Journal of Computer Science and Information Systems (JCoInS)
Program Studi Sistem Informasi, Fakultas Sains & Teknologi, Universitas Labuhanbatu
**Volume: 2, Nomor: 4, November 2021, Pages. 176-185**
**e-ISSN: 2747-2221**

# Perancangan Aplikasi Enkripsi Kata Menggunakan Algoritma *Playfair Cipher* Berbasis Web

**Muhammad Pristiwanto**

Manajemen Informatika, Fakultas Sains & Teknologi, Universitas Labuhanbatu

Email : muhammadpristiwanto@gmail.com

*Corresponding Author* : muhammadpristiwanto@gmail.com

***Abstract***

*In this day and age information/messages are not only sent by courier or traditionally but have been adapted to technological developments. One phenomenon that occurs because it involves internet technology in sending messages and exchanging data is the issue of wiretapping, counterfeiting and even theft of messages. Cryptography has a very important role in the era of digitalization which aims to secure information. Information that is privacy can be avoided from third persons and the information to be submitted can be protected. On the basis of this idea, it is necessary to create a medium or application that can be used to perform the encryption process and description of the message so that the message sent can be received by the recipient in a state of guaranteed legitimacy. This study uses the cryptographic algorithm Playfair Cipher. From the results of testing the application built, in the process of encryption and description, it can be proven to guarantee the security and confidentiality of messages.*

***Keywords : Perancangan Aplikasi Enkripsi Kata , Menggunakan Algoritma Playfair Cipher.***

## 1. Pendahuluan

Berkat perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran informasi. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan informasi atau dikenal dengan istilah Kriptografi.

Kriptografi merupakan salah satu cara untuk mengamankan informasi, yaitu dengan menyandikan pesan asli (*plaintext*) ke dalam bentuk pesan rahasia (*ciphertext*). Proses pengamanan ini melibatkan algoritma dan kunci. Kunci enkripsi dapat dengan mudah mengembalikan *plaintext* dari *ciphertext*.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkiripsi adalah proses mengubah pesan asli (*plaintext*) menjadi pesan yang disandikan (*ciphertext*) berdasarkan metode yang telah ditentukan yang mana proses enkripsi bekerja dengan kunci untuk mengkonversi *plaintext* ke dalam *ciphertext*.

Dekripsi adalah proses mengembalikan pesan yang disandikan (ciphertext) menjadi pesan asli (plaintext) sehingga informasi tersebut terjaga kerahasiaannya pada saat sampai ke tujuan yang mana proses dekripsi bekerja dalam urutan terbalik.

*Playfair Cipher* merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam polygram cipher, dimana *plaintext* diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut. Kunci kriptografinya adalah 25 buah huruf yang disusun di dalam bujursangkar 5x5 dengan menghilangkan huruf J dari abjad. Kemungkinan kuncinya adalah 25!. Pada umumnya, kunci yang digunakan adalah serangkaian kata yang mudah dimengerti. *Playfair cipher* memiliki mekanisme mengganti J dengan I.

## 2. Landasan Teori

Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto artinya rahasia dan graphia artinya tulisan (Ariyus, 2008). Kriptografi adalah Kriptografi adalah ilmu yang menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2006). Kriptografi visual merupakan sebuah teknik kriptografi yang memungkinkan informasi visual (gambar, teks, dll) yang di enkripsi sedemikian rupa sehingga dekripsi dapat dilakukan oleh sistem manual tanpa ada yang kompleks. Teknik kriptografi visual pertama kali di pelopori oleh Moni Naor dan Adi Shamir di Jakarta 1994 (Kunhu, 2016).

### Sejarah Kriptografi

Kriptografi memiliki sejarah yang menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu yang telah diperkenalkan oleh orang–orang Mesir dengan menggunakan hieroglyph yang merupakan jenis tulisan yang bukan bentuk standar untuk menulis pesan (Ariyus, 2008). Pada zaman Romawi kuno, dikisahkan tentang Julius Caesar yang ingin mengirimkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut dikirimkan melalui seorang kurir. Pesan tersebut mengandung sebuah rahasia, Julius Caesar tidak ingin pesannya terbuka di tengah jalan. Kemudian Julius Caesar memikirkan cara mengatasinya dengan mengacak pesan tersebut menjadi suatu pesanyang tidak dipahami oleh siapa pun terkecuali oleh jenderalnya saja. Sang jenderal diberi tahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut.

### Komponen Kriptografi

Menurut (Ariyus, 2008), kriptografi terdiri dari beberapa komponen dasar yaitu :

1. Enkripsi : Cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli disebut plaintext (text-biasa), yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi juga dapat diartikan sebagai cipher atau kode.
2. Dekripsi : Pesan yang telah dienkripsi dikembalikan ke bentuk awalnya. Algoritma yang digunakan untuk dekripsi berbeda dengan yang digunakan pada enkripsi. Dekripsi merupakan kebalikan dari enkripsi.

3. Kunci : Merupakan kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua jenis, yaitu kunci rahasia (private key) dan kunci umum(public key).
4. Ciphertext : Suatu pesan yang melalui proses dari enkripsi. Pesan yang ada pada teks-kode tidak dapat dibaca karena berupa karakter yang tidak mempunyai arti.
5. Plaintext : Sering disebut juga sebagai cleartext. Teks-asli atau teks-biasa ini merupakan pesan yang ditulis yang mempunyai makna atau arti. Teks asli ini yang diproses menggunakan algoritma kriptografi agar menjadi ciphertext (teks-kode).
6. Pesan : Merupakan data atau informasi yang dikirim melalui kurir, saluran komunikasi data, dsb) atau yang dapat disimpan di dalam media perekaman (kertas, storage, dsb).
7. Cryptanalysis : Merupakan analisis kode atau suatu ilmu untuk mendapatkan teksasli tanpa harus mengetahui kunci yang sah secara wajar. Analisis kode juga menemukan kelemahan dari algoritma kriptografi yang pada akhirnya dapat menemukan kunci atau teks-asli dari teks-kode yang dienkripsi dengan algoritma tertentu.

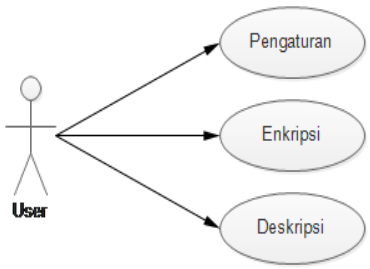
## 3. Metode Penelitian

Dalam pembuatan sistem alat bantu yang digunakan dalam membuat perancangan dan desain yaitu dengan menggunakan *Unified Modeling Language* (UML). *Unified Modelling Language* adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak.

## 4. Hasil dan Pembahasan

### *Use Case Diagram*

*Use Case* diagram adalah rangkaian atau uraian sekelompok yang saling terkait dan membentuk sistem secara teratur yang dilakukan atau diawasi oleh *actor*. *Use case* diagram dalam Perancangan Aplikasi Enkripsi Kata Menggunakan Algoritma *Playfair Cipher* yaitu:

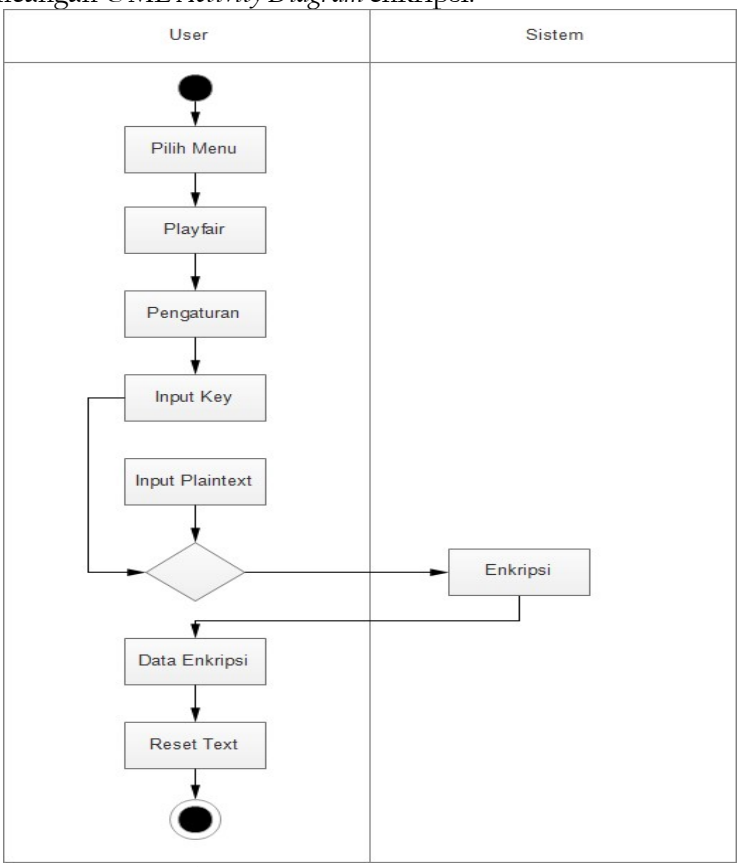



**Gambar 1. *Use Case* Diagram**

Pada gambar 1. *Use Case* Diagram menjelaskan aktivitas yang dapat dilakukan oleh user di sistem tersebut.

***Activity Diagram* Enkripsi**

Gambar perancangan UML *Activity Diagram* enkripsi.




**Gambar 2. *Activity Diagram* Enkripsi**

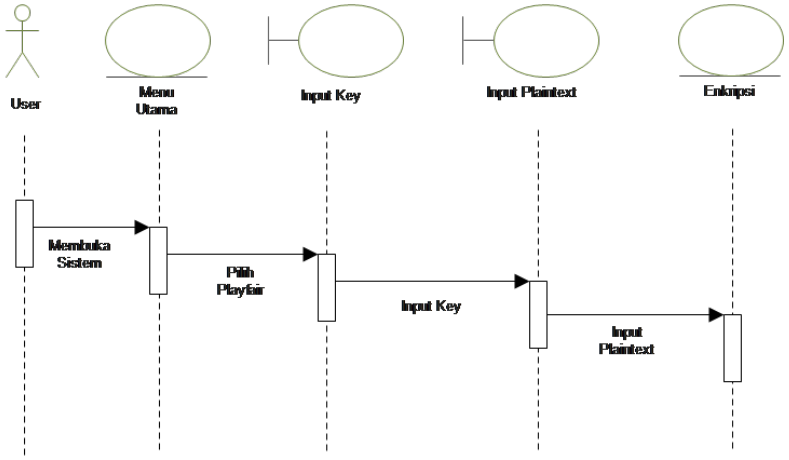
Pada Gambar 2 *Activity Diagram* Enkripsi menjelaskan bahwa :

1. *User* menjalankan sistem dan memilih menu *Playfair*.
2. Sebelum melakukan enkripsi, *user* mengubah pengaturan sesuai dengan keinginan dan memilih metode ENKRIPSI/DESKRIPSI.
3. *User* menginputkan *key*(kunci).
4. Kemudian user menginputkan *Plaintext*(teks) yang akan di enkripsi.
5. *User* akan mendapatkan hasil enkripsi dari sistem secara *realtime*(langsung).
6. Setelah mendapatkan hasil enkripsi, *user* dapat mereset/menghapus *plaintext* yang di inputkan dan hasil enkripsi.

**Squence Diagram**

Gambar Perancangan UML *Squence Diagram* enkripsi.

Journal of Computer Science and Information Systems (JCoInS)
Program Studi Sistem Informasi, Fakultas Sains & Teknologi, Universitas Labuhanbatu
Volume: 2, Nomor: 4, November 2021, Pages. 176-185
e-ISSN: 2747-2221

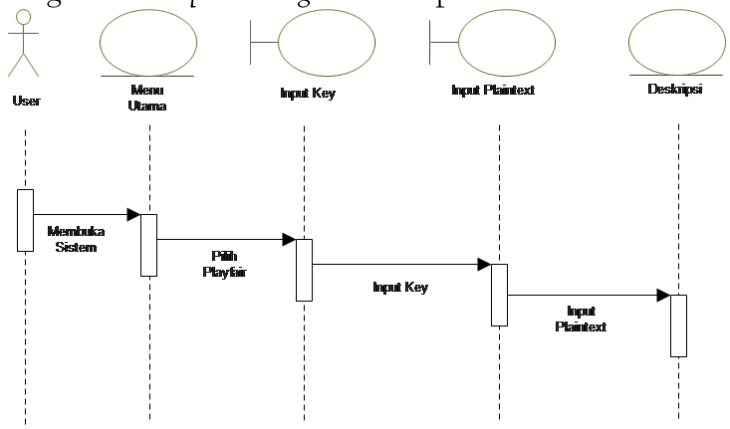



**Gambar 3. *Squence Diagram* enkripsi**

Pada gambar 3. *Squence Diagram* enkripsi menjelaskan bahwa :

1. *User* membuka sistem.
2. Setelah terbuka *user* memilih menu *Playfair*, dan mengatur/mengubah pengaturan sesuai dengan kebutuhan.
3. *User* menginputkan *KEY* dan memilih ENKRIPSI.
4. Kemudian *user* menginputkan *plaintext* untuk mendapatkan kalimat atau kata yang dienkripsi.

Gambar perancangan UML *Squence Diagram* deskripsi.



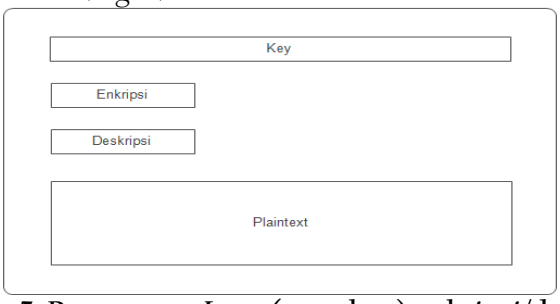

**Gambar 4. *Squence Diagram* deskripsi**

Pada gambar 4. *Squence Diagram* deskripsi menjelaskan bahwa :

1. *User* membuka sistem.
2. Setelah terbuka *user* memilih menu *Playfair*, dan mengatur/mengubah pengaturan sesuai dengan kebutuhan.
3. *User* menginputkan *KEY* dan memilih DESKRIPSI.
4. Kemudian *user* menginputkan *ciphertext* untuk mendapatkan kalimat atau kata yang dideskripsi.

**Rancangan *input*(masukan)**

Rancangan *input*(masukan) adalah rancangan sebuah form pengolahan pengaturan, *key* dan *plaintext* yang dimasukkan ke sistem kemudian di proses oleh sistem sehingga menghasilkan *output*(keluaran). Rancangan *input*(masukan) enkripsi/deskripsi adalah sebagai berikut :




**Gambar 5. Rancangan *Input*(masukan) enkripsi/deskripsi**

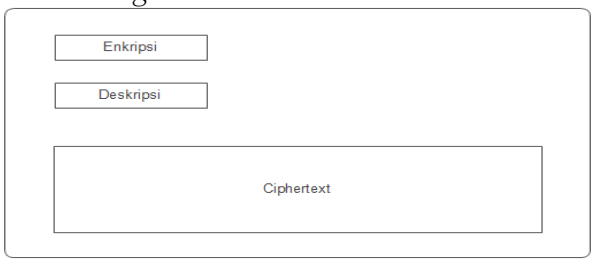
1. Nama Masukan : Form Enkripsi/Deskripsi
2. Fungsi : Untuk menginput Key enkripsi/deskripsi, plaintext
3. Distribusi : *User*
4. Keterangan : untuk enkripsi dan deskripsi

**Rancangan Proses**

Alat bantu yang digunakan dalam perancangan dan desain aplikasi enkripsi, adalah dengan menggunakan UML(*Unified Modelling Language*) adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak.

**Rancangan *Output*(keluaran)**

Rancangan *Output*(keluaran) dalam sistem adalah keluaran dari hasil proses yang dilakukan sistem. *Key* dan *Plaintext* yang diinputkan akan menghasilkan data keluaran berupa teks yang sudah menjadi *ciphertext*, begitu juga sebaliknya *ciphertext* dan *key* yang di *input*kan akan kembali menjadi *plaintext* pada form ini. Rancangan *output*(keluaran) enkripsi/deskripsi adalah sebagai berikut :

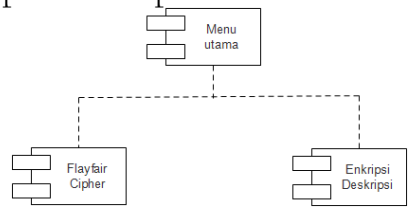



**Gambar 6. Rancangan *output*(keluaran) enkripsi/deskripsi**

1. Nama keluaran : Form Enkripsi/Deskripsi
2. Fungsi : Media hasil enkripsi/deskripsi
3. Distribusi : *User*
4. Keterangan : *Output* enkripsi dan deskripsi

**Rancangan *Interface***

Rancangan *Interface* aplikasi enkripsi




**Gambar 7. Rancangan *Componen Diagram* aplikasi enkripsi**

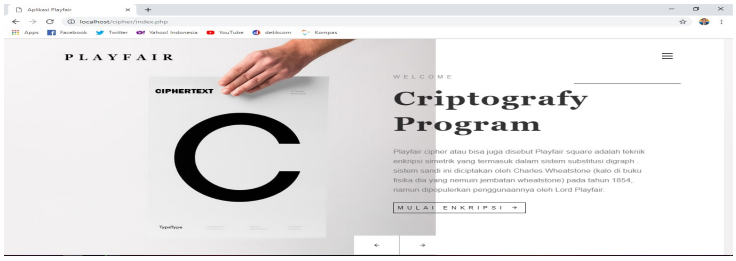
Pada gambar 7. Rancangan *Componen Diagram* aplikasi enkripsi menjelaskan rancangan pada sistem terdapat *form playfair cipher* dan *form* enkripsi/deskripsi.

**Analisa dan Riset**

Implementasi antarmuka dilakukan dengan setiap halaman aplikasi yang dibuat dan pengkodeannya dalam bentuk file program. Berikut ini adalah implementasi antarmuka yang dibuat.

**Halaman Utama**

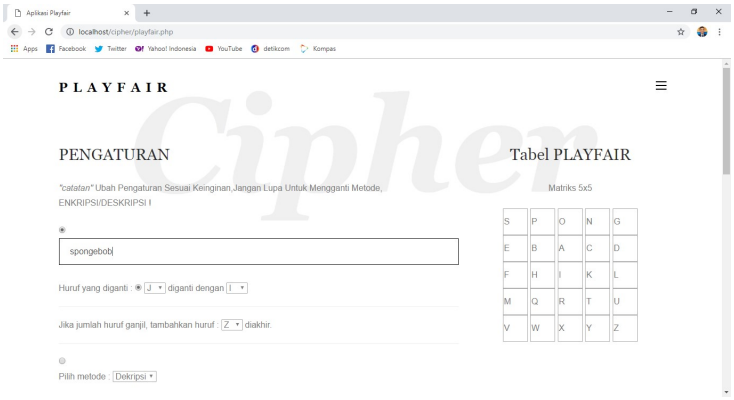
Halaman utama adalah halaman yang akan tampil pada awal aplikasi dibuka. Didalam halaman utama akan menampilkan sedikit tentang sejarah algoritma *Playfair* cipher.




**Gambar 8. Halaman Utama**

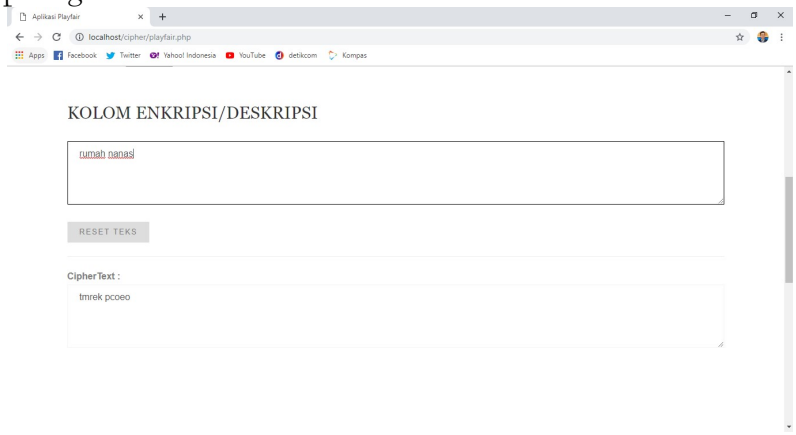
**Halaman Enkripsi/Deskripsi**

Halaman ini adalah tempat di mana kita menginputkan *key*(kata kunci), mengubah pengaturan sesuai dengan yang di butuhkan, memilih metode enkripsi/deskripsi, menginputkan *plaintext* kalimat/kata. Dihalaman ini juga terdapat tabel *Playfair* matrix 5x5 yang interaktif akan berubah sesuai dengan *key*(kata kunci) yang diinputkan.




**Gambar 9. Halaman Enkripsi/Deskripsi**

Dan setelah menginputkan key(kata kunci) "SPONGEBOB" dihalaman ini juga kita dapat menginputkan *plaintext* yang secara automatis akan langsung menghasilkan *chipertext* seperti gambar di bawah ini.




**Gambar 10. Halaman Ekripsi/Deskripsi**

Pada gambar 10 Halaman Enkripsi/deskripsi berisikan plaintext "RUMAH NANAS" yang secara automatis menghasilkan ciphertext "TMREK PCOEO" dan pada gambar tersebut terdapat sebuah tombol "RESET TEKS" yang berfungsi untuk mereset/menghapus *plaintext* dan *ciphertext.*

**Pengujian Fungsional**

Pengujian alpha dilakukan dengan menggunakan metode black box. Untuk pengujian alpha ini yaitu pada pengujian sebagai pengguna.

**Tabel 1. Skenario Pengujian**

| Uji Fitur | Detail Pengujian | Jenis Pengujian |
|---|---|---|
| ipsi | genkripsi kalimat/kata | *box* |
| ripsi | deskripsi kalimat/kata | *box* |

**Kasus dan Hasil Pengujian**

Berikut ini adalah hasil dari pengujian fungsional dari aplikasi:

**Tabel 2. Pengujian Enkripsi dan Deskripsi**

| Data Masukan | ang Diharapkan | Pengamatan | Kesimpulan |
|---|---|---|---|
| genkripsi kalimat<br>oh :<br>*text* : RUMAH<br>AS | ghasilkan<br>ertext "TMREK<br>EO" | m memproses<br>*text* dan<br>ghasilkan *Ciphertext* | rima |
| deskripsi kalimat<br>oh :<br>*rtext* : TMREK<br>EO | gembalikan<br>text "RUMAH<br>AS | m memproses<br>*rtext* dan<br>gembalikan *Plaintext* | rima |

## 5. Kesimpulan dan Saran

**Kesimpulan**

Pengujian alpha dilakukan dengan menggunakan metode black box. merupakan pengujian sistem yang bertujuan untuk menemukan kesalahan kesalahan atau kekurangan pada perangkat lunak yang diuji. Dalam pengujian disini masih dalam tahapan pengujian yang sebatas pengujian secara fungsionalitas saja. Perihal yang tidak diinginkan dapat terjadi tanpa pengujian secara spesifik terutama pada bagian interface dimana pemograman kemampuan dinamis elemen antarmuka berbaur menggunakan *Hyper Text Markup Language* (HTML) serta penyajian dokumen dengan *Cassading Style Sheet* (CSS). Sehingga dalam menjalankan sistem sebagai aplikasi berbasis web tentunya berpengaruh pada web browser untuk menjalankan sistem sebagai aplikasi berbasis web.

**Saran**

Hasil perancangan aplikasi kriptografi dengan metode *Playfair* Cipher berbasis web dapat disimpulkan bahwa proses enkripsi dan deskripsi kata atau kalimat dapat dilakukan secara komputasi sehingga tidak perlu menjabarkan proses enkripsi dan dekripsi secara manual yang dapat membuang-buang waktu, dengan kata lain aplikasi ini untuk mengefisiensikan waktu untuk proses enkrpsi dan dekripsi. Selain itu, dipilihnya metode *Playfair* cipher karena metode ini dikenal mudah dipahami dan mudah diimplementasikan.

## 6. Daftar Pustaka

A. M. Hasibuan, "Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone," MEANS (Media Inf. Anal. dan Sist., vol. 2, no. 1, pp. 29–35, Jun. 2017.

A. M. Mhd. Zulfansyuri Siambaton, "Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks," J. Ilmu Komput. dan Inform., vol. 02, no. April, pp. 66–71, 2018.

D. Ariyus, "Kriptografi keamanan data dan komunikasi," Yogyakarta Graha Ilmu,

D. D. Santoso and P. Tarigan, "Penerapan Algoritma Playfair Cipher sebagai Penyandian Kunci Dalam Pengamanan File Teks dengan Algoritma Rijndael," Pelita

Inform. Budi Darma, vol. 17, pp. 59–64, 2018.

H. D. M. H. Hutahaean, "Aplikasi Pembelajaran Kriptograpi berbasis Mobile menggunakan Computer Assisted Instruction," vol. 4, no. 1, pp. 2–5, 2019.

https://www.ssh.com/cryptography. [Accessed: 14-Dec-2019].

R. Munir, "Kriptografi," Inform. Bandung, 2006.

T. Limbong et al., "The implementation of computer based instruction model on Gost Algorithm Cryptography Learning," in IOP Conference Series: Materials Science and Engineering, 2018, vol. 420, no. 1, p. 12094.

Www.ssh.com, "Cryptography for Practitioners," 2019. [Online]. Available: