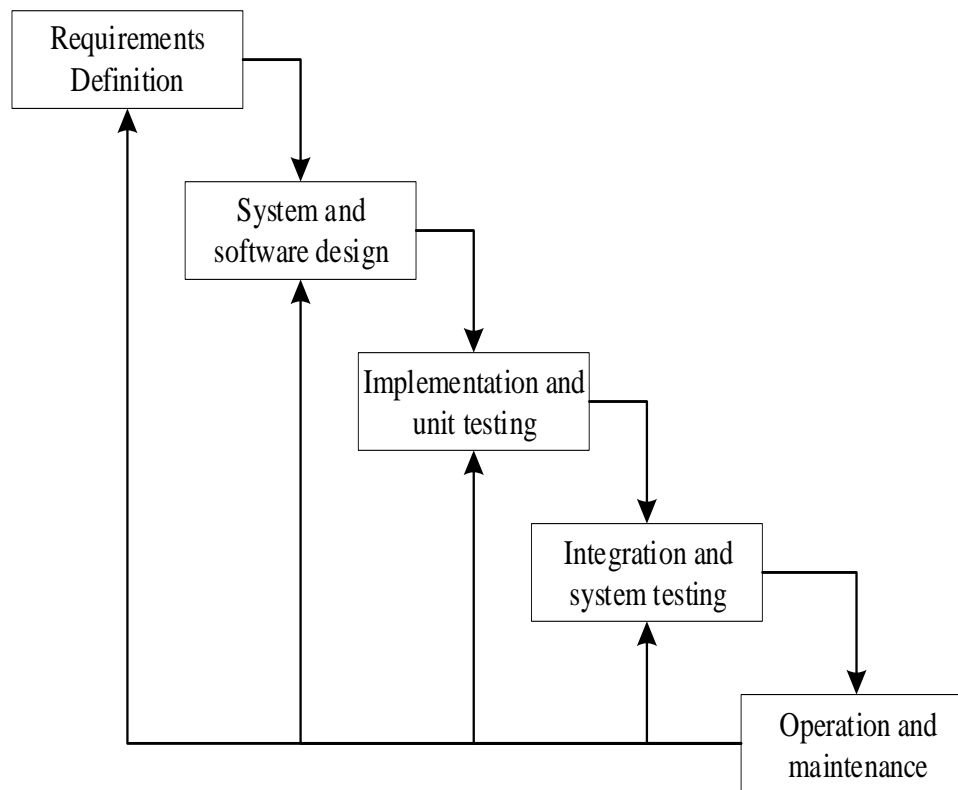
### **Database MySQL**

MySQL adalah sebuah basis data yang mengandung satu atau jumlah tabel. Tabel terdiri atas sejumlah baris dan setiap baris mengandung satu atau sejumlah tabel. Tabel terdiri atas sejumlah baris dan setiap baris mengandung satu atau sejumlah tabel (Hans, 2016).

## **METODE PENELITIAN**

Metode penelitian yang digunakan yaitu Metode *waterfall* dimana tahapan-tahapan dari metode ini, seperti Gambar 1.

Gambar 1. Metode Waterfall



Keterangan :

- 1) *Requirements analysis and definition*  
Layanan sistem, kendala, dan tujuan ditetapkan oleh hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.
- 2) *System and software design*  
Tahapan perancangan sistem mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.
- 3) *Implementation and unit testing*  
Pada tahap ini, perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya.
- 4) *Integration and system testing*  
Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak.
- 5) *Operation and maintenance*  
Tahapan ini merupakan tahapan yang paling panjang. Sistem dipasang dan digunakan secara nyata. *Maintenance* melibatkan pembetulan kesalahan yang tidak ditemukan pada tahapan-tahapan sebelumnya, meningkatkan implementasi dari unit sistem, dan meningkatkan layanan sistem sebagai kebutuhan baru.

## HASIL DAN PEMBAHASAN

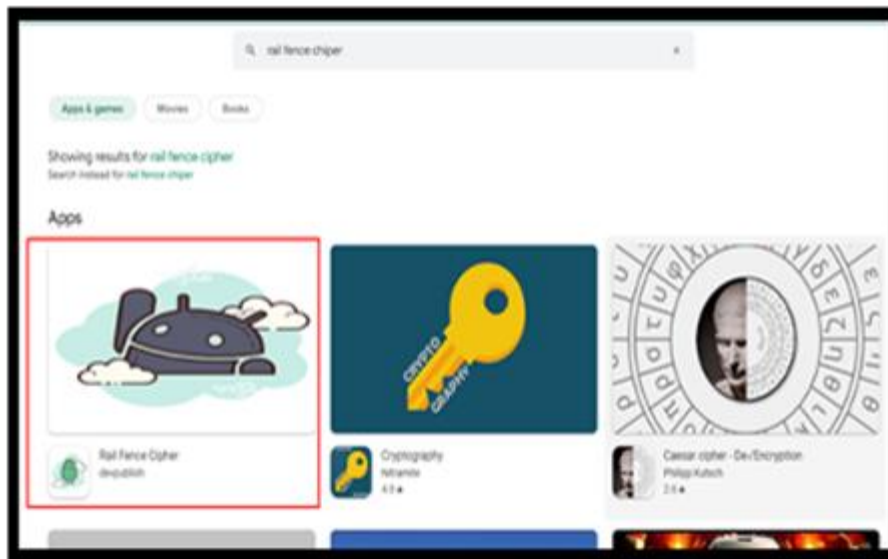
### Hasil

Aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* dibuat menggunakan bahasa pemrograman *Java (Android Studio)*, bahasa pemrograman *PHP (File web*

Service JSON) dan database MySQL. Aplikasi ini terdapat *link url* untuk menyimpan file PHP dan data pesan di database, adapun *link url* tersebut <http://railfencecipher.my.id/>. Selain itu pada aplikasi ini telah diterapkan algoritma *rail fence cipher* yang digunakan untuk menjaga kerahasiaan pesan tersebut yang disimpan di dalam database dari aplikasi.

Aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* telah di upload ke google playstore dengan memasukkan kata kunci rail fence cipher, sehingga akan tampil halaman seperti Gambar 2.

**Gambar 2. Aplikasi Rail Fence Cipher Di Google Playstore**



Pada sub bab ini akan dibahas dibagi menjadi 2 bagian tentang keamanan pesan dan aplikasi, sebagai berikut :

#### A. Keamanan Pesan

Untuk keamanan pesan telah diterapkan algoritma *rail fence cipher* dimana pesan yang akan dikirim diubah terlebih dahulu ke dalam bentuk acak, kemudian akan disimpan ke dalam database aplikasi. Proses pengacakan tersebut disebut juga dengan proses enkripsi. Hal ini membuat isi pesan yang tersimpan pada tabel di dalam database dalam bentuk acak (bukan pesan asli), seperti terlihat pada Gambar 3.

**Gambar 3. Isi Pesan Yang Terdapat Pada Tabel Di Dalam Database**

kdpesan	tglpesan	userkirim	userterima	isipesan
1	2023-06-05	zailani	diki	simtpg.aakbry eaa al p aana?
17	2023-06-05	diki	zailani	hi ah simknaeziai aa ea.
18	2023-06-05	diki	zailani	simtmlmeaa ea.
19	2023-06-05	diky	raden	hloal
20	2023-06-05	yudha	diky	hlo al
21	2023-06-08	diki	zailani	tsot
22	2023-06-12		diki	
23	2023-06-12		diki	ts ot
24	2023-06-12		diki	
25	2023-06-12	diki	yudha	
26	2023-06-14		diki	
27	2023-06-14	real	diki	tsigetn
28	2023-06-14	diki	real	pn lg
29	2023-06-15	diki	zailani	hi p aa aaaaabr?
30	2023-06-15	diki	zailani	tnua rolaetknpirts
31	2023-06-15	diki	zailani	tnua rolaetknpirts
32	2023-06-16	diki	zailani	TNUA ROIAETKNPIRTS

Pada Gambar 3. tersebut terlihat bahwa record di kolom isi pesan tersebut teracak, sehingga tidak dapat dibaca. Hal ini tentunya membuat aplikasi tersebut terjaga kerahasiaan pesan yang dikirim, karena terjadi proses pengacakan (enkripsi) pada pesan tersebut.

## B. Aplikasi

### 1. Menu Pembuka

**Gambar 4. Menu Pembuka**



Pada Gambar 4. tersebut terlihat bahwa terdapat 2 button yang dapat diakses, diantaranya

- a) Registrasi, digunakan user untuk membuka halaman registrasi bagi user yang belum mempunyai username dan password untuk akses login.
- b) Login, digunakan user untuk membuka halaman login bagi user yang sudah mempunyai username dan password untuk akses login.

### 2. Registrasi

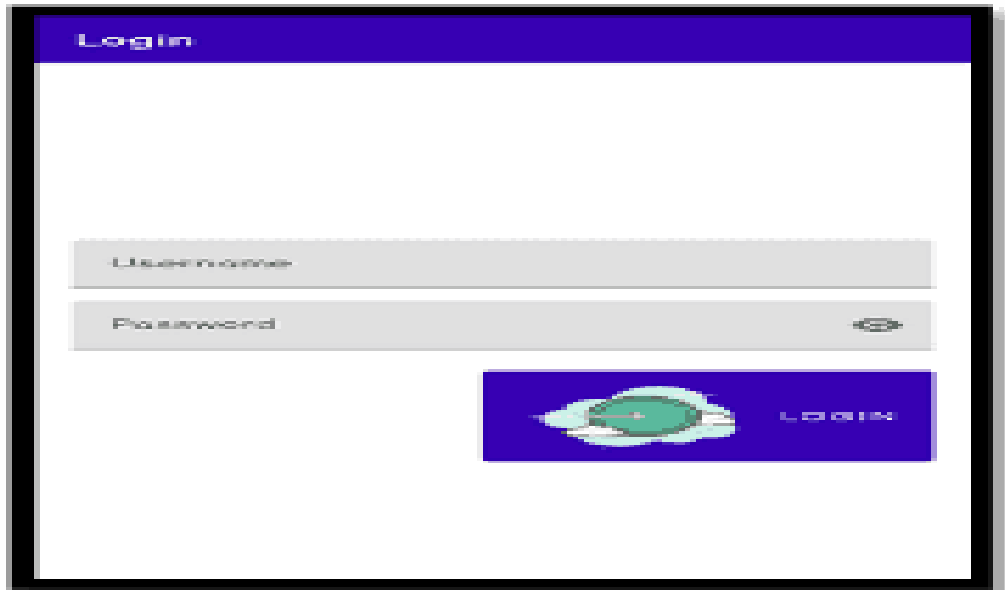
**Gambar 5. Registras**



Setelah berhasil registrasi, maka user dapat melakukan login di aplikasi menggunakan username dan password yang telah diregistrasi.

### 3. Login

**Gambar 6. Login**



Pada Gambar 6. tersebut terlihat bahwa terdapat field yang harus diisi yaitu username dan password.

### 4. Menu Utama

**Gambar 7. Menu Utama**



Pada Gambar 7. tersebut terlihat bahwa terdapat 3 tombol yang dapat diakses oleh user, antara lain :

- a) Kirim Pesan (Enkripsi), digunakan user untuk membuka halaman kirim pesan (enkripsi), sehingga dapat memulai mengirim pesan dengan memilih penerima pesan tersebut.

- b) Lihat Pesan (Dekripsi), digunakan user untuk membuka halaman lihat pesan (dekripsi), dimana akan menampilkan pesan-pesan yang telah dikirimkan oleh si pengirim.
- c) Info, digunakan user untuk mengetahui informasi tentang aplikasi.

#### 5. Kirim Pesan (Enkripsi)

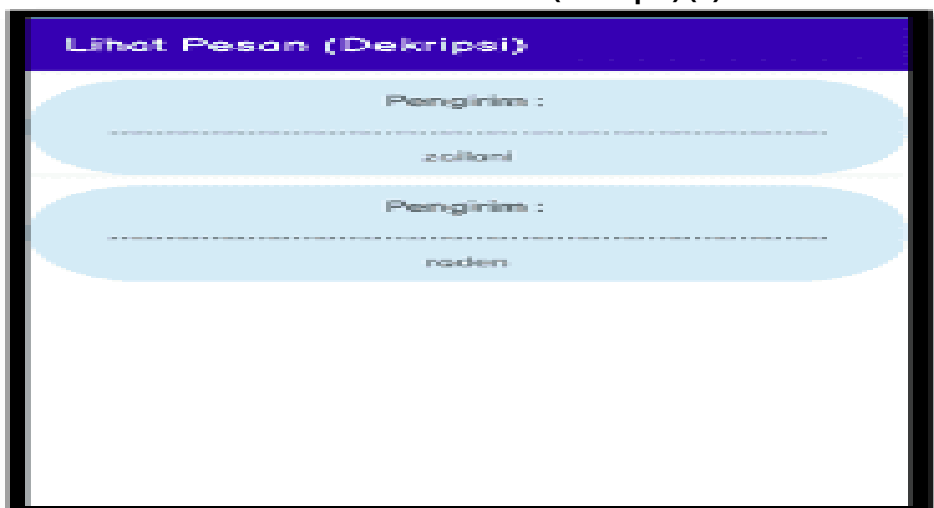
**Gambar 8. Kirim Pesan (Enkripsi)**



Pada Gambar 8. tersebut, user pengirim akan mengirim siapa penerima pesan, dalam hal ini adalah "diki". Kemudian mengisi plaintext (pesan) yang akan dikirim ke penerima yaitu "selamat pagi, apa kabarnya?". Setelah selesai memilih penerima pesan dan mengetik pesan yang akan dikirim, maka klik tombol kirim pesan untuk mengirim pesan tersebut ke penerima.

#### 6. Lihat Pesan (Dekripsi)

**Gambar 9. Lihat Pesan (Dekripsi) (1)**



Pada Gambar 9. terdapat list nama pengirim pesan. Jika ingin melihat pesan yang dikirim oleh pengirim pesan,



Gambar 10. Lihat Pesan (Dekripsi) (2)



7. Info

Gambar 11. Info



Pembahasan

Gambar 12. Pengiriman Pesan Dari Pengirim Ke Penerima



Pada Gambar 12. tersebut terdapat tombol kirim pesan, dimana akan memproses data penerima dan isi pesan tersebut ke dalam bentuk format JSON yang kemudian memanggil file php melalui url web <http://railfencecipher.my.id/>. Adapun file php tersebut, seperti Gambar 12.

**Gambar 13. File PHP Proses Enkripsi**

```

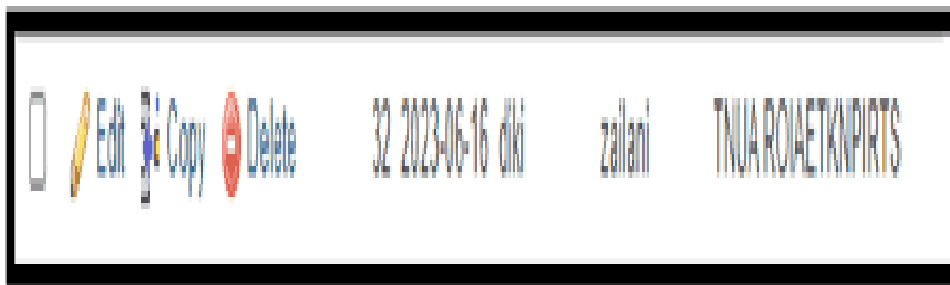
14 if ($kunci < 2) $kunci = 2;
15
16 for ($rail = 0; $rail < $kunci; $rail++)
17 {
18     for ($index = $rail; $index <= strlen($isipesan); $index += $kunci)
19     {
20         $isipesanenkripsi .= substr($isipesan, $index, 1);
21     }
22 }

```

Pada Gambar 13. tersebut merupakan penerapan dari algoritma rail fence cipher dimana terdapat fungsi perulangan, dimana `strlen($isipesan)` digunakan untuk menghitung jumlah karakter dari isi pesan asli, kemudian terdapat perintah `substr($isipesan, $index, 1)` digunakan untuk memotong atau mengambil string pada `$isipesan`, kemudian memasukkannya ke dalam variabel `$index` sebanyak jumlah karakter yang telah dihitung.

Setelah diproses oleh file php tersebut, maka data penerima dan isi pesan yang dikirim akan tersimpan ke dalam database. Namun isi pesan tersebut teracak karena sudah melalui algoritma rail fence cipher, seperti terlihat pada Gambar 14.

**Gambar 14. Isi Pesan Teracak di Database Aplikasi**



Pada Gambar 13. tersebut terlihat bahwa record pada kolom isi pesan tersebut teracak yang awalnya pesan asli "TENTUKAN PRIORITAS" menjadi "TNUA ROIAETKNPIRTS".

#### 1. Melihat Pesan Yang Telah Dikirim Dari Sisi Penerima Pesan (Dekripsi)

Melihat pesan yang telah dikirim dari sisi penerima pesan dapat dilakukan dengan memilih siapa pengirim pesan tersebut, dan kemudian akan menampilkan isi pesan yang telah dikirim oleh pengirim pesan, seperti Gambar 15.

Gambar 15. Proses Dekripsi



Pada Gambar 14. terlihat bahwa user penerima pesan dapat melihat isi pesan yang dikirim oleh si pengirim pesan dalam bentuk pesan asli secara langsung tanpa harus memasukkan kunci dekripsi. Hal ini dikarenakan ketika menampilkan isi pesan terdapat proses pemanggilan file PHP dari url <http://railfencecipher.my.id/>, dimana mengubah pesan teracak yang terdapat di dalam database yaitu "TNUA ROIAETKNPIRTS" menjadi "TENTUKAN PRIORITAS". Adapun file PHP tersebut seperti Gambar 15.

Gambar 16. File PHP Proses Dekripsi

```
$pesanenkrup = $x["isipesan"];  
  
$jmlkarakter = strlen($pesanenkrup);  
$rail = $jmlkarakter / 2;  
  
$rails = round($rail);  
  
if ($rails < 3) $rails = 3;  
for ($reil = 0; $reil < $rails; $reil++)  
{  
    for ($sindex = $reil; $sindex <= strlen($pesanenkrup); $sindex  
        += $rails)  
    {  
        $pesanasli .= substr($pesanenkrup, $sindex, 1);  
    }  
}
```

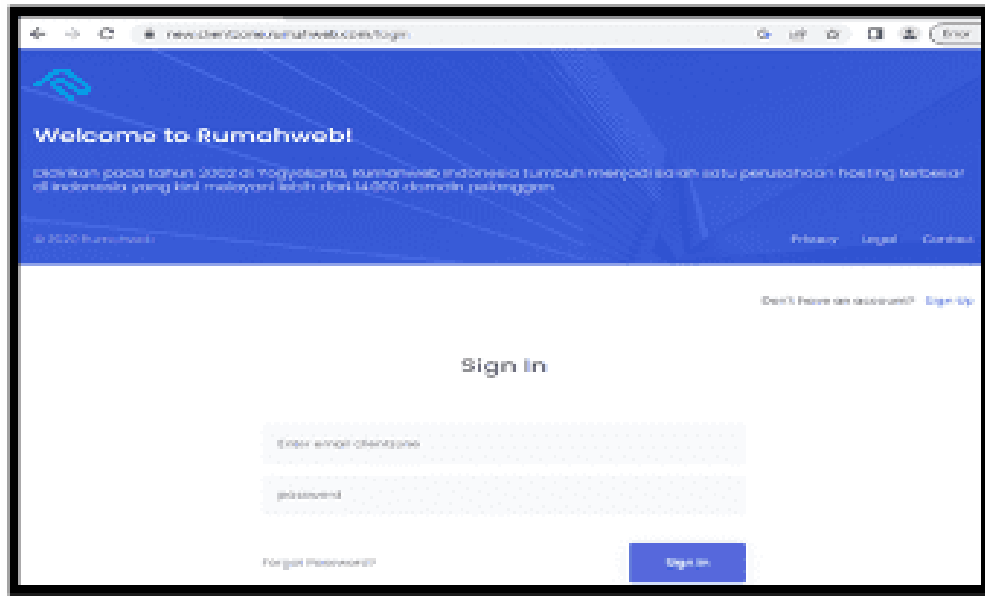
Pada Gambar 16. tersebut, terdapat proses dekripsi yang mengambil setiap isi pesan dari database ( $\$x["isipesan"]$ ) kemudian dimasukkan ke dalam variabel  $\$pesanenkrup$ . Setelah itu menghitung jumlah karakter yang ada di  $\$pesanenkrup$  dan dibagi dengan kunci 2, yang hasilnya akan menentukan berapa banyak baris dan kolom untuk proses dekripsi. Kemudian terdapat perintah  $\text{substr}(\$pesanenkrup, \$index, 1)$  digunakan untuk memotong atau mengambil string pada  $\$isipesan$ , dan memasukkannya ke dalam variabel  $\$index$  sebanyak jumlah karakter yang telah dihitung. Setelah itu hasil dekripsi tersebut akan dimasukkan ke dalam format JSON untuk ditampilkan ke antarmuka aplikasi android.

## 2. Domain dan Hosting Server

Hosting server dilakukan di Rumah Web, dengan mendaftarkan domain [www.railfencecipher.my.id](http://www.railfencecipher.my.id). Untuk melihat database dan file manager melalui hosting tersebut, tahapan dilakukan dengan cara :

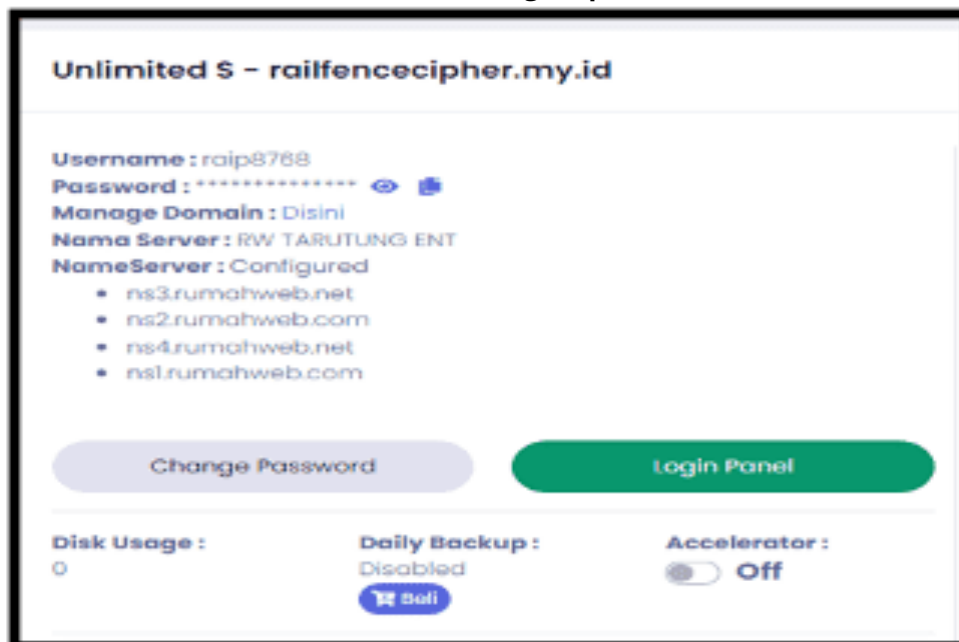
a) Membuka link <https://new.clientzone.rumahweb.com/login>, seperti terlihat pada Gambar 17.

**Gambar 17. Link Clientzonerumahweb.co**



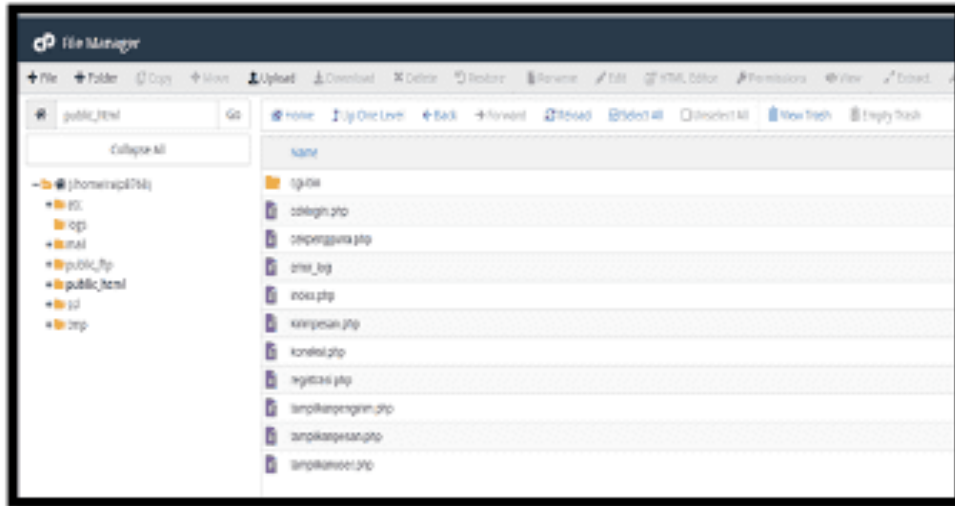
b) Setelah login, masuk ke cpanel dengan cara klik tombol login panel seperti terlihat pada Gambar 18.

**Gambar 18. Login Cpanel**



c) Melihat file manager dengan cara klik file manager, sehingga terlihat Gambar 19.

**Gambar 19. File Manager Aplikasi**



d) Untuk melihat database, dengan cara klik phpmyadmin, sehingga terlihat pada Gambar 19

**Gambar 20. Isi Tabel Pesan**

kdpesan	tglpesan	userkirim	userterima	isipesan
1	2023-06-05	zailani	diki	simtpg.aakbr? eaa ai p aana?
17	2023-06-05	diki	zailani	hi ah smknlaozial aa ea
18	2023-06-05	diki	zailani	simtrimeas ea.
19	2023-06-05	diky	raden	hloal
20	2023-06-05	yudha	diky	hlo al
21	2023-06-08	diki	zailani	tsat
22	2023-06-12		diki	ts
23	2023-06-12		diki	et.
24	2023-06-12		diki	
25	2023-06-12	diki	yudha	
26	2023-06-14		diki	
27	2023-06-14	real	diki	tsigats
28	2023-06-14	diki	real	pn ig
29	2023-06-15	diki	zailani	hi p aa aakbr?
30	2023-06-15	diki	zailani	tnua roiaetknpirts
31	2023-06-15	diki	zailani	tnua roiaetknpirts
32	2023-06-16	diki	zailani	TNUA ROIAETKNPIRTS

### Hasil Pengujian

Pengujian aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* dilakukan menggunakan Metode Black Box dengan mengidentifikasi fungsionalitas dari aplikasi melalui data yang benar dan data yang salah. Adapun hasil pengujian black box yang telah dilakukan, tampak pada tabel.1.

**Tabel 1. Hasil Pengujian** Blackbox

No.	Form Yang Diuji	Rencana Pengujian	Hasil Pengujian
1	Form Registrasi	Mengisi field pada data registrasi dan menyimpan data registrasi tersebut.	Sistem berhasil menyimpan data registrasi user ke dalam database aplikasi
2	Form Login	Memasukkan username dan password yang benar pada form login	Sistem berhasil menampilkan menu utama dari aplikasi

		Memasukkan username atau password yang salah pada form login	Sistem berhasil menolak akses login dengan menampilkan pesan kesalahan
3	Kirim Pesan	Melakukan pengiriman pesan teks dengan memilih penerima pesan dan mengisi pesan yang akan dikirim ke penerima	Sistem berhasil mengirim pesan kepada penerima
		Menjalankan web service JSON kirimpesan.php ketika pengirim pesan klik tombol "kirim pesan"	Sistem berhasil menjalankan web service JSON dan menyimpan data penerima dan isi pesan (dalam bentuk teracak) ke dalam database
4	Lihat Pesan	Melihat pesan-pesan yang masuk yang telah dikirim oleh setiap pengirim pesan	Sistem berhasil menampilkan list nama pengirim pesan di aplikasi
		Menjalankan web service JSON lihatpesan.php ketika penerima pesan membuka form lihat pesan	Sistem berhasil menjalankan web service JSON dan menampilkan informasi pesan yang dapat dibaca oleh penerima pesan
5	database pesan teks	Melihat database yang menyimpan pesan teks antara pengirim dan penerima pesan apakah berbentuk acak (cipherteks) atau berbentuk teks asli (plainteks)	Sistem berhasil menampilkan isi pesan teks dalam kondisi teracak (ciphertext) pada setiap record di database

## KESIMPULAN DAN SARAN

### Kesimpulan

1. Aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* dibuat menggunakan bahasa pemrograman *Java (Android Studio)*, bahasa pemrograman *PHP (File web Service JSON)* dan *database MySQL*.
2. Aplikasi ini terdapat *link url* untuk menyimpan file PHP dan data pesan di *database*, adapun *link url* tersebut <http://railfencecipher.my.id/>
3. Aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* telah di upload ke google playstore dengan memasukkan kata kunci *rail fence cipher*
4. Aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* ini dapat digunakan untuk membantu komunikasi antara kedua belah pihak baik pengirim dan penerima pesan. Selain itu pada aplikasi ini telah diterapkan algoritma *rail fence cipher* yang digunakan untuk menjaga kerahasiaan pesan tersebut yang disimpan di dalam database dari aplikasi.
5. Record pada kolom isi pesan di database dalam bentuk teracak, sehingga tidak dapat dibaca. Hal ini tentunya membuat aplikasi tersebut terjaga kerahasiaan pesan yang dikirim, karena terjadi proses pengacakan (enkripsi) pada pesan tersebut.
6. Berdasarkan hasil pengujian yang telah dilakukan, fungsional dari aplikasi kriptografi berbasis android menggunakan algoritma *rail fence cipher* berjalan dengan baik sesuai yang diharapkan dan pesan yang dikirim antara penerima dan pengirim terjaga kerahasiaan keamanan pesan tersebut karena sudah teracak.

## Saran

Berdasarkan penelitian yang penulis lakukan, maka penulis menyarankan agar dapat menggunakan aplikasi ini untuk dijadikan alternatif dalam bertukar informasi antara kedua belah pihak baik pengirim dan penerima pesan.

## DAFTAR PUSTAKA

- Alfajar, F. & Akbar, M., 2021. Implementasi Keamanan Chat Realtime Menggunakan Aes-Cbc Dan Base64. *Jisai Mercubuana Yogya*, Volume <https://jisai.mercubuana-yogya.ac.id/index.php/jisai/article/download/38/9>.
- Anggrawan, A., 2018. *Algoritma dan Pemrograman Implementasi Pada VB.Net dan Java*. Pertama penyunt. Yogyakarta: Andi Publisher.
- Ardi, 2020. Android dan Kriptografi Algoritma Rivest Code 6 Rekayasa Perangkat Lunak SMS (Short Messages Service). Medan: CV. Sentosa Deli Mandiri.
- Dewanta, F. & Nuha, H. H., 2021. *Pemrograman Java Untuk Aplikasi Berbasis Jaringan*. Malang: Ahlimedia Press.
- Efitra, 2021. *Belajar Dasar Pemrograman Java Via Smartphone Android*. Bogor: Guemedia Group.
- Girsang, N. D. et al., 2019. *Kombinasi Algoritma Kriptografi Transposisi Rail Fence Cipher dan Route Cipher*. Medan, Seminar Nasional Teknologi Informatika (Semantika) Vol. 2 No.1 ISBN : 978-602-50006-1-4.
- Hans, A. F., 2016. Sistem Informasi Perpustakaan Online Berbasis Web. *E-Journal Teknik Elektro dan Komputer*, Volume Vol.5 No.2 .
- <https://developer.android.com/studio/intro?hl=id>, 2022. *Mengenal Android Studio*. [Online] Available at: <https://developer.android.com/studio/intro?hl=id>
- Jamaludin & Romindo, 2020. *Kriptografi : Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA*. Medan: Yayasan Kita Menulis.
- Jannah, M., Sarwandi & Creative, C., 2019. *Mahir Bahasa Pemrograman PHP*. Jakarta: PT. Elex Media Komputindo.
- Latifah, R., Ambo, S. N. & Kurnia, S. I., 2017. *Modifikasi Algoritma Caesar Cipher dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus*. Jakarta, Seminar Nasional Sains dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta.
- Prabowo, R. & Pramusinto, W., 2018. Implementasi Kriptografi Dengan Algoritma Vigenere Cipher, AES 128 dan RC 4 Untuk Aplikasi Pesan Instan Berbasis Android. *Jurnal Skanika*, Volume Vol.1 No.3.
- Purba, D. F. & Puspasari, R., 2020. Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android. *Jurnal FTIK*, Volume Vol.1 No.1.
- Purnamasari, D., 2021. Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher Untuk Keamanan Data Teks Menggunakan Python. *Journal of Information Education*, Volume Vol.4 No.1.
- Ratna, D., 2018. Implementasi Algoritma Rail Fence Cipher Dalam Keamanan Data Gambar 2 Dimensi. *Jurnal Pelita Informatika*, Volume Vol.17. No. 3. ISSN : 2301-9425.
- Rosna, D., Johan & Imam, M., 2019. Aplikasi Kriptografi Dalam Mengamankan Pesan Teks Dengan Metode Algoritma RC4 Berbasis Android. *Jurnal Penelitian Teknik Informatika*, Volume Vol.3 No.1 e-ISSN:2431-2019.
- Safitri, L. & Basuki, S., 2020. Analisa dan Perancangan Sistem Informasi Text Chatting Berbasis Android Web View. *Jurnal Ipsikom*, Volume Vol.8 No.2 e-ISSN:2686-6382.

- Utomo, I. W., Latifah, R. & Risanty, R. D., 2020. Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher dan Vigenere Cipher. *Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, Volume Vol.9 No.2 e-ISSN:2598-3016.
- Yanti, N. R., Alimah & Ritonga, D. A., 2018. Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. *Jurnal Sains Komputer dan Informatika (J-Sakti)*, Volume Vol.2 No.1 e-ISSN:2549-7200.