SKRIPSI

STEGANOGRAFI CITRA MENGGUNAKAN KRIPTOGRAFI *HYBRID PLAYFAIR CIPHER* DAN *CAESAR CIPHER*

NURUL FITRIANI ANDI MU'MI

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PEGETAHUAN ALAM
UNIVERSITAS NEGERI MAKASSAR

2017

SKRIPSI

STEGANOGRAFI CITRA MENGGUNAKAN KRIPTOGRAFI*HYBRID PLAYFAIR CIPHER* DAN *CAESAR CIPHER*

Diajukan kepada Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Negeri Makassar untuk memenuhi persyaratan guna memperoleh gelar Sarjana Sains Matematika

NURUL FITRIANI ANDI MU'MI
(1311142011)

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PEGETAHUAN ALAM
UNIVERSITAS NEGERI MAKASSAR

2017

PERNYATAAN KEASLIAN

Saya bertanda tangan di bawah ini menyatakan bahwa skripsi ini adalah hasil karya sendiri, dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar. Bila dikemudian hari ternyata pernyataan saya terbukti tidak benar, maka saya bersedia menerima sanksi yang telah ditetapkan oleh FMIPA UNM Makassar.

Yang membuat pernyataan

Nama : Nurul Fitriani Andi Mu'mi

NIM : 1311142011

Tanggal : Juli 2017

PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIK

Sebagai civitas akademi Universitas Negeri Makassar, saya bertanda tangan di bawah ini:

Nama	: Nurul Fitriani Andi Mu'mi
Nim	: 1311142011
Program Studi	: Matematika
Jurusan	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

Demi kepentingan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Negeri Makassar **Hak Bebas Royalti Noneksklusif** ***(Non-exclusive Royalti-Free Right)*** atas skripsi saya yang berjudul : ***Steganografi Citra Menggunakan Hybrid Kriptografi Playfair Cipher dan Caesar Cipher*** beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Negeri Makassar berhak menyimpan, mengalih media/formatkan, mengelolah dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Makassar

Pada tanggal : Juli 2017

Menyetujui

Pembimbing I

Yang menyatakan

H. Sukarna, S.Pd., M.Si.
NIP. 19730313 200003 1 001

Nurul Fitriani Andi Mu'mi
NIM.1311142011

MUTIARA HIKMAH DAN PERSEMBAHAN

Kegagalan merupakan kesempatan untuk memulai kembali, dengan lebih cerdas ~ Henry Ford

Sesungguhnya bersama kesulitan pasti ada kemudahan. Maka apabila engkau telah selesai (dari sesuatu urusan), tetaplah bekerja keras (untuk urusan yang lain) ~ QS. 94 : 6-7

Karya sederhana ini kupersembahkan untuk :

Ayahku Tahir Mulyadi dan Ibuku Marliyah atas semua doa, cinta, dan kasih sayangnya yang tidak dapat terbalaskan dengan apapun. Ayah dan ibu, besar harapanmu untuk kebahagiaan dan kesuksekan kami, dengan ini aku persembahkan karya sederhana ini sebagai tanda telah melalui satu tahap perjalanan panjang ini.

Terima kasih atas segalanaya.

Saudaraku Rachmat Irawan Wara A.M., Tenri Abeng A.M., dan Muh. Faturrahman Sidiq atas semua perhatian dan kasih sayang serta candaan dan dorongan selama ini.

Terima kasih.

ABSTRAK

NURUL FITRIANI ANDI MU'MI, 2017. Steganografi Citra Menggunakan Kriptografi *Hybrid Playfair Cipher* dan *Caesar Cipher*. **Skripsi** Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Makassar (dibimbing oleh H. Sukarna dan H. Rahmat Syam).

Penelitian ini merupakan penelitian terapan di bidang komputasi berkaitan dengan kriptografi *playfair cipher* dan *caesar cipher* serta steganografi, bertujuan untuk mengetahui konsep matematis kriptografi *Hybrid playfair cipher* dan *caesar cipher* serta steganografi pada penyisipan pesan. Metode *playfair cipher* digunakan pada proses enkripsi dilanjutkan dengan *metode caesar cipher*. Hasil enkripsi dari gabungan kedua metode disisipkan pada citra (proses *embedding*). Simulasi Penyisipan Pesan yang telah dienkripsi disimulasikan dengan MATLAB sebagai alat bantu komputasi. Citra hasil simulasi disimpan dengan format bitmap (.bmp). Adapun bentuk matematika proses enkripsi pesan menggunakan *hybrid playfair cipher* dan *caesar cipher* yaitu $E(E(P,K1),K2) = C$, proses dekripsi yaitu $D(D(C,K2),K1) = P$ dan proses steganografi citra yaitu $M(K2(K1(P,K1),K2),G) = S$. Hasil penelitian ini menunjukkan bahwa dengan menggunakan gabungan metode kriptografi *playfair cipher* dan *caesar cipher* dalam penyandian, pesan yang disandikan semakin sulit dikembalikan ke pesan asal oleh pihak yang tidak berwenang. Dengan menyisipkannya ke dalam citra membuat pengamat tidak menyadari adanya informasi yang disisipkan pada citra yang berperan sebagai pesan.

Kata Kunci : *Kriptografi, Playfair, Caesar, Cipher, Steganografi*

ABSTRACT

NURUL FITRIANI ANDI MU'MI, 2017. Image Steganography Using *Hybrid Cryptography* of *Playfair Cipher* and *Caesar Cipher*. **Thesis.** Department of Mathematics, Faculty of Mathematics and Natural Sciences. State University of Makassar (guided by H. Sukarna and H. Rahmat Syam).

This research is an applied research in the field of computation related to playfair cipher cryptography, caesar cipher cryptography and steganography, aims to find out the mathematical concepts of Image Steganography using Hybrid Cryptography of Playfair Cipher and Caesar Cipher. The playfair cipher method is used in the encryption process then followed by the caesar cipher method. Encryption results from the combination of both methods are inserted to the image (embedding process). The simulation of the encrypted steganography uses MATLAB as the computational tool. The image of the simulation result is stored with bitmap (.bmp) format. Mathematical form of the message encryption process using hybrid playfair cipher and caesar cipher is $E(E(P,K1),K2) = C$, decryption process is $D(D(C,K2),K1) = P$ and image steganography process is $M(K2(K1(P,K1),K2),G) = S$. Based on the results of this research, found that by using the combination of cryptography method of playfair cipher and caesar cipher in encoding will cause the encoded will be harder to return to the original message by unauthorized party and by inserting the encoded message into an image will make observer not aware of the existence of the inserted information on an image that has a role as message.

Keyword : *Cryptography, Playfair, Caesar, Cipher, Steganography*

KATA PENGANTAR

Assalamu ‘Alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirobbil ‘alamin, segala puji syukur kehadirat Allah SWT, atas berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul "***Steganografi Citra Menggunakan Kriptografi Hybrid Playfair Cipher dan Caesar Cipher***", sebagai salah satu syarat menyelesaikan studi di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Makassar. Shalawat serta salam semoga senantiasa tercurahkan kepada nabi besa Muhammad SAW sebagai *uswatun hasanah* dalam meraih kesuksesan dunia akhirat.

Terima kasih yang tak terhingga penulis hanturkan kepada Ayahanda Tahir Mulyadi dan Ibunda Marliyah atas segala doa, kasih sayang, cinta, nasihat, motivasi, serta berbagai macam bantuan, baik secara moril maupun materil. Terima kasih atas bimbingan serta ketulusan dalam merawat penulis dari lahir hingga sekarang. Dan tak lupa terima kasih kepada kakak dan adik-adik serta keluarga atas segala dorongan dan bantuannya selama ini. Semoga Allah membalas semua kebaikannya dengan pahala yang berlipat ganda.

Iringan doa dan ucapan terima kaih yang sebesar-besarnya penulis sampaikan, terutama kepada :

1. Bapak Prof. Dr. H. Husain Syam, M.TP. selaku Rektor Universitas Negeri Makassar

2. Bapak Prof. Dr. Abdul Rahman, M.Pd., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas negeri Makassar.
3. Bapak Dr. Awi, M.Si., selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Makassar.
4. Ibu Wahida Sanusi, S.Si., M.Si., Ph.D., selaku Ketua Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas negeri Makassar.
5. Bapak H. Sukarna, S.Pd., M.Si., selaku pembimbing I dan H. Rahmat Syam, S.T., M.Kom., selaku pembimbing II atas segala bimbingan dan arahan yang diberikan kepada penulis dalam menyelesaikan skripsi ini.
6. Ibu Wahida Sanusi, S.Si., M.Si., Ph.D., selaku penguji I dan Bapak Sulaiman, S.Si., M.Kom., M.M., selaku Penguji II atas segala saran dan arahan yang diberikan kepada penulis dalam menyelesaikan skripsi ini.
7. Bapak/Ibu dosen Matematika FMIPA UNM yang telah menyalurkan ilmunya secara ikhlas serta mendidik penulis. Semoga apa yang diberikan senantiasa menjadi amal jariyah.
8. Muh. Raid Salman T., S.Si. terimakasih atas bantuannya kepada penulis dalam menyelesaikan skripsi ini.
9. Saudara dan sahabat yang selalu mendukung, menolong, dan mengingatkan dalam segala hal Rahmah, Ica, Pute, Wati, Dilla, Ririn, Raid, Edy, Qadri, Meisy, Yanti, Wawan, dan Wakia. Terimakasih atas semua kebersamaan dan dukungan selama ini.

10. Teman-Teman, kakak-kakak dan adik-adik asisten Rahmah, Ica, Pute, Wati, Hilma, Edy, Raid, Kak Ayu, Kak Widya, Kak Lina, Kak Wana, Rahmat, Indah, Agusriani, Rifki, Ade, Astri, dan Amni yang selalu mendoakan.
11. Teman-teman seperjuangan Program Studi Matematika Angkatan 2013 Meisi, Diki, Ketrin, Rahmah, Taslim, Aswar, Amma, Pute, Ayu, Rahmat, Dia, Eni, Anti, Ody, Ida, Edy, Hikmah, Yanti, Imam, Arif, April, Sukma, Erna, Izki, Raid, Nasra, Dayat, Gusman, Ica, Qadri, Gita, Mimin, Ilham, Eka, Sella, Wakia, Dilla, Wawan, Selvi, Faisah, Noni, Anto, dan Wati.

Serta orang-orang yang telah berjasa kepada penulis yang tidak dapat dituliskan oleh penulis. Penulis berharap semoga bantuan yang telah diberikan mendapatkan balasan dari Allah, sebagai amal jariyah dan pahala yang berlipat ganda di sisi-Nya.

Akhirnya, semoga skripsi ini dapat bermanfaat bagi segenap pembaca.

Wassalamu 'alaikum warahmatullahi wabarakatuh.

Makassar, Juli 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

Kriptografi	:	Ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim ke suatu tempat ke tempat lain.
Steganografi	:	Ilmu seni dalam menyembunyikan informasi dengan memasukkan informasi atau pesan tersebut ke dalam media lain.
Kriptografi Kunci Simetri	:	Kunci yang proses enkripsi dan dekripsi menggunakan kunci yang sama yang bersifat rahasia dan hanya boleh diketahui oleh pengirim dan penerima pesan. Kunci simetri biasa juga disebut dengan kunci privat.
Kriptografi Kunci Asimetri	:	Kunci yang proses enkripsi dan dekripsinya menggunakan kunci yang berbeda yaitu kunci publik dan kunci privat.
Plaintext	:	Pesan, data ataupun suatu informasi yang dapat dibaca dan maknanya dapat dimengerti.
Ciphertext	:	Suatu bentuk pesan yang tersandikan, sehingga maknanya tidak dapat dimengerti.
Enkripsi	:	Proses menyandikan *plaintext* menjadi *ciphertext*.
Dekripsi	:	Proses mengembalikan *ciphertext* menjadi *plaintext* atau pesan asal.
Playfair cipher	:	Salah satu metode kriptografi yang menggunakan matriks kunci untuk nelakukan proses enkripsi.

Caesar cipher	:	Salah satu metode kriptografi yang menggunakan kunci pergeseran untuk melakukan proses enkripsi.
Embedding	:	Proses penyisipan pesan pada media yang ditentukan
Ekstraksi	:	Proses mengeluarkan pesan yang disembunyikan dalam sebuah media.
LSB	:	Salah satu metode steganografi. Cara penyisipan pesannya yaitu dengan mengganti nilai bit terakhir gambar dengan bit pesan yang akan disisipkan.
Cover Image	:	Media yang digunakan untuk menyisipkan pesan.
Stego Image	:	Hasil dari proses penyisipan pesan atau proses *embedding*.
Key	:	Parameter yang digunakan untuk mentransformasikan proses penenkripsian dan pendekripsian pesan.
Citra	:	Gambar pada bidang dua dimensi. Pada penelitian ini citra digunakan sebagai media penyisipan pesan.

DAFTAR SIMBOL

E : Proses enkripsi

D : Proses dekripsi

P : *Plaintext*

C : *Ciphertext*

$C1$: *Ciphertext1*

G : *Cover image*

S : *Stego image*

K : Proses ekstraksi

$K1$: Kunci1 (kunci yang digunakan pada *playfair cipher*

$K2$: Kunci2 (kunci yang digunakan pada *caesar cipher*)

> : Lebih dari

< : Kurang dari

BAB I

PENDAHULUAN

A. Latar Belakang

Keamanan dalam proses pengiriman pesan sangatlah penting. Pesan merupakan pernyataan rahasia yang dibuat oleh seseorang dan ditujukan kepada orang lain yang dikehendaki. Sangat pentingnya nilai informasi dari sebuah pesan menyebabkan seringkali pesan yang ingin disampaikan tidak sampai kepada penerima, melainkan jatuh ke tangan orang lain yang tidak diinginkan. Untuk mengatasi masalah keamanan informasi, salah satu solusinya adalah diterapkan ilmu kriptografi.

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti rahasia (*secret*) dan *graphia* berarti tulisan (*writing*). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Pradipta, 2016). Pesan yang dirahasiakan dinamakan *plaintext*, sedangkan pesan hasil penyandian disebut *ciphertext*. Proses penyandian *plaintext* menjadi *ciphertext* disebut enkripsi dan proses membalikkan *ciphertext* menjadi *plaintext* asalnya disebut dekripsi.

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *cryptology*, bertujuan menjaga kerahasiaan informasi yang terkandung dalam data agar informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Oleh karena itu kriptografi dikatakan sebagai metode yang tangguh dalam menjaga

kerahasiaan informasi karena dalam kriptogafi data yang dikirimkan melalui jaringan akan disamarkan sedemikianrupa menggunakan algoritma sandi. Data tetap aman kendati setiap orang dapat mengaksesnya secara bebas. Sehingga kalaupun data tersebut dapat dibaca, maka tidak dapat dipahami oleh pihak yang tidak berhak (Setyaningsih, 2009). Terdapat dua teknik dalam kriptografi yang digunakan untuk penyandian teks yaitu kriptografi klasik (kriptografi simetri) dan kriptografi modern (kriptografi asimetri).

Kriptografi simetri disebut juga kriptografi kunci pribadi karena kunci enkripsi dan kunci dekripsinya sama dan harus dirahasiakan. Kriptografi asimetri disebut juga kriptografi kunci publik karena kunci enkripsi dan kunci dekripsinya berbeda, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Terdapat beberapa metode penyandian yang digunakan di kriptografi simetri, dintaranya adalah *Playfair cipher* dan *caesar cipher*.

Playfair cipher digunakan oleh tentara Inggris pada saat Perang Boer II dan Perang Dunia I. Ditemukan pertama kali oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tanggal 26 Maret 1854. *Playfair* merupakan *digraphs cipher*, artinya setiap proses enkripsi dilakukan pada setiap dua huruf atau pasangan huruf (Santi, 2010).

Caesar cipher merupakan teknik enkripsi substitusi yang pertama kali dikenal dan paling sederhana ditemukan oleh Julius Caesar (Siambaton, 2016). *Caesar cipher* termasuk sandi substitusi, di mana setiap huruf pada *plaintext* digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet (Seftyanto, dkk., 2012).

Pesan rahasia yang berupa pesan acak dari hasil enkripsi menggunakan salah satu metode pada kriptografi ini yaitu *Playfair cipher* dan *caesar cipher*, dapat menimbulkan kecurigaan karena pesan acak tidak memiliki makna secara kasat mata, sehingga mudah dicurigai. Untuk mengatasi masalah ini digunakan teknik penyembunyian pesan yaitu dengan steganografi.

Steganografi merupakan suatu ilmu seni dalam menyembunyikan informasi dengan memasukkan informasi atau pesan tersebut ke dalam media lain. Sehingga keberadaan informasi tersebut tidak diketahui oleh orang lain (Cahyadi, 2012). Media yang dapat dimanfaatkan untuk steganografi yaitu citra digital, teks, video, dan audio.

Secara matematis, citra merupakan fungsi kontinu dengan intensitas cahaya pada bidang dua dimensi (Kusumanto dan Tompunu, 2011). Citra digital merupakan media steganografi yang banyak digunakan untuk menyisipkan pesan. Penyisipan pesan kedalam citra dapat menggunakan beberapa metode dalam steganografi, salah satunya menggunakan metode *Least Significant* Bit (LSB). Metode *Least Significant Bit* merupakan metode yang sederhana dan banyak digunakan diantara metode steganografi lainnya.

Beberapa penelitian sebelumnya yang berkaitan yaitu Wardani (2013) Pemecahan Sandi Kriptografi dengan Menggabungkan Metode *Hill Cipher* dan *Caesar Cipher*. Husein (2014) Implementasi *Caesar Cipher* untuk Penyembunyian Pesan Teks Rahasia pada Citra dengan Menggunakan Metode *Least Significant Bit*. Setiawan, dkk. (2012) Aplikasi Keamanan Pesan Menggunakan Algoritma

Steganografi dan Kriptografi. Choudhary, dkk. (2013) *A Generalized Version of Playfair Cipher*.

Berdasarkan uraian di atas, akan dikaji lebih lanjut tentang kripografi dan steganografi dengan topik ***"Steganografi Citra Menggunakan Kriptografi Hybrid Playfair Cipher dan Caesar Cipher"***.

B. Rumusan Masalah

Bedasarkan latar belakang maka dapat dibuat rumusan masalah sebagai berikut.

1. Bagaimana proses enkripsi dan dekripsi pesan secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher*?
2. Bagaimana proses penyisipan pesan pada citra secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher*?
3. Bagaimana simulasi program penyisipan pesan pada citra menggunakan MATLAB?

C. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut.

1. Untuk mengetahui proses enkripsi dan dekripsi pesan secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher*.
2. Untuk mengetahui proses penyisipan pesan pada citra secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher*.
3. Untuk mengetahui hasil simulasi program penyisipan pesan pada citra menggunakan MATLAB.

D. Batasan Masalah

Penelitian ini membahas mengenai penyisipan pesan menggunakan *hybrid playfair cipher* dan *Caesar cipher*. Untuk memberikan ruang lingkup yang jelas terhadap penelitian yang dilakukan, maka dibuat batasan yaitu:

1. Jenis *plaintext* yang digunakan berupa karakter dalam bentuk huruf kapital A-Z, angka 1-9, dan tanda spasi.
2. Panjang pesan yaitu kurang dari atau sama dengan jumlah kolom matriks citra.
3. Ukuran baris citra minimal 8 *pixel*.
4. Citra yang disisipkan pesan yaitu citra Red dari citra RGB.
5. Citra yang telah disisipkan pesan disimpan dalam bentuk bitmap (bmp.)

E. Manfaat Penelitian

Manfaat dari penelitian ini dapat diuraikan sebagai berikut:

1. Bagi penulis

   Untuk menambah pengetahuan dalam mengkaji permasalahan yang berkaitan dengan keilmuan lain seperti komputasi matematika, khususnya penyisipan pesan pada citra menggunakan *hybrid playfair cipher* dan *caesar cipher*s dengan bantuan program MATLAB, serta permasalahan matematika dalam menyelesaikan masalah tersebut.

2. Bagi mahasiswa matematika

   Sebagai referensi untuk mengetahui tentang kriptografi dan steganografi secara matematis, dan teknik penyisipan pesan pada citra dengan bantuan MATLAB.

BAB II

KAJIAN PUSTAKA

A. Kriptografi

1. Pengertian Kriptografi

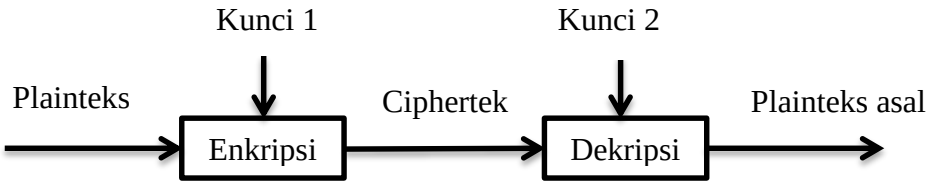
Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas (Sadikin, 2012:9).

Kriptografi berasal dari bahasa Yunani "*cryptos*" artinya rahasia (*secret*), sedangakan "*graphein*" artinya tulisan rahasia (*writing*). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti maknanya. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih sekedar *privacy*, tetapi juga untuk tujuan data *integrity*, *autentication*, dan *non-repudiation* (Arif dan Fanani, 2016).

Beberapa definisi mengenai kriptografi menurut Zuli dan Irawan (2014).

1. Kriptografi adalah cabang matematika yang menyediakan teknik untuk memungkinkan informasi rahasia yang akan dikirim melalui jaringan publik.
2. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan.
3. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas, data, serta otentikasi.

Menurut Munir (2010:203) Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. Pesan yang dirahasiakan dinamakan plainteks, sedangkan pesan hasil penyandian disebut cipherteks. Proses penyandian plainteks menjadi cipherteks disebut enkripsi dan proses membalikkan cipherteks menjadi plainteks asalnya disebut dekripsi. Gambar 2.1 memperlihatkan diagram kedua proses yang dimaksud (Munir, 2010:203).



Gambar 2.1 Proses Enkripsi dan Dekripsi Pesan

Berdasarkan Gambar 2.1, jika kunci 1 sama dengan kunci 2, maka sistem kriptografinya dinamakan sistem kriptografi kunci simetri. Sebaliknya, jika kunci 1 tidak sama dengan kunci 2 sistem kriptografinya dinamakan sistem kriptografi asimetri.

Kriptografi simetri disebut juga kriptografi kunci pribadi karena kunci enkripsi dan kunci dekripsinya sama dan harus dirahasiakan. Kriptografi asimetri

disebut juga kriptografi kunci publik karena kunci enkripsi dan kunci dekripsinya berbeda, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi (Munir, 2010).

2. Sejarah Kriptografi

Menurut sejarahnya, kriptografi sudah lama digunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang disebut *scytale*. *Scytle* terdiri dari sebuah pita panjang dari daun papyrus yang dililitkan pada sebatang silinder. Pesan yang akan dikirim ditulis secara horizontal. Jika pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia. Untuk membaca pesan, penerima melilitkan kembali silinder yang diameternya sama dengan diameter silinder pengirim. Teknik kriptografi ini dikenal dengan nama transposisi cipher (Munir, 2010:205).

3. Terminologi Kriptografi

Beberapa istilah (terminologi) dalam keriptografi dapat dijelaskan sebagai berikut (Munir dalam Susilowati, 2016)).

a. *Plaintext*: pesan, data ataupun suatu informasi yang dapat dibaca dan maknanya dapat dimengerti.
b. *Ciphertext*: suatu bentuk pesan yang tersandikan, sehingga maknanya tidak dapat dimengerti.
c. Pengirim: entitas yang mengirim pesan kepada entitas penerima.
d. Penerima: entitas yang menerima pesan dari entitas pengirim.

e. Media komunikasi data: media tempat lalu lintas data atas informasi pada proses pengiriman dan penerimaan data/informasi.
f. Enkripsi: proses untuk menyandikan *plaintext* menjadi *ciphertext*.
g. Dekripsi: proses pengurai sandi dari *ciphertext* menjadi *plaintext*.
h. Kunci (*key*): parameter yang digunakan untuk mentransformasi proses pengenkripsian dan pendekripsian pesan..
i. Kunci simetri: kunci yang proses enkripsi dan dekripsi menggunakan kunci yang sama yang bersifat rahasia dan hanya boleh diketahui oleh pengirim dan penerima pesan. Kunci simetri biasa juga disebut dengan kunci privat.
j. Kunci asimetri: kunci yang proses enkripsi dan dekripsinya menggunakan kunci yang berbeda yaitu kunci publik dan kunci privat.

4. Algoritma Kriptografi

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, algoritma kunci kriptografi dapat dibedakan menjadi 2 bagian, yaitu algoritma kriptografi kunci simetri dan algoritma kriptografi kunci asimetri (Susilowati, 2016).

a. Algoritma Kriptografi Kunci Simetri

Algoritma kriptografi kunci simetri disebut dengan algoritma kriptografi klasik, algoritma kriptografi kunci rahasia, algoritma kriptografi kunci privat atau algoritma kriptogrfi konvensional. Hal tersebut dikarenakan kunci yang digunakan sama pada proses enkripsi dan dekripsi pesan. Keamanan menggunakan sistem ini terletak pada kerahasiaan kunci yang digunakan.

Contoh algoritma kunci simetri yaitu transformasi, hill, *caesar, playfair,* dan sebagainya.

b. Algoritma Kriptografi Kunci Asimetri

Algoritma kriptografi kunci asimetri disebut algoritma kunci publik, sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun. Sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan. Pada kriptografi jenis ini, setiap orang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Contoh algoritma kriptografi kunci publik diantaranya RSA, ElGamal, DSA, dan sebagainya.

5. Tujuan Kriptografi

Menurut Santi (2010) ada empat tujuan mendasar dari kriptografi yang menerapkan aspek keamanan informasi, yaitu:

1. Kerahasiaan

   Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.

2. Integritas Data

   Berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pendistribusian data lein ke dalam data yang asli.

3. Otentifikasi

   Berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diotentikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.

4. Non-repudiasi

   Non-repudiasi merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengirim atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

B. Notasi Matematis pada Kriptografi

Jika cipherteks dilambangkan dengan *C* dan plainteks dilambangkan dengan *P*, maka fungsi enkripsi *E* memetakan *P* ke *C*, sebagaimana pada persamaan (2.1).

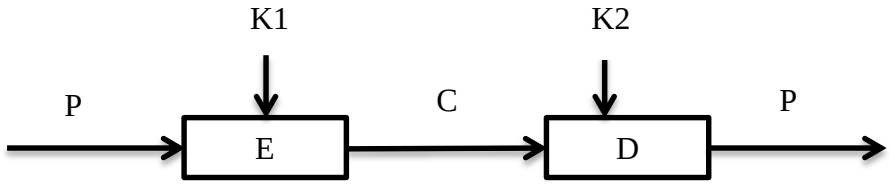
$$E(P) = C \tag{2.1}$$

Proses kebalikannya, fungsi dekripsi *D* memetakan *C* ke *P*, sebagaimana pada persamaan (2.2).

$$D(C) = P \tag{2.2}$$

Atau dengan kata lain, *D* adalah fungsi inversi dari *E*, atau $D = E^{-1}$ (Munir, 2010:206).

Bentuk matematika proses enkripsi dan dekripsi kriptografi secara umum ditunjukkan pada Gambar 2.2.



Keterangan:

E	:	Proses enkripsi pesan (*plaintext*)
P	:	*Plaintext*
C	:	*Ciphertext*
D	:	Proses dekripsi *ciphertext*
K1	:	Kunci 1
K2	:	Kunci 2

Gambar 2.2 Proses Enkripsi dan Dekripsi Secara Matematis

Berdasarkan Gambar 2.1, maka diperoleh model matematika sebagaimana pada persamaan (2.3) dan persamaan (2.4).

$$E(P, K_1) = C \tag{2.3}$$

$$D\big(E(P, K_1)\big) = \text{P} \qquad \text{atau } D(C, K_2) = P \tag{2.4}$$

Keterangan:

E_{K1}	:	Enkripsi pesan (*plaintext*) menggunakan kunci 1
P	:	*Plaintext*
C	:	*Ciphertext*
D_{K2}	:	Dekripsi *ciphertext* menggunakan kunci 2

C. Playfair Cipher

Playfair cipher pertama kali digunakan untuk tujuan-tujuan taktis oleh pasukan Inggris dalam Perang Boer II dan Perang Dunia I. Australia dan Jerman juga menggunakan sandi ini untuk tujuan yang sama dalamPerang Dunia II. *Payfair cipher* ditemukan oleh ahli Fisika berkebangsaan Inggris bernama Sir Charles

Wheatstone namun dipromosikan oleh Baron Lyon Playfair pada tahun 1854 (Zuli dan Irawan, 2014).

Playfair cipher merupakan *digraphs cipher* artinya setiap proses enkripsi maupun dekripsi dilakukan pada setiap dua huruf (secara berpasang-pasangan) (Setyaningsih, 2009).

Playfair menggunakan matriks 5×5. Semua alfabet kecuali J diletakan ke dalam tabel matriks. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak boleh ada huruf yang berulang. Kunci dimasukkan ke dalam tabel matriks 5×5, isian pertama yaitu kunci. Selanjutnya, tulis huruf-huruf berikutnya secara berurut mulai baris pertama (Santi, 2010).

Misalnya

Key = METODE

Maka kunci yang digunakan

Key = METOD

Matriks kunci METODE dapat dilihat pada persamaan (2.5).

$$X = \begin{bmatrix} M & E & T & O & D \\ A & B & C & F & G \\ H & I & K & L & N \\ P & Q & R & S & U \\ V & W & X & Y & Z \end{bmatrix} \quad (2.5)$$

Menurut Santi (2010) aturan-aturan proses enkripsi pesan menggunakan *playfair cipher* yaitu sebagai berikut:

1. Jika kedua huruf terletak pada baris dan kolom yang berbeda maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan

huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan sekolom dengan huruf pertama.

2. Jika kedua huruf terletak pada baris yang sama dan kolom yang berbeda maka huruf pertama menjadi huruf setelahnya dalam satu baris yang sama(ke arah kanan). Begitupun dengan huruf kedua, menjadi huruf setelahnya dalam satu baris yang berbeda (ke arah kanan).
3. Jika kedua huruf terletak pada kolom yang sama dan baris yang berbeda maka huruf pertama menjadi huruf setelahnya dalam satu kolom yang sama (ke arah bawah). Begitupun dengan huruf kedua, menjadi huruf setelahnya dalam satu kolom yang berbeda (ke arah bawah).
4. Jika kedua huruf sama, maka letakkan huruf Z diantaranya (sesuai kesepakatan).
5. Jika jumlah huruf *plaintext* ganjil, maka tambahkan huruf Z pada akhir kalimat.

Menurut Santi (2010) aturan-aturan proses dekripsi pesan yaitu sebagai berikut:

1. Jika kedua huruf terletak pada baris dan kolom yang berbeda maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan sekolom dengan huruf pertama.
2. Jika kedua huruf terletak pada baris yang sama dan kolom yang berbeda maka huruf pertama menjadi huruf sebelumnya dalam satu baris yang sama (ke arah kiri). Begitupun dengan huruf kedua, menjadi huruf sebelumnya dalam satu baris yang berbeda (ke arah kiri).

3. Jika kedua huruf terletak pada kolom yang sama dan baris yang berbeda maka huruf pertama menjadi huruf sebelumnya dalam satu kolom yang sama (ke arah atas). Begitupun dengan huruf kedua, menjadi huruf sebelumnya dalam satu kolom yang berbeda (ke arah atas).

Secara matematis, proses enkripsi pesan menggunakan *playfair cipher* yaitu sebagaimana pada persamaan (2.6).

Misalkan A : matriks berukuran $m \times n$

p : entri pada matriks E

m, x : baris

y, n : kolom

Maka diperoleh:

$$A(p_{mn}, p_{xy}) = \begin{cases} (p_{my}, p_{xn}) & ; \quad m \neq x, n \neq y \\ (p_{m(n+1)}, p_{x(y+1)}); & m = x, n \neq y \\ (p_{(m+1)n}, p_{(x+1)y}); & m \neq x, n = y \end{cases} \tag{2.6}$$

Secara matematis, proses dekripsi pesan menggunakan *playfair cipher* yaitu sebagaimana pada persamaan (2.7).

Misalka B : matriks berukuran $m \times n$

c : entri pada matriks D

m, x : baris

y, n : kolom

Maka diperoleh:

$$B(c_{mn}, c_{xy}) = \begin{cases} (c_{my}, c_{xn}) & ; \quad m \neq x, n \neq y \\ (c_{m(n-1)}, c_{x(y-1)}); & m = x, n \neq y \\ (c_{(m-1)n}, c_{(x-1)y}); & m \neq x, n = y \end{cases} \tag{2.7}$$

Contoh 2.1

Kata kuncinya = BILANGAN

Key = BILANG

Plaintext = BOCORAN SOAL UJIAN

Adapun proses eknripsi yaitu:

Langkah pertama : Membuat matriks kunci, yaitu dengan cara kunci dimasukkan ke dalam matriks 5×5 seperti persamaan (2.8).

$$Y = \begin{bmatrix} B & I & L & A & N \\ G & C & D & E & F \\ H & K & M & O & P \\ Q & R & S & T & U \\ V & W & X & Y & Z \end{bmatrix} \quad (2.8)$$

Langkah kedua : Karena terdapat huruf J pada plaintext, maka huruf J digantikan dengan huruf I menjadi BOCORAN SOAL UIIAN.

Langkah ketiga : Karena terdapat dua huruf yang sama berdampingan, maka disisipkan huruf Z diantaranya. Diperoleh BOCORAN SOAL UIZIAN

Langkah keempat : Menambahkan huruf Z di akhir kalimat, karena jumlah huruf *plaintext* ganjil. BOCORAN SOAL UIZIANZ

Langkah kelima :Menghilangkan spasi pada *plaintext* dan mengubah susunan *plaintext* menjadi pasangan huruf. BO CO RA NS OA LU IZ IA NZ

Langkah keenam : Enkripsi pesan sesuai aturan. Sehingga diperoleh

BO : AH

CO : EK

RA : TI

NS : LU

OA : TE

LU : NS

IZ : NW

IA : LN

NZ : FN

Jadi, *ciphertext* dari kata BOCORANSOALUIZIANZ yaitu AHEKTILUTENSNWLNFN.

Proses dekripsi yaitu:

Langkah pertama : Menghilangkan spasi pada *ciphertext* dan mengubah susunan *ciphertext* menjadi pasangan huruf. AH EK TI LU TE NS NW LN FN

Langkah kedua : Dekripsi pesan sesuai aturan. Sehingga diperoleh

AH : BO

EK : CO

TI : RA

LU : NS

TE : OA

NS : LU

NW : IZ

LN : IA

FN : NZ

Jadi, *plaintext* dari kata AHEKTILUTENSNWLNFN yaitu BOCORANSOALUIZIANZ. Kemungkinan pesan yang akan disampaikan yaitu BOCORAN SOAL UJIAN.

D. Caesar Cipher

Caesar cipher adalah teknik kriptografi yang digunakan oleh Kaisar Romawi, Julius Caesar, untuk menyandikan pesan yang dikirim kepada para gubernurnya. Pada *caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alfabet. Dalam hal ini kuncinya adalah jumlah pergeseran huruf. Misalnya susunan alfabet setelah digeser sejauh 3 huruf dapat dilihat pada Tabel 2.1 (Munir, 2010:207).

Tabel 2.1. Susunan Alfabet Setelah Digeser Sejauh 3 Huruf

Plainteks	:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipherteks	:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Jadi huruf A dalam plainteks disubtitusi dengan huruf D, demikian seterusnya. Pada metode ini, setiap huruf diubah dalam bentuk *integer* seperti berikut.

A	=	0	N	=	13
B	=	1	O	=	14
C	=	2	P	=	15
D	=	3	Q	=	16
E	=	4	R	=	17
F	=	5	S	=	18

G	=	6	T	=	19
H	=	7	U	=	20
I	=	8	V	=	21
J	=	9	W	=	22
K	=	10	X	=	23
L	=	11	Y	=	24
M	=	12	Z	=	25

Maka secara matematis pergeseran 3 huruf alfabet ekuivalen dengan melakukan operasi modulo terhadap plainteks *P* menjadi cipherteks *C* dengan persamaan (2.8).

$$C = E(P) = (P + 3)\ mod\ 26 \tag{2.8}$$

Secara umum fungsi enkripsi dan dekripsi pada *Caesar cipher* dapat dibuat lebih umum dengan menggeser huruf alfabet sejauh *k.* Sehingga persamaan (2.9) untuk fungsi enkripsi dan persamaan (2.10) untuk fungsi dekripsi dimana *k* berlaku sebagai kunci rahasia (Munir, 2010:207-208).

$$C = E(P) = (P + k) mod\ 26 \tag{2.9}$$

$$P = D(C) = (C - k) mod\ 26 \tag{2.10}$$

Contoh 2.2

Plaintext= KUNCI JAWABAN UJIAN

Key = 3 pergeseran

Adapun proses eknripsi yaitu:

Langkah pertama : Hilangkan spasi pada *plaintext*. Ubah p*laintext* kedalam bentuk *integer*, maka diperoleh

K = 10; U = 20; N = 13; C = 2; I = 8; J = 9;

A = 0; W = 22; B = 1.

Langkah kedua : Enkripsi *palintext* dalam bentuk *integer* menggunakan persamaan (2.9).

K➔ $E(K) = (10 + 3) mod\ 26 = 13\ mod\ 26 = 13 = N$

U➔ $E(U) = (20 + 3) mod\ 26 = 23\ mod\ 26 = 23 = X$

N➔ $E(N) = (13 + 3) mod\ 26 = 16\ mod\ 26 = 16 = Q$

C➔ $E(C) = (2 + 3) mod\ 26 = 5\ mod\ 26 = 5 = F$

I➔ $E(I) = (8 + 3) mod\ 26 = 11\ mod\ 26 = 11 = L$

J➔ $E(J) = (9 + 3) mod\ 26 = 12\ mod\ 26 = 12 = M$

A➔ $E(A) = (0 + 3) mod\ 26 = 3\ mod\ 26 = 3 = D$

W➔ $E(W) = (22 + 3) mod\ 26 = 25\ mod\ 26 = 25 = Z$

A➔ $E(A) = (0 + 3) mod\ 26 = 3\ mod\ 26 = 3 = D$

B➔ $E(B) = (1 + 3) mod\ 26 = 4\ mod\ 26 = 4 = E$

A➔ $E(A) = (0 + 3) mod\ 26 = 3\ mod\ 26 = 3 = D$

N➔ $E(N) = (13 + 3) mod\ 26 = 16\ mod\ 26 = 16 = Q$

U➔ $E(U) = (20 + 3) mod\ 26 = 23\ mod\ 26 = 23 = X$

J➔ $E(J) = (9 + 3) mod\ 26 = 12\ mod\ 26 = 12 = M$

I➔ $E(I) = (8 + 3) mod\ 26 = 11\ mod\ 26 = 11 = L$

A➔ $E(A) = (0 + 3) mod\ 26 = 3\ mod\ 26 = 3 = D$

N➔ $E(N) = (13 + 3) mod\ 26 = 16\ mod\ 26 = 16 = Q$

Jadi, *ciphertext* dari kata KUNCIJAWABANUJIAN adalah NXQFLMDZDEDQXMLDQ

Proses dekripsi yaitu:

Langkah pertama : Dekripsi *ciphertext* menggunakan persamaan (2.10), diperoleh

N➔ $D(N) = (13 - 3) mod\ 26 = 10\ mod\ 26 = 10 = K$

X➔ $D(X) = (23 - 3) mod\ 26 = 20\ mod\ 26 = 20 = U$

Q➔ $D(Q) = (16 - 3) mod\ 26 = 13\ mod\ 26 = 13 = N$

F➔ $D(F) = (5 - 3) mod\ 26 = 2\ mod\ 26 = 2 = C$

L➔ $D(L) = (11 - 3) mod\ 26 = 8\ mod\ 26 = 8 = I$

M➔ $D(M) = (12 - 3) mod\ 26 = 9\ mod\ 26 = 9 = J$

D➔ $D(D) = (3 - 3) mod\ 26 = 0\ mod\ 26 = 0 = A$

Z➔$D(Z) = (25 - 3) mod\ 26 = 22\ mod\ 26 = 22 = W$

D➔ $D(D) = (3 - 3) mod\ 26 = 0\ mod\ 26 = 0 = A$

E➔ $D(E) = (4 - 3) mod\ 26 = 1\ mod\ 26 = 1 = B$

D➔ $D(D) = (3 - 3) mod\ 26 = 0\ mod\ 26 = 0 = A$

Q➔ $D(Q) = (16 - 3) mod\ 26 = 13\ mod\ 26 = 13 = N$

X➔ $D(X) = (23 - 3) mod\ 26 = 20\ mod\ 26 = 20 = U$

M➔ $D(M) = (12 - 3) mod\ 26 = 9\ mod\ 26 = 9 = J$

L➔ $D(L) = (11 - 3) mod\ 26 = 8\ mod\ 26 = 8 = I$

D➔ $D(D) = (3 - 3) mod\ 26 = 0\ mod\ 26 = 0 = A$

Q➔ $D(Q) = (16 - 3) mod\ 26 = 13\ mod\ 26 = 13 = N$

Plaintext dari kata NXQFLMDZDEDQXMLDQ adalah KUNCIJAWABANUJIAN. Jadi pesan yang akan disampaikan yaitu KUNCI JAWABAN UJIAN.

E. Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang berarti tersembunyi atau terselubung dan *graphia* yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung" (Darmayanti, 2016).

Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan dapat berupa media teks, gambar, audio atau video (Sadikin, 2012:10).

Menurut Katzenbeisser dan Petitcolas (2000:20) sistem steganografi yang tidak menggunakan kunci pertukaran informasi rahasia atau tidak menggunakan kunci steganografi, disebut steganografi murni. Secara umum, proses *embedding* dapat dideskripsikan sebagai $E: C \times M \rightarrow C$, di mana C adalah cover image dan M adalah pesan rahasia. Proses *extraction* yaitu $D: C \rightarrow M$, mengeluarkan pesan rahasia dari cover image. Jelas bahwa $|C| \geq |M|$ (Katzenbeisser dan Petitcolas, 2000:20).

Definisi 2.1 (Katzenbeisser dan Petitcolas, 2000:20)
Steganografi terdiri dari empat bagian yaitu C, M, D, dan E, di mana C merupakan cover atau media penyisipan, M adalah pesan rahasia dengan $|C| > |M|$, $E: C \times M \rightarrow C$ *fungsi embedding dan* $D: C \rightarrow M$ *merupakan fungsi ekstraksi, dengan* $D\big(E(c, m)\big) = m$ *untuk semua* $m \in M$ *dan* $c \in C$ *adalah sistem kriptografi murni.*

Menurut Cahyadi (2012), terdapat beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik steganografi antara lain:

1. Teks

   Dalam algoritma steganografi yang menggunakan teks sebagai media penyisipan biasanya digunakan teknik NLP sehingga teks yang telah disisipkan pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.

2. Audio

   Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar, sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.

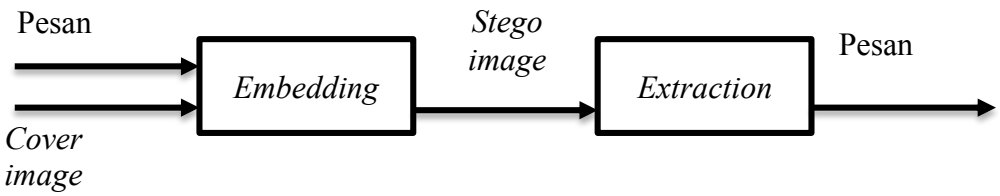
3. Citra

   Format ini juga sering digunakan karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma steganografi untuk media penampung yang berupa citra.

4. Video

   Format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

Proses steganografi secara umum dengan media citra dapat dilihat pada Gambar 2.3 yaitu sebagai berikut.



Gambar 2.3 Proses *Embedding* dan Ekstraksi

Berdasarkan Gambar 2.3 proses steganografi menggunakan media citra diawali dengan menginput pesan dan *cover image* (citra yang digunakan sebagai media penyisipan). Selanjutnya dilakukan proses *embedding*, sehingga diperoleh *stegi image* citra yang telah disisipkan pesan). *Stego image* inilah yang akan dikirim ke penerima pesan. Penerima pesan melakukan *extraction* (proses pengeluaran pesan pada citra). Setelah melakukan proses *extraction*, maka pesan yang dikirim dapat dibaca.

Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu (Cahyadi, 2012):

1. *Imperectibility*

   Keberadaan pesan rahasia dalam media penampung tidak dapat dideteksi oleh inderawi.

   Contoh :

   Misalnya, jika media penyisipannya yang digunakan berupa citra, maka penyisipan pesan membuat *stegoimage* susah diketahui secara kasat mata bahwa di dalamnya terdapat suatu informasi yang disisipkan.

2. *Fidelity*

   Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan itu tidak dapat dipersepsi oleh inderawi.

Contoh :

Misalnya media penyisipannya berupa citra. Citra sebelum dan sesudah disisipkan pesan tidak dapat dilihat dengan jelas secara kasat mata karena perubahan warna citra setiap pixel tidak dapat dibedakan.

3. *Recovery*

Pesan yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan steganografi adalah *data hidding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.

Contoh :

Misalkan pesan yang akan disisipkan yaitu “SAYA”. Setelah pesan tersebut disisipkan dalam citra, maka pesan ini harus dapat dikeluarkan kembali dalam *stegoimage* dengan cara diekstraksi

F. *Least Significant Bit* (LSB)

LSB merupakan salah satu metode dalam steganografi. Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext.* Pada susunan bit di dalam sebuah byte (di mana 1 byte = 8 bit), ada bit yang paling berarti yaitu *Most Significant Bit* (MSB) dan bit yang paling kurang berarti yaitu *Least Significant Bit* (LSB). Sebagai contoh byte 11010010, angka bit 1 yang digaris-bawahi adalah bit MSB dan angka bit 0 yang digaris-bawahi adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB

tidak mengubah warna merah tersebut secara berarti. Maka manusia tidak dapat membedakan perubahan kecil tersebut secara kasat mata (Arif dan Fanani, 2016). Teknik LSB menggantikan bit terakhir pada gambar dengan bit yang akan disembunyikan (pesan) (Setiawan, dkk., 2012).

Terdapat dua proses utama dalam penyisipan pesan menggunakan metode LSB, yaitu proses *embedding* dan proses *extraction*. Proses *embedding* adalah proses penyisipan pesan rahasia ke dalam suatu media. Proses *extraction* adalah proses pengambilan pesan rahasia dari suatu media (Husein, 2014).

Sebelum melakukan proses *embedding*, pesan yang akan disisipkan terlebih dahulu diubah dalam bentuk biner. Begitupun pada proses *extraction*. Setelah melakukan proses *extraction,* bilangan biner yang keluar dari citra diubah dalam bentuk desimal agar dapat diketahui isi pesannya.

Contoh 2.3

Misalkan bit pada sebuah gambar dengan ukuran 3×3 pixel sebagai berikut (Setiawan, dkk., 2012):

(00111111 11101001 11001000)

(00111111 11001000 11101001)

(11000000 00100111 11101001)

Misalkan pesan yang akan disisipkan adalah huruf "N"

Langkah pertama : Mengubah huruf N ke dalam bentuk desimal. Bentuk desimal dari huruf N yaitu 14.

Langkah kedua : Mengubah bentuk desimal 14 ke bentuk biner (lihat Tabel 2.2)

Tabel 2.2 Mengubah Bentuk Desimal ke Bentuk Biner

									Nilai
Desimal	0	0	0	0	8	4	2	0	14
Pangkat	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Biner	0	0	0	0	1	1	1	0	00001110

Jadi diperoleh bilangan biner dari 14 yaitu 00001110.

Langkah ketiga : Setiap bit pesan disisipkan ke dalam bit terakhir pada citra dengan menggunakan metode LSB. Maka dihasilkan

(00111111 11101000 11001000)

(00111110 11001001 11101001)

(11000001 00100110 11101001)

G. Citra

Secara harfiah, citra (*image*) adalah gambar pada bidang dwimatra (dua dimensi). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, seperti mata pada manusia, kamera, pemindai (*scanner*), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam (Munir, 2004:2). Citra digital dibentuk oleh kumpulan titik yang dinamakan *pixel*. Setiap *pixel* digambarkan sebagai satu kotak kecil. Setiap *pixel* mempunyai koordinat posisi. Gambar 2.4 menunjukkan sistem koordinat yang dipakai untuk menyatakan citra digital (Kadir dan Susanto, 2013:10). Sistem

koordinat yang diacu adalah sistem koordinat kartesian, di mana sumbu mendatar menyatakan sumbu-*x* dan sumbu tegak menyatakan sumbu-*y*.

Berdasarkan jenisnya citra digital dibagi menjadi 3 jenis (Sutoyo dalam Imran, 2009:11) yaitu:

1. Citra biner

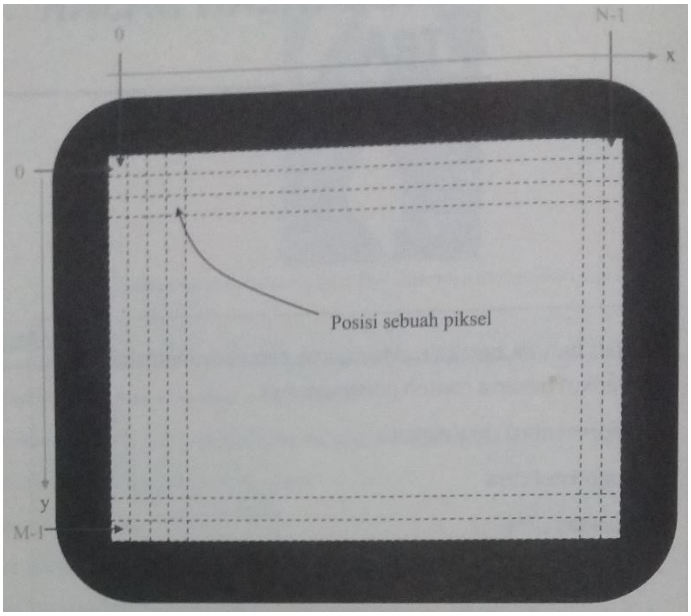
   Citra biner hanya memiliki dua warna yaitu hitam dan putih. Warna hitam bernilai 0 dan warna putih bernilai 1.

2. Citra abu

   Citra abu mempunyai kemungkinan warna hitam untuk minimal dan warna putih untuk nilai maksimal. Banyaknya warna tergantung pada jumlah bit yang disediakan di memori untuk menampung kebutuhan warna tersebut. Semakin besar jumlah bit warna yang disediakan di memori, maka semakin halus gradasi warna yang terbentuk.

3. Citra warna

   Setiap pixel pada citra warna memiliki warna yang merupakan kombinasi tiga warna dasar yaitu merah, hijau, dan biru (*RGB= Red, Green, Blue*). Jadi citra warna disusun oleh tiga buah matriks yaitu matriks komponen merah (*red*), matriks komponen hijau (*green*), dan matriks komponen biru (*blue*).



Gambar 2.4 Sistem Koordinat Citra Berukuran $M \times N$ (M baris dan N kolom)

Fungsi intensitas cahaya pada bidang dwimatra secara matematis disimbolkan dengan $f(x, y)$, di mana (Munir, 2004:15).

(x, y) : koordinat pada bidang dwimatra

$f(x, y)$: intensitas cahaya pada titik (x, y)

Karena cahaya merupakan bentuk energi, maka intensitas cahaya bernilai antara 0 sampai tak terhingga (dapat ditulis $0 \leq f(x, y) < \infty$) (Munir, 2004:16).

Proses pembentukan intensitas cahaya diperlihatkan pada Gambar 2.7.2 . sumber cahaya menyinari permukaan objek. Jumlah pancaran cahaya yang diterima objek pada koordinat (x, y) adalah $i(x, y)$. Objek memantulkan cahaya yang diterimanya dengan derajat pantulan $r(x, y)$. Persamaan (2.11) menunjukkan hasil kali antara $i(x, y)$ dan $r(x, y)$ yang menyatakan intensitas cahaya pada koordinat (x, y) yang ditangkap oleh sensor visual pada sistem optik (Munir, 2004:16-17).

$$f(x, y) = i(x, y) \, . r(x, y) \qquad (2.11$$

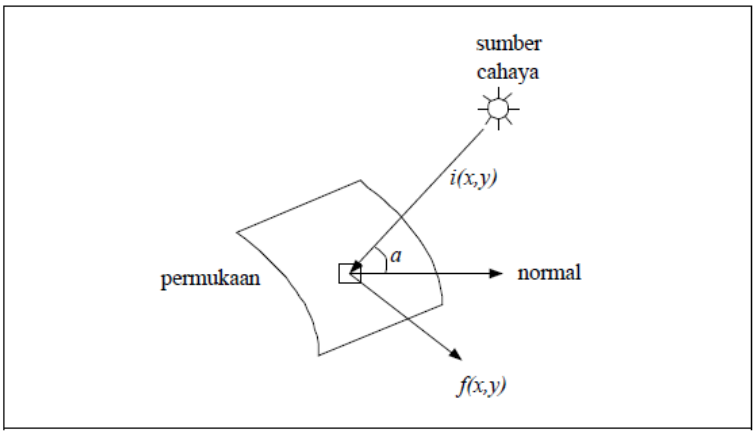
Di mana

$i(x,y)$: jumlah cahaya yang berasal dari sumbernya, $0 \leq i(x,y) < \infty$

$r(x,y)$: derajat kemampuan objek memantulkan cahaya, $0 \leq r(x,y) \leq 1$

Sehingga

$0 \leq f(x,y) < \infty$



Gambar 2.5 Pembentukan Citra

Nilai $i(x,y)$ ditentukan oleh sumber cahaya. Sedangkan $r(x,y)$ ditentukan oleh karakteristik objek di dalam gambar. Nilai $r(x,y) = 0$ mengindikasikan gambaran total. Sedangkan $r(x,y) = 1$ menyatakan pemantulan total (Munir, 2004:17).

H. *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* MSE

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan desibel (dB). PSNR digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR terlebih dahulu harus ditentukan nilai

Mean Square Error (MSE). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi, MSE adalah nilai error kuadrat rata-rata antara citra asli (*cover-image*) dengan citra hasil penyisipan (*stego-image*)) (Darmayanti dan Hars, 2016). Rumus untuk menghitung MSE dan PSNR dapat dilihat pada persamaan (2.12) dan persamaan (2.13) (Arif dan Fanani, 2016).

$$MSE = \frac{1}{mn}\sum_{x=1}^{m}\sum_{y=1}^{n}\big(f(x,y) - g(x,y)\big)^2 \quad (2.12)$$

Keterangan:

MSE	:	Nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi
m	:	Panjang citra (*pixel*)/jumlah baris matriks gambar
n	:	Lebar citra (*pixel*)/jumlah kolom matriks gambar
(x,y)	:	Koordinat masing-masing *pixel*
f	:	*Stego image*
g	:	*Cover image*

$$PSNR = 20 \cdot \log\left(\frac{Max}{\sqrt{MSE}}\right) \quad (2.13)$$

Keterangan:

PSNR	:	perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal (*dB*)
Max	:	Nilai maksimum *pixel stego image*

I. Aritmatika Modulo

Aritmatika mudulo memainkan peranan yang penting dalam komputasi integer, khususnya pada aplikasi kriptografi (Munir, 2010:191). Aritmatika modulo

digunakan agar operasi aritmatika selalu menghasilkan integer pada lingkup yang sama. Misalnya pada kriptorafi klasik digunakan alfabet latin "A" sampai dengan "Z", petakan lebih dahulu {A, ..., Z} menjadi {0, ..., 25}. Aritmatika modulo digunakan agar transformasi penyandian selalu bernilai {0, ..., 25} sehingga memiliki pasangan simbol yang digunakan (Sadikin, 2012:28).

1. Operator Modulo

Operator yang digunakan dalam modulo adalah mod. Operator mod memberikan sisa pembagian (Munir, 2010:191).

Definisi 2.2 (Munir, 2010:191)
Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \bmod m$ (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Dengan kata lain, $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.
Notasi: $a \bmod m = r$ sedemikian sehingga $a = mq + r$,
dengan $0 \leq r < m$.

Contoh 2.4

a) 15 mod 2 = 1 (15 dibagi 2 hasilnya = 7 (nilai q) dan sisa = 1 atau ditulis sebagai $15 = 2.7 + 1$)

b) 13 mod 5 = 3 (13 dibagi 5 hasilnya = 2 dan sisa = 3 atau ditulis sebagai $13 = 5.2 + 3$)

2. Kongruen

Hasil operasi modulo sembarang bilangan integer a dengan sebuah bilangan integer positif n selalu pada kisaran 0 sampai dengan $n - 1$. Dengan begitu operasi modulo n terhadap sembarang bilangan integer a merupakan pemetaan dari himpunan bilangan integer ($\mathbb{Z}$) ke himpunan bilangan $\{0, \dots, n -$

1} (dinotasikan sebagai $\mathbb{Z}_n$) atau dikenal sebagai himpunan residu modulo n (Sadikin, 2012:29).

Definisi 2.3 (Tiro, dkk., 2008:264)
Jika m suatu bilangan positif maka a kongruen dengan b modulo m (ditulis $a \equiv b(mod\ m)$) jika dan hanya jika m membagi $(a-b)$ atau ditulis $m|(a-b)$. Jika m tidak membagi $(a-b)$ maka dikatakan a tidak kongruen dengan b modulo m (ditulis $a \not\equiv b(mod\ m)$).

Contoh 2.5

a) $10 \equiv 2(mod\ 2)$ sebab $2|(10-2)$ atau $2|8$

b) $12 \equiv 3(mod\ 9)$ sebab $9|(12-3)$ atau $9|9$

J. MATRIKS

Definisi 2.4 (Rorres, 2004:26)
Suatu matriks (matrix) adalah jajaran empat persegi panjang dari bilangan-bilangan. Bilangan-bilangan dari jajaran tersebut disebut entri dari matriks

Ukuran suatu matriks dinyatakan dalam bentuk baris dan kolom. Suatu matriks yang yang terdiri dari satu kolom disebut matriks kolom. Suatu matriks yang hanya terdiri dari satu baris disebut matriks baris (Rorres, 2004:26)

Definisi 2.5 (Munir, 2010:98)
Matriks adalah susunan skalar elemen-elemen dalam bentuk baris dan kolom. Matriks A yang berukuran dari m baris dan n kolom $(m \times n)$ adalah:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Entri a_{ij} disebut elemen matriks pada baris ke-*i* dan kolom ke-*j*. Jika $m = n$, maka matriks tersebut dinamakan juga matriks bujur sangkar (Munir, 2010:98).

K. MATLAB (Matrix Laboratory)

MATLAB adalah sebuah bahasa pemrograman dengan kerja tinggi untuk komputasi teknis, yang mengintegrasikan komputasi, visualisasi, dan pemrograman di dalam lingkungan yang mudah penggunaannya dalam memecahkan persoalan dengan solusinya yang dinyatakan dengan notasi matematis. Penggunaan MATLAB yaitu (Wijaya, dkk., 2007:1):

1) Matematika dan komputasi
2) Pengembangan algoritma
3) Pemodelan, simulasi dan pembuatan 'prototipe'
4) Analisis data, eksplorasi dan visualisasi
5) Grafik untuk sains dan teknik
6) Pengembangan aplikasi, termasuk pembuatan antarmuka grafis untuk pengguna

Menurut Wijaya, dkk. (2007:2) MATLAB adalah sebuah sistem interaktif yang menggunakan elemen data dasarnya yaitu *array* yang tidak membutuhkan dimensi. Nama MATLAB merupakan singkatan dari *"matrix laboratory"*. Pada awalnya MATLAB dibuat untuk mempermudah pengembangan perangkat lunak berbasis matriks oleh proyek LINPACK dan EISPACK. Fitur-fitur MATLAB untuk penyelesaian spesifik disebut *"toolboxes"*. *Toolboxes* adalah koleksi komprehensif dari fungsi-fungsi MATLAB yang memperlebar lingkungan MATLAB dalam menyelesaikan kelas-kelas tertentu dari permasalahan. Beberapa *toolbox* yang tersedia meliputi bidang: pengolahan sinyal, sistem kendali, jaringan syaraf, logika *fuzzy*, *wavelet*, simulasi dan lain sebagainya.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

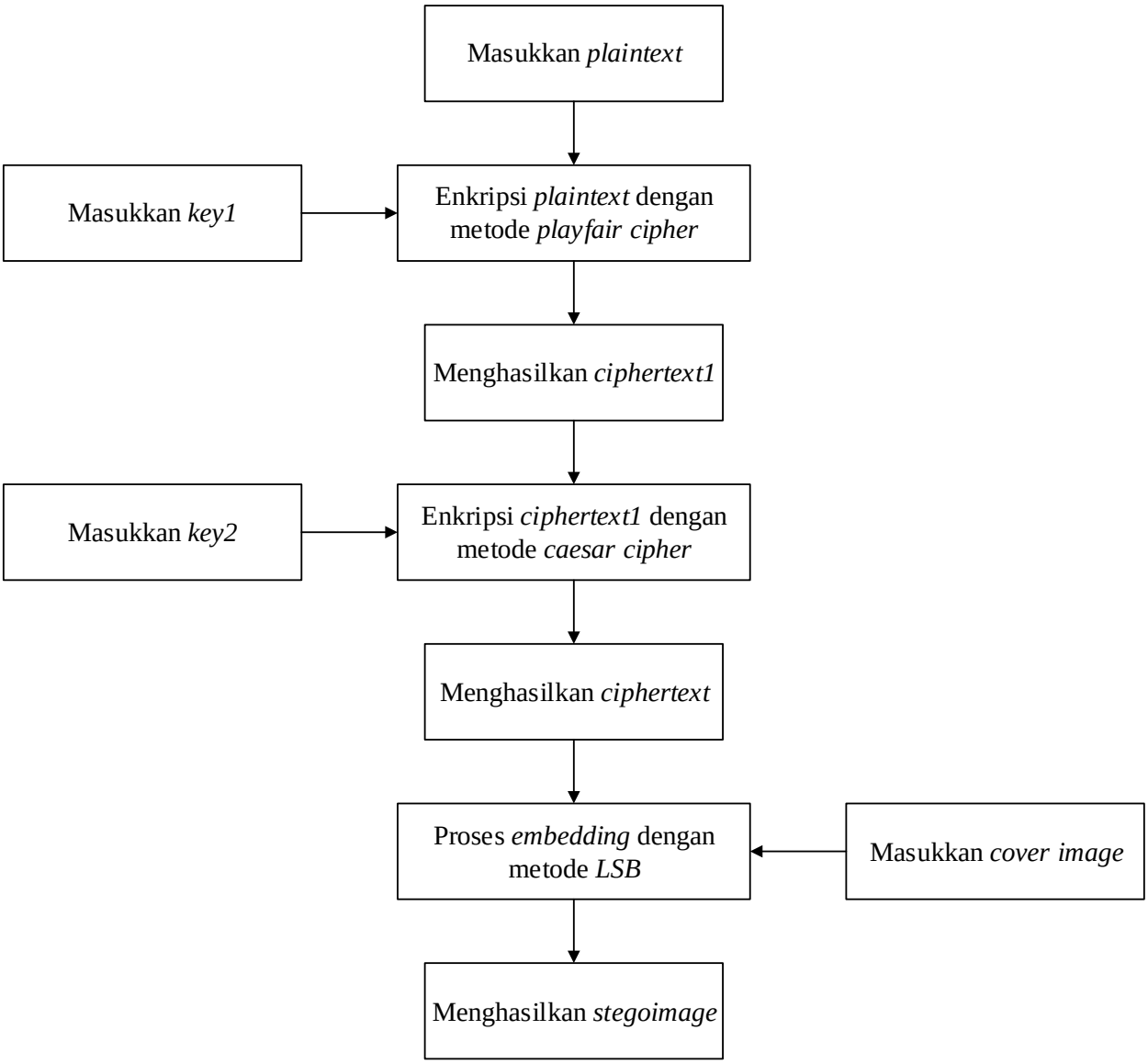
Jenis penelitian yang dilakukan adalah penelitian terapan, yaitu penelitian yang bertujuan untuk menyelesaikan masalah yang ada dengan menerapkan teori-teori yang mendasari penelitian yang dikaji dengan terlebih dahulu menyusun konsep-konsep yang berkaitan dengan kriptografi dan steganografi secara matematis, dengan MATLAB sebagai alat bantu komputasi.

B. Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di Perpustakaan dan Laboratorium Komputer Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Makassar pada bulan Desember 2016 sampai bulan Juni 2017.

C. Prosedur Penelitian

Penelitian ini dilakukan dengan terlebih dahulu mempelajari materi-materi dasar untuk penelitian ini seperti kriptografi, steganografi, serta penggunaan program MATLAB. Selanjutnya melakukan proses enkripsi dan *embedding* (sebagaimana pada Gambar 3.1) serta proses dekripsi dan ekstraksi untuk memperoleh pesan asal (sebagaimana pada Gambar 3.2).

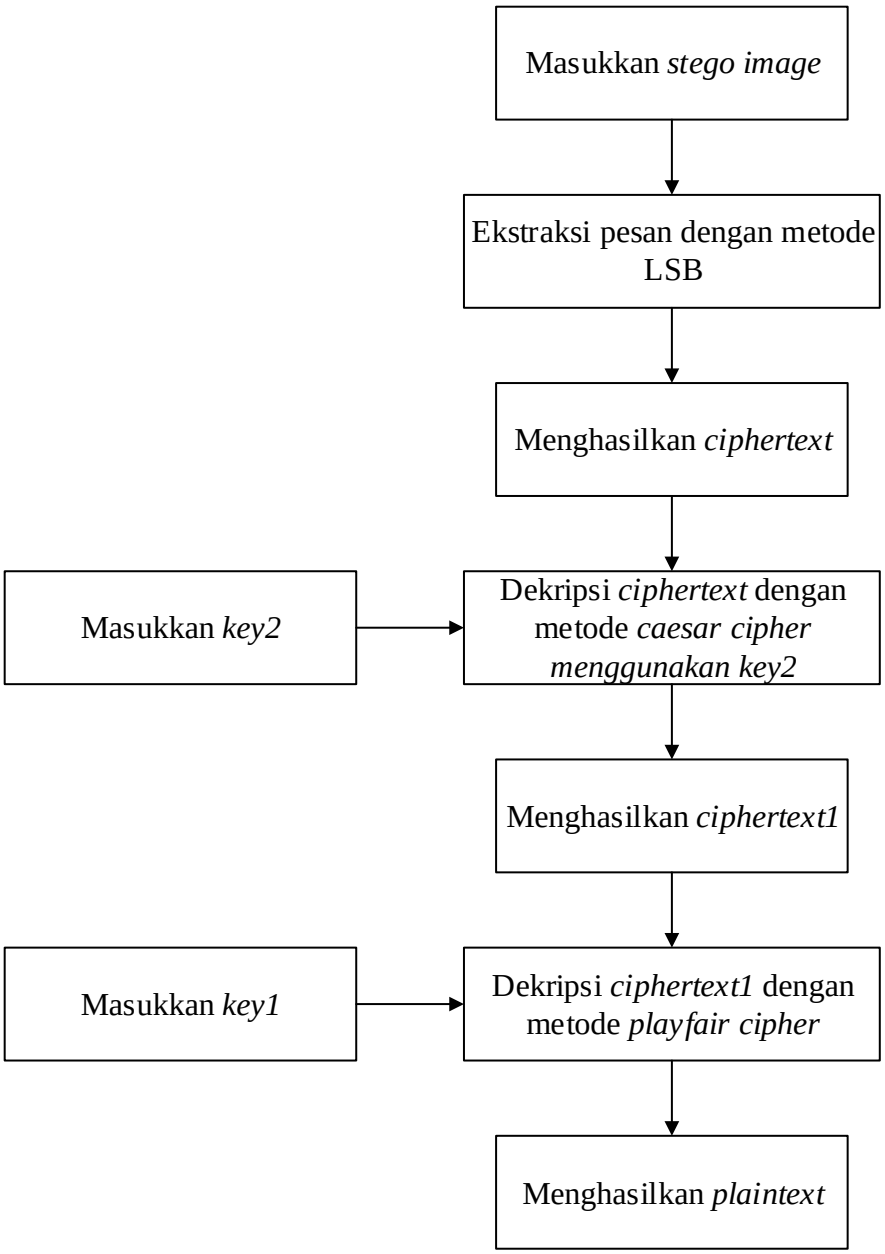


Gambar 3.1 Proses Enkripsi dan *Embedding* Menggunakan Metode *Playfair Cipher* dan *Caesar Cipher*

Proses enkripsi dan *embedding* menggunakan metode *playfair cipher* dan *caesar cipher* seperti pada Gambar 3.1 dapat dijelaskan sebagai berikut:

1. Menyiapkan pesan yang akan dirahasiakan (*plaintext*).
2. Menentukan kunci untuk metode *playfair cipher*.
3. Enkripsi pesan menggunakan metode *playfair cipher* sehingga menghasilkan *ciphertext1*.

4. Menentukan besar pegeseran sebagai kunci untuk metode *caesar cipher*.
5. Enkripsi pesan dari hasil enkripsi metode *playfair cipher* (*ciphertext1*) menggunakan metode *caesar cipher* sehingga menghasilkan *ciphertext*.
6. Menyiapkan media penyisipan (citra atau gambar yang akan disisipkan pesan).
7. Menyisipkan *ciphertext* pada citra menggunakan metode LSB dengan bantuan MATLAB.
8. Menghasilkan *stego image* yaitu citra yang telah disisipkan pesan.



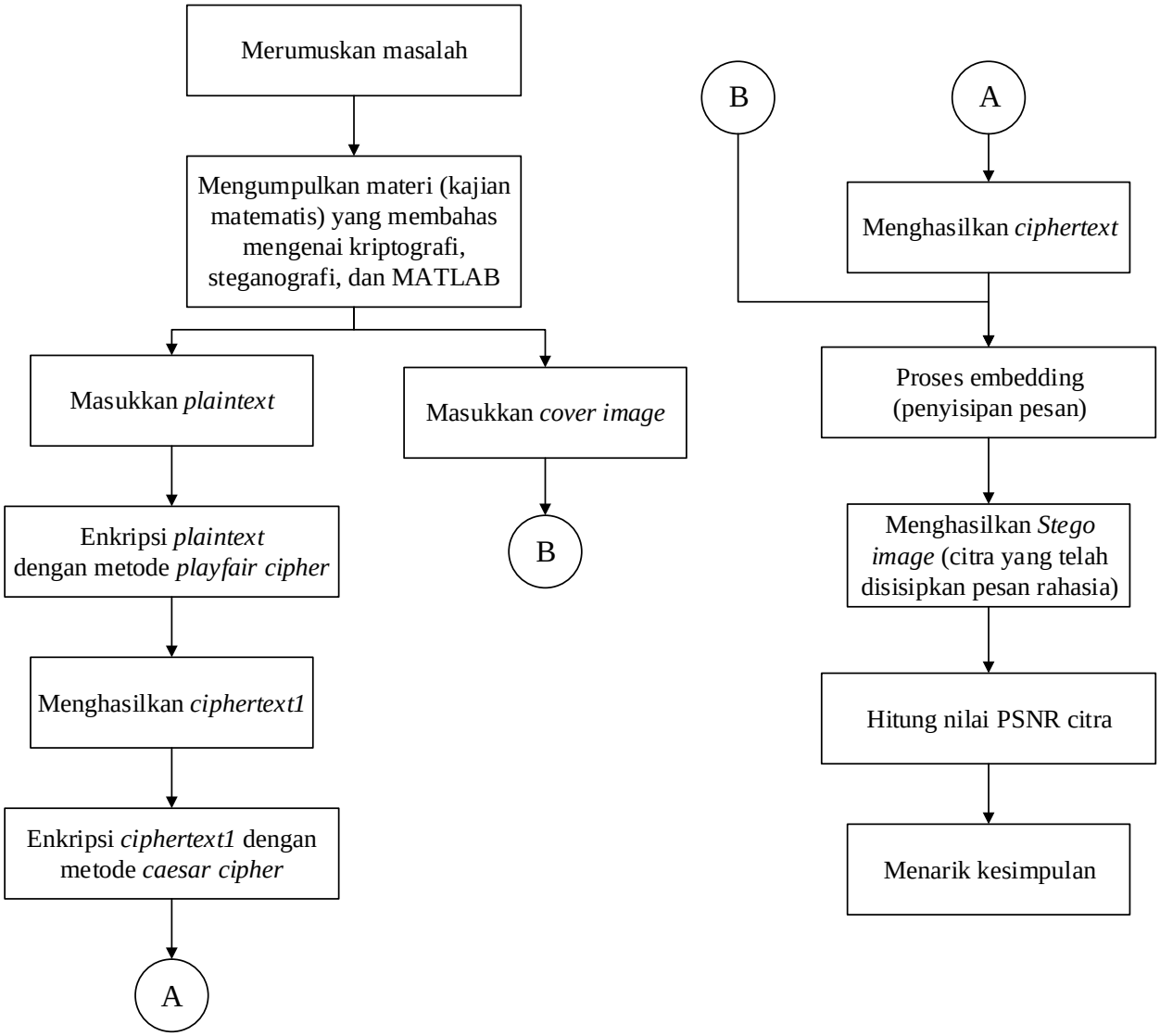
Gambar 3.2 Proses Dekripsi dan Ekstraksi Menggunakan Metode *Playfair Cipher* dan *Caesar Cipher*

Proses dekripsi dan ekstraksi menggunakan metode *playfair cipher* dan *caesar cipher* seperti pada Gambar 3.2 dapat dijelaskan sebagai berikut:

1. Siapkan *stego image*.
2. Ekstraksi pesan pada citra menggunakan metode LSB dengan bantuan MATLAB.
3. Tampil *ciphertext* yang telah disisipkan.
4. Dekripsi *ciphertext* dengan metode *caesar cipher* (menggunakan kunci yang sama saat enkripsi *ciphertext1*) sehingga menghasilkan *ciphertext1*.
5. Dekripsi *ciphertext1* dengan metode *playfair cipher* (menggunakan kunci yang sama saat enkripsi pesan) sehingga menghasilkan *plaintext* atau pesan asal.

D. Skema Penelitian

Skema Penyisipan Pesan pada Citra Menggunakan *Playfair Cipher* dan *Caesar Cipher* dapat dilihat pada gambar 3.3.



Gambar 3.3 Skema Penyisipan Pesan pada Citra Menggunakan *Playfair Cipher* dan *Caesar Cipher*

Berdasarkan Gambar 3.3 maka langkah pertama yang dilakukan yaitu merumuskan masalah-masalah yang akan diteliti. Selanjutnya mengumpulkan materi (kajian matematis) yang membahas mengenai kriptografi (Khusunya metode

playfair cipher dan *caesar cipher*), steganografi, dan MATLAB. Setelah itu dilakukan proses enkripsi pertama, yaitu mengenkripsi menggunakan metode *playfair cipher*, setelah dienkripsi maka diperoleh *ciphertext1*. *Ciphertxt1* dienkripsi lagi menggunakan metode *Caesar Cipher*, sehingga diperoleh *ciphertext*. Siapkan citra yang digunakan sebagai media untuk menyisipkan pesan. Selanjutnya, sisipkan *ciphertext* yang telah diperoleh ke dalam citra (proses *embedding*) dengan metode LSB. Kemudian hitung nilai PSNRnya untuk mengetahui besar perbedaan citra sebelum dan sesudah disisipkan pesan. Terakhir, menarik kesimpulan dari hasil penelitian.

BAB IV

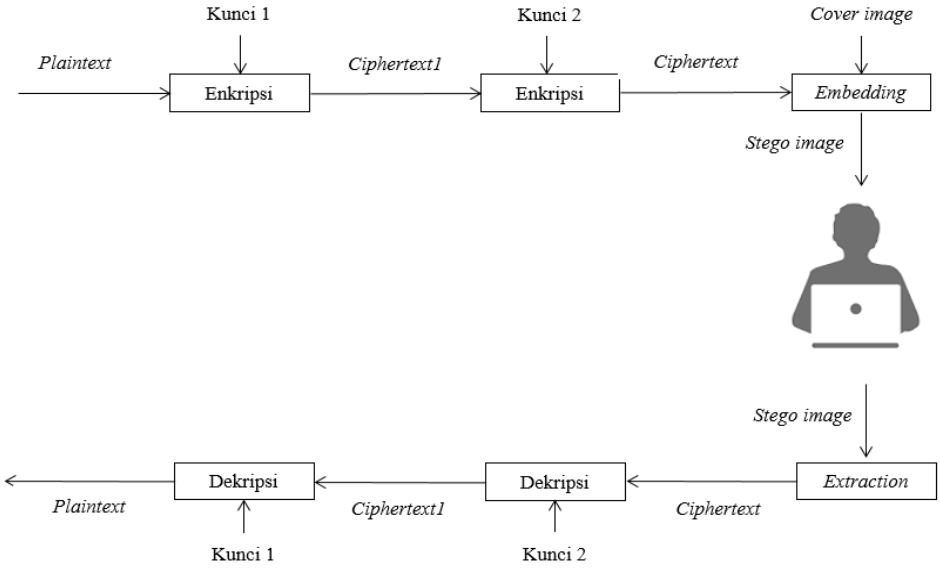
HASIL DAN PEMBAHASAN

A. Hasil

Data yang digunakan untuk pesan *(plaintext)* yaitu berupa karakter dalam bentuk huruf kapital A-Z, angka 1-9, dan tanda spasi (␣) (lihat Tabel 4.1), di mana pesan tersebut akan dilakukan proses enkripsi menggunakan metode kriptografi *playfair cipher*, kemudian hasilnya *(ciphertext1)* dienkripsi lagi menggunakan metode kriptografi *caesar cipher* dan menghasilkan *ciphertext*. *Ciphertext* ini kemudian disisipkan ke dalam citra digital. Hasil dari citra yang telah disisipkan pesan ini dinamakan *stego image*. *Stego image* inilah yang akan dikirim kepada penerima pesan. Penerima pesan harus megekstraksi kembali untuk mengeluarkan pesan yang tersisip dalam citra. Selanjutnya pesan tersebut didekripsi kembali menggunakan *caesar cipher* kemudian *playfair cipher* untuk memperoleh pesan asal. Adapun proses yang dimaksud dapat digambarkan seperti Gambar 4.1. Enkripsi dan dekripsi dengan kunci 1 menggunakan metode *playfair cipher*, sedangkan enkripsi dan dekripsi dengan kunci 2 menggunakan metode *caesar cipher*.

Tabel 4.1 Data Karakter yang Digunakan

Kolom 1 – 18																
Spasi	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
Kolom 19 – 36																	
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Gambar 4.1 Proses Penyisipan dan Pengeluaran Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

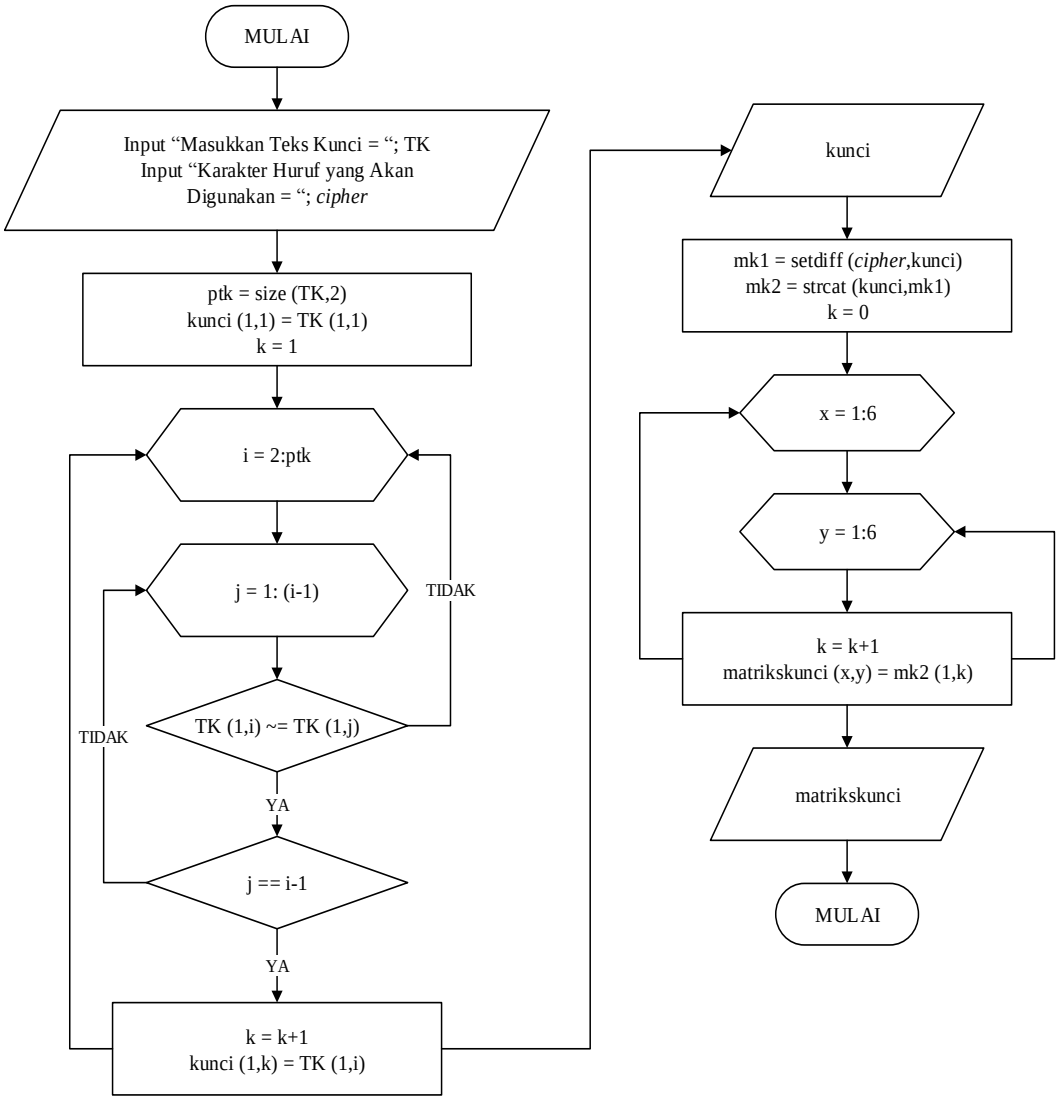
Metode kriptografi *playfair cipher* yang digunakan dalam penelitian ini sedikit berbeda dari peraturan awalnya. Dimana peraturan awal pada kriptografi metode *playfair cipher*, huruf J pada matriks kunci dihilangkan dan digantikan dengan huruf I. Akan tetapi di sini huruf J tetap ada dalam matriks kunci dan tidak dihilangkan ataupun digantikan. Sedangkan peraturan huruf sama yang berdekatan, bukan lagi disisipkan dengan huruf Z, tetapi disisipkan dengan angka 1. Jika jumlah

karakter dalam *plaintext* ganji, maka ditambahkan angka 1 diakhir kalimat. Matriks kunci yang digunakan yaitu matriks 6×6.

1. Enkripsi dan Dekripsi Pesan Menggunakan *Playfair Cipher*

a. Menentukan Matriks Kunci

Sebelum membuat matriks kunci, perhatikan teks kunci yang telah ditentukan. Teks kunci inilah yang akan digunakan untuk membentuk matriks kunci. Kunci yang digunakan berupa karakter yang telah ditentukan (lihat Tabel 4.1) dan tidak boleh ada huruf yang berulang. Kemudian kunci tersebut digabungkan dengan karakter yang tidak terdapat pada kunci dengan menuliskan kunci dulu baru sisa karakterter. Jika dalam peraturan awal dari metode ini huruf J dalam matriks kunci dihilangkan, maka dalam kasus ini huruf J tetap ada dan tidak ada dari karakter yang telah ditentukan yang akan dihilangkan (semua karakter digunakan). Selanjutnya gabungan kunci dan karakter disusun ke dalam matriks 6×6 dimulai dari baris pertama lalu kemudian baris selanjutnya (penyusunan matriks dilakukan dari kiri ke kanan). Proses untuk membuat matriks kunci dapat dilihat pada Gambar 4.2.



Gambar 4.2 Proses Pembuatan Matriks Kunci

Contoh 4.1

Teks kunci : SERAGAM

Kunci : SERAGM

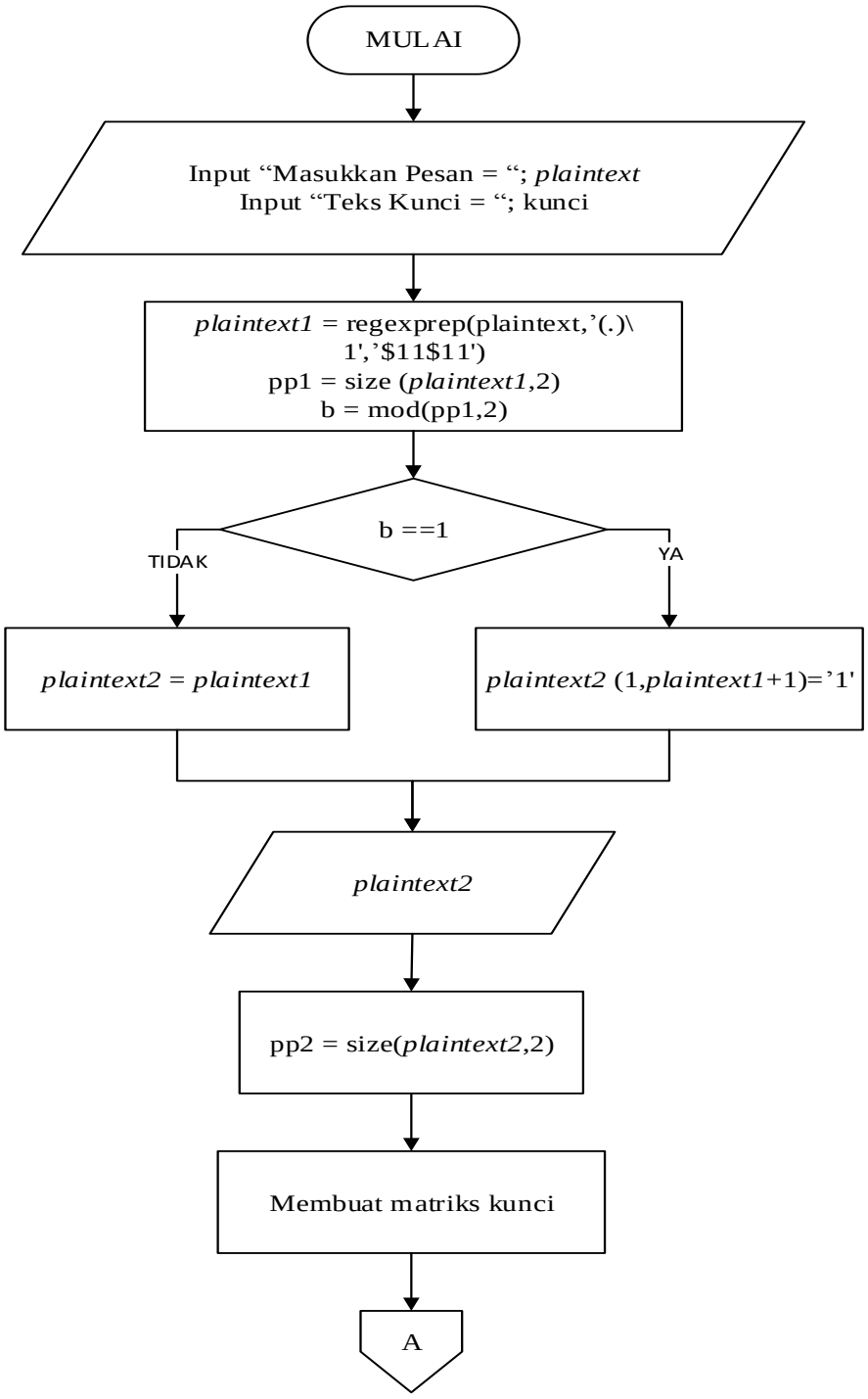
Maka diperoleh matriks kunci seperti pada persamaan (4.1).

$$Z = \begin{bmatrix} S & E & R & A & G & M \\ \_ & 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & B & C \\ D & F & H & I & J & K \\ L & N & O & P & Q & T \\ U & V & W & X & Y & Z \end{bmatrix} \quad (4.1)$$

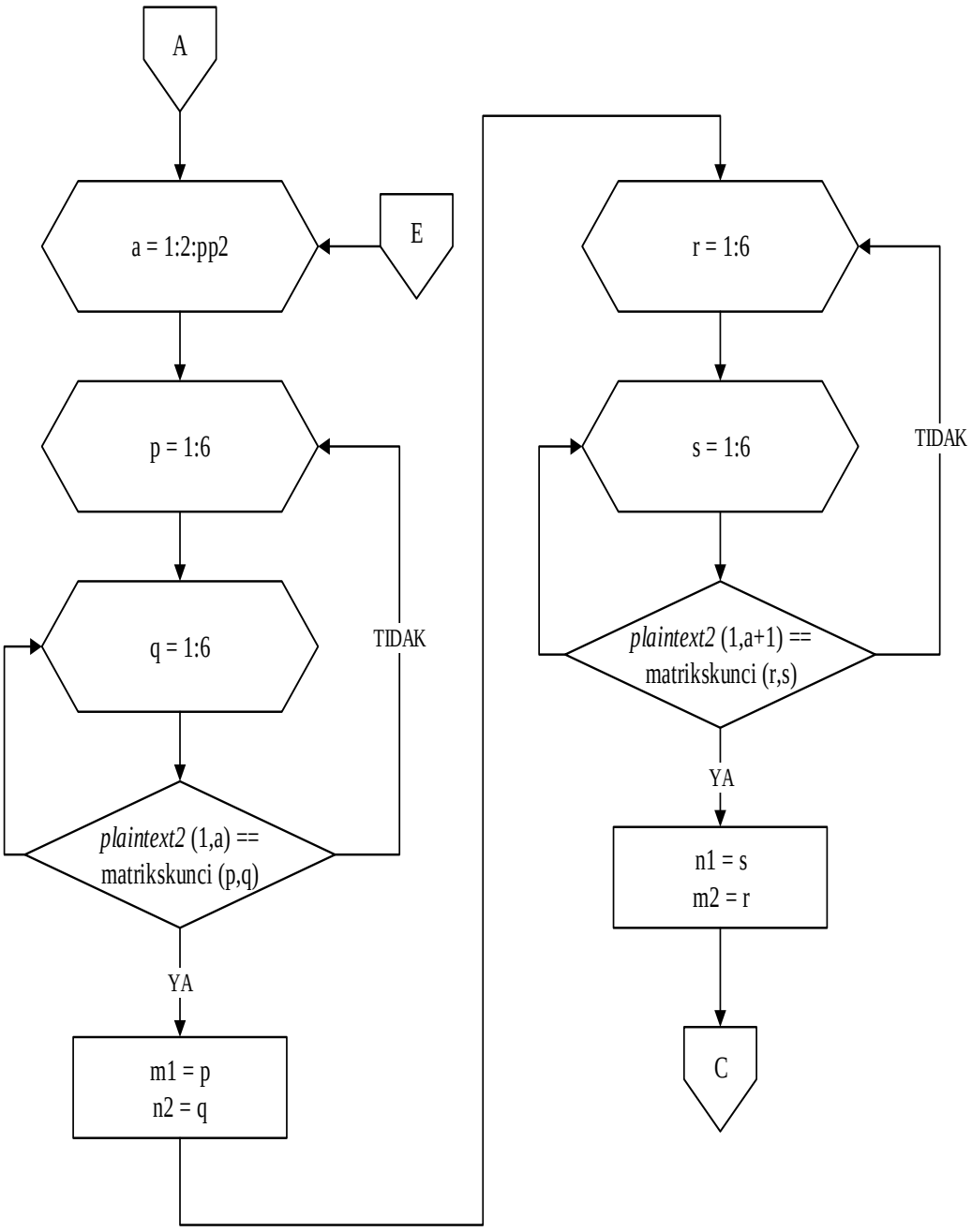
b. Proses Enkripsi

Proses enkripsi pesan menggunakan *playfair cipher* dilakukan dengan terlebih dahulu mengolah *plaintext*, yaitu dengan memeriksa jika terdapat huruf sama yang berdekatan atau berdampingan pada *plaintext* maka disisipkan angka 1 diantaranya. Setelah itu menghitung jumlah karakter *plaintext* tersebut. Jika jumlah karekternya ganjil maka ditambahkan angka 1 diakhir kalimat. Setelah melakukan proses pemeriksaan pada *plaintext*, selanjutnya jadikan *plaintext* tersebut menjadi berpasangan. Selanjutnya membuat matriks kunci. Kemudian ambil setiap pasangan karakter dan enkripsi setiap pasangan tersebut menggunakan matriks kunci.

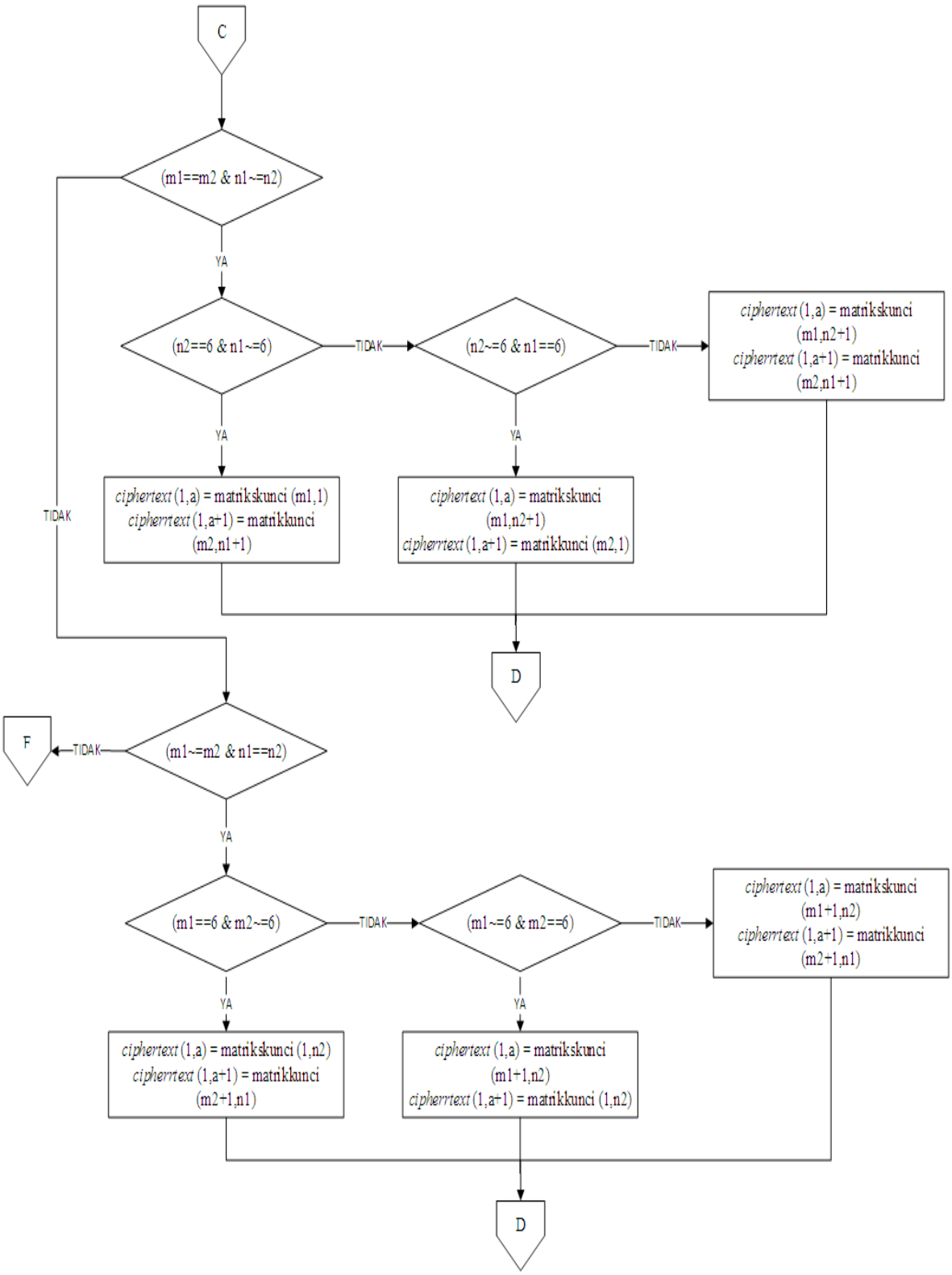
Proses enkripsi pesan menggunakan *playfair cipher* dapat dilihat pada Gambar 4.3 yang terdiri dari Gambar (a) Proses pengolahan *plaintext* dan matriks kunci, Gambar (b) Proses penentuan pasangan karakter, Gambar (c) Proses enkripsi pesan dengan melihat aturan pertama dan aturan kedua, dan Gambar (d) Proses enkripsi pesan dengan melihat aturan ketiga dan hasil penyandian pesan yang berupa *ciphertext*.



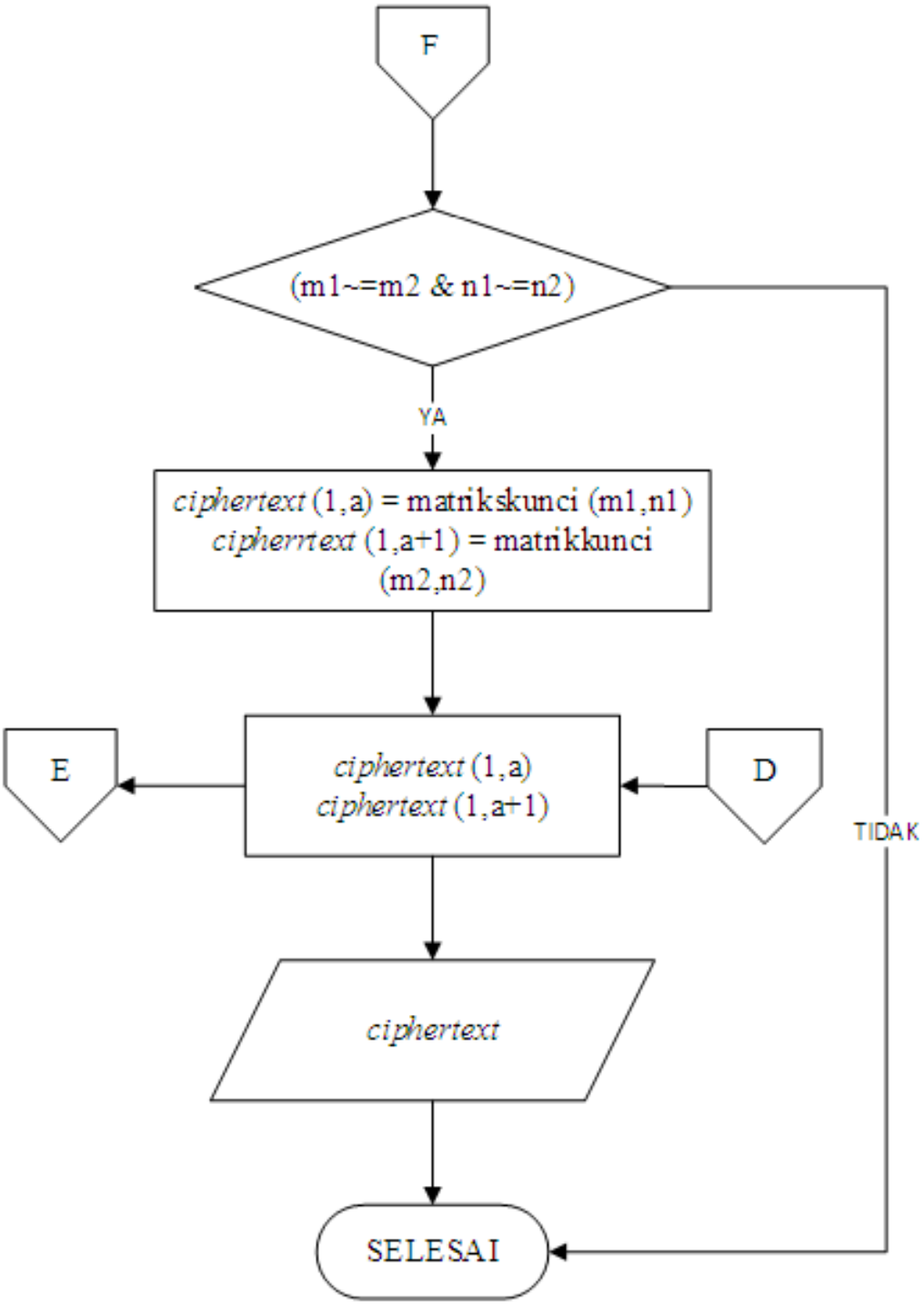
Gambar (a) Proses Pengolahan *Plaintext* dan Matriks Kunci



Gambar (b) Proses Penentuan Pasangan Karakter



Gambar (c) Proses Enkripsi Pesan dengan Melihat Aturan Pertama dan Aturan Kedua



Gambar (d) Proses Enkripsi Pesan dengan Melihat Aturan Ketiga dan Hasil *Ciphertext*

Gambar 4.3 Proses Enkripsi Pesan Menggunakan *Playfair Cipher* (Gambar (a), Gambar (b), Gambar(c), dan Gambar(d))

Contoh 4.2

Plaintext : NANTI SAYA AMBIL

Teks kunci : SERAGAM

Kunci : SERAGM

Proses enkripsinya dapat dilihat pada Tabel 4.2.

Tabel 4.2 Contoh Proses Enkripsi *Playfair Cipher*

Langkah		**Proses Enkripsi**
Pertama	:	Gabungkan kunci dengan karakter yang tidak terdapat dalam kunci. SERAGM 123456789BCDFHIJKLNOPQTUVWXYZ
Kedua	:	Membuat matriks kunci dari gabungan karakter tersebut. Matriks kunci SERAGAM dapat dilihat pada persamaan (4.1).
Ketiga	:	Periksa *plaintext*, jika terdapat huruf sama yang berdekatan atau berdampingan maka sisipkan angka 1 diantaranya dan jika jumlah karakternya ganjil maka tambahkan angka 1 diakhir kalimat. Karena tidak terdapat huruf sama yang berdekatan dan jumlah karakternya genap, maka tidak disisipan maupun ditambahkan dengan angka 1. NANTI SAYA AMBIL
Keempat	:	Jadikan *plaintext* menjadi karakter berpasang-pasangan. NA NT I␣ SA YA ␣A MB IL Keterangan: misalkan tanda "␣" adalah spasi
Kelima	:	Ambil setiap pasangan huruf dan ikuti syarat enkripsi *playfair cipher* untuk memperoleh *ciphertext*. Maka diperoleh

NA : PE

NT : OL

I␣ : D3

SA : EG

YA : XG

␣A : 3S

MB : GC

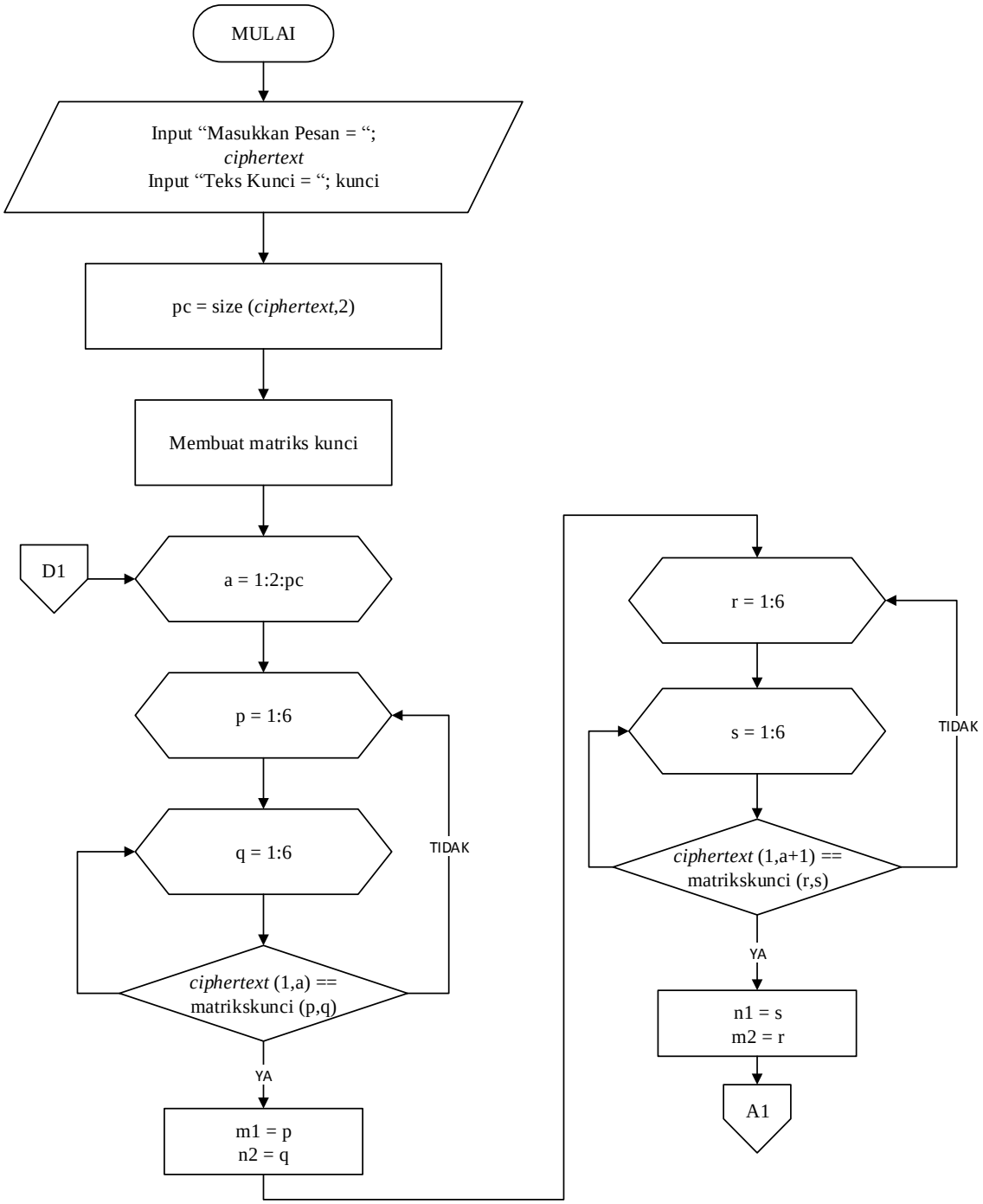
IL : DP

Jadi, *ciphertextnya* yaitu PEOLD3EGXG3SGCDP

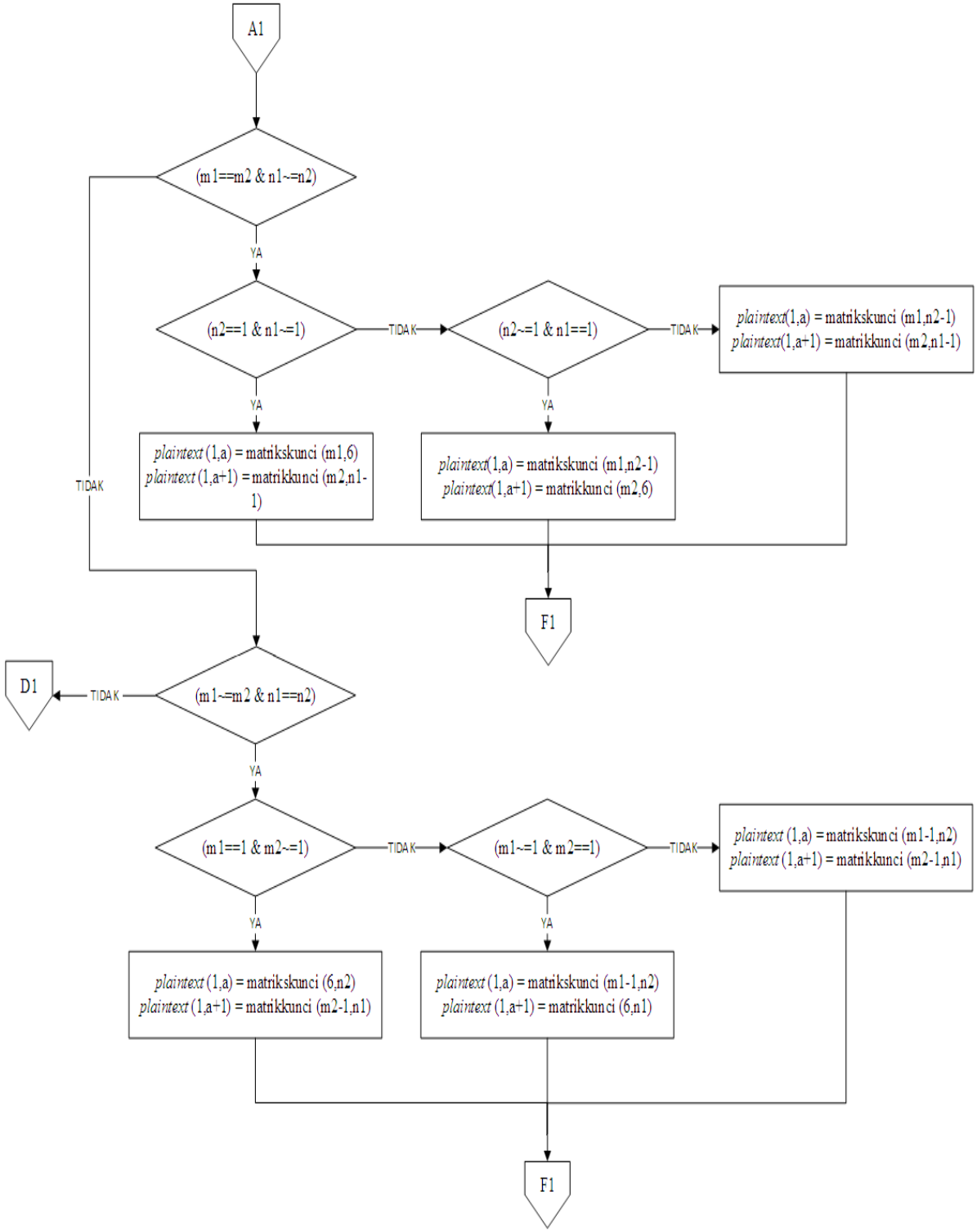
c. Proses Dekripsi

Matriks kunci yang digunakan dalam proses dekripsi pesan ini sama yang digunakan pada proses enkripsi. Langkah pertama yaitu menjadikan karakter *ciphertext* menjadi karakter berpasangan. Kemudian ambil setiap pasangan karakter tersebut dan dekripsi menggunakan matriks kunci dengan mengikuti aturan-aturan dekripsinya sehingga menghasilkan pesan asal.

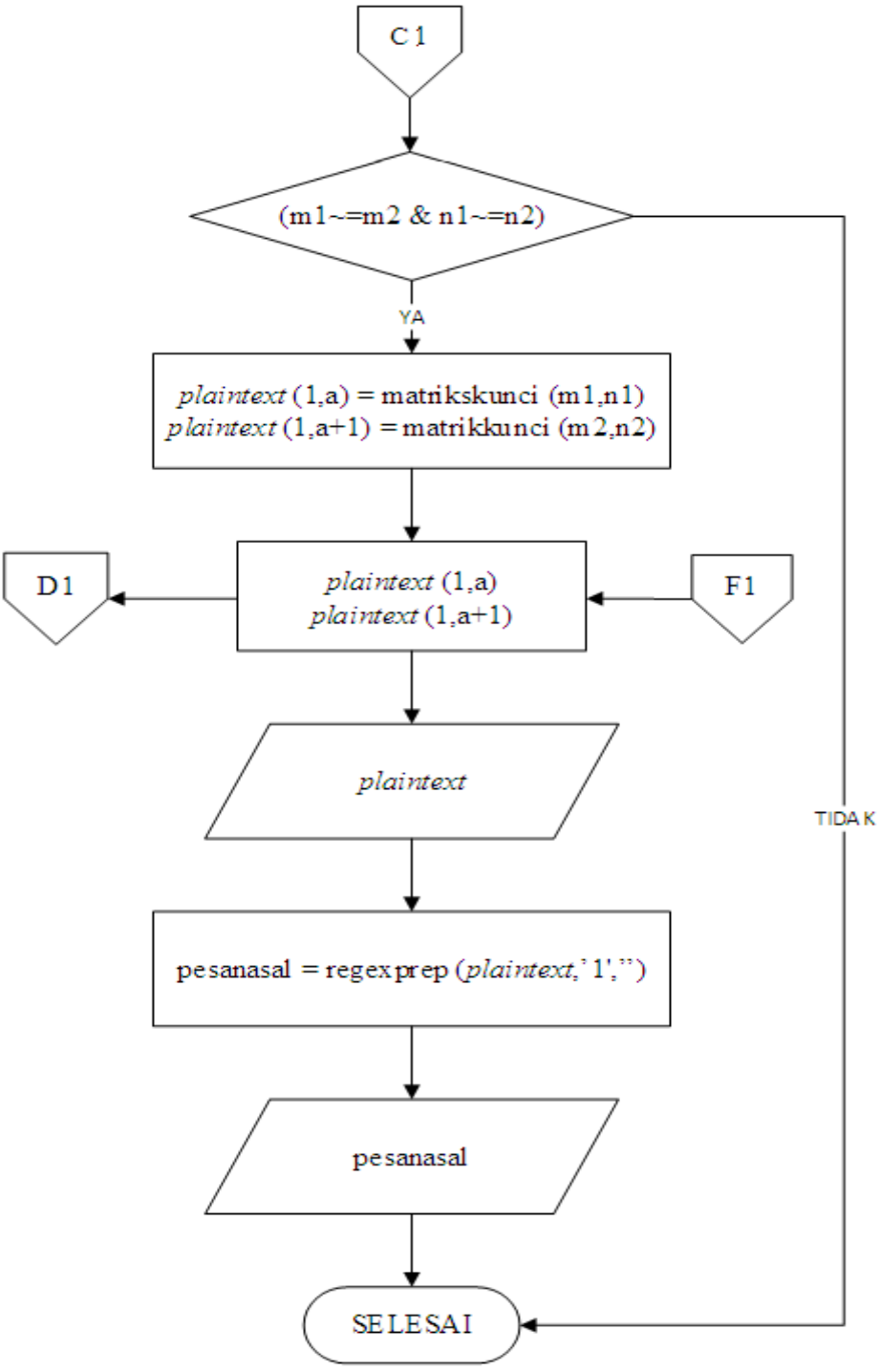
Proses dekripsi pesan menggunakan *playfair cipher* dapat dilihat pada Gambar 4.4 yang terdiri dari Gambar (a) Proses pengolahan *ciphertext* dan matriks kunci, Gambar (b) Proses dekripsi *ciphertext* dengan melihat aturan pertama dan aturan kedua, dan Gambar (c) Proses dekripsi menggunakan *playfair cipher* dengan melihat aturan ketiga dan hasil dari proses dekripsi yaitu pesan asal.



Gambar (a) Proses Pengolahan *Ciphertext* dan Matriks Kunci



Gambar (b) Proses Dekripsi *Ciphertext* dengan Melihat Aturan Pertama dan Aturan Kedua



Gambar (c) Proses Dekripsi *Ciphertext* dengan Melihat Aturan Ketiga dan Hasil Pesan Asal

Gambar 4.3 Proses Dekripsi Pesan Menggunakan *Playfair Cipher* (Gambar (a), Gambar (b), dan Gambar(c))

Contoh 4.3

Ciphertext : PEOLD3EGXG3SGCDP

Teks kunci : SERAGAM

Kunci : SERAGM

Proses dekripsinya dapat dilihat pada Tabel 4.3.

Tabel 4.3 Contoh Proses Dekripsi *Playfair Cipher*

Langkah		**Proses Dekripsi**
Pertama	:	Kunci yang digunakan harus sama dengan kunci yang digunakan pada saart enkripsi pesan.
Kedua	:	Jadikan *ciphertext* menjadi karakter berpasang-pasangan. PE OL D3 EG XG 3S GC DP
Ketiga	:	Ambil setiap pasangan huruf dan ikuti syarat dekripsi *playfair cipher* untuk memperoleh pesan asal (*plaintext*). Maka diperoleh PE : NA OL : NT D3 : I␣ EG : SA XG : YA 3S : ␣A GC : MB DP : IL Keterangan: tanda "␣" adalah spasi

Jadi, *plaintext* asalnya yaitu NANTI ␣SAYA ␣AMBIL atau NANTI SAYA AMBIL.

2. Enkripsi dan Dekripsi Pesan Menggunakan *Caesar Cipher*

a. Membuat Kunci Pergeseran

Kunci pergeseran dalam *caesar cipher* ditentukan dengan menggunakan operasi modulo. Terlebih dahulu, tentukan angka pergeseran yang diinginkan. Setelah itu, dilakukan operasi modulo 36 pada angka yang telah ditentukan. Hasilnya itulah yang digunakan untuk melakukan pergeseran.

Contoh 4.4

1) Misalkan angka pergeserannya 4. Maka

$$kunci = 4 \; mod \; 36 = 4$$

Jadi kunci pergeserannya yaitu sebanyak 4 pergeseran.

2) Angka pergeserannya yaitu 46.

$$kunci = 46 \; mod \; 36 = 10$$

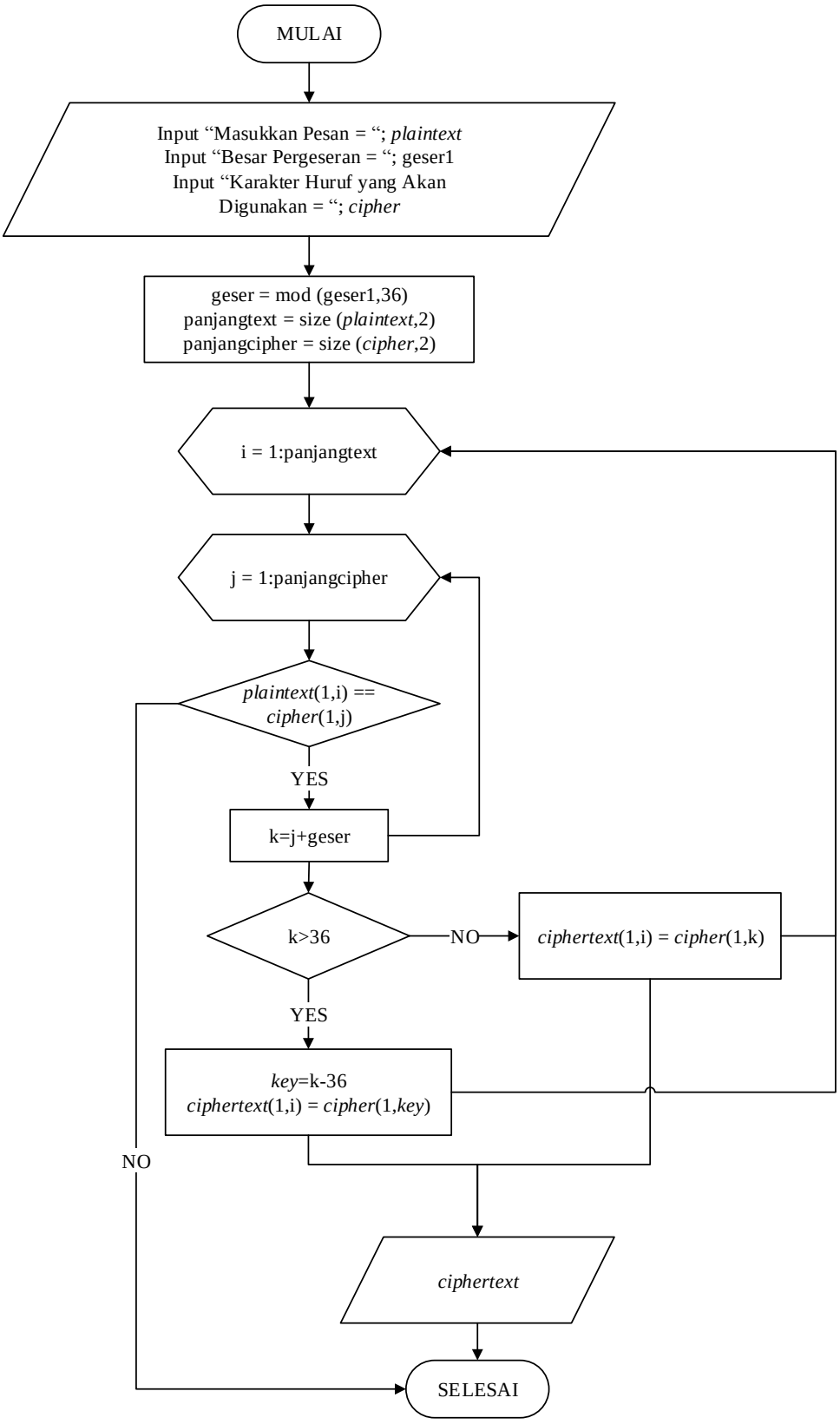
Jadi kunci pergeserannya sebanyak 10 pergeseran.

b. Proses Enkripsi

Proses enkripsi dilakukan dengan terlebih dahulu membuat kunci pergeseran untuk menentukan besar pergeseran yang akan dilakukan, yaitu dengan cara $kunci = geser(mod \; 36)$. Setelah itu penentuan *ciphertext* dengan kondisi sebagaimana pada persamaan (4.2), di mana *C* adalah *ciphertext* dan *k* adalah hasil penjumlahan letak kolom karakter *plaintext* pada karakter yang digunakan.

$$C(1,k) = \begin{cases} k-36 & ,k > 36 \\ k & ,k\ lainnya \end{cases} \quad (4.2)$$

Berdasarkan persamaan (4.2), $C(1,k)$ menjelaskan bahwa hasil dari *ciphertext* yaitu karakter yang berada pada baris pertama kolom ke-*k* pada karakter yang telah ditentukan (lihat Tabel 4.1). Proses enkripsi pesan menggunakan *caesar cipher* dapat dilihat pada gambar 4.5.



Gambar 4.5 Proses Enkripsi Pesan dengan *Caesar Cipher*

Contoh 4.5

Plaintext : ADA HAL PENTING YANG INGIN KUSAMPAIKAN BESOK PAGI

Besar pergeseran : 5

Proses enkripsinya dapat dilihat pada Tabel 4.4.

Tabel 4.4 Contoh Proses Enkripsi *Caesar Cipher*

Langkah		**Proses Enkripsi**
Pertama	:	Terlebih dahulu tentukan kunci pergeseran dengan menggunakan modulo. Kunci pergeseran = 5 mod 36 = 5 Jadi, kunci pergeserannya sebanyak 5 pereseran
Kedua	:	Perhatikan *plaintext* dan lihat berada dihuruf keberapa pada karakter yang digunakan (Tabel 4.1). Selanjutnya posisi *plaintext* pada Tabel 4.1 dijumlahkan dengan kunci pergeseran. $A = 11 + 5 = 16$ $D = 14 + 5 = 19$ $A = 11 + 5 = 16$ $spasi = 1 + 5 = 6$ $H = 18 + 5 = 24$ $A = 11 + 5 = 16$ $L = 22 + 5 = 27$ $spasi = 1 + 5 = 6$

$$P = 26 + 5 = 31$$

$$E = 15 + 5 = 20$$

$$N = 24 + 5 = 29$$

$$T = 30 + 5 = 35$$

$$I = 19 + 5 = 24$$

$$N = 24 + 5 = 29$$

$$G = 17 + 5 = 22$$

$$spasi = 1 + 5 = 6$$

$$Y = 35 + 5 = 40$$

$$A = 11 + 5 = 16$$

$$N = 24 + 5 = 29$$

$$G = 17 + 5 = 22$$

$$spasi = 1 + 5 = 6$$

$$I = 19 + 5 = 24$$

$$N = 24 + 5 = 29$$

$$G = 17 + 5 = 22$$

$$I = 19 + 5 = 24$$

$$N = 24 + 5 = 29$$

$$spasi = 1 + 5 = 6$$

$$K = 21 + 5 = 26$$

$$U = 31 + 5 = 36$$

$$S = 29 + 5 = 34$$

		$A = 11 + 5 = 16$ $M = 23 + 5 = 29$ $P = 26 + 5 = 31$ $A = 11 + 5 = 16$ $I = 19 + 5 = 24$ $K = 21 + 5 = 26$ $A = 11 + 5 = 16$ $N = 24 + 5 = 29$ $spasi = 1 + 5 = 6$ $B = 12 + 5 = 17$ $E = 15 + 5 = 20$ $S = 29 + 5 = 34$ $O = 25 + 5 = 30$ $K = 21 + 5 = 26$ $spasi = 1 + 5 = 6$ $P = 26 + 5 = 31$ $A = 11 + 5 = 16$ $G = 17 + 5 = 22$ $I = 19 + 5 = 24$
Ketiga	:	Setelah dijumlahkan dengan kunci pergeseran, selanjutnya penentuan *ciphertext* yaitu dengan kondisi sebagaimana pada persamaan (4.2).

Maka diperoleh

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk D

$k = 19$

$C(1, k) = C(1,19) = I$

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk spasi

$k = 6$

$C(1, k) = C(1,6) = 5$

Untuk H

$k = 23$

$C(1, k) = C(1,23) = M$

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk L

$k = 27$

$C(1, k) = C(1,27) = Q$

Untuk spasi

$k = 6$

$C(1, k) = C(1,6) = 5$

Untuk P

$k = 31$

$C(1, k) = C(1,31) = U$

Untuk E

$k = 20$

$C(1, k) = C(1,20) = J$

Untuk N

$k = 29$

$C(1, k) = C(1,29) = S$

Untuk T

$k = 35$

$C(1, k) = C(1,35) = Y$

Untuk I

$k = 24$

$C(1, k) = C(1,24) = N$

Untuk N

$k = 29$

$C(1, k) = C(1,29) = S$

Untuk G

$k = 22$

$C(1,k) = C(1{,}22) = L$

Untuk spasi

$k = 6$

$C(1,k) = C(1{,}6) = 5$

Untuk Y

$k = 40 - 36 = 4$

$C(1,k) = C(1{,}4) = 3$

Untuk A

$k = 16$

$C(1,k) = C(1{,}16) = F$

Untuk N

$k = 29$

$C(1,k) = C(1{,}29) = S$

Untuk G

$k = 22$

$C(1,k) = C(1{,}22) = L$

Untuk spasi

$k = 6$

$C(1,k) = C(1{,}6) = 5$

Untuk I

$k = 24$

$C(1,k) = C(1{,}24) = N$

Untuk N

$k = 29$

$C(1, k) = C(1,29) = S$

Untuk G

$k = 22$

$C(1, k) = C(1,22) = L$

Untuk I

$k = 24$

$C(1, k) = C(1,24) = N$

Untuk N

$k = 29$

$C(1, k) = C(1,29) = S$

Untuk spasi

$k = 6$

$C(1, k) = C(1,6) = 5$

Untuk K

$k = 26$

$C(1, k) = C(1,26) = P$

Untuk U

$k = 36$

$C(1, k) = C(1,36) = Z$

Untuk S

$k = 34$

$C(1, k) = C(1,34) = X$

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk M

$k = 28$

$C(1, k) = C(1,28) = R$

Untuk P

$k = 31$

$C(1, k) = C(1,31) = U$

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk I

$k = 24$

$C(1, k) = C(1,24) = N$

Untuk K

$k = 26$

$C(1, k) = C(1,26) = P$

Untuk A

$k = 16$

$C(1,k) = C(1,16) = F$

Untuk N

$k = 29$

$C(1,k) = C(1,29) = S$

Untuk spasi

$k = 6$

$C(1,k) = C(1,6) = 5$

Untuk B

$k = 17$

$C(1,k) = C(1,17) = G$

Untuk E

$k = 20$

$C(1,k) = C(1,20) = J$

Untuk S

$k = 34$

$C(1,k) = C(1,34) = X$

Untuk O

$k = 30$

$C(1,k) = C(1,30) = T$

Untuk K

$k = 26$

$C(1,k) = C(1,26) = P$

Untuk spasi

$k = 6$

$C(1, k) = C(1,6) = 5$

Untuk P

$k = 31$

$C(1, k) = C(1,31) = U$

Untuk A

$k = 16$

$C(1, k) = C(1,16) = F$

Untuk G

$k = 22$

$C(1, k) = C(1,22) = L$

Untuk I

$k = 24$

$C(1, k) = C(1,24) = N$

Jadi *ciphertextnya* yaitu

FIF5MFQ5UJSYNSL53FSL5NSLNS5PZXFRUFNPFS5GJXTP5

UFLN

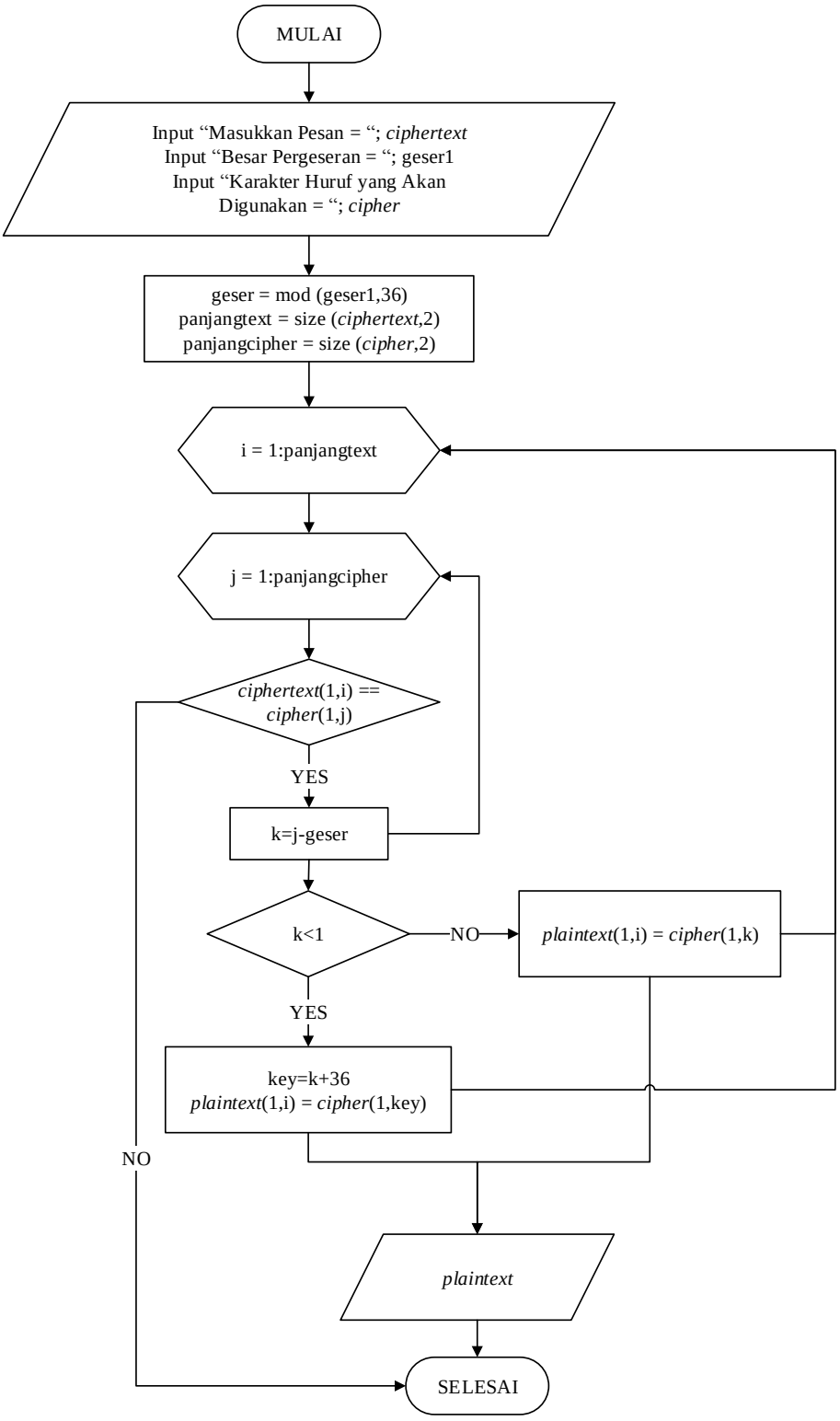
c. Proses Dekripsi

Penentuan kunci pergeseran pada proses dekripsi ini sama dengan yang dilakukan pada proses enkripsi, dan penentuan *plaintext* atau pesan asal yaitu dengan cara kondisi sebagaimana pada persamaan (4.3), di mana *l* adalah hasil

dari pengurangan letak kolom karakter *ciphertext* pada karakter yang digunakan dengan kunci pergeseran.

$$P(1,l) = \begin{cases} l+36 & ,l < 1 \\ l & ,k\ lainnya \end{cases} \quad (4.3)$$

Berdasarkan persamaan (4.3), $D(1,l)$ menjelaskan bahwa hasil dari *plaintext* yaitu karakter yang berada pada baris pertama kolom ke-l pada karakter yang telah ditentukan (lihat Tabel 4.1). Proses dekripsi pesan menggunakan *caesar cipher* dapat dilihat pada Gambar 4.6.



Gambar 4.6 Proses Dekripsi dengan *Caesar Cipher*

Contoh 4.6

Misalkan *ciphertext* yang akan didekripsi yaitu hasil enkripsi dari Contoh 4.5 dengan jumlah pergeseran yang sama. Proses dekripsinya dapat dilihat pada Tabel 4.5.

Tabel 4.5 Contoh Proses Dekripsi *Caesar Cipher*

Langkah		**Proses Dekripsi**
Pertama	:	Cara menentukan kunci pergeseran untuk proses dekripsi sama pada proses enkripsi. Kunci pergeseran = 5 mod 36 = 5 Jadi, kunci pergeserannya sebanyak 5 pereseran
Kedua	:	Langkah kedua pada proses dekripsi agak berbeda denga proses enkripsi. Jika pada proses enkripsi posisi *plaintext* dijumlahkna dengan kunci pergeseran, maka pada proses di sini posisi *ciphertext* dikurangkan denga kunci pergeseran. Hasilnya sebagai berikut $\mathrm{F} = 16 - 5 = 11$ $\mathrm{I} = 19 - 5 = 14$ $\mathrm{F} = 16 - 5 = 11$ $5 = 6 - 5 = 1$ $\mathrm{M} = 23 - 5 = 18$ $\mathrm{F} = 16 - 5 = 11$ $\mathrm{Q} = 27 - 5 = 22$ $5 = 6 - 5 = 1$

$$U = 31 - 5 = 26$$

$$J = 20 - 5 = 15$$

$$S = 29 - 5 = 24$$

$$Y = 35 - 5 = 30$$

$$N = 24 - 5 = 19$$

$$S = 29 - 5 = 24$$

$$L = 22 - 5 = 17$$

$$5 = 6 - 5 = 1$$

$$3 = 4 - 5 = -1$$

$$F = 16 - 5 = 11$$

$$S = 29 - 5 = 24$$

$$L = 22 - 5 = 17$$

$$5 = 6 - 5 = 1$$

$$N = 24 - 5 = 19$$

$$S = 29 - 5 = 24$$

$$L = 22 - 5 = 17$$

$$N = 24 - 5 = 19$$

$$S = 29 - 5 = 24$$

$$5 = 6 - 5 = 1$$

$$P = 26 - 5 = 21$$

$$Z = 36 - 5 = 31$$

$$X = 34 - 5 = 29$$

		$F = 16 - 5 = 11$ $R = 28 - 5 = 23$ $U = 31 - 5 = 26$ $F = 16 - 5 = 11$ $N = 24 - 5 = 19$ $P = 26 - 5 = 21$ $F = 16 - 5 = 11$ $S = 29 - 5 = 24$ $5 = 6 - 5 = 1$ $G = 17 - 5 = 12$ $J = 20 - 5 = 15$ $X = 34 - 5 = 29$ $T = 30 - 5 = 25$ $P = 26 - 5 = 21$ $5 = 6 - 5 = 1$ $U = 31 - 5 = 26$ $F = 16 - 5 = 11$ $L = 22 - 5 = 17$ $N = 24 - 5 = 19$
Ketiga	:	Setelah dikurangkan dengan kunci pergeseran, selanjutnya penentuan *plaintext* yaitu dengan kondisi sebagaimana pada persamaan (4.3).

Maka diperoleh

Untuk F

$k = 11$

$P(1, k) = P(1,11) = A$

Untuk I

$k = 14$

$P(1, k) = P(1,14) = D$

Untuk F

$k = 11$

$P(1, k) = P(1,11) = A$

Untuk 5

$k = 1$

$P(1, k) = P(1,1) = spasi$

Untuk M

$k = 18$

$P(1, k) = P(1,18) = H$

Untuk F

$k = 11$

$P(1, k) = P(1,11) = A$

Untuk Q

$k = 22$

$P(1, k) = P(1,22) = L$

Untuk 5

$k = 1$

$P(1,k) = P(1,1) = spasi$

Untuk U

$k = 26$

$P(1,k) = P(1,26) = P$

Untuk J

$k = 15$

$P(1,k) = P(1,15) = E$

Untuk S

$k = 24$

$P(1,k) = P(1,24) = N$

Untuk Y

$k = 30$

$P(1,k) = P(1,30) = T$

Untuk N

$k = 19$

$P(1,k) = P(1,19) = I$

Untuk S

$k = 24$

$P(1,k) = P(1,24) = N$

Untuk L

$k = 17$

$P(1,k) = P(1,17) = G$

Untuk 5

$k = 1$

$P(1,k) = P(1,1) = spasi$

Untuk 3

$k = -1 = -1 + 36 = 35$

$P(1,k) = P(1,35) = Y$

Untuk F

$k = 11$

$P(1,k) = P(1,11) = A$

Untuk S

$k = 24$

$P(1,k) = P(1,24) = N$

Untuk L

$k = 17$

$P(1,k) = P(1,17) = G$

Untuk 5

$k = 1$

$P(1,k) = P(1,1) = spasi$

Untuk N

$k = 19$

$P(1,k) = P(1,19) = I$

Untuk S

$k = 24$

$P(1, k) = P(1,24) = N$

Untuk L

$k = 17$

$P(1, k) = P(1,17) = G$

Untuk N

$k = 19$

$P(1, k) = P(1,19) = I$

Untuk S

$k = 24$

$P(1, k) = P(1,24) = N$

Untuk 5

$k = 1$

$P(1, k) = P(1,1) = spasi$

Untuk P

$k = 21$

$P(1, k) = P(1,21) = K$

Untuk Z

$k = 31$

$P(1, k) = P(1,31) = U$

Untuk X

$k = 29$

$P(1, k) = P(1,29) = S$

Untuk F

$k = 11$

$P(1, k) = P(1,11) = A$

Untuk R

$k = 23$

$P(1, k) = P(1,23) = M$

Untuk U

$k = 26$

$P(1, k) = P(1,26) = P$

Untuk F

$k = 11$

$P(1, k) = P(1,11) = A$

Untuk N

$k = 19$

$P(1, k) = P(1,19) = I$

Untuk P

$k = 21$

$P(1, k) = P(1,21) = K$

Untuk F

$k = 11$

$P(1,k) = P(1,11) = A$

Untuk S

$k = 24$

$P(1,k) = P(1,24) = N$

Untuk 5

$k = 1$

$P(1,k) = P(1,1) = spasi$

Untuk G

$k = 12$

$P(1,k) = P(1,12) = B$

Untuk J

$k = 15$

$P(1,k) = P(1,15) = E$

Untuk X

$k = 29$

$P(1,k) = P(1,29) = S$

Untuk T

$k = 25$

$P(1,k) = P(1,25) = O$

Untuk P

$k = 21$

$P(1,k) = P(1,21) = K$

Untuk 5

$k = 1$

$P(1,k) = P(1,1) = spasi$

Untuk U

$k = 26$

$P(1,k) = P(1,26) = P$

Untuk F

$k = 11$

$P(1,k) = P(1,11) = A$

Untuk L

$k = 17$

$P(1,k) = P(1,17) = G$

Untuk N

$k = 19$

$P(1,k) = P(1,19) = I$

Jadi pesan asal (*plaintext*) yang ingin disampaikan yaitu

ADA HAL PENTING YANG INGIN KUSAMPAIKAN BESOK PAGI

3. Penyisipan Pesan pada Citra

a. Mengubah Karakter ke ASCII

Bentuk karakter pesan yang dimaksud di sini yaitu huruf kapital A-Z, angka 1-9, dan tanda spasi. Pesan terlebih dahulu diubah ke dalam bentuk

ASCII agar dapat dilakukan proses penyisipan. Adapun bentuk ASCII dari karakter yang digunakan dapat dilihat pada Tabel 4.6.

Tabel 4.6 Bentuk ASCII Karakter

KARAKTER	ASCII	KARAKTER	ASCII
SPASI	32	I	73
1	49	J	74
2	50	K	75
3	51	L	76
4	52	M	77
5	53	N	78
6	54	O	79
7	55	P	80
8	56	Q	81
9	57	R	82
A	65	S	83
B	66	T	84
C	67	U	85
D	68	V	86
E	69	W	87
F	70	X	88
G	71	Y	89
H	72	Z	90

b. Mengubah ASCII Karakter dan Nilai Matriks Gambar ke Biner dan Sebaliknya

Pengubahan ASCII karakter dan nilai matriks gambar ke biner bertujuan agar nantinya masing-masing bit nilai biner dari ASCII karakter dapat disisipkan dalam bit terakhir setiap biner matriks gambar. Pengubahan ascii karakter dan nilai matriks gambar ke biner dapat dilihat pada persamaan (4.4).

$$biner = ascii(mod, 2) \tag{4.4}$$

Contoh 4.7

Pesan : AD

Nilai matriks citra red berukuran 8×1 :

$$\begin{bmatrix} 195 \\ 176 \\ 184 \\ 185 \\ 184 \\ 181 \\ 184 \\ 190 \end{bmatrix}$$

Perhatikan bahwa:

Pertama ubah pesan ke ASCII

A : 65

D : 68

A : 65

Selanjutnya ASCII pesan dan nilai matriks citra red di ubah ke biner (lihat Tabel 4.7 untuk biner ASCII pesan dan Tabel 4.8 untuk biner citra red). Nilai biner ditentukan dari bit terkhir atau bit paling belakang (dari bit ke-8 sampai bit ke-1).

Tabel 4.7 Contoh Pengubahan Nilai ASCII Pesan ke Biner

ASCII	**Bit ke-**	**Nilai Bit**	**Sisa Nilai**	**Nilai Biner**
A=65	8	$65\ mod\ 2 = 1$	$\frac{65-1}{2} = \frac{64}{2}$ $= 32$	01000001
	7	$32\ mod\ 2 = 0$	$\frac{32-0}{2} = \frac{32}{2}$ $= 16$	

	6	$16\ mod\ 2 = 0$	$\frac{16-0}{2} = \frac{16}{2}$ $= 8$	
	5	$8\ mod\ 2 = 0$	$\frac{8-0}{2} = \frac{8}{2} = 4$	
	4	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	
D=68	8	$68\ mod\ 2 = 0$	$\frac{68-0}{2} = \frac{68}{2}$ $= 34$	
	7	$34\ mod\ 2 = 0$	$\frac{34-0}{2} = \frac{34}{2}$ $= 17$	
	6	$17\ mod\ 2 = 1$	$\frac{17-1}{2} = \frac{16}{2}$ $= 8$	01000100
	5	$8\ mod\ 2 = 0$	$\frac{8-0}{2} = \frac{8}{2} = 4$	
	4	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	

	1	0	0	
A=65	8	$65\ mod\ 2 = 1$	$\frac{65-1}{2} = \frac{64}{2}$ $= 32$	01000001
	7	$32\ mod\ 2 = 0$	$\frac{32-0}{2} = \frac{32}{2}$ $= 16$	
	6	$16\ mod\ 2 = 0$	$\frac{16-0}{2} = \frac{16}{2}$ $= 8$	
	5	$8\ mod\ 2 = 0$	$\frac{8-0}{2} = \frac{8}{2} = 4$	
	4	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	

Tabel 4.8 Contoh Pengubahan Nilai Matriks Citra Red ke Biner

Nilai Matriks Citra Red	**Bit ke-**	**Nilai Bit**	**Sisa Nilai**	**Nilai Biner**

195	8	$195\ mod\ 2 = 1$	$\frac{195-1}{2}$ $= \frac{194}{2} = 97$	11000011
	7	$97\ mod\ 2 = 1$	$\frac{97-1}{2} = \frac{96}{2}$ $= 48$	
	6	$48\ mod\ 2 = 0$	$\frac{48-0}{2} = \frac{48}{2}$ $= 24$	
	5	$24\ mod\ 2 = 0$	$\frac{24-0}{2} = \frac{24}{2}$ $= 12$	
	4	$12\ mod\ 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	
	3	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	2	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
176	8	$176\ mod\ 2 = 0$	$\frac{176-0}{2}$ $= \frac{176}{2} = 88$	10110000
	7	$88\ mod\ 2 = 0$	$\frac{88-0}{2} = \frac{88}{2}$ $= 44$	

	6	$44\ mod\ 2 = 0$	$\frac{44-0}{2} = \frac{44}{2}$ $= 22$	
	5	$22\ mod\ 2 = 0$	$\frac{22-0}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
184	8	$184\ mod\ 2 = 0$	$\frac{184-0}{2}$ $= \frac{184}{2} = 92$	10111000
	7	$92\ mod\ 2 = 0$	$\frac{92-0}{2} = \frac{92}{2}$ $= 46$	
	6	$46\ mod\ 2 = 0$	$\frac{46-0}{2} = \frac{46}{2}$ $= 23$	
	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	

	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
185	8	$185\ mod\ 2 = 1$	$\frac{185-1}{2}$ $= \frac{184}{2} = 92$	10111001
	7	$92\ mod\ 2 = 0$	$\frac{92-0}{2} = \frac{92}{2}$ $= 46$	
	6	$46\ mod\ 2 = 0$	$\frac{46-0}{2} = \frac{46}{2}$ $= 23$	
	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	

	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
184	8	$184\ mod\ 2 = 0$	$\frac{184-0}{2}$ $= \frac{184}{2} = 92$	10111000
	7	$92\ mod\ 2 = 0$	$\frac{92-0}{2} = \frac{92}{2}$ $= 46$	
	6	$46\ mod\ 2 = 0$	$\frac{46-0}{2} = \frac{46}{2}$ $= 23$	
	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
181	8	$181\ mod\ 2 = 1$	$\frac{181-1}{2}$ $= \frac{180}{2} = 90$	10110101

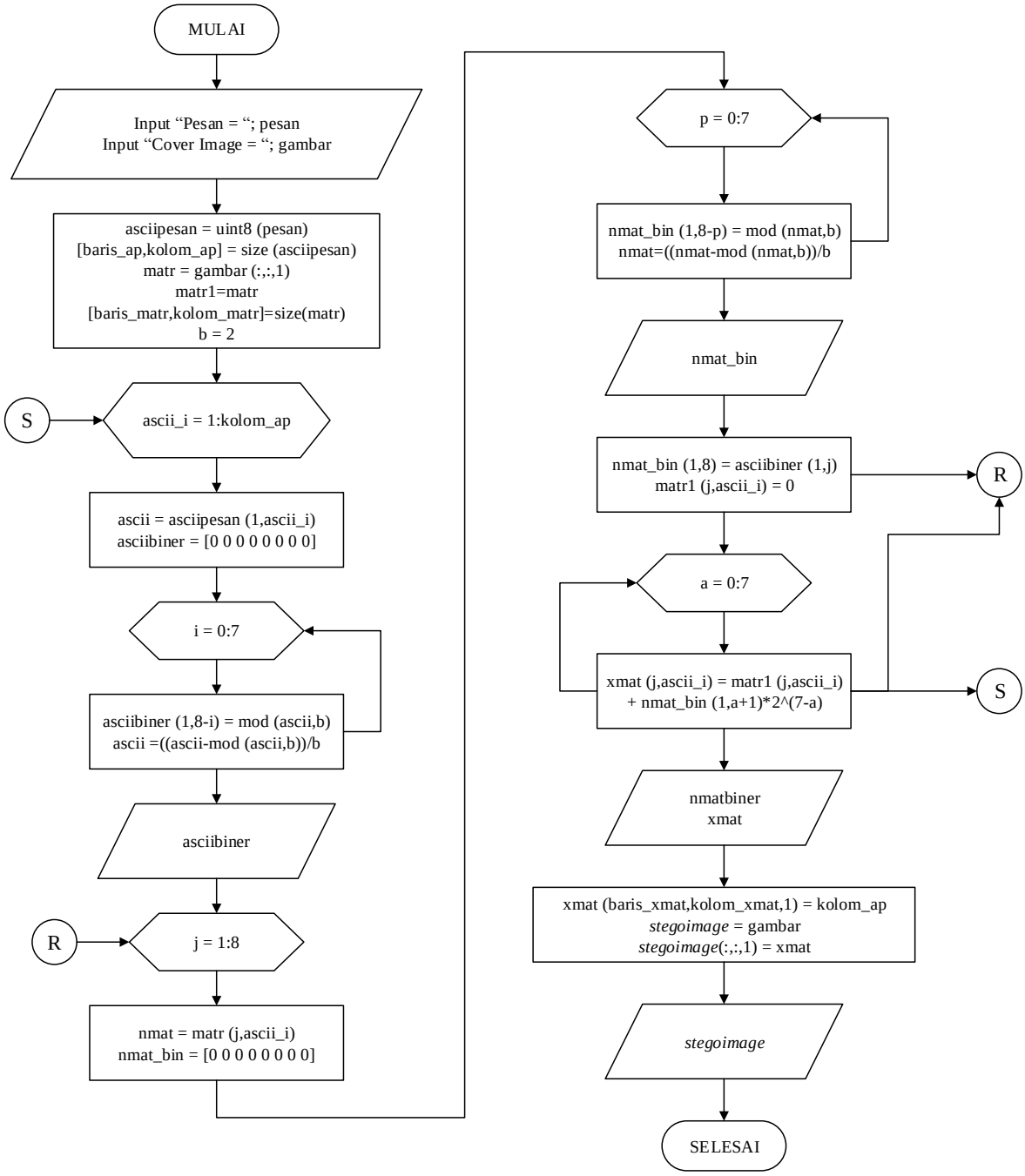
	7	$90\ mod\ 2 = 0$	$\frac{90-0}{2} = \frac{90}{2}$ $= 45$	
	6	$45\ mod\ 2 = 1$	$\frac{45-1}{2} = \frac{44}{2}$ $= 22$	
	5	$22\ mod\ 2 = 0$	$\frac{22-0}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
184	8	$184\ mod\ 2 = 0$	$\frac{184-0}{2}$ $= \frac{184}{2} = 92$	
	7	$92\ mod\ 2 = 0$	$\frac{92-0}{2} = \frac{92}{2}$ $= 46$	10111000
	6	$46\ mod\ 2 = 0$	$\frac{46-0}{2} = \frac{46}{2}$ $= 23$	

	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
190	8	$190\ mod\ 2 = 0$	$\frac{190-0}{2}$ $= \frac{190}{2} = 95$	
	7	$95\ mod\ 2 = 1$	$\frac{95-1}{2} = \frac{94}{2}$ $= 47$	
	6	$47\ mod\ 2 = 1$	$\frac{47-1}{2} = \frac{46}{2}$ $= 23$	10111110
	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	

	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$

c. Proses Penyisipan Pesan (*Embedding*)

Pada proses penyisipan ini digunakan salah satu matode steganografi yaitu metode *LSB (Least Significant Bit)*. Metode ini menyisipkan pesan dengan cara mengganti bit terakhir dari matriks gambar dengan bit biner pesan. Sehingga perubahan yang terjadi pada gambar tidak terlalu berbeda dengan gambar sebelum disisipkan karena nilai matriks gambar berubah 1 bit lebih tinggi atau 1 bit lebih rendah. Lebih lanjut, proses penyisipan tersebut dapat dilihat pada Gambar 4.7.



Gambar 4.7 Proses Penyisipan Pesan

Contoh 4.8

Pesan : A

ASCII pesan : 65

Nilai matriks citra red berukuran 8×1 :

$$\begin{bmatrix} 195 \\ 176 \\ 184 \\ 185 \\ 184 \\ 181 \\ 184 \\ 190 \end{bmatrix}$$

Proses penyisipannya dapat dilihat pada Tabel 4.9

Tabel 4.9 Contoh Proses Penyisipan Pesan

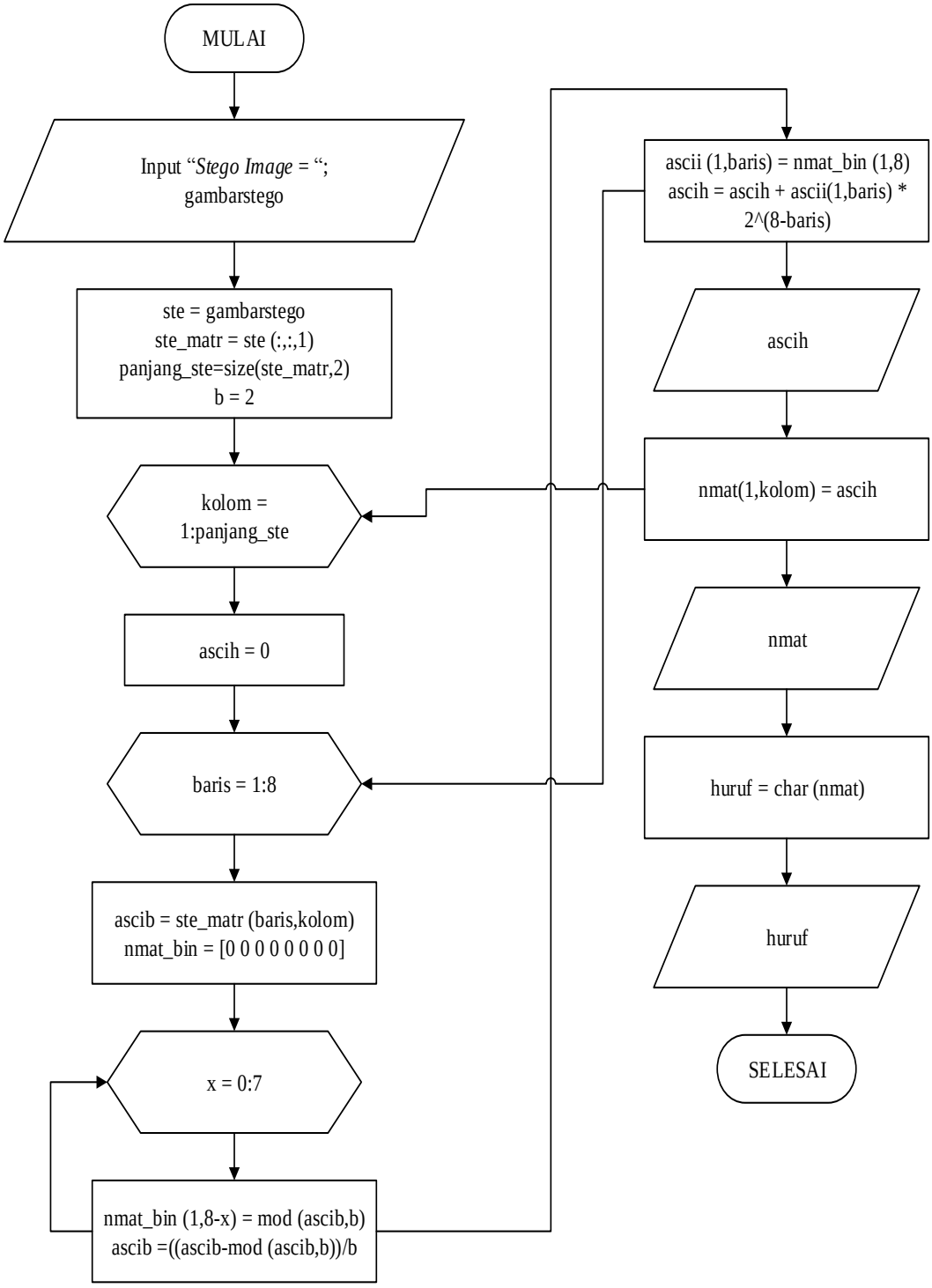
Langkah		**Proses Penyisipan Pesan**
Pertama	:	Mengubah ASCII karakter dan nilai matriks citra ke biner. Perubahan ASCII karakter dan nilai matriks citra ke biner dapat dilihat pada Tabel 4.7 dan Tabel 4.8
Kedua	:	Mengganti bit terakhir citra dengan bit pesan. Diketahui: - Pesan A = 65 = 01000001 - Matriks Citra Red $195 = 11000011$ $176 = 10110000$ $184 = 10111000$ $185 = 10111001$ $184 = 10111000$ $181 = 10110101$ $184 = 10111000$ $190 = 10111110$ Dengan mengganti bit terakhir citra red denga bit-bit pesan maka diperoleh:

		11000001**0** 10110001**1** 10111000**0** 10111000**0** 10111000**0** 10110100**0** 10111000**0** 10111111**1** Angka yang dicetak tebal merupakan nilai bit terakhir citra red setelah digantikan dengan bit pesan. Jadi nilai biner tersebut adalah nilai biner matriks citra red yang telah disisipkan pesan
Ketiga	:	Mengubah nilai biner matriks citra red yang telah disisipkan pesan ke bentuk desimal. ➢ $11000001\mathbf{0} = 194$ ➢ $10110001\mathbf{1} = 177$ ➢ $10111000\mathbf{0} = 184$ ➢ $10111000\mathbf{0} = 184$ ➢ $10111000\mathbf{0} = 184$ ➢ $10110100\mathbf{0} = 180$ ➢ $10111000\mathbf{0} = 184$ ➢ $10111111\mathbf{1} = 191$ Nilai desimal inilah yang merupakan nilai matriks citra red yang baru atau nilai matriks citra yang telah disisipkan pesan

d. Proses Ekstraksi (*Ekstraction*)

Proses ekstraksi merupakan proses untuk mengeluarkan pesan yang disembunyikan di dalam citra. Proses ektraksi ini juga menggunakan

steganografi *LSB* seperti cara menyisipkan pesannya. Lebih lanjut, proses ekstraksi tersebut dapat dilihat pada Gambar 4.8.



Gambar 4.8 Proses Ekstraksi Pesan

Contoh 4.9

Nilai matriks citra red berukuran 8×1 :

$$\begin{bmatrix} 194 \\ 177 \\ 184 \\ 184 \\ 184 \\ 180 \\ 184 \\ 191 \end{bmatrix}$$

Proses ekstraksinya dapat dilihat pada Tabel 4.10.

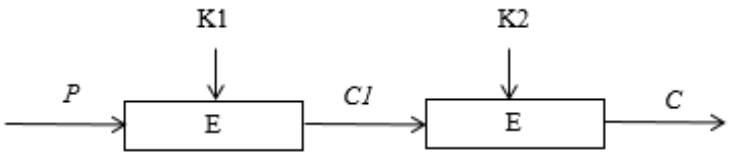
Tabel 4.10 Contoh Proses Ekstraksi

Langkah		**Proses Ekstraksi**
Pertama	:	Mengubah nilai matriks citra red ke biner. $194 = 11000010$ $177 = 10110001$ $184 = 10111000$ $184 = 10111000$ $184 = 10111000$ $180 = 10110100$ $184 = 10111000$ $191 = 10111111$
Kedua	:	Mengambil bit terakhir setiap citra (perhatikan tulisan yang dicetak tebal). $194 = 1100000\mathbf{1}$ $177 = 1011000\mathbf{1}$ $184 = 1011100\mathbf{0}$ $184 = 1011100\mathbf{0}$ $184 = 1011100\mathbf{0}$ $180 = 1011010\mathbf{0}$ $184 = 1011100\mathbf{0}$ $191 = 1011111\mathbf{1}$ Diperoleh: 01000001

		Nilai biner tersebut merupkan biner pesan yang disisipkan dalam citra.
Ketiga	:	Mengubah nilai biner pesan yang disisipkan ke bentuk desimal agar dapat diketahui pesan yang dimaksud. $01000001 = 65$ Nilai desimal inilah yang merupakan nilai bentuk ASCII dari pesan tersebut. Maka dengan melihat Tabel 4.1.1 diketahui bahwa pesan yang ingin disampaikan atau pesan yang disembunyikan tersebut berupa huruf "A".

4. Enkripsi Pesan Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Pada proses enkripsi ini digunakan gabungan dari 2 metode dalam kriptografi yaitu *playfair cipher* dan *caesar cipher*. Pesan terlebih dahulu dienkripsi menggunakan *playfair cipher* lalu hasil enkripsinya dienkripsi kembali menggunakan *caesar cipher*. Adapun model proses enkripsinya secara matematis dapat dilihat pada Gambar 4.9.



Keterangan:

E	:	Proses enkripsi pesan (*plaintext*)
P	:	*Plaintext*
$C1$	:	*Ciphertext1* (Hasil enkripsi *plaintext* mengunakan *playfair cipher*)
C	:	*Ciphertext* (Hasil enkripsi *ciphertext1* mengunakan *caesar cipher*)
K1	:	Kunci1 (Kunci enkripsi untuk *playfair cipher*)
K2	:	Kunci2 (Kunci enkripsi untuk *caesar cipher*)

Gambar 4.9 Model Enkripsi Pesan Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

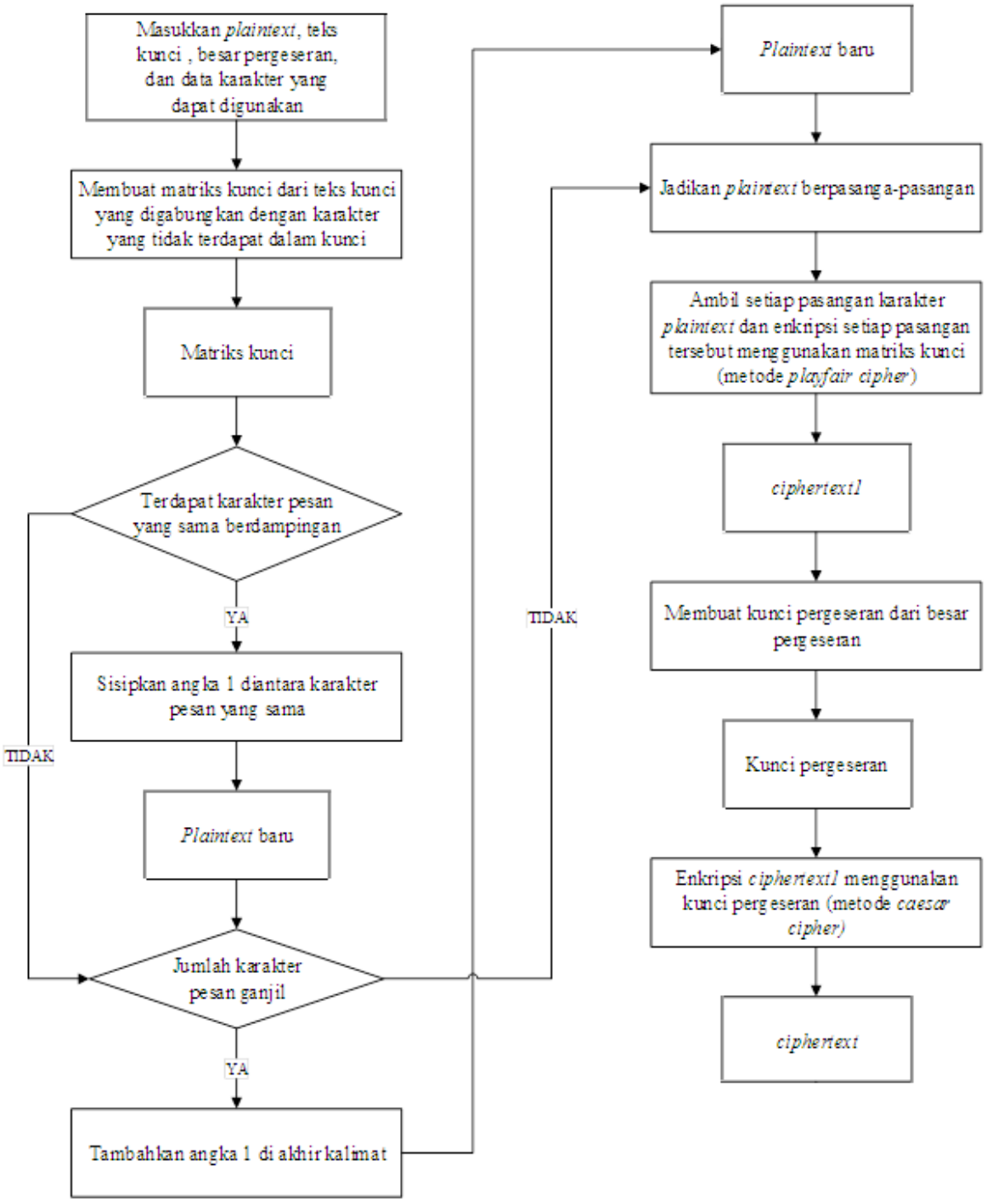
Berdasarkan Gambar 4.9, maka diperoleh model matematika proses enkripsi pesan menggunakan *playfair* cipher dan *caesar cipher* sebagaimana pada persamaan (4.5) dan persamaan (4.6), serta model matematika proses enkripsi pesan menggunakan *hybrid playfair* cipher dan *caesar cipher* ditunjukkan pada persamaan (4.6).

$$E(P, K1) = C1 \tag{4.5}$$

$$E(C1, K2) = C \tag{4.6}$$

$$E\big(E(P, K1)\big) = C \tag{4.7}$$

Adapun proses mengenkripsi pesan menggunakan *hybrid playfair* cipher dan *caesar cipher* yaitu seperti pada Gambar 4.10.



Gambar 4.10 Proses Enkripsi Pesan Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Contoh 4.10

Plaintext : TES

Teks kunci : SERAGAM

Kunci : SERAGM

Besar pergeseran : 3

Proses enkripsinya dapat dilihat pada Tabel 4.11.

Tabel 4.11 Enkripsi Pesan dengan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Langkah		**Proses Enkripsi**
Pertama	:	Karena kuncinya sama dengan kunci yang dipakai pada Contoh 4.1, maka matriks kuncinya bisa dilihat pada persamaan (4.1).
Kedua		Mengecek pada *plaintext* terdapat huruf sama yang berdekatan atau tidak, dan mengecek jumlah karakternya ganjil atau genap. Setelah diperiksa tidak terdapat huruf sama yang berdekatan. Tetapi, jumlah karakternya ganjil. Jadi diakhir kalimat ditambahkan angka 1. Diperoleh: TES1
Ketiga	:	Jadikan *plaintext* menjadi karakter berpasang-pasangan. TE S1
Keempat	:	Ambil setiap pasangan karakter dan ikuti syarat enkripsi *playfair cipher* untuk memperoleh *ciphertext1*. Maka diperoleh TE : NM S1 : E ␣ Keterangan: tanda "␣" adalah spasi

	Jadi, *ciphertext1* yaitu NME ␣
Kelima	Tentukan kunci pergeseran dengan menggunakan modulo. Kunci pergeseran = 3 mod 36 = 3 Jadi, kunci pergeserannya sebanyak 3 pereseran
Keenam	Perhatikan *ciphertext1* dan lihat berada dikolom keberapa pada karakter yang digunakan (Tabel 4.1). Selanjutnya posisi *ciphertext1* pada Tabel 4.1 dijumlahkan dengan kunci pergeseran. $N = 24 + 3 = 27$ $M = 23 + 3 = 26$ $E = 15 + 3 = 18$ $spasi = 1 + 3 = 4$
Ketujuh	Setelah dijumlahkan dengan kunci pergeseran selanjutnya penentuan *ciphertext*. Dengan menggunakan persamaan (4.2) maka diperoleh Untuk N $k = 27$ $C(1, k) = C(1{,}27) = Q$ Untuk M $k = 26$ $C(1, k) = C(1{,}26) = P$ Untuk E

$k = 18$

$C(1, k) = C(1,18) = H$

Untuk spasi

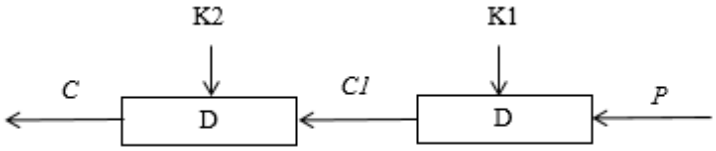
$k = 4$

$C(1, k) = C(1,4) = 3$

Jadi *ciphertext* yaitu QPH3

5. Dekripsi Pesan Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Pada proses dekripsi langkah awal yang dilakukan yaitu menggunakan metode *caesar cipher* kemudian hasil dekripsi *caesar cipher* didekripsi lagi menggunakan *playfair cipher* sehingga menghasilkan pesan asal. Model proses dekripsi secara matematis ditunjukkan pada Gambar 4.11.



Keterangan:

D	:	Proses dekripsi pesan (*plaintext*)
P	:	*Plaintext*
C	:	*Ciphertext* (Hasil dekripsi *plaintext* mengunakan *caesar cipher*)
$C1$	:	*Ciphertext1* (Hasil dekripsi *ciphertext1* mengunakan *playfair cipher*)
K1	:	Kunci1 (Kunci dekripsi untuk *playfair cipher*)
K2	:	Kunci2 (Kunci dekripsi untuk *caesar cipher*)

Gambar 4.11 Model Dekripsi Pesan Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Berdasarkan Gambar 4.11, diperoleh model matematika proses dekripsi pesan menggunakan *caesar* cipher dan *playfair cipher* sebagaimana pada persamaan (4.8) dan persamaan (4.9), serta model matematika proses dekripsi pesan

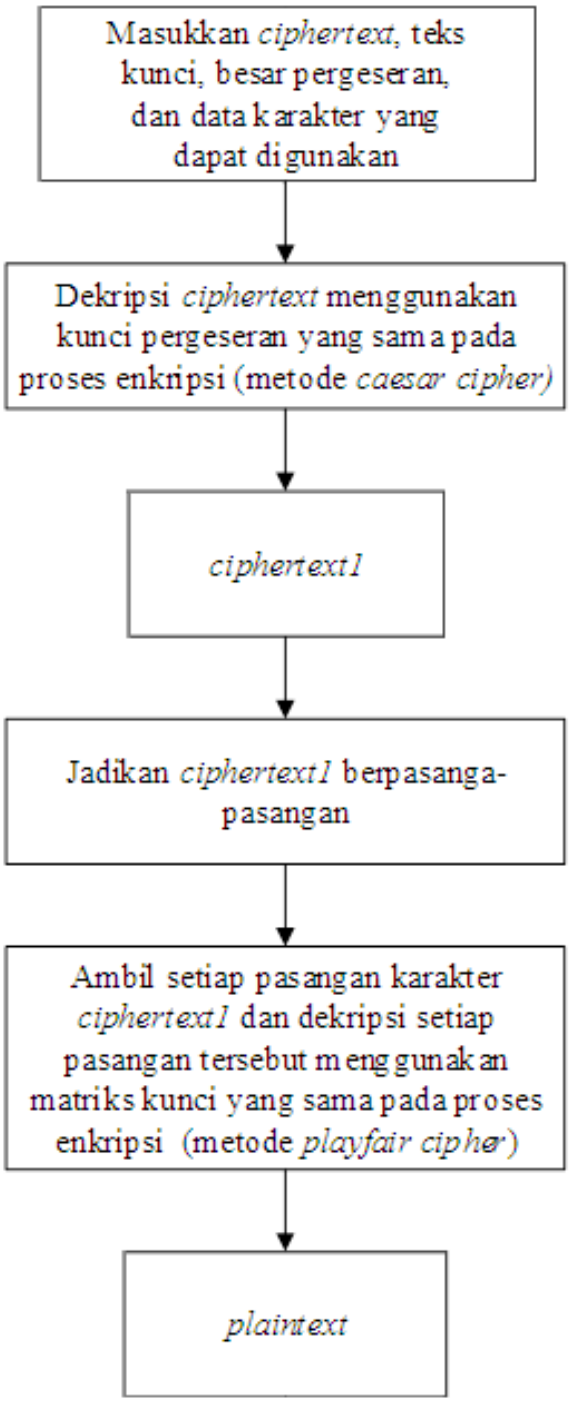
menggunakan *hybrid playfair* cipher dan *caesar cipher* ditunjukkan pada persamaan (4.10)

$$D(C, K2) = C1 \tag{4.8}$$

$$D(C1, K1) = P \tag{4.9}$$

$$D(D(C, K2), K1) = P \tag{4.10}$$

Proses Dekripsi pesan menggunakan *hybrid playfair cipher* dan *caesar cipher* dapat dilihat pada Gambar 4.12.



Gambar 4.12 Proses Dekripsi Pesan Menggunakan *Hybrid Playfair* C*ipher* dan C*aesar Cipher*

Contoh 4.11

Ciphertext : QPH3

Teks kunci : SERAGAM

Kunci : SERAGM

Besar pergeseran : 3

Proses dekripsinya dapat dilihat pada Tabel 4.12.

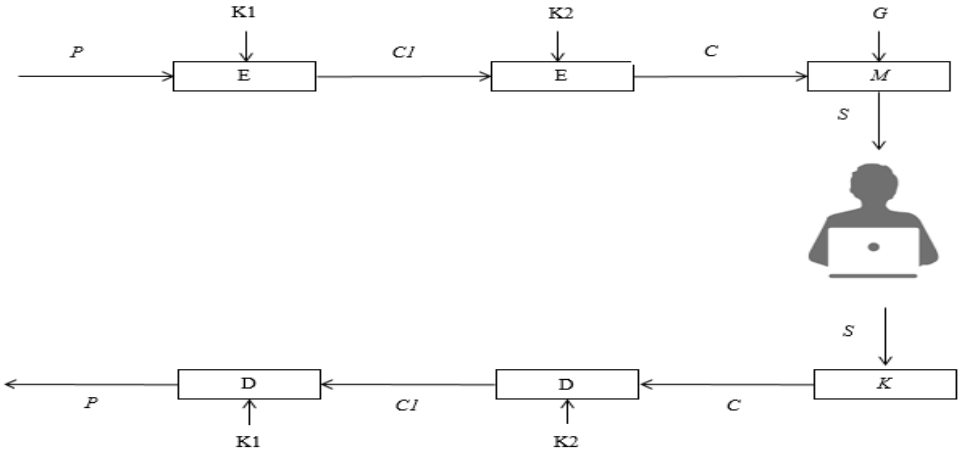
Tabel 4.12 Dekripsi Pesan dengan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Langkah	**Proses Dekripsi**
Pertama	Kunci pergeseran yang akan digunakan harus sama dengan kunci pergeseran yang digunakan pada saat enkripsi. Jadi kunci pergeserannya sebanyak 3 pergeseran
Kedua	Selanjutnya posisi *ciphertext* pada Tabel 4.1.1 dikurangkan dengan kunci pergeseran. $Q = 27 - 3 = 24$ $P = 26 - 3 = 23$ $H = 18 - 3 = 15$ $3 = 4 - 3 = 1$
Ketiga	Setelah dikurangkan dengan kunci pergeseran, selanjutnya penentuan *ciphertext1*.) Dengan menggunakan persamaan (4.3) maka diperoleh Untuk Q $l = 24$ $P(1, l) = P(1,24) = N$

		Untuk P $l = 23$ $P(1, l) = P(1{,}23) = M$ Untuk H $l = 15$ $P(1, k) = P(1{,}15) = E$ Untuk 3 $l = 1$ $P(1, l) = P(1{,}1) = spasi$ Jadi *ciphertext1* yaitu NME ␣ Keterangan: tanda "␣" adalah spasi
Keempat	:	Matriks kunci yang akan digunakan harus sama dengan matriks kunci yang digunakaan saat enkripsi. Jadi matriks kuncinya dapat dilihat pada persamaan (4.1).
Kelima		Jadikan *ciphertext1* menjadi karakter berpasang-pasangan. NM E ␣
Keenam	:	Ambil setiap pasangan huruf dan ikuti syarat dekripsi *playfair cipher* untuk memperoleh *plaintext*. Maka diperoleh NM : TE E ␣ : S1 Keterangan: tanda "␣" adalah spasi Jadi, *ciphertext1* yaitu TES1 atau TES

6. Penyisipan Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Penyisipan pesan pada citra merupakan metode steganografi yang memanfaatkan media citra untuk menyembunyikan pesan di dalamnya. Sehingga pengamat tidak mengetahui bahwa di dalam citra tersebut terdapat suatu pesan atau informasi. Pada proses penyisipan ini, hal pertama yang dilakukan yaitu enkripsi pesan menggunakan *hybrid playfair cipher* dan *caesar cipher*. Kemudian hasil dari enkripsi tersebut disembunyikan atau disisipkan ke dalam citra. Secara matematis, proses tersebut dapat dilihat pada Gambar 4.13.



Keterangan:

E	:	Proses enkripsi pesan (*plaintext*)
P	:	*Plaintext*
$C1$	:	*Ciphertext1* (Hasil enkripsi *plaintext* mengunakan *playfair cipher*)
C		*Ciphertext* (Hasil enkripsi *ciphertext1* mengunakan *caesar cipher*)
K1	:	Kunci1 (Kunci enkripsi untuk *playfair cipher*)
K2	:	Kunci2 (Kunci enkripsi untuk *caesar cipher*)
M	:	Proses penyisipan pesan
G	:	Media penyisipan pesan (*cover image*). Medianya berupa citra
S	:	Hasil dari penyisipan pesan pada citra (citra yang telah disisipkan pesan (*stego image*)).
K	:	Proses ekstraksi
D	:	Proses dekripsi pesan

Gambar 4.13 Model Penyisipan dan Ekstraksi Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Berdasarkan Gambar 4.13, maka diperoleh model matematika proses penyisipan pesan pada citra sebagaimana persamaan (4.11) dan proses ekstraksi pesan pada citra sebagaimana persamaan (4.12).

$$M(C, G) = S \tag{4.11}$$

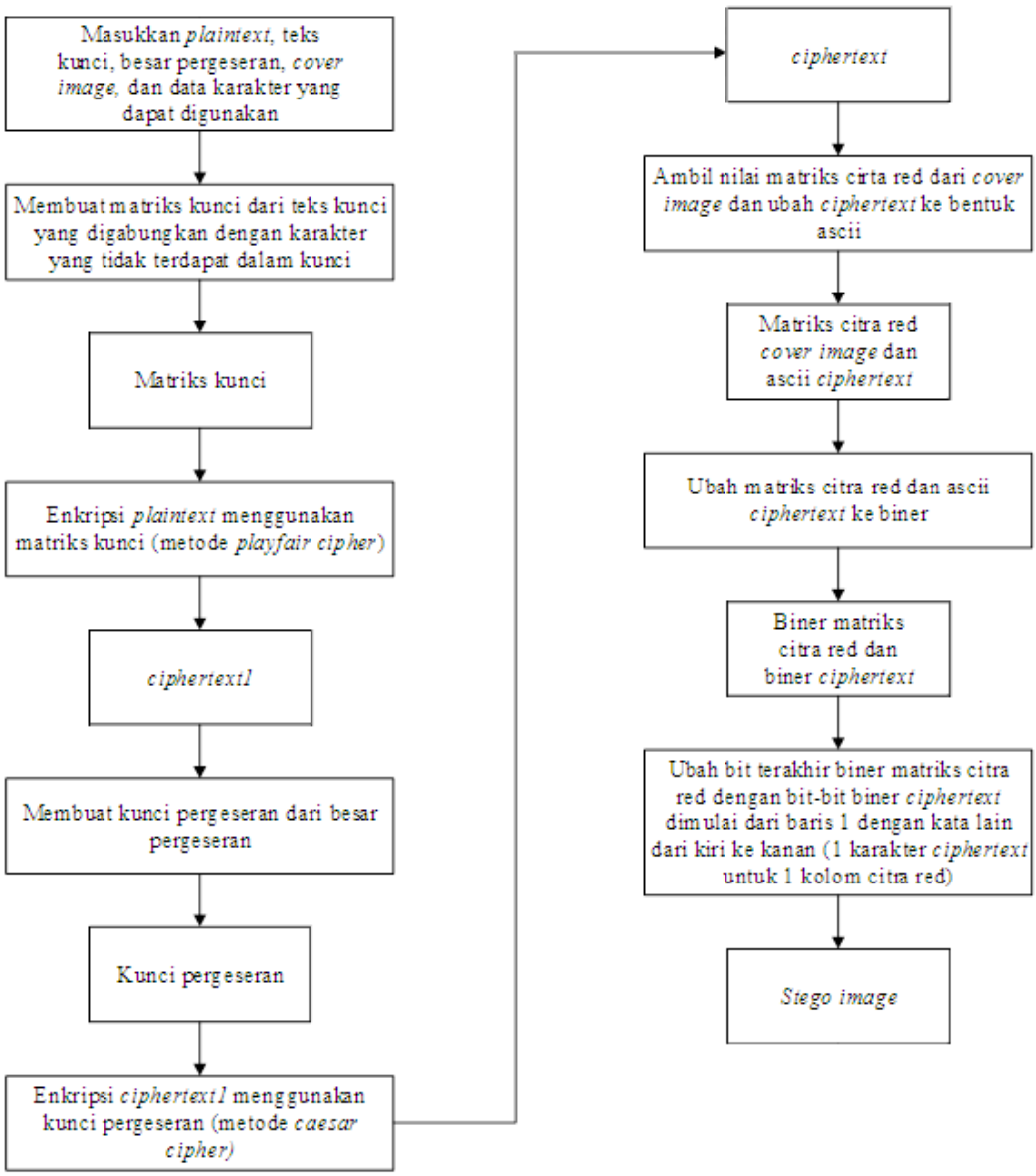
$$K(S) = C \tag{4.12}$$

Dengan mensubtitusi persamaa (4.7) ke persamaan (4.11) diperoleh model matematika proses penyisipan pesan pada citra menggunakan *hybrid playfair cipher* dan *caesar cipher* sebagaimana pada persamaan (4.13). Substitusi pula persamaan (4.12) ke persamaan (4.10) untuk memperoleh model matematika proses dekripsi pesan pada citra yang telah diekstrak dengan menggunakan *hybrid playfair cipher* dan *caesar cipher* sebagaimana ditunjukkan persamaan (4.14)

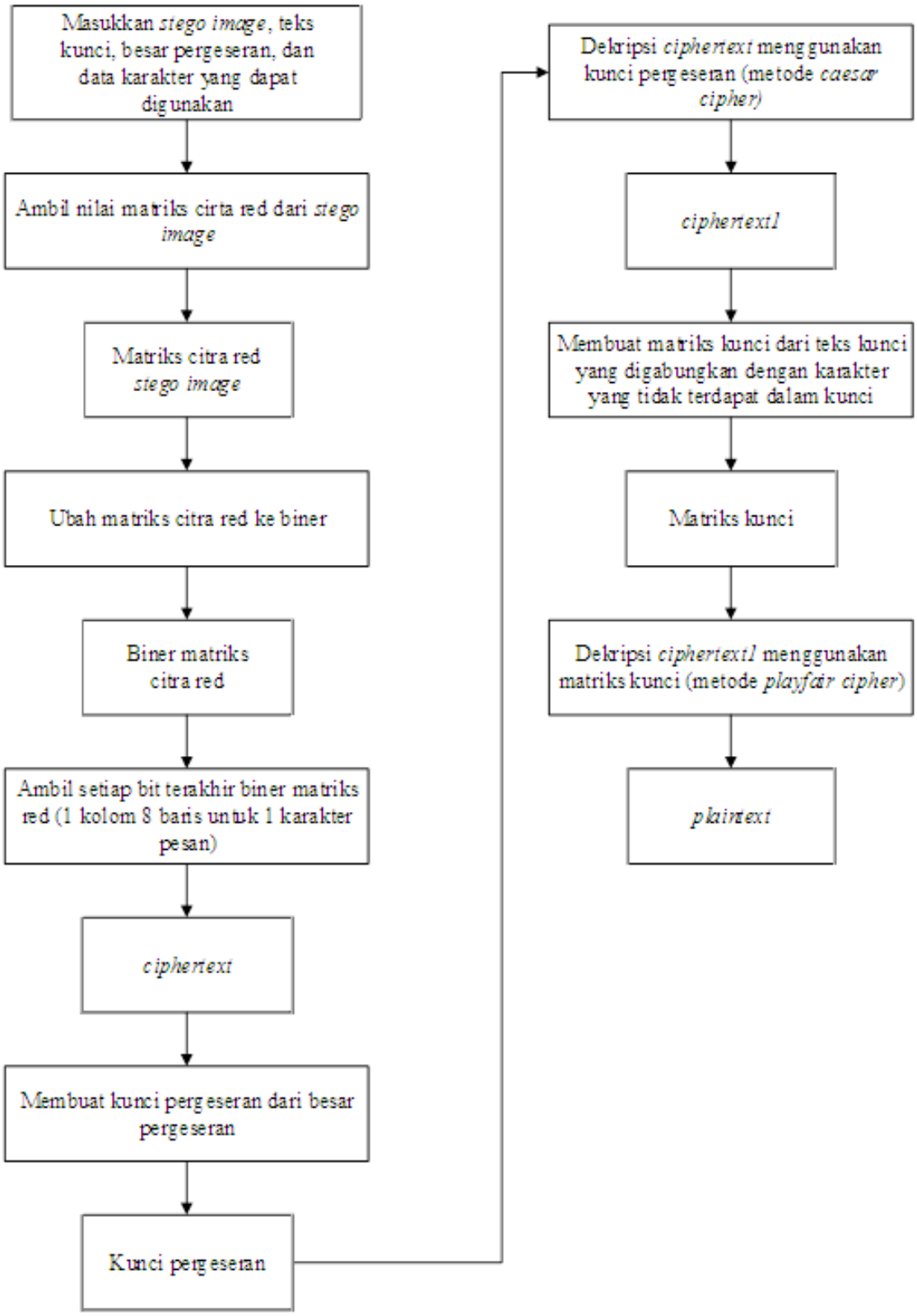
$$M(E(E(P, K1), K2), G) = S \tag{4.13}$$

$$D(D(K(S), K2), K1) = P \tag{4.14}$$

Secara rinci, proses penyisipan pesan pada citra menggunakan *hybrid playfair cipher* dan *caesar cipher* dapat dilihat pada Gambar 4.14 dan proses pengembalian ke pesan asal dapat dilihat pada Gambar 4.15.



Gambar 4.14 Proses Penyisipan Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*



Gambar 4.15 Proses Ekstraksi Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Contoh 4.12

Plaintext : TES

Teks kunci : SERAGAM

Kunci : SERAGM

Besar pergeseran : 3

Matriks Citra 8×1 pixel:

$$W = \begin{bmatrix} 195 & 68 & 200 & 195 \\ 176 & 78 & 155 & 176 \\ 184 & 195 & 24 & 184 \\ 185 & 37 & 190 & 185 \\ 184 & 176 & 174 & 184 \\ 181 & 99 & 99 & 181 \\ 184 & 35 & 84 & 184 \\ 191 & 10 & 1 & 191 \end{bmatrix}$$

Perubahan nilai matriks kolom 2 dan kolom 3 ke bentuk biner dapat dilihat pada Tabel 4.13 dan proses penyisipannya ditunjukkan pada Tabel 4.14.

Tabel 4.13 Contoh Pengubahan Nilai Matriks Citra kolom 2 dan kolom 3 ke Biner

Nilai Matriks Citra Red	**Bit ke-**	**Nilai Bit**	**Sisa Nilai**	**Nilai Biner**
68	8	$68 \; mod \; 2 = 0$	$\frac{68-0}{2} = \frac{68}{2}$ $= 34$	01000100
	7	$34 \; mod \; 2 = 0$	$\frac{34-0}{2} = \frac{34}{2}$ $= 17$	

	6	$17\ mod\ 2 = 1$	$\frac{17-1}{2} = \frac{16}{2}$ $= 8$	
	5	$8\ mod\ 2 = 0$	$\frac{8-0}{2} = \frac{8}{2} = 4$	
	4	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	
78	8	$78\ mod\ 2 = 0$	$\frac{78-0}{2} = \frac{78}{2}$ $= 39$	
	7	$39\ mod\ 2 = 1$	$\frac{39-1}{2} = \frac{38}{2}$ $= 19$	
	6	$19\ mod\ 2 = 1$	$\frac{19-1}{2} = \frac{18}{2}$ $= 9$	01001110
	5	$9\ mod\ 2 = 1$	$\frac{9-1}{2} = \frac{8}{2} = 4$	
	4	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	

	1	0	0	
195	8	$195 \; mod \; 2 = 1$	$\frac{195-1}{2}$ $= \frac{194}{2} = 97$	11000011
	7	$97 \; mod \; 2 = 1$	$\frac{97-1}{2} = \frac{96}{2}$ $= 48$	
	6	$48 \; mod \; 2 = 0$	$\frac{48-0}{2} = \frac{48}{2}$ $= 24$	
	5	$24 \; mod \; 2 = 0$	$\frac{24-0}{2} = \frac{24}{2}$ $= 12$	
	4	$12 \; mod \; 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	
	3	$6 \; mod \; 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	2	$3 \; mod \; 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	1	$1 \; mod \; 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
37	8	$37 \; mod \; 2 = 1$	$\frac{37-1}{2} = \frac{36}{2}$ $= 18$	00100101

	7	$18\ mod\ 2 = 0$	$\frac{18-0}{2} = \frac{18}{2}$ $= 9$	
	6	$9\ mod\ 2 = 1$	$\frac{9-1}{2} = \frac{8}{2} = 4$	
	5	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	4	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	3	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	2	0	0	
	1	0	0	
176	8	$176\ mod\ 2 = 0$	$\frac{176-0}{2}$ $= \frac{176}{2} = 88$	
	7	$88\ mod\ 2 = 0$	$\frac{88-0}{2} = \frac{88}{2}$ $= 44$	10110000
	6	$44\ mod\ 2 = 0$	$\frac{44-0}{2} = \frac{44}{2}$ $= 22$	
	5	$22\ mod\ 2 = 0$	$\frac{22-0}{2} = \frac{22}{2}$ $= 11$	

	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
99	8	$99\ mod\ 2 = 1$	$\frac{99-1}{2} = \frac{98}{2}$ $= 49$	01100011
	7	$49\ mod\ 2 = 1$	$\frac{49-1}{2} = \frac{48}{2}$ $= 24$	
	6	$24\ mod\ 2 = 0$	$\frac{24-0}{2} = \frac{24}{2}$ $= 12$	
	5	$12\ mod\ 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	
	4	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	3	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	

35	8	$35\ mod\ 2 = 1$	$\frac{35-1}{2} = \frac{34}{2}$ $= 17$	00100011
	7	$17\ mod\ 2 = 1$	$\frac{17-1}{2} = \frac{16}{2}$ $= 8$	
	6	$8\ mod\ 2 = 0$	$\frac{8-0}{2} = \frac{8}{2} = 4$	
	5	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	4	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	3	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	2	0	0	
	1	0	0	
10	8	$10\ mod\ 2 = 0$	$\frac{10-0}{2} = \frac{10}{2}$ $= 5$	00001010
	7	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	6	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	5	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	4	0	0	
	3	0	0	

	2	0	0	
	1	0	0	
200	8	$200\ mod\ 2 = 0$	$\frac{200-0}{2}$ $= \frac{200}{2} = 100$	
	7	$100\ mod\ 2 = 0$	$\frac{100-0}{2}$ $= \frac{100}{2} = 50$	
	6	$50\ mod\ 2 = 0$	$\frac{50-0}{2} = \frac{50}{2}$ $= 25$	
	5	$25\ mod\ 2 = 1$	$\frac{25-1}{2} = \frac{24}{2}$ $= 12$	11001000
	4	$12\ mod\ 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	
	3	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	2	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
155	8	$155\ mod\ 2 = 1$	$\frac{155-1}{2}$ $= \frac{154}{2} = 77$	10011011

	7	$77\ mod\ 2 = 1$	$\frac{77-1}{2} = \frac{76}{2}$ $= 38$	
	6	$38\ mod\ 2 = 0$	$\frac{38-0}{2} = \frac{38}{2}$ $= 19$	
	5	$19\ mod\ 2 = 1$	$\frac{19-1}{2} = \frac{18}{2}$ $= 9$	
	4	$9\ mod\ 2 = 1$	$\frac{9-1}{2} = \frac{8}{2} = 4$	
	3	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
24	8	$24\ mod\ 2 = 0$	$\frac{24-0}{2} = \frac{24}{2}$ $= 12$	
	7	$12\ mod\ 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	00011000
	6	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	5	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	4	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	

	3	0	0	
	2	0	0	
	1	0	0	
190	8	$190\ mod\ 2 = 0$	$\frac{190-0}{2}$ $= \frac{190}{2} = 95$	
	7	$95\ mod\ 2 = 1$	$\frac{95-1}{2} = \frac{94}{2}$ $= 47$	
	6	$47\ mod\ 2 = 1$	$\frac{47-1}{2} = \frac{46}{2}$ 23	
	5	$23\ mod\ 2 = 1$	$\frac{23-1}{2} = \frac{22}{2}$ $= 11$	10111110
	4	$11\ mod\ 2 = 1$	$\frac{11-1}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	

174	8	$174\ mod\ 2 = 0$	$\frac{174-0}{2}$ $= \frac{174}{2} = 87$	10101110
	7	$87\ mod\ 2 = 1$	$\frac{87-1}{2} = \frac{86}{2}$ $= 43$	
	6	$43\ mod\ 2 = 1$	$\frac{43-1}{2} = \frac{42}{2}$ $= 21$	
	5	$21\ mod\ 2 = 1$	$\frac{21-1}{2} = \frac{20}{2}$ $= 10$	
	4	$10\ mod\ 2 = 0$	$\frac{10-0}{2} = \frac{10}{2}$ $= 5$	
	3	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	
	2	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	1	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
99	8	$99\ mod\ 2 = 1$	$\frac{99-1}{2} = \frac{98}{2}$ $= 49$	01100011
	7	$49\ mod\ 2 = 1$	$\frac{49-1}{2} = \frac{48}{2}$ $= 24$	

	6	$24\ mod\ 2 = 0$	$\frac{24-0}{2} = \frac{24}{2}$ $= 12$	
	5	$12\ mod\ 2 = 0$	$\frac{12-0}{2} = \frac{12}{2}$ $= 6$	
	4	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	3	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	
84	8	$84\ mod\ 2 = 0$	$\frac{84-0}{2} = \frac{84}{2}$ $= 42$	
	7	$42\ mod\ 2 = 0$	$\frac{42-0}{2} = \frac{42}{2}$ $= 21$	
	6	$21\ mod\ 2 = 1$	$\frac{21-1}{2} = \frac{20}{2}$ $= 10$	01010100
	5	$10\ mod\ 2 = 0$	$\frac{10-0}{2} = \frac{10}{2}$ $= 5$	
	4	$5\ mod\ 2 = 1$	$\frac{5-1}{2} = \frac{4}{2} = 2$	

	3	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	2	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	1	0	0	
1	8	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	7	0	0	
	6	0	0	
	5	0	0	00000001
	4	0	0	
	3	0	0	
	2	0	0	
	1	0	0	

Tabel 4.14 Proses Penyisipan Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Langkah		**Proses Penyisipan**
Pertama	:	Enkripsi pesan mengunakan *playfair cipher*. Kemudian hasil dari enkripsi tersebut dienkripsi lagi menggunakan *caesar cipher*. Karena *plaintext*, kunci, dan besar pergeserannya sama pada Contoh 4.10 maka diperoleh *ciphertextnya* yaitu QPH3
Kedua		Mengubah *ciphertext* ke ASCII (lihat Tabel 4.8). Q=27 P=26 H=18 3=4

Ketiga : Mengubah ASCII *ciphertext* dan nilai matriks citra ke biner. Perubahan ASCII *ciphertext* dapat dilihat pada Tabel 4.15. Perubahan matriks citra ke biner dapat dilihat pada Tabel 4.8 untuk kolom 1 dan kolom 4, Tabel 4.13 untuk kolom 2 dan kolom 3.

Keempat : Mengganti bit terakhir citra dengan bit *ciphertext*.

Diketahui:

Ciphertext

Q = 27 = 00011011

P = 26 = 00011010

H = 18 = 00010010

3 = 4 = 00000100

Matriks Citra Red

11000011	01000100	11001000	11000011
10110000	01001110	10011011	10110000
10111000	11000011	00011000	10111000
10111001	00100101	10111110	10111001
10111000	10110000	10101110	10111000
10110101	01100011	01100011	10110101
10111000	00100011	01010100	10111000
10111111	00001010	00000001	10111110

Biner Q disisipkan di kolom 1, P di kolom 2, H di kolom 3, dan 3 di kolom 4. Dengan mengganti bit terakhir citra denga bit-bit pesan maka diperoleh:

1100001**0**	0100010**0**	1100100**0**	1100001**0**
1011000**0**	0100111**0**	1001101**0**	1011000**0**
1011100**0**	1100001**0**	0001100**0**	1011100**0**
1011100**1**	0010010**1**	1011111**1**	1011100**0**
1011100**1**	1011000**1**	1010111**0**	1011100**0**
1011010**0**	0110001**0**	0110001**0**	1011010**1**
1011100**1**	0010001**1**	0101010**1**	1011100**0**
1011111**1**	0000101**0**	0000000**0**	1011111**0**

	Angka yang dicetak tebal merupakan nilai bit terakhir citra setelah digantikan dengan bit pesan. Jadi nilai biner tersebut adalah nilai biner matriks citra yang telah disisipkan pesan
Kelima	Mengubah nilai biner matriks citra yang telah disisipkan pesan ke bentuk desimal. Kolom 1 dan kolom 2 $11000001 = 194$ $01000100 = 68$ $10110000 = 176$ $01001110 = 78$ $10111000 = 184$ $11000010 = 194$ $10111001 = 185$ $00100101 = 37$ $10111001 = 185$ $10110001 = 177$ $10110100 = 180$ $01100010 = 98$ $10111001 = 185$ $00100011 = 35$ $10111111 = 191$ $00001010 = 10$ Kolom 3 dan kolom 4 $11001000 = 200$ $11000010 = 194$ $10011010 = 154$ $10110000 = 176$ $00011000 = 24$ $10111000 = 184$ $10111111 = 191$ $10111000 = 184$ $10101110 = 174$ $10111000 = 184$ $01100010 = 98$ $10110101 = 181$ $01010101 = 85$ $10111000 = 184$ $00000000 = 0$ $10111110 = 190$ Nilai desimal inilah yang merupakan nilai matriks citra yang baru atau nilai matriks citra yang telah disisipkan pesan
Keenam	Hitung nilai PSNR untuk mengetahui kualitas citra sesudah disisipkan pesan. Terlebih dahulu cari nilai MSEnya. Semakin rendah nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi. Nilai PSNR yang baik yaitu lebih dari 30-50 dB (Zulfikar, dkk., 2016).

Dengan menggunakan persamaan (2.12) diperoleh

$$MSE = \frac{1}{mn}\sum_{x=1}^{m}\sum_{y=1}^{n}\big(f(x,y) - g(x,y)\big)^2$$

$$= \frac{1}{8.4}\sum_{x=1}^{8}\sum_{y=1}^{4}\big(f(x,y) - g(x,y)\big)^2$$

$$= \frac{1}{8.4}((194-195)^2 + (68-68)^2 + (200-200)^2$$
$$+ (194-195)^2 + (176-176)^2 + (78-78)^2$$
$$+ (154-155)^2 + (176-176)^2 + (184-184)^2$$
$$+ (194-195)^2 + (24-24)^2 + (184-184)^2$$
$$+ (185-185)^2 + (37-37)^2 + (191-190)^2$$
$$+ (184-185)^2 + (185-184)^2 + (177-176)^2$$
$$+ (174-174)^2 + (184-184)^2 + (180-181)^2$$
$$+ (98-99)^2 + (98-99)^2 + (181-181)^2$$
$$+ (185-184)^2 + (35-35)^2 + (85-84)^2$$
$$+ (184-184)^2 + (191-190)^2 + (10-10)^2$$
$$+ (0-1)^2 + (190-190)^2)$$

$$= \frac{1}{32}((-1)^2 + (0)^2 + (0)^2 + (-1)^2 + (1)^2 + (0)^2 + (-1)^2$$
$$+ (0)^2 + (0)^2 + (-1)^2 + (0)^2 + (0)^2 + (0)^2$$
$$+ (0)^2 + (1)^2 + (-1)^2 + (1)^2 + (1)^2 + (0)^2$$
$$+ (0)^2 + (-1)^2 + (-1)^2 + (-1)^2 + (0)^2 + (1)^2$$
$$+ (0)^2 + (1)^2 + (0)^2 + (1)^2 + (0)^2 + (-1)^2$$
$$+ (0)^2)$$

$$= \frac{1}{32}(1+0+0+1+1+0+1+0+0+1+0+0+0+0$$
$$+1+1+1+1+0+0+1+1+1+0+1+0$$
$$+1+0+1+0+1+0)$$

$$= \frac{1}{32}(16) = 0{,}5$$

Substitusi $MSE = 0{,}5$ ke persamaan (2.13)

$$PSNR = 20 \cdot \log\left(\frac{Max}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log\left(\frac{200}{\sqrt{0{,}5}}\right)$$

$$= 20 \cdot \log\left(\frac{200}{0{,}7071067812}\right)$$

$$= 20 \cdot \log(282{,}8427124692)$$

$$= 20 \cdot 2{,}4515449935$$

$$= 49{,}0308998698 \text{ dB}$$

Jadi, berdasarkan nilai PSNR dan MSE, perubahan citra setelah disisipkan pesan tidak berbeda dengan citra sebelum disisipkan jika dilihat secara kasat mata.

Tabel 4.15 Contoh Perubahan ASCII ke Biner

ASCII	Bit ke-	Nilai Bit	Sisa Nilai	Nilai Biner
Q=27	8	$27\ mod\ 2 = 1$	$\frac{27-1}{2} = \frac{26}{2}$ $= 13$	00011011
	7	$13\ mod\ 2 = 1$	$\frac{13-1}{2} = \frac{12}{2}$ $= 6$	
	6	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	5	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	
	4	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	3	0	0	
	2	0	0	
	1	0	0	
P=26	8	$26\ mod\ 2 = 0$	$\frac{26-0}{2} = \frac{26}{2}$ $= 13$	00011010
	7	$13\ mod\ 2 = 1$	$\frac{13-1}{2} = \frac{12}{2}$ $= 6$	
	6	$6\ mod\ 2 = 0$	$\frac{6-0}{2} = \frac{6}{2} = 3$	
	5	$3\ mod\ 2 = 1$	$\frac{3-1}{2} = \frac{2}{2} = 1$	

	4	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	3	0	0	
	2	0	0	
	1	0	0	
H=18	8	$18\ mod\ 2 = 0$	$\frac{18-0}{2} = \frac{18}{2}$ $= 9$	
	7	$9\ mod\ 2 = 1$	$\frac{9-1}{2} = \frac{8}{2} = 4$	
	6	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	5	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	00010010
	4	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	
	3	0	0	
	2	0	0	
	1	0	0	
3=4	8	$4\ mod\ 2 = 0$	$\frac{4-0}{2} = \frac{4}{2} = 2$	
	7	$2\ mod\ 2 = 0$	$\frac{2-0}{2} = \frac{2}{2} = 1$	
	6	$1\ mod\ 2 = 1$	$\frac{1-1}{2} = \frac{0}{2} = 0$	00000100
	5	0	0	
	4	0	0	

	3	0	0	
	2	0	0	
	1	0	0	

Contoh 4.13

Teks kunci : SERAGAM

Kunci : SERAGM

Besar pergeseran : 3

Matriks *stego image*:

$$\begin{bmatrix} 194 & 68 & 200 & 194 \\ 176 & 78 & 154 & 176 \\ 184 & 194 & 24 & 184 \\ 185 & 37 & 191 & 184 \\ 185 & 177 & 174 & 184 \\ 180 & 98 & 98 & 181 \\ 185 & 35 & 85 & 184 \\ 191 & 10 & 0 & 190 \end{bmatrix}$$

Proses ekstraksinya dapat dilihat pada Tabel 4.16.

Tabel 4.16 Proses Ekstraksi Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Langkah		**Proses Ekstraksi**
Pertama	:	Mengubah nilai matriks citra red ke biner. Kolom 1 dan kolom 2 $11000010 = 194$ $\quad 01000100 = 68$ $10110000 = 176$ $\quad 01001110 = 78$ $10111000 = 184$ $\quad 11000010 = 194$ $10111001 = 185$ $\quad 00100101 = 37$ $10111001 = 185$ $\quad 10110001 = 177$ $10110100 = 180$ $\quad 01100010 = 98$ $10111001 = 185$ $\quad 00100011 = 35$ $10111111 = 191$ $\quad 00001010 = 10$

Kolom 3 dan kolom 4

$11001000 = 200$	$11000010 = 194$
$10011010 = 154$	$10110000 = 176$
$00011000 = 24$	$10111000 = 184$
$10111111 = 191$	$10111000 = 184$
$10101110 = 174$	$10111000 = 184$
$01100010 = 98$	$10110101 = 181$
$01010101 = 85$	$10111000 = 184$
$00000000 = 0$	$10111110 = 190$

Kedua : Mengambil bit terakhir setiap citra (perhatikan tulisan yang dicetak tebal).

Kolom 1 dan kolom 2

11000001**0**	01000100	11001000	11000010
10110000	01001110	10011010	10110000
10111000	11000010	00011000	10111000
10111001	00100101	10111111	10111000
10111001	10110001	10101110	10111000
10110100	01100010	01100010	10110101
10111001	00100011	01010101	10111000
10111111	00001010	00000000	10111110

Diperoleh:

00011011, 00011010, 00010010, dan 00000010

Nilai biner tersebut merupkan biner pesan yang disisipkan dalam citra.

Ketiga : Mengubah nilai biner pesan yang disisipkan ke bentuk desimal agar dapat diketahui pesan yang dimaksud.

$$00011011 = 27$$

$$00011010 = 26$$

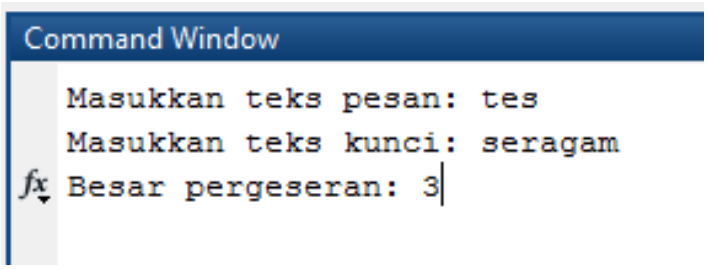
$$00010010 = 18$$

$$00000010 = 4$$

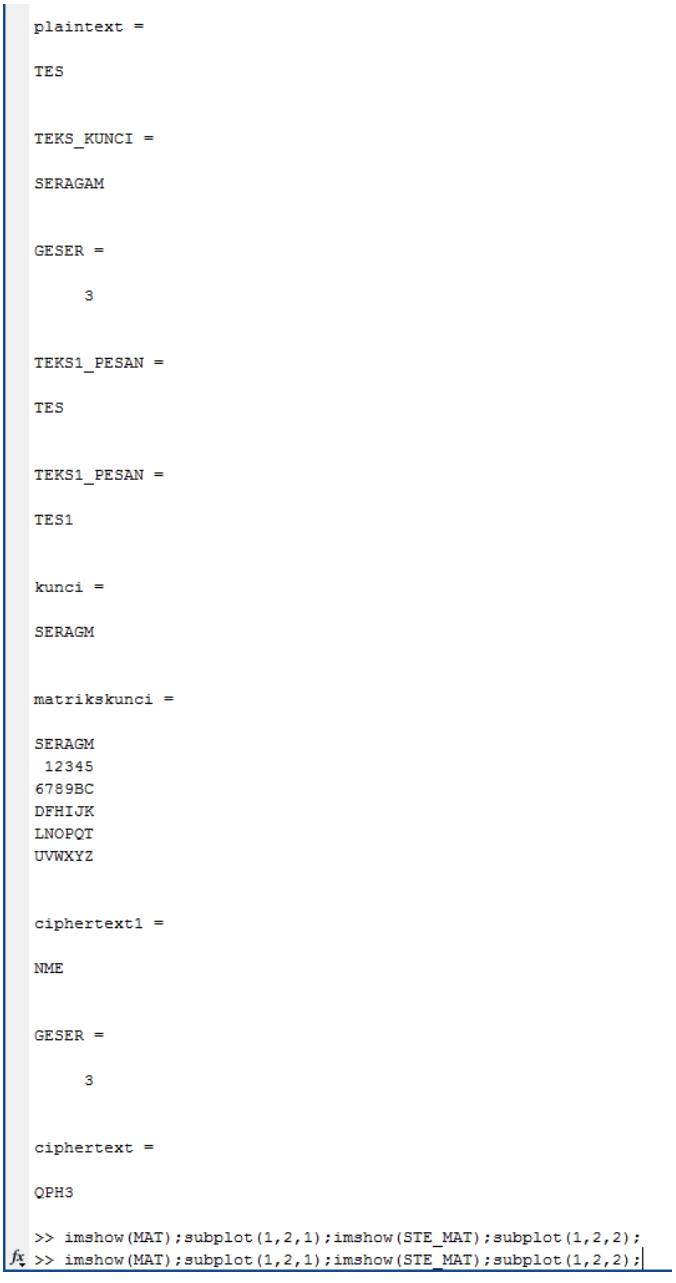
	Nilai desimal inilah yang merupakan nilai bentuk ASCII dari pesan tersebut. Maka dengan melihat Tabel 4.1 diketahui bahwa pesan yang disisipkan yaitu QPH3. Pesan QPH3 disebut *ciphertext*.
Kempat	Dekripsi *ciphertext* mengunakan *caesar cipher*. Kemudian hasil dari enkripsi tersebut dienkripsi lagi menggunakan *playfair cipher*. Karena *ciphertext*, kunci, dan besar pergeserannya sama pada Contoh 4.10 maka diperoleh pesan asal atau *plaintext* yaitu TES1 atau TES

7. Simulasi Program Penyisipan Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

a. Tentukan gambar atau citra yang akan disisipkan pesan (pada simulasi ini digunakan citra berukuran 80×80 pixel). Masukkan *plaintext*, teks kunci, serta besar pergeseran. Selanjutnya terjadi proses enkripsi pertama dengan metode *playfair cipher* menggunakan teks kunci. Kemudian hasil dari enkripsi tersebut dienkripsi lagi dengan metode *Caesar cipher*, sehingga menghasilkan *ciphertext*. Ciphertext inilah yang disisipkan pada citra. Langkah selanjutnya membaca matriks citra dan mengambil matriks citra red nya. *Ciphertext* disisipkan ke dalam matriks citra red sehingga diperoleh *stego image*. Kemudian *stego image* disimpan pada direktori yang diinginkan. Hasil simulasi programnya dapat dilihat pada Gambar 4.16 untuk proses input dan Gambar 4.17 untuk proses output.

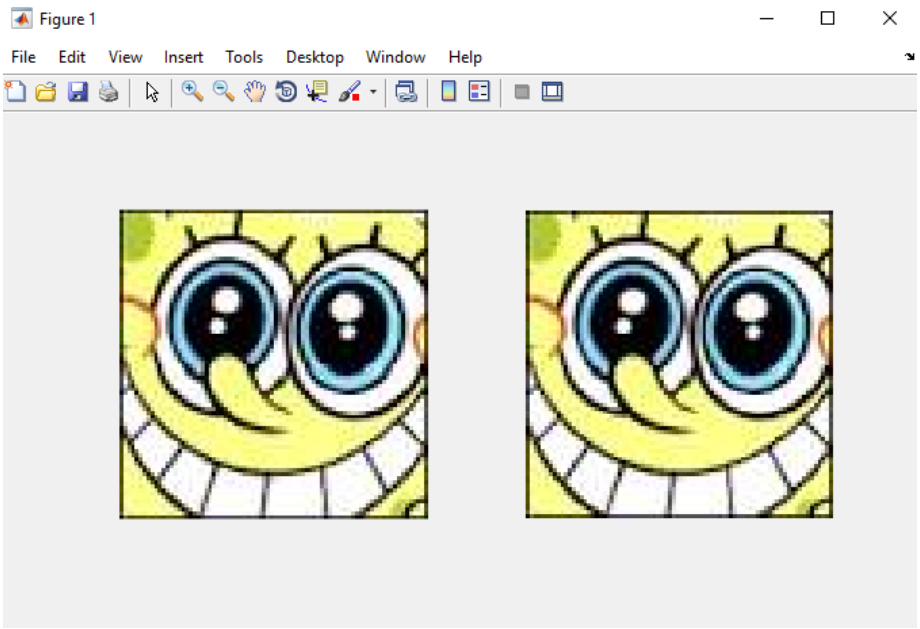


Gambar 4.16 Proses Penginputan



Gambar 4.17 Hasil Penyisipaan Pesan

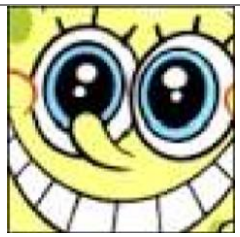
b. Untuk dapat melihat citra sebelum dan sesudah disisipkan lakukan perintah subplot (lihat Gambar 4.17 perintah subplot dan Gambar 4.18 adalah tampilan citra sesudah dan sebelum disisipkan). Berdasarkan Gambar 4.18, gambar sebelah kiri adalah gambar sebelum disisipkan pesan dan gambar sebelah kanan adalah gambar setelah disisipkan pesan.



Gambar 4.18 Citra Sebelum dan Sesudah Disisipkan Pesan

Hasil simulasi program dengan melakukan tiga percobaan menyisipkan pesan dapat dilihat pada Tabel 4.17, dan hasil perhitungan nilai MSE dan PSNR dapat dilihat pada Tabel 4.18.

Tabel 4.17 Hasil Simulasi Program Penyisipan Pesan pada Citra Menggunakan *Hybrid Playfair Cipher* dan *Caesar Cipher*

Pesan	**Citra Sebelum Disisipkan Pesan**	**Citra Setelah Disisipkan Pesan**
TES		
BESOK PAGI		
LAIN KALI		

Tabel 4.18 Perhitungan Nilai MSE dan PSNR Citra

Pesan	**Perhitungan Nilai MSE**		**Perhitungan Nilai PSNR (dB)**	
	Manual	Simulasi	Manual	Simulasi
TES	0,00125	0,0013	77,1617034686	77,1611
BESOK PAGI	0,0021875	0,0022	74,7313229982	74,7311
LAIN KALI	0,0028125	0,0028	73,6398782957	73,6393

Menurut Zulfikar, dkk., (2016) nilai PSNR yang baik yaitu lebih dari 30-50 dB. Jadi berdasarkan hasil perhitungan nilai MSE dan PSNR pada Tabel 4.18, citra sebelum dan sesudah disisipkan pesan secara kasat mata susah dibedakan.

B. Pembahasan

Beberapa penelitian sebelumnya yang berkaitan kriptografi, steganografi maupun yang membahas keduanya telah dilakukan oleh Wardani (2013) yang berjudul Pemecahan Sandi Kriptografi dengan Menggabungkan Metode *Hill Cipher* dan *Caesar Cipher*, Husein (2014) Implementasi *Caesar Cipher* untuk Penyembunyian Pesan Teks Rahasia pada Citra dengan Menggunakan Metode *Least Significant Bit*, Setiawan, dkk. (2012) Aplikasi Keamanan Pesan Menggunakan Algoritma Steganografi dan Kriptografi, serta Choudhary, dkk. (2013) *A Generalized Version of Playfair Cipher*.

Wardani (2013) meneliti tentang kriptografi dengan menggabungkan dua metode dalam kriptografi, yaitu *hill cipher* dan *caesar cipher*. Proses pengoperasian enkripsi menggunakan *caesar cipher* terlebih dahulu. Kemudian hasil dari enkripsi tersebut dienkripsi lagi menggunakan *hill cipher*. Terdapat 30 jenis karakter pesan yang digunakan dalam penelitian yaitu alfabet A-Z, tanda titik, tanda koma, tanda tanya, dan tanda seru. Wardani menggunakan besar kunci pergeseran pada *caesar cipher* yaitu sebanyak 3 pergeseran dan menggunakan matriks berordo 2×2 sebagai kunci pada *hill cipher*.

Husein (2014) meneliti tentang gabungan kriptografi dengan steganografi. Pada kriptografi digunakan metode *caesar cipher* dan metode penyisipan *Least Significant Bit* untuk steganografi. Jumlah pergeseran huruf alfabet yang digunakan

pada *caesar cipher* sebanyak 7 pergeseran. Karakter pesan yang digunakan sebanyak 26 karakter yaitu alfabet A-Z. Proses penyisipan pesan dilakukan dengan bantuan program Visual Basic.Net 2008.

Setiawan, dkk., (2012) penelitiannya berfokus pada pembuatan aplikasi pengamanan pesan. Penelitian tersebut menggunakan kriptografi dan steganografi dalam pengamanan pesan. Aplikasi tersebut dibuat menggunakan bahasa pemrograman java dengan tools NetBeans IDE 7.0. algoritma yang digunakan dalam aplikasi tersebut adalah algoritma steganografi *Least Significant Beat* dan algoritma kriptografi *Vigenere Cipher*. Hasil akhir dari penelitian tersebut adalah sebuah aplikasi steganografi pada citra menggunakan metode *Least Signidicant Bit* (*LSB*) dan *vigenere* yang dapat dijalankan pada komputer. Citra yang dapat digunakan pada aplikasi tersebut yaitu citra berformat .jpg, .png, .gif, dan .bmp. aplikasi tersebut dapat menyisipkan pesan pada gambar serta dapat melakukan proses enkripsi dan dekripsi pada pesan yang ingin disisipkan.

Choudhary, dkk. (2013) penelitiannya tentang kriptografi metode *playfair cipher* secara umum. Pada penelitian tersebut karakter yang digunakan untuk matriks kunci yaitu alfabet A-X dan tanda #. Huruf J tetap ada dan huruf Y dan Z tidak dipakai. Jika jumlah karakter pesannya ganjil maka ditambahkan dengan tanda # diakhir kalimat.

Penelitian tentang Steganografi Citra Menggunakan Kriptografi *Hybrid Playfair Cipher* dan *Caesar Cipher* dilakukan dengan rujukan penelitian-penelitian sebelumnya. Pada penelitian ini dilakukan penggabungan metode kriptografi *playfair cipher* dan *caesar cipher* untuk menyandikan pesan, supaya jika pesan

tersebut sampai di tangan pihak yang tidak diinginkan maka pihak tersebut tidak mudah mengembalikan pesan yang telah disandikan tersebut ke pesan asalnya. Selanjutnya untuk mengelabui indera penglihatan manusia maka digunakan metode steganografi untuk menyisipkan pesan tersebut ke dalam suatu. Media yang digunakan di sini berupa citra, yaitu terlebih dahulu mengubah pesan dan nilai matriks ke biner. Sehingga setiap bit biner pesan dapat disisipkan ke bit terakhir biner citra. Setelah pesan disisipkan ke citra, tentukan nilai PSNR. Hasil dari PSNR citra yang telah disisipkan pada citra dalam penelitian ini menghasilkan bahwa citra sebelum disisipkan dan setelah disisipkan pesan tidak terdapat perbedaan atau perbedaannya tidak terlihat jelas jika dilihat secara kasat mata.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan dari hasil penelitian, maka dapat ditarik kesimpulan sebagai berikut:

1. Proses enkripsi pesan secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher* yaitu:

   $$E(E(P, K1), K2) = C$$

   Proses dekripsi pesan secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher* yaitu:

   $$D(D(C, K2), K1) = P$$

2. Proses penyisipan pesan pada citra secara matematis menggunakan *hybrid playfair cipher* dan *caesar cipher* yaitu:

   $$M(K2(K1(P, K1), K2), G) = S$$

3. Hasil dari simulasi program yaitu citra awal sebelum disisipkan pesan dan sesudah disisipkan pesan secara kasat mata susah dibedakan.

B. Saran

Adapun saran kepada peneliti selanjutnya dianjurkan sebagai berikut:

1. Mengkaji lebih lanjut mengenai kombinasi algoritma kriptografi dengan metode dan data yang lain selain teks, seperti gambar, video, ataupun audio.
2. Menggunakan media penyisipan, file teks, video, ataupun audio.

DAFTAR PUSTAKA

Arif, M.H., Fanani, A. Z., 2016, Kriptografi Hill Cipher dan Leas Significant Bit untuk Keamanan Pesan pada Citra, *CSRID Journal*, Vol.8, No.1.

Cahyadi, T., 2012, Implementasi steganografi LSD dengan enkripsi Vigenere Cipher pada Citra JPEG, *Jurnal TransientI*, Vol. 1, NO. 4.

Choudhary, J., Gupta, R., K., Singh, S., 2013, A Generalized Version of Playfair Cipher, *compusoft*, *An Internationak Journal of Advance Computer Technology*, Volume-II, Issue-VI

Darmayanti, Harsa, K.A., 2016, Sistem Steganografi pada Citra Digital Menggunakan Least Significant Bit, *Prosiding Seminar Sains*, Vol. 1, No. 1.

Husein, M., 2014, Implementasi Caesar Cipher untuk Penyembunyian Pesan Teks Rahasia pada Citra dengan Menggunakan Metode Least Significant Bit, *Jurnal Pelita Informatika Budi Darma*, Vol. VII, No. 2.

Imran, 2016, Metode Laplace Gauss dan Aplikasinya pada Deteksi Tepi Citra, *Skripsi*, Prodi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Makassar: Makassar

Kadir, A., Susanto, A., 2013, *Teori dan Aplikasi Pengolahan Citra Digital*, Andi: Yogyakarta.

Katzenbeisser, S., dan Petitcolas, F., A., P., 2000, *Information Hidding Techniques for Steganography and Digital Watermarking*, Artech House: Boston, London

Kromodimoeljo, S., 2010, *Teori dan Aplikasi Kriptografi*, SPK IT Consulting.

Kusumanto, R., Tompunu, A. N., 2011, Pengolahan Citra Digital untuk Mendeteksi Obyek menggunakan Pengolahan Warna Model Normalisasi RGB, *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*, ISBN 979-26-0255-0.

Munir, R., 2010, *Matematika Diskrit*, Edisi Revisi Keempat, Informatika: Bandung

Munir, S., 2004, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika: Bandung.

Noer S., R.C., 2010, Implementasi Algoritma Enkripsi Playfair pada File Teks, *Jurnal Teknologi Informasi DINAMIK*, Vol. XV, No.1.

Pradipta, A., 2016, Implementasi Metode Caesar Cipher Alphabet Majemuk dalam Kriptografi untuk Pengamanan Informasi, *Indonesian Journal on Networking and* Security, Vol. 5, No. 3.

Rorres, A., 2004, *Aljabar Linear Elementer Versi Aplikasi*, Edisi Kedelapan, Jilid 1, Erlangga: Jakarta.

Sadikin, R., 2012, *Kriptografi untuk Keamanan Jaringan*, Andi: Yogyakarta.

Santi, R.C.N., 2010, Implementasi Algoritma Enkripsi Playfair pada File Teks, *Jurnal Teknologi Informasi DINAMIK*, Vol. XV, No.1.

Seftyanto, D., Apriani, M., Haryanto, T., 2012, Peran Algoritma Caesar Cipher dalam Membangun Karakter Akan Kesadaran Keamanan Informasi, *Prosiding Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY*.

Setiawan, W., Juwairiah, Sofyan, H., 2012, Aplikasi Keamanan Pesan Menggunakan Algoritma Steganografi dan Kriptografi, *Jurnal Telematika*, Vol.8, No.2.

Setyaningsih, E., 2009, Penyandian Citra Menggunakan Metode Playfair Cipher, *Jurnal Teknologi*, Vol. 2, No.2.

Siambaton, M., Z., 2016, Kombinasi Algoritma Pixel Value Differencing dengan Algoritma Caesar Cipher pada Proses Steganografi, *Journal of Computer Engineering, System and Science*, Vol. 1, No. 2.

Susilowati, 2016, Implementasi Algoritma Kriptografi RSA pada Keamanan Data Transkip Nilai Mahasiswa UNM Jurusan Matematika Menggunakan Bahasa Pemrograman PHP, *Skripsi*, Prodi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Makassar: Makassar.

Tiro, M.A., Darwis, M., Sukarna, Aswi, 2008, *Pengenalan Teori Bilangan*, Andira: Makassar.

Wardani, I.E., 2013, Pemecahan Sandi Kriptografi dengan Menggabungkan Metode Hill Cipher dan Metode Caesar Cipher, *Jurnal Cauchy*, Vol.2, No.4.

Wijaya, Marvin C., Prijono, Agus, 2007, *Pengolahan Citra Dijital Menggunakan MATLAB*, Informatika: Bandung.

Zulfikar, D H., Harjoko A., 2016, Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapannya Point Operation Image Enhancement, *IJCCS*, Vol 10, No.1

Zuli, F., dan Irawan, A., 2014, Penerapan Kombinasi Sandi Caesar dan Vigenere untuk Pengamanan Data Pesan pada Surat Elektronik, *Jurnal Sistem Informasi*, Vol.7, No. 2.