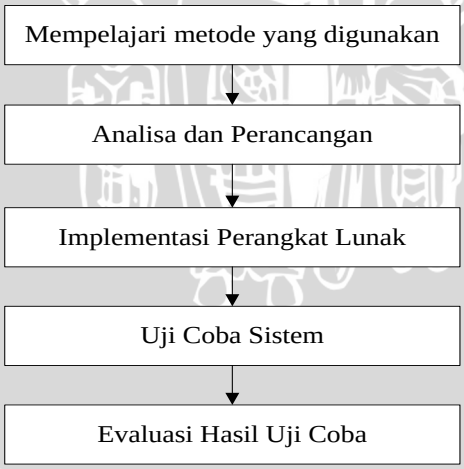
BAB III
METODE PENELITIAN DAN PERANCANGAN

Pada bab metode penelitian dan perancangan ini akan dibahas rancangan dan langkah–langkah yang dilakukan dalam pembuatan aplikasi pengamanan pesan dengan menggunakan algoritma 3DES dan steganografi. Penelitian dilakukan dengan tahapan-tahapan sebagai berikut:

1. Mempelajari metode yang digunakan dari berbagai sumber seperti yang telah dijelaskan pada Bab 2.
2. Menganalisa dan merancang perangkat lunak dengan metode yang akan digunakan.
3. Membuat perangkat lunak berdasarkan analisis dan perancangan yang dilakukan.
4. Uji coba enkripsi, dekripsi, penyembunyian, dan ekstraksi pesan pada citra digital menggunakan perangkat lunak yang telah dibuat.
5. Evaluasi dan analisa hasil uji coba perangkat lunak.

Langkah–langkah penelitian ini ditunjukkan oleh Gambar 3.1



Gambar 3.1 Tahapan–tahapan Penelitian

3.1 Analisa Perangkat Lunak

Pada subbab ini akan dibahas mengenai deskripsi perangkat lunak dan batasan perangkat lunak.

3.1.1 Deskripsi Perangkat Lunak

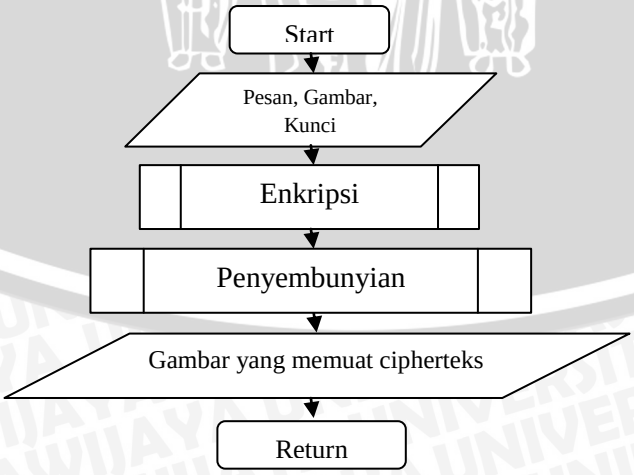
Perangkat lunak yang merupakan implementasi dari Algoritma 3DES (untuk kriptografi) dan Algoritma GifShuffle (untuk steganografi) digunakan untuk menjaga keamanan pesan berupa file teks agar tidak mudah dibaca dan dimanfaatkan oleh pihak yang tidak berkepentingan. Pesan akan diolah melalui proses enkripsi sehingga pesan teracak. Hasil dari proses enkripsi (*ciphertext*) akan disembunyikan ke dalam citra digital sehingga tidak terlihat seperti sebuah pesan. Kemudian dilakukan proses ekstraksi untuk mengeluarkan *ciphertext* dari citra digital. Dekripsi merupakan proses akhir dalam perangkat lunak ini yang berfungsi untuk mengembalikan *ciphertext* menjadi pesan aslinya.

3.1.2 Batasan Perangkat Lunak

Pada perangkat lunak ini menggunakan data berupa file teks yang akan disembunyikan pada citra digital dengan format gif tidak bergerak. Sedangkan kunci yang digunakan dalam perangkat lunak merupakan karakter ASCII.

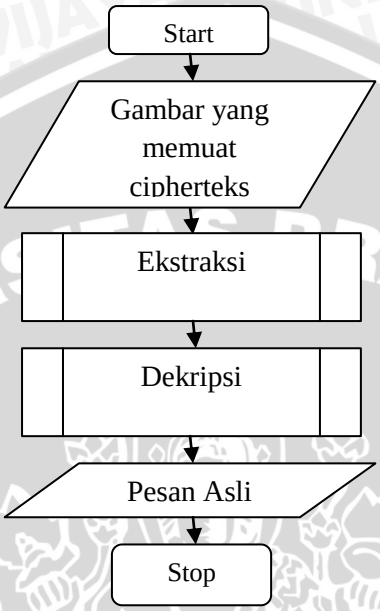
3.2 Perancangan Perangkat Lunak

Perancangan perangkat lunak dibagi menjadi beberapa tahapan yaitu tahap enkripsi, tahap penyembunyian, tahap ekstraksi, dan tahap dekripsi. Tahap enkripsi merubah pesan asli menjadi *ciphertext*. Kemudian *ciphertext* disembunyikan ke dalam gambar pada tahap penyembunyian. Tahapan enkripsi dan penyembunyian ditunjukkan pada Gambar 3.2.



Gambar 3.2 Flowchart Tahap Enkripsi dan Penyembunyian

Tahapan selanjutnya yaitu tahap ekstraksi, mengambil *ciphertext* di dalam gambar. Setelah di dapatkan *ciphertext* maka dilanjutkan tahap dekripsi untuk mendapatkan pesan asli dari *ciphertext*. Tahapan ekstraksi dan dekripsi ditunjukkan pada Gambar 3.3.



Gambar 3.3 Flowchart Tahap Ekstraksi dan Dekripsi

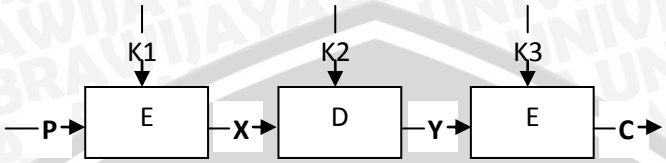
3.2.1 Tahap Enkripsi

Pada tahap ini dilakukan proses pengambilan kunci, pesan, dan gambar. Kunci yang dimaksud yaitu password yang akan digunakan untuk melakukan enkripsi. Pesan yaitu data yang akan dienkripsi. Gambar yaitu media untuk penyembunyian hasil enkripsi pesan.

Proses pengambilan pesan, proses untuk mengambil data (file teks) atau inputan teks yang akan ditujukan kepada pihak kedua oleh pihak pertama. Proses pengambilan gambar, proses untuk mengambil gambar sebagai media untuk penyembunyian pesan.

Proses pengambilan kunci, proses menentukan kata kunci yang akan digunakan oleh pengguna untuk melakukan enkripsi pesan. Pengambilan kunci dilakukan dengan memasukkan kunci pada *field* yang telah disediakan dengan panjang karakter maksimal 24 karakter.

Tahap enkripsi dilakukan setelah tahap pengambilan pesan, gambar, dan kunci. Pada tahap ini dilakukan enkripsi terhadap pesan dengan menggunakan algoritma 3DES. Enkripsi dengan menggunakan algoritma 3DES ditunjukkan pada Gambar 3.4.



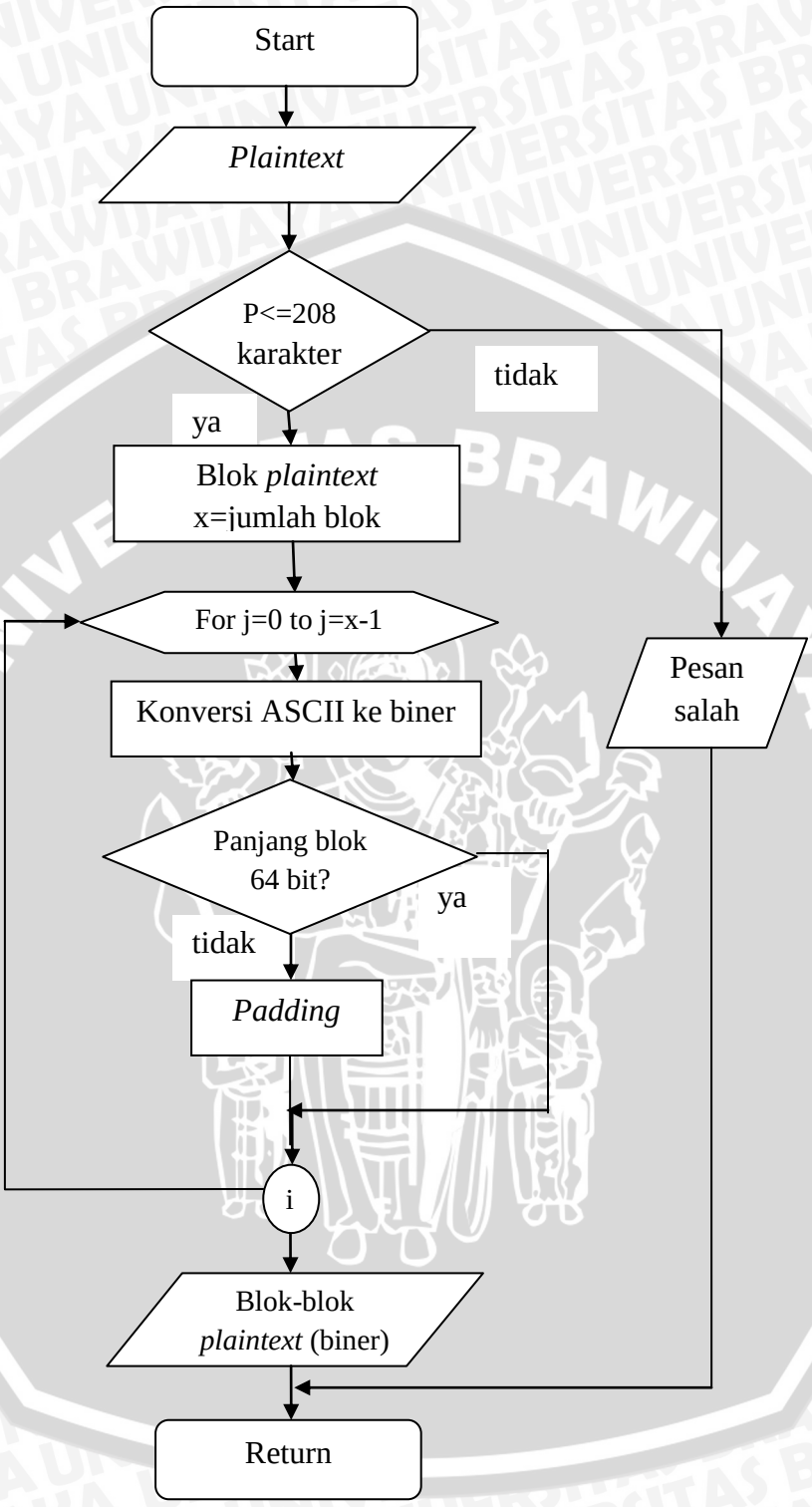
Gambar 3.4 Blok Diagram Enkripsi 3DES

Proses enkripsi dari algoritma 3DES dimulai dengan melakukan enkripsi DES (E) pada *plaintext* (P) dengan kunci pertama (K1). Kemudian *ciphertext* (X) dilakukan dekripsi DES (D) menggunakan kunci kedua (K2) dan diakhiri dengan enkripsi DES (E) menggunakan kunci ketiga (K3).

a) Enkripsi DES (E) dengan kunci K1

Enkripsi DES terdiri beberapa proses seperti yang telah dijelaskan pada bab 2. Proses awal yaitu menentukan blok *plaintext*. Selanjutnya melakukan pembangkitan kunci internal dan *enciphering*.

Proses pembentukan blok *plaintext*, *plaintext* dirubah menjadi blok-blok *plaintext*, dimana isi setiap blok *plaintext* sebesar 8 karakter. Setelah dibentuk blok *plaintext*, dilakukan konversi dari ASCII ke biner untuk mendapatkan bilangan biner sebanyak 64 bit. Untuk menutupi kekurangan jumlah bit maka dilakukan proses menambahan bit-bit isian pada blok terakhir dari inputan *plaintext*. Proses blok *plaintext* ditujukkan pada Gambar 3.5.



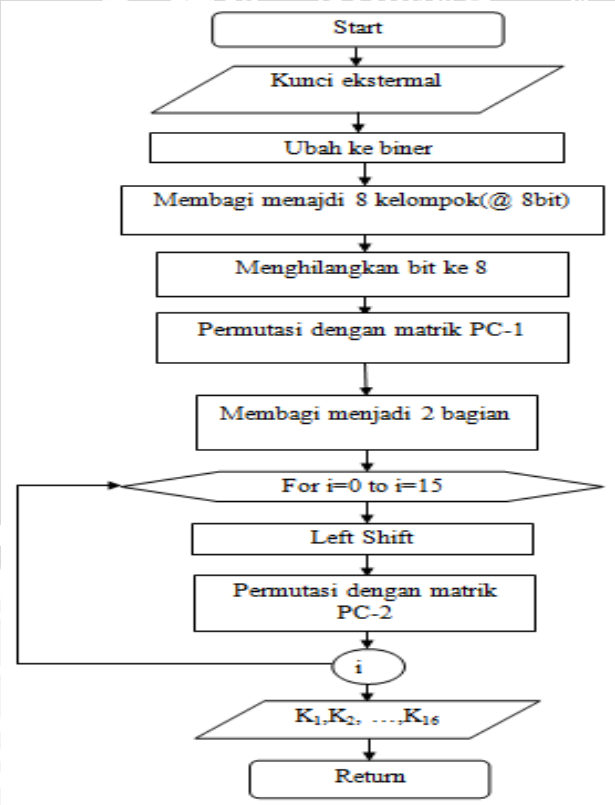
Gambar 3.5 Flowchart Pembentukan blok *plaintext*

Sebelum putaran pertama, terhadap blok *plaintext* dilakukan permutasi awal (*Initial Permutation* atau IP) untuk mengacak *plaintext* sehingga urutan bit-bit di dalamnya berubah.

Proses pembangkitan kunci internal. Langkah-langkah dalam proses pembangkitan kunci internal adalah sebagai berikut:

1. Kunci internal dibangkitakan dari kunci eksternal.
2. Setiap karakter dikonversikan ke dalam bilangan biner.
3. Hasil konversi kemudian dikelompokkan menjadi 8 kelompok yang terdiri dari masing-masing 8 bit.
4. Tiap bit ke-8 dari 8 byte kunci tersebut diabaikan.
5. Melakukan permutasi dengan menggunakan matriks permutasi kompresi PC-1.
6. Membagi hasil permutasi kompresi PC-1 menjadi 2 bagian, atas dan bawah, yang masing-masing panjangnya 28-bit, dan masing-masing disimpan di dalam C_0 dan D_0.
7. Melakukan pergeseran bit ke kiri(left shift).
8. Setelah mengalami pergeseran bit, kemudian kunci dipermutasi dengan matriks permutasi kompresi PC-2 yang akan menghasilkan kunci internal ke-i.
9. Mengulang langkah 7 sampai 8 sebanyak 15 kali.

Flowchart untuk pembangkitan kunci internal ditunjukkan Gambar 3.6.



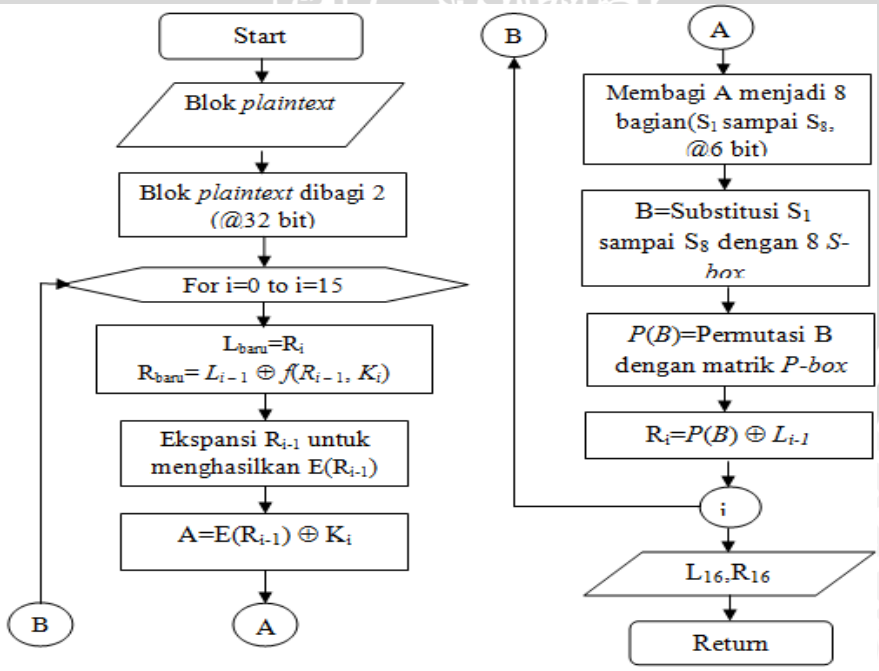
Gambar 3.6 Flowchart Pembangkitan Kunci Internal

Proses *enciphering*, blok *plaintext* setelah melewati proses permutasi awal dilakukan enkripsi 16 kali putaran. Blok *plaintext* terbagi menjadi dua bagian, kiri (*L*) dan kanan (*R*), yang masing-masing panjangnya 32 bit.

Langkah-langkah untuk proses *enciphering* adalah sebagai berikut:

1. Blok *plaintext* dibagi menjadi dua bagian (L dan R) dengan ukuran masing-masing 32 bit.
2. Blok *R* menjadi masukan untuk fungsi transformasi(*f*) sedangkan blok L baru langsung diambil dari blok R.
3. Melakukan ekspansi terhadap R_{i-1}32 bit untuk menghasilkan $E(R_{i-1})$ 48 bit.
4. $E(R_{i-1})$ di-XOR-kan dengan kunci K_i menghasilkan vektor *A* 48 bit.
5. Vektor A dikelompokan menjadi 8 kelompok(masing-masing 6 bit, S_1 sampai S_8).
6. Substitusi dengan menggunakan delapan buah kotak-S (*S-box*), S_1 sampai S_8 (menghasilkan vector B 32 bit).
7. Permutasi dengan menggunakan matriks permutasi *P* (*P-box*).
8. Bit-bit *P*(*B*) di-*XOR*-kan dengan L_{i-1} untuk mendapatkan R_i.
9. Mengulang langkah 2 sampai 8 sebanyak 15 kali hingga didapatkan L_{16},R_{16}.

Flowchart untuk proses *enciphering* ditunjukkan Gambar 3.7.



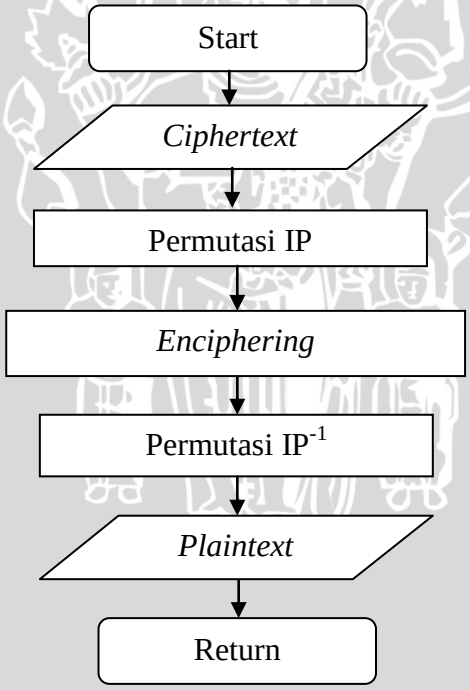
Gambar 3.7 Flowchart Proses *Enciphering*

Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan. Proses permutasi menggunakan matriks permutasi awal balikan.

b) Dekripsi DES (D)

Proses dekripsi terhadap *ciphertext* merupakan kebalikan dari proses enkripsi. Pada proses dekripsi urutan kunci yang digunakan adalah K_{16}, K_{15}, …, K_1. Blok *ciphertext* (R_{16}, L_{16}) adalah blok masukan awal untuk proses dekripsi. Blok (R_{16}, L_{16}) diperoleh dengan mempermutasikan *ciphertext* dengan matriks permutasi IP.

Pra-keluaran dari proses dekripsi adalah adalah (L_0, R_0). (L_0, R_0) dipermutasikan dengan IP^{-1} akan didapatkan kembali blok *plaintext* semula. Kunci-kunci dekripsi diperoleh dengan menggeser C_i dan D_i dengan cara pergeseran kanan (*right shift*). Proses dekripsi DES ditunjukkan pada Gambar 3.8.

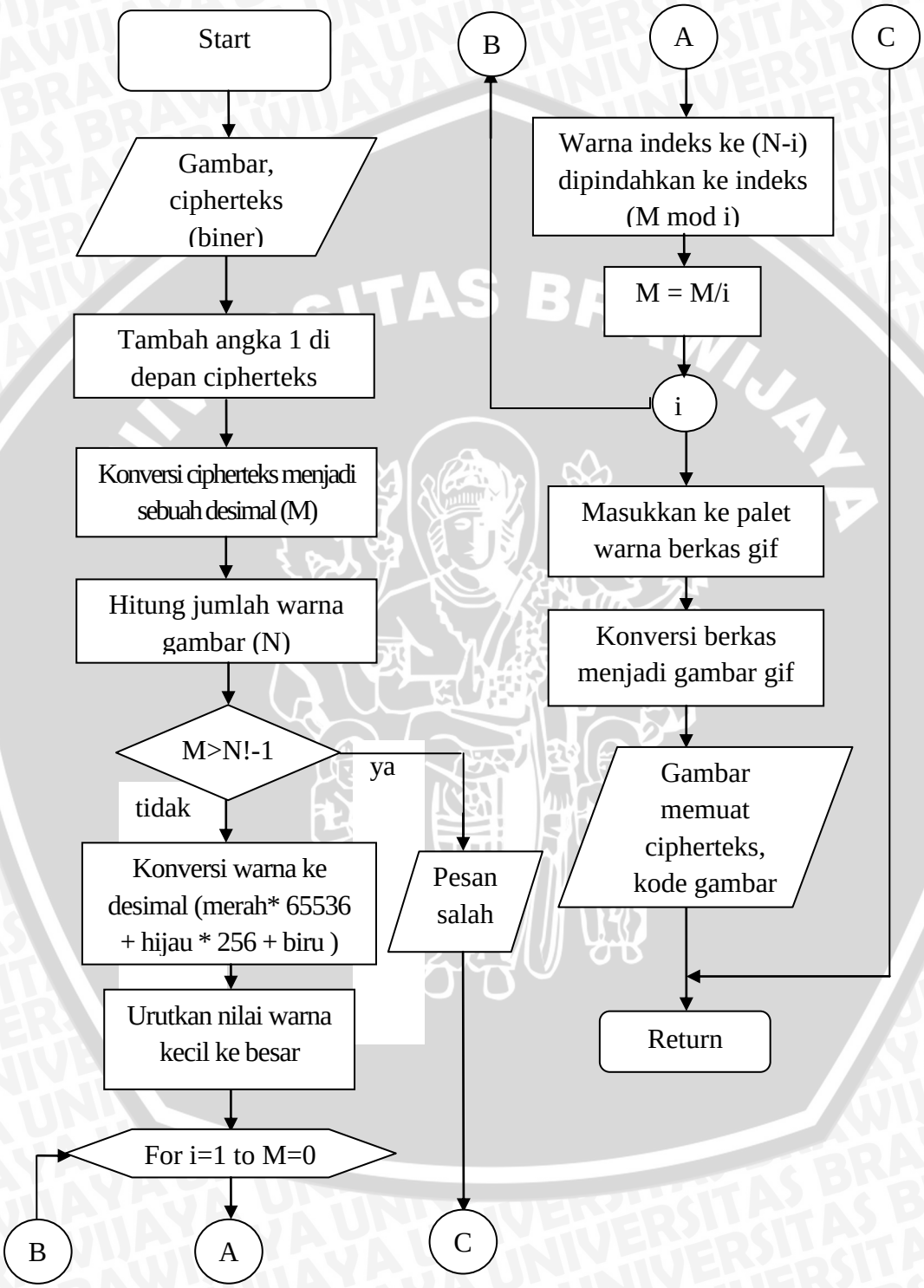


Gambar 3.8 Flowchart Dekripsi DES

3.2.2 Tahap Penyembunyian

Penyembunyian *ciphertext* ke dalam citra dilakukan dengan metode GifShuffle. Langkah-langkah untuk proses penyembunyian telah dijelaskan pada bab 2.2.2. *Flowchart* menyesuaikan dengan modifikasi yang dilakukan terhadap

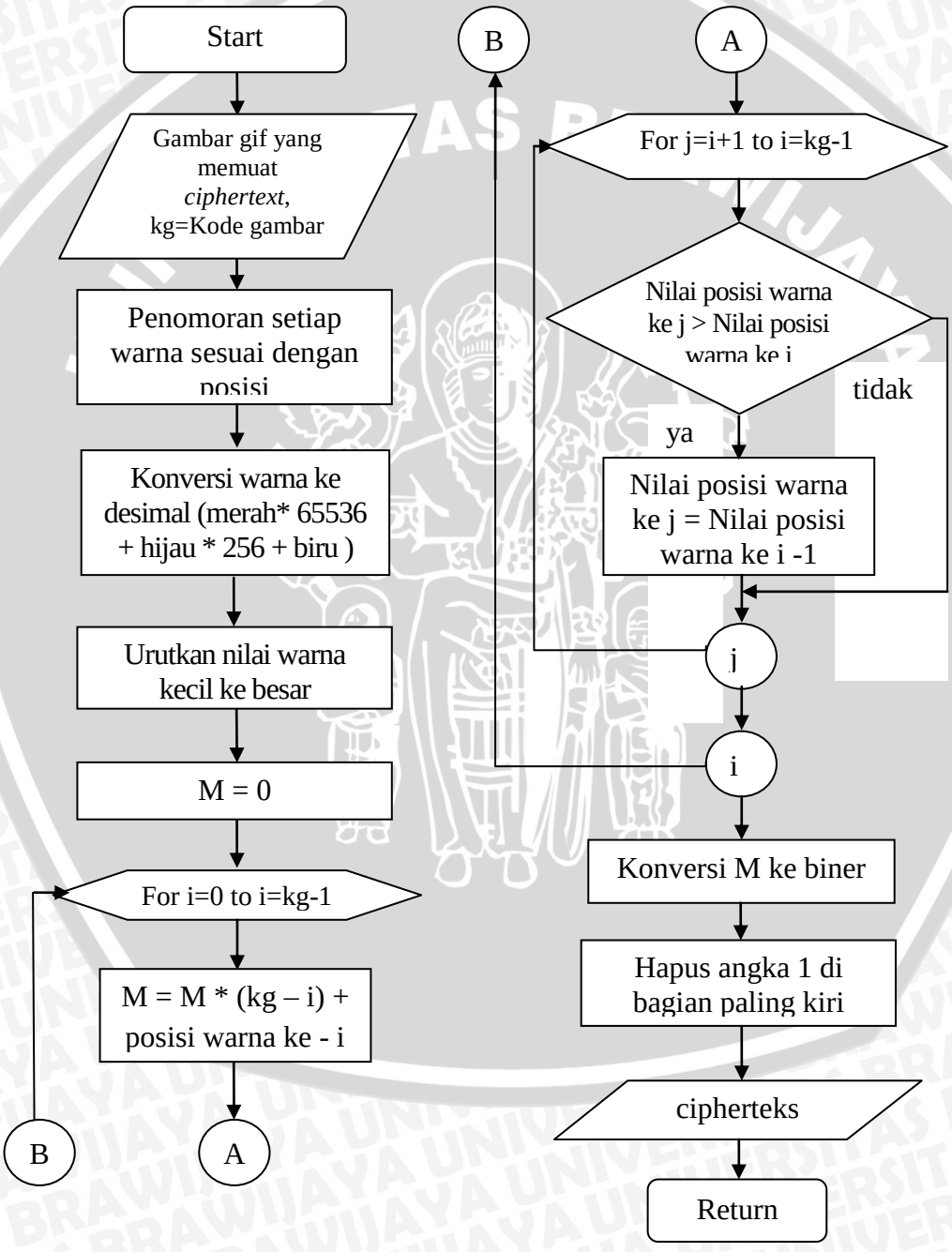
pemanfaatan warna. *Flowchart* untuk proses penyembunyian ditunjukkan Gambar 3.9.



Gambar 3.9 Flowchart Penyembunyian GifShuffle

3.2.3 Tahap Ekstraksi

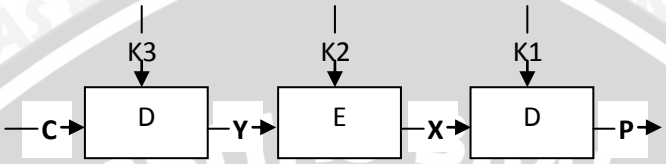
Skema ekstraksi GifShuffle merupakan kebalikan dari proses penyisipan. Jumlah warna yang digunakan berdasarkan hasil warna pada proses penyembunyian. Pada *flowchart* jumlah warna yang digunakan dinotasikan dengan "kg". Ekstraksi dengan menggunakan algoritma GifShuffle ditunjukkan pada Gambar 3.10.



Gambar 3.10 Flowchart Ekstraksi GifShuffle

3.2.4 Tahap Dekripsi

Tahap ini merupakan kebalikan dari tahap enkripsi yang berfungsi untuk mengembalikan *ciphertext* menjadi *plaintext*. Pada tahap ini dilakukan dekripsi terhadap pesan dengan menggunakan algoritma 3DES. Dekripsi dengan menggunakan algoritma 3DES ditunjukkan pada Gambar 3.11.



Gambar 3.11 Blok Diagram Dekripsi 3DES

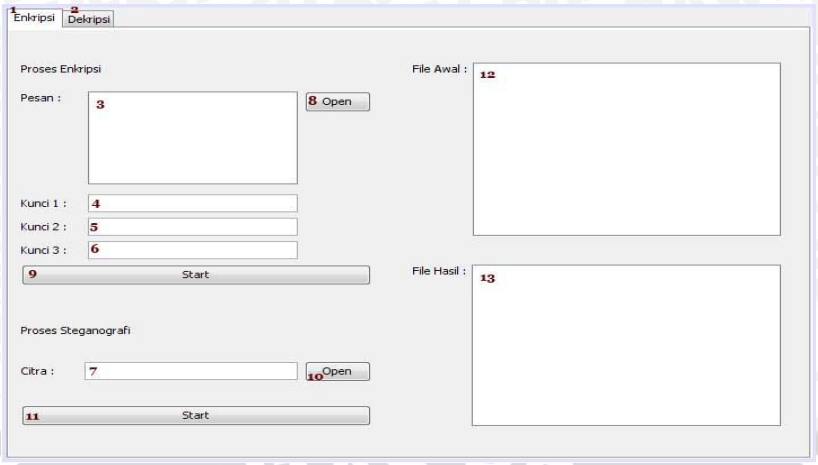
Proses dekripsi dari algoritma Triple DES terdiri dari 2 proses utama, yaitu enkripsi dan dekripsi dengan menggunakan algoritma DES. Proses enkripsi dan dekripsi DES yang digunakan pada dekripsi 3DES sama dengan proses enkripsi dan dekripsi DES yang digunakan pada enkripsi 3DES, pada bab 3.2.1.

3.3 Perancangan Antar Muka

Pada subbab ini akan dibahas mengenai perancangan antar muka perangkat lunak.

3.3.1 Antar Muka Menu Enkripsi

Antar muka pada menu enkripsi memuat dua tahap, yaitu enkripsi dengan algoritma 3DES dan proses penyembunyian. Rancangan antar muka perangkat lunak pada menu enkripsi ditunjukan pada Gambar 3.12.



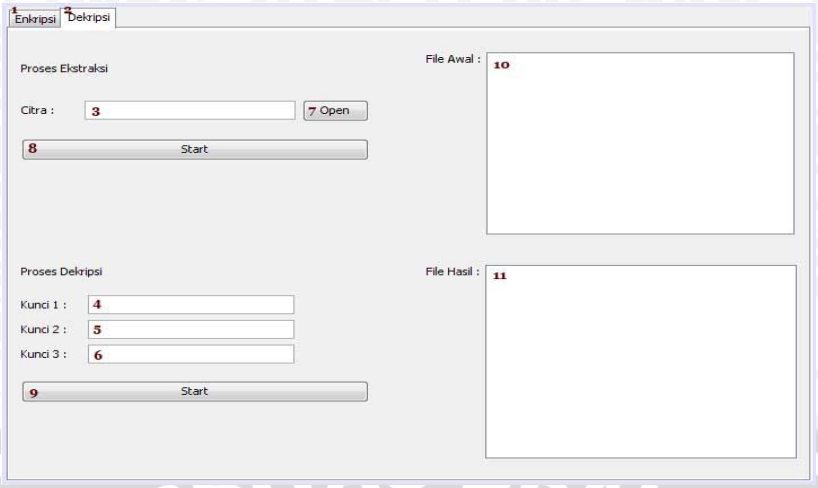
Gambar 3.12 User Interface Perangkat Lunak Menu Enkripsi

Keterangan gambar:

1. Tombol untuk menu enkripsi.
2. Tombol untuk menu dekripsi.
3. *Field* yang menampung pesan text.
4. *Field* untuk input kunci 1.
5. *Field* untuk input kunci 2.
6. *Field* untuk input kunci 3.
7. *Field* yang menampung citra.
8. Tombol untuk input pesan text.
9. Tombol mulai proses enkripsi.
10. Tombol untuk input pesan citra.
11. Tombol mulai proses penyembunyian.
12. Area untuk memuat file awal.
13. Area untuk memuat file hasil.

3.3.2 Antar Muka Menu Dekripsi

Antar muka pada menu dekripsi memuat dua tahap, yaitu proses ekstraksi dan enkripsi dengan algoritma 3DES. Rancangan antar muka perangkat lunak pada menu dekripsi ditunjukan pada Gambar 3.13.



Gambar 3.13 User Interface Perangkat Lunak Menu Enkripsi

Keterangan gambar:

1. Tombol untuk menu enkripsi.
2. Tombol untuk menu dekripsi.
3. *Field* yang menampung citra.
4. *Field* untuk input kunci 1.
5. *Field* untuk input kunci 2.
6. *Field* untuk input kunci 3.
7. Tombol untuk input citra.
8. Tombol mulai proses ekstraksi.
9. Tombol mulai proses dekripsi.
10. Area untuk memuat file awal.
11. Area untuk memuat file hasil.

3.4 Perancangan Uji Coba dan Evaluasi

Perancangan pengujian perangkat lunak kriptografi dan steganografi ini dimaksudkan agar dapat mengetahui kinerja dari perangkat lunak. Selain itu, sebagai bahan untuk mengevaluasi hasil dari implementasi analisa dan perancangan perangkat lunak.

3.4.1 Pengujian Keakuratan dan Nilai Avalanche Effect Algoritma 3DES

Pengujian ini dilakukan untuk menguji keakuratan proses enkripsi dan dekripsi algoritma 3DES pada perangkat lunak. Pada proses dekripsi dilakukan dengan memasukkan kunci yang berbeda. Pengujian nilai *Avalanche Effect*

dengan perubahan pada bit kunci ditunjukan pada Tabel 3.1. Pengujian nilai *Avalanche Effect* dengan perubahan pada bit *plaintext* ditunjukan pada Tabel 3.2.

Tabel 3.1 Pengujian Nilai Avalanche Effect Kunci

No	Kunci	Posisi bit Kunci yang Diubah	*Avalance effect (%)*

Keterangan:

- Kunci: kunci/password yang digunakan.
- Posisi bit Kunci yang Diubah: perubahan pada salah satu bit kunci secara random.
- *Avalanche Effect*: nilai *Avalanche Effect* perubahan satu bit kunci.

Tabel 3.2 Pengujian Nilai Avalanche Effect Plaintext

No	File *Plaintext*	Ukuran *Plaintext* (bit)	Posisi bit *Plaintext* yang Diubah	*Avalance effect (%)*

Keterangan:

- Kunci: kunci/password yang digunakan.
- Ukuran *Plaintext* (bit): panjang bit pada *plaintext*.
- Posisi bit *Plaintext* yang Diubah: perubahan pada salah satu bit *plaintext* secara random.
- *Avalanche Effect*: nilai *Avalanche Effect* perubahan satu bit *plaintext*.

3.4.2 Pengujian Citra Hasil Proses Steganografi

Pengujian ini dilakukan untuk mengetahui perubahan pada citra hasil steganografi dengan citra asli serta mengetahui hasil ekstraksi jika terjadi

kesalahan pada saat memasukkan kode citra. Pengujian citra ditunjukan pada Tabel 3.3. Pengujian MSE ditunjukan pada Tabel 3.4.

Tabel 3.3 Pengujian Citra Hasil Steganografi

No	*Ciphertext*	Citra Asli	Citra Hasil Steganografi

Keterangan:

- *Ciphertext*: hasil enkripsi pesan yang akan disisipkan pada citra asli.
- Citra Asli: citra sebelum proses steganografi.
- Citra Hasil Steganografi: citra setelah proses steganografi.

Tabel 3.4 Pengujian PSNR

No	Ukuran File Teks	Citra	PSNR

Keterangan:

- Ukuran File Teks: ukuran dari pesan.
- Citra: Gambar yang digunakan.
- PSNR: Nilai PSNR.

3.5 Perhitungan Manual

Dalam perhitungan manual, contoh yang diambil adalah input pesan "rahasia", dengan tiga kunci yaitu "enkripsi", "dekripsi", dan "threedes". Penyisipan "01000001" pada citra gif dengan jumlah warna 6 buah.

3.5.1 Perhitungan Proses Enkripsi 3DES

Proses enkripsi 3DES telah dijelaskan pada bab 2.4. Perhitungan manual dimulai dari permutasi awal. Setiap blok *plaintext* terdiri dari 8 karakter. Sebagai contoh *plaintext* yang dimasukkan yaitu "rahasia" akan dijadikan menjadi blok *plaintext*. Blok *plaintext* yang didapatkan yaitu:

Blok 1: rahasia

Selanjutnya blok *plaintext* yang masih menggunakan ASCII dikonversi menjadi biner, didapatkan:

Blok 1: 01110010011000010110100001100001011100110110100101100001

karena masih memiliki kekurangan bit maka dilakukan proses *padding*.

Blok 1: 0111001001100001011010000110000101110011011010010110000100000000

Setelah terbentuk blok *plaintext* maka dilakukan permutasi awal sebagai berikut:

01111111 00010001 00000000 01111010 00000000 01111111 00100100 00010001

Langkah selanjutnya yaitu menentukan kunci internal pertama. Kunci internal pertama dibangkitkan dari inputan kunci pertama yaitu "enkripsi". Kunci diubah ke bentuk biner dan didapatkan "01100101 01101110 01101011 01110010 01101001 01110000 01110011 01101001". Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan.

Setelah mendapakan 8 kelompok, dilakukan permutasi dengan PC-1 sehingga didapatkan:

0000000 0111111 1111111 1110110 0100111 0000000 1110010 1101000

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 0000000 0111111 1111111 1110110

D_0 : 0100111 0000000 1110010 1101000

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.5.

Tabel 3.5 Kunci Internal Dari Kunci Eksternal Pertama

Kunci	Isi Kunci
K_1	111000001011111011100110010010000010110010011011
K_2	111100001011011001110110101000001011010100110001
K_3	111001001101111001110110101010110000111000100010
K_4	111001101111001101110110010111000100101100010010
K_5	101011101101011101110011000101010100000001011100
K_6	111011110101001101111011110000011011000011000000

K_7	101011111101001111011001101000001010011000101101
K_8	000111110101101111011011001110100001111010000110
K_9	001111110100101111011001000010100011000100100110
K_{10}	000111110111100110011101101001000110100110100100
K_{11}	000111110010110111011101011000000000101011010011
K_{12}	010111110110110010101101110101111000000000011011
K_{13}	110110111010110110101100000001110001011101001000
K_{14}	110110001010111010101111000110001011000101100100
K_{15}	111100011011111000101110011000001100110010100100
K_{16}	111100001011111010101110000000101111100011001000

Selanjutnya melakukan proses *enciphering*. Blok *plaintext* dibagi menjadi dua bagian kiri dan kanan.

L : 01111111 00010001 00000000 01111010

R : 00000000 01111111 00100100 00010001

Setiap blok *plaintext* mengalami 16 kali putaran enkripsi. Hasil putaran ditunjukkan pada Tabel 3.6.

Tabel 3.6 *Enciphering* Blok *Plaintext* Tahap Pertama

Putaran	Hasil *Enciphering*
1	000000000111111100100100000100011001111101110111100011000011110 1
2	100111110111011110001100001111011110111001111101010010001010011 1
3	111011100111110101001000101001110011010011101110000010011110011 1
4	001101001110111000001001111001110001000110010001010011000101111 1
5	000100011001000101001100010111110001100001001001100100110111101 1
6	000110000100100110010011011110110000111010000101110100010010110 1
7	000011101000010111010001001011010011111010101101000101010111100 1
8	001111101010110100010101011110011111010010010011010000001111000 1
9	111101001001001101000000111100010100011111000001110010010001011 0
10	010001111100000111001001000101100111010111111001001101011001001 1
11	011101011111100100110101100100110000111011000100011001011100101 0
12	000011101100010001100101110010100010000001000000111100000010111 0

13	00100000010000001111000000101110110000110110010110011001100001110
14	11000011011001011001100110001110111001001101001110011111001101000
15	11100100110100111001111001101000100010100001000001100001000100 11
16	10001010000100000110000100010011110111011001000100111011010010011

Untuk mendapatkan hasil *enciphering* 16 putaran dilakukan dengan cara sebagai berikut:

Putaran 1:

L_1 : 00000000 01111111 00100100 00010001

R_1 : 01111111 00010001 00000000 01111010 $\oplus$ $f(R_0, K_1)$

$f(R_0, K_1)$ didapatkan dari:

Melakukan ekspansi R_0 dengan matrik permutasi ekspansi, diperoleh 100000 000000 001111 111110 100100 001000 000010 100010

Selanjutnya R_0 ekspansi di $\oplus$ K_1, diperoleh

011000 001011 110100 011000 110110 001010 110000 111001

Selanjutnya substitusi dengan S-box, diperoleh

S_1 : 0101; S_2 : 0010; S_3 : 0010; S_4 : 1011; S_5 : 0101; S_6 : 0010

S_7 : 1010; S_8 : 0011

Selanjutnya dilakukan permutasi dengan menggunakan matriks permutasi *P* (*P-box*), diperoleh

11100000 01100010 10001100 01000111

Selanjutnya di XOR kan dengan L

R_1 :

01111111000100010000000001111010 $\oplus$ 11100000011000101000110001000111

, diperoleh

R_1 : 10011111 01110011 10001100 00111101

Putaran 2:

L_2 : 10011111 01110011 10001100 00111101

R_2 : 00000000 01111111 00100100 00010001$\oplus$ $f(R_1, K_2)$

$f(R_1, K_2)$ didapatkan dari:

Melakukan ekspansi R_1 dengan matrik permutasi ekspansi, diperoleh 110011 111110 101110 100111 110001 011000 000111 111011

Selanjutnya R_1 ekspansi di $\oplus$ K_2, diperoleh

001111 110101 110111 010001 011001 010011 010011 001010

Selanjutnya substitusi dengan S-box, diperoleh

S_1 : 0001; S_2 : 0111; S_3 : 0011; S_4 : 0100; S_5 : 0011; S_6 : 0001

S_7 : 0011; S_8 : 1111

Selanjutnya dilakukan permutasi dengan menggunakan matriks permutasi *P* (*P-box*), diperoleh 01101110 00000110 01111100 10110110

Selanjutnya di XOR kan dengan L_1

R_2 :

00000000 01111111 00100100 00010001 $\oplus$ 01101110 00000110 01111100 10110110

, diperoleh

R_2 : 01101110 01111001 01011000 10100111

Dan seterusnya sampai putaran ke 16.

Setelah selesai proses *enciphering*, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh,

0100101111010111000001001100000001100111000111000100110011000001

Selanjutnya dilakukan proses dekripsi dengan menggunakan kunci kedua, yaitu “dekripsi”. Kunci diubah ke bentuk biner dan didapatkan “01100100011001010110101101110010011010010111000001110011011010 01”. Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan. Selanjutnya dilakukan permutasi dengan PC-1 sehingga didapatkan: 0000000 0111111 1111111 1110110 0100110 0000000 1110010 1001000

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 00000000111111111111111110110

D_0 : 01001100000000111001010010 00

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.7.

Tabel 3.7 Kunci Internal Dari Kunci Eksternal Kedua

Kunci	Isi Kunci
K_1	111000001011111011100110010010000010110000010011
K_2	111100001011011001110110101000001001000100110001
K_3	111001001101111001110110100000110000111000100010
K_4	111001101111001101110110010111000000101100010000
K_5	101011101101011101110011000100010100000001011100
K_6	111011110101001101111011010000011011000010000000
K_7	101011111101001111011001101000000010010000101101
K_8	000111110101101111011011001010100001101010000110
K_9	001111110100101111011001000101000100000100100010
K_{10}	000111110111100110011101101001000110100100000100
K_{11}	000111110010110111011101011000000000001011010010
K_{12}	010111110110110010101101110101011000000000001011
K_{13}	110110111010110110101100000001100001011001001000
K_{14}	110110001010111010101111000110001011000101100100
K_{15}	111100011011111000101110001000001100110010100000
K_{16}	111100001011111010101110000000100111100011001000

Permutasi awal blok *plaintext* sebagai berikut:

1101101100100010011101101001001110001010000100000110000100010011

Selanjutnya melakukan proses deciphering. Blok *ciphertext* dibagi menjadi dua bagian kiri dan kanan.

L : 11011011001000100111011010010011

R : 10001010000100000110000100010011

Setiap blok *ciphertext* mengalami 16 kali putaran enkripsi. Hasil putaran ditunjukkan pada Tabel 3.8.

Tabel 3.8 Deciphering Blok *Ciphertext* Tahap Kedua

Putaran	Hasil *Enciphering*
1	1000101000010000011000010001001111110100110100111011111001100000
2	1111010011010011101111100110000010101010011110110101010110011101
3	1010101001111011010101011001110100000100010111000001110111100111
4	0000010001011100000111011110011110101001110001111111010111110000
5	1010100111000111111101011111000001111000001100001000100101001011
6	0111100000110000100010010100101110110001010100100001010110111010
7	1011000101010010000101011011101001100111100101111111011010100111
8	0110011110010111111101101010011110111111100100011110000011000110
9	1011111110010001111000001100011010010001100010001000100110100000
10	1001000110001000100010011010000011110000001110101110011001101011
11	1111000000111010111001100110101110101100111010100100011101101111
12	1010110011101010010001110110111111011011010000000101100111010101
13	1101101101000000010110011101010111111011100111111110110101001011
14	1111101110011111110110101001011110111100000000100000010111111011
15	1011110000000010000001011111101100111010100111101111110100100111
16	0011101010011110111111010010011111010111110011100110110010101010

Setelah selesai proses deciphering, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh,

0100101011110011011111101011110111010001000111101011100011111001

Selanjutnya dilakukan proses enkripsi dengan menggunakan kunci ketiga, yaitu “threedes”. Kunci diubah ke bentuk biner dan didapatkan “011101000110100001110010011001010110010101100100011001010111001 1”. Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan. Selanjutnya dilakukan permutasi dengan PC-1 sehingga didapatkan: 00000000 11111111 11111111 10001000 01000111 1001000000100101

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 00000000111111111111111110110

D_0 : 0100110000000011100101001000

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.9.

Tabel 3.9 Kunci Internal Dari Kunci Eksternal Ketiga

Kunci	Isi Kunci
K_1	111100001011111001100110000101010010001101001000
K_2	111000001011111001110110010101000000011000010101
K_3	111001001111011001110110010110110000000011001100
K_4	111001101101011101110010000000001111000110001001
K_5	111011101101001101110011001000100011010000100101
K_6	101011111101001101011011111010100000100110100010
K_7	001011110101001111011011000001000100101100011011
K_8	001111110101100111011001010101110001000001010000
K_9	000111110101100111011001110010001000001001010110
K_{10}	000111110110100111011101010101011100011010001000
K_{11}	000111110110110110001101000110000001010001001001
K_{12}	010110110010110110101101100010101111000000100100
K_{13}	110110011010110010101101001000000110111110100000
K_{14}	110100011010111010101110101110000000100000010011
K_{15}	111100001011111010100110110001110100001000010010
K_{16}	111100001011111000100110100000011000101110000010

Permutasi awal blok *ciphertext* sebagai berikut:

110101111100111001101100101010100011101010011110111111010010011 1

Selanjutnya melakukan proses deciphering. Blok *ciphertext* dibagi menjadi dua bagian kiri dan kanan.

L : 11010111110011100110110010101010

R : 00111010100111101111110100100111

Setiap blok *ciphertext* mengalami 16 kali putaran. Hasil putaran ditunjukkan pada Tabel 3.10.

Tabel 3.10 *Enciphering* Blok *Ciphertext* Tahap Ketiga

Putaran	Hasil *Enciphering*
1	00111010100111101111110100100111100100011010011110101101110111011100
2	10010001101001111010110111011100011000001011000101001011010000010
3	01100000101100010100101101000010101100011011010110001110001000010
4	10110001101101011000111000100010111011101011011111100100110100001
5	11101110101101111110010011010001101001001011000111011111000101000
6	10100100101100011101111100010100011110110001100101011001010001111
7	01111011000110010101100101000111100100010101111100011001011000000
8	10010001010111110001100101100000000001110111010001101110011010000
9	00000111011101000110111001101000001101010111111111111110110010100
10	00110101011111111111111011001010000110110001000110011011001010101
11	00110110001000110011011001010101101000111000101101000011110111111
12	10100011100010110100001111011111111111011010000010110001111100111
13	11111011010000010110001111100111110011001001000101000110110101110
14	10011001001000101000110110101110000010010111100101001000011001111
15	00001001011110010100100001100111111001000000011110101011110101000
16	11100100000001111010101111010100001001100011011010101000101111110

Setelah selesai proses *enciphering*, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh hasil akhir dari proses enkripsi 3DES sebagai berikut,

00101000011110011111001100001101000100111101110110000010100011111

3.5.2 Perhitungan Proses Penyembunyian

Pada perhitungan proses penyembunyian diambil contoh *ciphertext* yang akan disisipkan adalah 01111010 ke dalam sebuah berkas GIF dengan jumlah warna pada palet warna sebanyak 6 buah. Langkah-langkah proses perhitungan adalah sebagai berikut:

1. Menambah angka 1 di depan *ciphertext*, didapatkan 101111010.
2. Melakukan konversi ke bentuk desimal, didapatkan 378 (M).
3. Jumlah warna 6 buah(N). Karena 378 < 6!-1 maka pesan dapat disisipkan.

4. Urutan warna pada palet warna citra:

Ke	0	1	2	3	4	5
Nilai	16555215	16721724	16492138	16772111	16496222	16890155

Diurutkan berdasarkan nilai dari kecil ke besar:

Ke	0	1	2	3	4	5
Nilai	16492138	16496222	16555215	16721724	16772111	16890155

5. Iterasi variabel i dari mulai 1 sampai N.
   Warna indeks ke-(N-i) dipindahkan ke indeks ke-(M mod i),
   M = M/i.
   - Iterasi 1 (i = 1):
     Warna indeks ke-5 dipindahkan ke-0, M = 378
   - Iterasi 2 (i = 2):
     Warna indeks ke-4 dipindahkan ke-0, M = 189
   - Iterasi 3 (i = 3):
     Warna indeks ke-3 dipindahkan ke-0, M = 63
   - Iterasi 4 (i = 4):
     Warna indeks ke-2 dipindahkan ke-3, M = 15
   - Iterasi 5 (i = 5):
     Warna indeks ke-1 dipindahkan ke-0, M = 3
   - Iterasi 6 (i = 6):
     Warna indeks ke-0 dipindahkan ke-3

   Didapatkan urutan warna menjadi

Ke	0	1	2	3	4	5
Nilai	16496222	16721724	16772111	16492138	16890155	16555215

6. Urutan palet warna ini kemudian dimasukkan kembali ke berkas citra GIF untuk menghasilkan citra yang telah disisipi pesan.

3.5.3 Perhitungan Proses Ekstraksi

Pada proses ekstraksi, diambil contoh hasil GifShuffle. Langkah-langkah proses perhitungan adalah sebagai berikut:

1. Warna pada palet warna diberi nomor sesuai posisinya.

Ke	0	1	2	3	4	5
Nilai	16496222	16721724	16772111	16492138	16890155	16555215

2. Mengurutkan warna dari nilai kecil ke besar.

Posisi	3	0	5	1	2	4
Nilai	16492138	16496222	16555215	16721724	16772111	16890155
Ke	0	1	2	3	4	5

3. M = 0.
4. Proses iterasi.
   - i = 0

     M = 0 * (6 – 0) + 3 = 3

     j = 1

     posisi ke 1 > posisi ke 0, tidak

     j = 2

     posisi ke 2 > posisi ke 0, ya maka posisi ke 2 = 5 – 1

     j = 3

     posisi ke 3 > posisi ke 0, tidak

     j = 4

     posisi ke 4 > posisi ke 0, tidak

     j = 5

     posisi ke 5 > posisi ke 0, ya maka posisi ke 5 = 4 – 1

     Hasil:

Posisi	0	4	1	2	3
Nilai	16496222	16555215	16721724	16772111	16890155
Ke	1	2	3	4	5

- i = 1

  M = 3 * (6 – 1) + 0 = 15

  j = 2

  posisi ke 2 > posisi ke 1, ya maka posisi ke 2 = 4 – 1

  j = 3

  posisi ke 3 > posisi ke 1, ya maka posisi ke 3 = 1 – 1

  j = 4

  posisi ke 4 > posisi ke 1, ya maka posisi ke 4 = 2 – 1

  j = 5

  posisi ke 5 > posisi ke 1, ya maka posisi ke 5 = 3 – 1

  Hasil:

Posisi	3	0	1	2
Nilai	16555215	16721724	16772111	16890155
Ke	2	3	4	5

- i = 2

  M = 15 * (6 – 2) + 3 = 63

  j = 3

  posisi ke 3 > posisi ke 2, tidak

  j = 4

  posisi ke 4 > posisi ke 2, tidak

  j = 5

  posisi ke 5 > posisi ke 2, tidak

  Hasil:

Posisi	0	1	2
Nilai	16721724	16772111	16890155
Ke	3	4	5

- i = 3

  M = 63 * (6 – 3) + 0 = 189

j = 4

posisi ke 4 > posisi ke 3, ya maka posisi ke 4 = 1 – 1

j = 5

posisi ke 5 > posisi ke 3, ya maka posisi ke 5 = 2 – 1

Hasil:

Posisi	0	1
Nilai	16772111	16890155
Ke	4	5

- i = 4

  M = 189 * (6 – 4) + 0 = 378

  j = 5

  posisi ke 5 > posisi ke 4, maka posisi ke 5 = 1 – 1

- i = 5

  M = 378 * (6 – 5) + 0 = 378

5. Konversi M menjadi bentuk biner, didapatkan 101111010.
6. Menghilangkan angka 1 di bagian paling kiri, didapatkan 01111010.

3.5.4 Perhitungan Proses Dekripsi 3DES

Proses dekripsi 3DES telah dijelaskan pada bab 2.4. Perhitungan manual dimulai dari permutasi awal. Setiap blok *ciphertext* terdiri dari 8 karakter. Sebagai contoh *ciphertext* yang dimasukkan yaitu hasil dari perhitungan proses enkripsi 3DES “0010100001111001111100110000110100010011110111011000001010001111”.

Setelah terbentuk blok *ciphertext* maka dilakukan permutasi awal sebagai berikut:

0010011000110110101010001011111011100100000001111010101111010100

Kunci internal pertama dibangkitkan dari inputan kunci ketiga yaitu “threedes”. Kunci diubah ke bentuk biner dan didapatkan “01110100011010000111001001100101011001010110010001100101011100 11”. Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan.

Setelah mendapakan 8 kelompok, dilakukan permutasi dengan PC-1 sehingga didapatkan:

00000000111111111111111110001000010001111001000 0 00100101

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 00000000111111111111111111000

D_0 : 10000100011110010000000100101

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.11.

Tabel 3.11 Kunci Internal Dari Kunci Eksternal Ketiga

Kunci	Isi Kunci
K_1	111100001011111001100110000101010010001101001000
K_2	111000001011111001110110010101000000011000010101
K_3	111001001111011001110110010110110000000011001100
K_4	111001101101011101110010000000001111000110001001
K_5	111011101101001101110011001000100011010000100101
K_6	101011111101001101011011111010100000100110100010
K_7	001011110101001111011011000001000100101100011011
K_8	001111110101100111011001010101110001000001010000
K_9	000111110101100111011001110010001000001001010110
K_{10}	000111110110100111011101010101011100011010001000
K_{11}	000111110110110110001101000110000001010001001001
K_{12}	010110110010110110101101100010101111000000100100
K_{13}	110110011010110010101101001000000110111110100000
K_{14}	110100011010111010101110101110000000100000010011
K_{15}	111100001011111010100110110001110100001000010010
K_{16}	111100001011111000100110100000011000101110000010

Selanjutnya melakukan proses deciphering. Blok *plaintext* dibagi menjadi dua bagian kiri dan kanan.

L : 00100110001101101010100010111110

R : 11100100000001111010101111010100

Setiap blok *plaintext* mengalami 16 kali putaran. Hasil putaran ditunjukkan pada Tabel 3.12.

Tabel 3.12 Deciphering Blok *Ciphertext* Tahap Pertama

Putaran	Hasil Deciphering
1	11100100000001111010101111010100000010010111100101001000011001111
2	00001001011110010100100001100111100110010010001010001101101011110
3	10011001001000101000110110101110111110110100000101100011111001111
4	11111011010000010110001111100111101000111000101101000011110111111
5	10100011100010110100001111011111001101100010001100110110010101011
6	00110110001000110011011001010101001101010111111111111110110010100
7	00110101011111111111111011001010000000111011101000110111001101000
8	00000111011101000110111001101000100100010101111100011001011000000
9	10010001010111110001100101100000011110110001100101011001010001111
10	01111011000110010101100101000111101001001011000111011111000101000
11	10100100101100011101111100010100111011101011011111100100110100011
12	11101110101101111110010011010001101100011011010110001110001000010
13	10110001101101011000111000100010011000001011000101001011010000010
14	01100000101100010100101101000010100100011010011110101101110111001100
15	10010001101001111010110111011100001110101001111011111101001001111
16	00111010100111101111110100100111110101111100111001101100101010101 0

Setelah selesai proses deciphering, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh,

0100101011110011011111101011110111101000100011110101110001111001.

Selanjutnya dilakukan proses enkripsi dengan menggunakan kunci kedua, yaitu “dekripsi”. Kunci diubah ke bentuk biner dan didapatkan “011001000110010101101011011100100110100101110000011100110110100 1”.

Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan. Selanjutnya dilakukan permutasi dengan PC-1 sehingga didapatkan: 0000000 0111111 1111111 1110110 0100110 0000000 1110010 1001000

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 00000000111111111111111110110

D_0 : 01001100000000111001010010000

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.13.

Tabel 3.13 Kunci Internal Dari Kunci Eksternal Kedua

Kunci	Isi Kunci
K_1	111000001011111011100110010010000010110000010011
K_2	111100001011011001110110101000001001000100110001
K_3	111001001101111001110110100000110000111000100010
K_4	111001101111001101110110010111000000101100010000
K_5	101011101101011101110011000100010100000001011100
K_6	111011110101001101111011010000011011000010000000
K_7	101011111101001111011001101000000010010000101101
K_8	000111110101101111011011001010100001101010000110
K_9	001111110100101111011001000010100010000100100010
K_{10}	000111110111100110011101101001000110100100000100
K_{11}	000111110010110111011101011000000000001011010010
K_{12}	010111110110110010101101110101011000000000001011
K_{13}	110110111010110110101100000001100001011001001000
K_{14}	110110001010111010101111000110001011000101100100
K_{15}	111100011011111000101110001000001100110010100000
K_{16}	111100001011111010101110000000100111100011001000

Permutasi awal blok *ciphertext* sebagai berikut:

110101111100111001101100101010100011101010011111011111110100100111

Selanjutnya melakukan proses *enciphering*. Blok *ciphertext* dibagi menjadi dua bagian kiri dan kanan.

L : 11010111110011100110110010101010

R : 00111010100111101111110100100111

Setiap blok *ciphertext* mengalami 16 kali putaran. Hasil putaran ditunjukkan pada Tabel 3.14.

Tabel 3.14 Enkripsi Blok *Ciphertext* Tahap Kedua

Putaran	Hasil *Enciphering*
1	00111010100111101111110100100111101111000000010000010111111011
2	10111100000000100000010111111011111111011100111111101101010010111
3	11111011100111111101101010010111110110110100000001011001110101
4	11011011010000000101100111010101101011001110101001000111011011111
5	10101100111010100100011101101111111100000011101011100110011010111
6	11110000001110101110011001101011100100011000100010001001101000000
7	10010001100010001000100110100000101111111001000111100000110001110
8	10111111100100011110000011000110011001111001011111110110101001111
9	01100111100101111111011010100111101100010101001000010101101110101
10	10110001010100100001010110111010011110000011000010001001010010111
11	01111000001100001000100101001011101010011100011111110101111100000
12	10101001110001111111010111110000000001000101110000011101111001111
13	00000100010111000001110111100111101010100111101101010101100111011
14	10101010011110110101010110011101111101001101001110111111001100000
15	11110100110100111011111001100000100010100001000001100001000100111
16	10001010000100000110000100010011110110110010001001110110100100111

Setelah selesai proses *enciphering*, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh,

01001011110101110000010011000000011001110001110001001100110000001

Selanjutnya dilakukan proses dekripsi dengan menggunakan kunci pertama, yaitu “enkripsi”. Kunci diubah ke bentuk biner dan didapatkan “01100101011011100110101101110010011010010111000001110011011010011”.

Kunci dibagi menjadi 8 kelompok dan bit ke 8 setiap kelompok diabaikan. Selanjutnya dilakukan permutasi dengan PC-1 sehingga didapatkan: 00000000111111111111111101100100111 0000000 1110010 1101000

Setelah permutasi dengan PC-1, dibagi menjadi 2 bagian, atas (C_0) dan bawah (D_0).

C_0 : 00000000111111111111111110110

D_0 : 01001110000000111001011010000

Kemudian melakukan pergeseran bit sesuai dengan Gambar 2.9 dan dilakukan permutasi dengan PC-2 hingga didapatkan 16 kunci internal yang ditunjukkan pada Tabel 3.15.

Tabel 3.15 Kunci Internal Dari Kunci Eksternal Pertama

Kunci	Isi Kunci
K_1	111000001011111011100110010010000010110010011011
K_2	111100001011011001110110101000001011010100110001
K_3	111001001101111001110110101010110000111000100010
K_4	111001101111001101110110010111000100101100010010
K_5	101011101101011101110011000101010100000001011100
K_6	111011110101001101111011110000011011000011000000
K_7	101011111101001111011001101000001010011000101101
K_8	000111110101101111011011001110100001111010000110
K_9	001111110100101111011001000010100011000100100110
K_{10}	000111110111100110011101101001000110100110100100
K_{11}	000111110010110111011101011000000000101011010011
K_{12}	010111110110110010101101110101111000000000011011
K_{13}	110110111010110110101100000001110001011101001000
K_{14}	110110001010111010101111000110001011000101100100
K_{15}	111100011011111000101110011000001100110010100100
K_{16}	111100001011111010101110000000101111100011001000

Permutasi awal blok *ciphertext* sebagai berikut:

1101101100100010011101101001001110001010000100000110000100010011

Selanjutnya melakukan proses deciphering. Blok *ciphertext* dibagi menjadi dua bagian kiri dan kanan.

L : 11011011001000100111011010010011

R : 10001010000100000110000100010011

Setiap blok *ciphertext* mengalami 16 kali putaran enkripsi. Hasil putaran ditunjukkan pada table 3.16.

Tabel 3.16 Deciphering Blok *Ciphertext* Tahap Ketiga

Putaran	Hasil Deciphering
1	10001010000100000110000100010011111001001101001110011111001101000
2	11100100110100111001111001101000110000110110010110011001100001110
3	11000011011001011001100110001110001000000100000011110000000101110
4	00100000010000001111000000101110000011101100010001100101110010010
5	00001110110001000110010111001010011101011111100100110101100100011
6	01110101111110010011010110010011010001111100000111001001000010110
7	01000111110000011100100100010110111101001001001101000000011110001
8	11110100100100110100000011110001001111101010110100010101011111001
9	00111110101011010001010101111001000011010000101110100010010110 1
10	00001110100001011101000100101101000110000100100110010011011110 11
11	00011000010010011001001101111011000100011001000101001100010111 11
12	00010001100100010100110001011111001101001110111000001001111001 11
13	00110100111011100000100111100111111011100111110101001000101001 11
14	11101110011111010100100010100111100111110111011110001100001111 01
15	10011111011101111000110000111101000000001111111001001000001000 1
16	00000000011111110010010000010001011111110001000100000000011110 10

Setelah selesai proses deciphering, maka dilakukan permutasi dengan matriks permutasi awal balikan dan diperoleh hasil akhir dari proses dekripsi 3DES sebagai berikut,

01110010011000010110100001100001011100110110100101100001000000000.

Selanjutnya diubah ke bentuk ASCII dan akan diperoleh pesan asli yaitu “rahasia”.