PERANGKAT LUNAK KRIPTOGRAFI FILE TEKS MENJADI BENTUK CITRA DIGITAL MENGGUNAKAN METODE KERBEROS

Romanus Damanik
Fakultas Ilmu Komputer, Universitas Katolik St.Thomas SU
E-mail : romanusdamanik@yahoo.com

ABSTRACT

Rapid development of current computer technology often lead to abuse of the technology in a criminal action. One of the most common is the theft of the Password (password), personal accounts until confidential documents. To that end, the perceived need for a form of safeguard against the things above in order to comfort the user in using computer technology. Encryption is one method to randomize the words so that it cannot be read and understood by anyone else except by users who use them and those who were given the right to use it. The Kerberos method is a method of encryption that originally applied to secure a computer network. Kerberos authentication works by comparing input data with the given keywords. Based on the workings of the Kerberos method, be designed a device for data security in the form of a text message is converted into the form of a digital image. Through the processing of Binary value from the message text inputed. will be generated a digital image is the result of a binary-binary encryption of text messages through the Kerberos method. This type of data security is more secure than cryptography that produce the same output with the Plaintext, such as cryptographic text messages that generate output in the form of a digital berbedayaitucitra denganbentuk message.

Keywords: *Cryptography, Kerberos, Conversion, Digital Imag*

ABSTRAK

Pesatnya perkembangan teknologi komputer saat ini sering mengakibatkan penyalahgunaan teknologi tersebut dalam tindakan kriminal. Salah satu yang paling sering terjadi adalah pencurian Password (kata sandi), Account pribadi hingga dokumen-dokumen rahasia. Untuk itu, dirasakan perlunya suatu bentuk pengamanan terhadap hal-hal di atas guna kenyamanan user dalam menggunakan teknologi komputer. Enkripsi adalah salah satu metode untuk mengacak kata-kata sehingga tidak dapat dibaca dan dimengerti oleh orang lain kecuali oleh user yang menggunakannya dan orang yang diberi hak untuk menggunakannya. Metode Kerberos merupakan sebuah metode enkripsi yang awalnya diterapkan untuk mengamankan suatu jaringan komputer. Kerberos bekerja dengan cara membandingkan autentikasi data input dengan kata kunci yang diberikan. Berdasarkan cara kerja metode Kerberos ini, dapat dirancang sebuah perangkat pengamanan data berupa pesan teks yang diubah menjadi bentuk sebuah citra digital. Melalui pengolahan nilai Biner dari pesan teks yang diinputkan. akan dihasilkan sebuah citra digital yang merupakan hasil enkripsi dari biner-biner pesan teks melalui metode Kerberos. Jenis pengamanan data ini lebih aman dibandingkan kriptografi yang menghasilkan output yang sama dengan Plaintext awal, seperti kriptografi pesan teks yang menghasilkan output berupa pesan denganbentuk yang berbedayaitucitra digital.

Kata Kunci: *Kriptografi, Kerberos, Konversi, Citra Digital*

PENDAHULUAN

Ada beberapa metode kriptografi yang dapat digunakan untuk mengamankan dokumen, antara lain adalah metode *Kerberos*. Metode *Kerberos* merupakan sebuah metode enkripsi yang awalnya diterapkan untuk mengamankan suatu jaringan komputer. *Kerberos* bekerja dengan cara membandingkan autentikasi data input dengan kata kunci yang diberikan. Jika autentikasi dan kata kunci valid, maka proses *Dekripsi* dapat dilakukan. Metode *Kerberos* bekerja dengan menggunakan prinsip pengolahan nilai *Biner*, dimana *biner-biner* pada suatu data akan di ekstrak untuk dibandingkan dengan *biner* kata kunci. Berdasarkan prinsip kerja tersebut, metode *Kerberos* dikenal sebagai *Secret Key Cryptography*.[1]

Citra *Digital*

Citra digital dapat didefinisikan sebagai fungsi dua variabel f(x,y), dimana x dan y adalah koordinat spasial dan nilai f(x,y) adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada Gambar dibawah ini . Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (Red, Green, Blue - RGB).[2]

Kriptografi

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi dalam www.mycrypto.net yaitu : [3]

1. Kerahasiaan (*Confidentiality*)
   Kerahaasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas Data (Data *Integrity*)
   Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Otentikasi (*Autentication*)
   Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Ketiadaan Peyangkalan (*Non-repudiation*).
   Non-repudiasi adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Kriptografi sebagai bidang ilmu tentu saja memiliki beberapa istilah tersendiri yang harus diketahui, beberapa istilah yang sering digunakan dalam kriptografi adalah:

1. *Plaintext*, merupakan pesan asli yang ingin dikirimkan dan dijaga keamananya. Pesan ini tidak lain dari informasi tersebut.
2. *Ciphertext*, merupakan pesan yang telah dikodekan (disandikan) sehingga sipa untuk dikirim.
3. *Cipher*, merupakan algoritma matematis yang digunakan untuk proses peyandian *plaintext* menjadi *ciphertext*.
4. Enkripsi, (*encryption*) merupakan proses yang dilakukan untuk meyandikan *plaintext* sehingga menjadi *ciphertext*.

5. Dekripsi, (*decryption*) merupakan proses yabg dilakukan untuk memperoleh kembali *plaintext* dari *ciphertext*.
6. Kriptanalisis
   Ilmu dan seni untuk membuka suatu *chipertext* secara ilegal.
7. Kriptografi, Ilmu matematika yang mendasari ilmu kriptografi dan kriptanalisis. (www.mycrypto.net). [3]

Metode Kerberos

Kerberos merupakan layanan autentikasi yang dikembangkan oleh MIT (*Massachusetts Institute of Technology*) Amerika Serikat, dengan bantuan dari Proyek *Athena*. Tujuannya adalah untuk memungkinkan pengguna (*user*) dan layanan (*service*) untuk saling mengautentikasi satu dengan yang lainnya. Dengan kata lain, saling menunjukkan identitasnya

Prinsip Kerja Metode *Kerberos*

Sistem autentikasi data pada metode *kerberos* bekerja dengan cara membentuk kata kunci khusus untuk setiap data autentikasi yang disebut *shared secret*. *Shared secret* disini adalah bahwa kata kunci tersebut hanya diketahui oleh pengguna dan server yang mengolah autentikasi tersebut. Pada metode *kerberos*, validasi autentikasi data, pengguna diberikan sebuah *Shared Secret Key* yang dibentuk oleh metode kerberos berdasarkan data yang diinputkannya. Dengan cara ini, akan dihasilkan *shared secret kemy* yang berbeda untuk setiap proses autentikasi dengan data yang sama.[4]

Adapun proses kerja autentikasi data pada metode *kerberos* adalah sebagai berikut :

1. Penginputan Data Autentikasi
2. Pembentukan Kunci Bersama
3. Pembentukan Kunci
4. Verifikasi Kunci

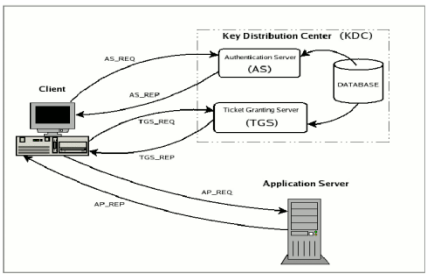
Operasi Dasar Dalam Sistem *Kerberos*

Adapun beberapa operasi tersebut antara lain :

1. AS_REQ
   Merupakan operasi yang digunakan untuk menerima permintaan data login baru dari pengguna. Pesan ini ditujukan kepada komponen KDC pada sistem.
2. AS_REP
   Merupakan operasi yang berisi jawaban dari KDC terhadap pesan sebelumnya. Pada dasarnya pesan ini mengandung TGT (dienkripsi menggunakan TGS *Secret Key*) dan *Session Key* (dienkripsi menggunakan *Secret Key* dari pengguna).
3. TGS_REQ
   Merupakan operasi yang digunakan untuk menerima *request* dari pengguna kepada *Ticket Granting Server* (TGS) untuk mendapatkan *service* ticket. Paket ini mengandung TGT yang didapat dari pesan sebelumnya dan *Authenticator* yang dibuat oleh pengguna dan dienkripsi dengan *Session Key*.
4. TGS_REP
   Merupakan operasi yang berisi jawaban dari *Ticket Granting Server* terhadap pesan sebelumnya. Dalam paket ini terdapat *Service Ticket* yang diminta (dienkripsi dengan *Secret Key* dari layanan) dan *Session Key* milik layanan yang dibuat oleh TGS dan dienkripsi dengan *Session Key* sebelumnya yang dibuat oleh KDC.
5. AP_REQ
   Merupakan operasi yang menerima request yang dikirimkan oleh pengguna kepada layanan/aplikasi agar dapat mengakses layanannya. Komponennya adalah *Service Ticket* yang didapat dari TGS dengan jawaban sebelumnya dan authenticator yang dibuat oleh pengguna, tetapi kali ini dienkripsi

menggunakan *Session Key* milik layanan (dibuat oleh TGS).

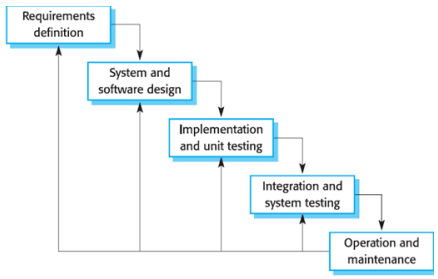
6. AP_REP
   Merupakan operasi yang berisi jawaban yang diberikan oleh layanan kepada pengguna untuk membuktikan bahwa layanan tersebut adalah benar merupakan layanan yang ingin diakses oleh pengguna. [5]



Gambar 1. Urutan Operasi Dalam Sistem *Kerberos*

METODE PENELITIAN

Metode pengembangan sistem yang digunakan dalam penelitian ini mengikuti model Waterfall System development Life cycle (Sommerville 1995). Diagram dari metode ini digambarkan pada gambar 2 :



Gambar 2 . Waterfall System Development Life Cycle)

1. Definisi Kebutuhan
   Dari proses ini akan diperoleh gambaran sistem seara umum, tujuan dari sistem serta spesifikasi perangkat keras dan perangkat lunak yang diperlukan untuk pengembangan sistem.
2. Perancangan Sistem dan Perangkat Lunak
   Pada fase ini beberapa hal yang akan dilakukan adalah perancangan input, output, proses, struktur data dan basis data.
   Proses-proses yang dirancanga adalah proses dari sistem keseluruhan dan proses-proses yang mendukung berjalannya sistem. Proses-proses dirancang sedemikian rupa sehingga dapat diimplementasikan dalam bentuk model-model.
3. Implementasi dan Pengujian Unit
   Setelah dirancang seluruh prosesnya beserta struktur dan basis datanya telah ditentukan maka tahap implementasi dan pengujian terhadap modul-modul pendkung dari sistem.
4. Integrasi dan Pengujian Sistem
   Modul-modul yang telah diimplementasikan kemudian diitegrasikan menjadi suatu sistem yang utuh untuk mengetahui apakah sistem berjalan sesuai dengan tujuan yang dinyatakan dalam definisi kebutuhan, maka dilakukan pengujian sistem secara keseluruhan.
5. Operasi dan Pemeliharaan
   Karena sistem yang dibangun adalah untuk tujuan penelitian, maka proses operasi dan pemeliharaan tidak dilakukan.

HASIL DAN PEMBAHASAN

Dalam analisa ini, akan digunakan sebuah contoh kasus untuk mengenkripsi sebuah pesan teks “testing metode kerberos”. Langkah pertama yang dilakukan adalah melakukan *Request* kepada server kerberos dimana server kerberos yang dimaksud merupakan database dari sql yang telah di instalkan kedalam aplikasi untuk mendapatkan kunci keamanan secara otomatis. Server kerberos yang akan

digunakan adalah server dalam bentuk *Library* SQLite dimana file *Library* dapat diunduh pada alamat : *http://www.sqlite.org/sqlite-dll-win32-x86-3070603.zip.[..] Library* ini berisi sebuah fungsi PRNG (*Pseudo Random Number Generator*) yang akan menghasilkan sebuah nilai balikan dalam bentuk *biner* terhadap *Record* di dalam aplikasi yang akan dirancang. Pesan teks yang dikirimkan akan disimpan dalam sebuah tabel *Temporary* atau sebuah variabel setelah terlebih dahulu dikonversi dalam bentuk biner. Dengan menggunakan "testing metode kerberos" sebagai *Record* yang akan disimpan di dalam tabel SQLite, maka SQLite akan mengkonversi teks tersebut menjadi bentuk biner berikut :

01110100 t	01100101 e	01110011 s
01110100 t	01101001 i	01101110 n
01100111 g	00100000 (spasi)	01101101 m
01100101 e	01110100 t	01101111 o
01100100 d	01100101 e	00100000 (spasi)
01101011 k	01100101 e	01110010 r
01100010 p	01100101 e	01110010 r
01101111 o	01110011 s	

Pesan dalam bentuk *Biner* ini kemudian akan disimpan ke dalam tabel SQLite dimana SQLite adalah variabel penampung bilangan *Biner* yang akan digunakan untuk mengembalikan kepada pengguna sebagai *Shared Key* pada proses enkripsi.

Sebagai contoh, dihasilkan nilai *Biner* 1000010111. Nilai ini akan dikembalikan kepada pengguna sebagai *Shared key* pada proses enkripsi.

Setelah *Shared Key* diperoleh dari Server, selanjutnya akan dilakukan *Request* untuk melakukan proses enkripsi serta penyerahan *Shared Key* yang diterima dari Server. Server *Chiper Text* akan melakukan proses XOR terhadap *Record* yang tersimpan di dalam tabel SQLite dengan *Shared Key* yang diinputkan pengguna.

Berdasarkan contoh kasus di atas, maka dilakukan proses XOR terhadap seluruh elemen *Record* dengan langkah sebagai berikut :

1. *Record* 01110100 (t)
   C_1 = 01110100 XOR 1000010111
   = 1001100011
2. *Record* 01100101 (e)
   C_2 = 01100101 XOR 1000010111
   = 101101110
3. *Record* 01110011 (s)
   C_3 = 01110011 XOR 1000010111
   = 1001100100
4. *Record* 01110100 (t)
   C_4 = 01110100 XOR 1000010111
   = 1001100011
5. *Record* 01101001 (i)
   C_5 = 01101001 XOR 1000010111
   = 1001111110
6. *Record* 01101110 (n)
   C_6 = 01101110 XOR 1000010111
   = 1001111001
7. *Record* 01100111 (g)
   C_7 = 01100111 XOR 1000010111
   = 1001110000
8. *Record* 00100000 (spasi)
   C_8 = 00100000 XOR 1000010111
   = 1000110111
9. *Record* 01101101 (m)
   C_9 = 01101101 XOR 1000010111
   = 101100110
10. *Record* 01100101 (e)
    C_{10} = 01100101 XOR 1000010111
    = 101101110
11. *Record* 01110100 (t)
    C_{11} = 01110100 XOR 1000010111
    = 1001100011
12. *Record* 01101111 (o)
    C_{12} = 01101111 XOR 1000010111
    = 1001111000
13. *Record* 01100100 (d)
    C_{13} = 01100100 XOR 1000010111
    = 1001110011
14. *Record* 01100101 (e)
    C_{14} = 01100101 XOR 1000010111

= 101101110

15. *Record* 00100000 (spasi)
    C_{15} = 00100000 XOR 1000010111
    = 1000110111
16. *Record* 01101011 (k)
    C_{16} = 01101011 XOR 1000010111
    = 1001111100
17. *Record* 01100101 (e)
    C_{17} = 01100101 XOR 1000010111
    = 101101110
18. *Record* 01110010 (r)
    C_{18} = 01110010 XOR 1000010111
    = 1001100101
19. *Record* 01100010 (b)
    C_{19} = 01100010 XOR 1000010111
    = 1001110101
20. *Record* 01100101 (e)
    C_{20} = 01100101 XOR 1000010111
    = 101101110
21. *Record* 01110010 (r)
    C_{21} = 01110010 XOR 1000010111
    = 1001100101
22. *Record* 01101111 (o)
    C_{22} = 01101111 XOR 1000010111
    = 1001111000
23. *Record* 01110011 (s)
    C_{23} = 01110011 XOR 1000010111
    = 1001100100

Dari hasil proses ini, diperoleh chiper text sebagai berikut :

1001100011 101101110 1001100100 1001100011 1001111110 1001111001 1001110000 100011011 1101100110 101101110 1001100011 1001111000 1001110011 101101110 1000110111 1001111100 101101110 1001100101 1001110101 101101110 1001100101 1001111000 1001100100

Sampai pada langkah ini, metode *Chiper Text* telah selesai. Namun, untuk lebih menjamin keamanan data hasil enkripsi tersebut, nilai-nilai *Biner* ini akan diubah menjadi bentuk citra digital. Untuk melakukan hal tersebut, nilai-nilai biner ini harus dikonversi terlebih dahulu ke dalam bentuk desimal. Adapun hasil konversi *Chiper Text* dalam bentuk *Biner* tersebut ke dalam bentuk desimal adalah sebagai berikut :

611 366 612 611 638 633 624 567 358 366 611 632 627 366 567 636 366 613 629 366 613 632 612

Nilai desimal ini akan digunakan sebagai nilai *Pixel* yang akan dikonversi dalam mode warna RGB. Untuk melakukan konversi ini, digunakan persamaan berikut :

R = P MOD 256
G = P MOD 256
B = P MOD 256 .....(1)

Dengan menggunakan persamaan tersebut, diperoleh nilai RGB dari masing-masing nilai *Pixel* tersebut sebagai berikut :

1. *Pixel* 611
   R = 99
   G = 2
   B = 0

Nilai RGB di dapat dengan cara membagikan dengan menggunakan persamaan 1.

Pixel 611= 611 : 256 = 2 (nilai G)

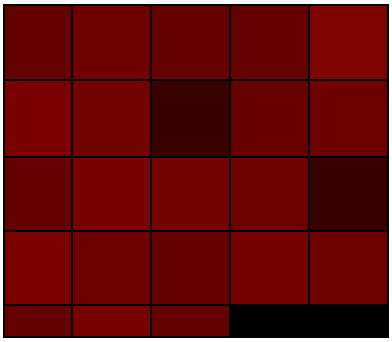
Sisa dari pembagiannya 99 (nilai R), dan 0 (nilai B)

2. *Pixel* 366
   R = 110
   G = 1
   B = 0
3. *Pixel* 612
   R = 100
   G = 2
   B = 0
4. *Pixel* 611
   R = 99
   G = 2
   B = 0
5. *Pixel* 638
   R = 126
   G = 2
   B = 0
6. *Pixel* 633
   R = 121
   G = 2
   B = 0
7. *Pixel* 624
   R = 112
   G = 2

B = 0

8. *Pixel* 567
   R = 55
   G = 2
   B = 0
9. *Pixel* 358
   R = 102
   G = 1
   B = 0
10. *Pixel* 366
   R = 110
   G = 1
   B = 0
11. *Pixel* 611
   R = 99
   G = 2
   B = 0
12. *Pixel* 632
   R = 120
   G = 2
   B = 0
13. *Pixel* 627
   R = 115
   G = 2
   B = 0
14. *Pixel* 366
   R = 110
   G = 1
   B = 0
15. *Pixel* 567
   R = 55
   G = 2
   B = 0
16. *Pixel* 636
   R = 124
   G = 2
   B = 0
17. *Pixel* 366
   R = 110
   G = 1
   B = 0
18. *Pixel* 613
   R = 101
   G = 2
   B = 0
19. *Pixel* 629
   R = 117
   G = 2
   B = 0
20. *Pixel* 366
   R = 110
   G = 1
   B = 0
21. *Pixel* 613
   R = 101
   G = 2
   B = 0
22. *Pixel* 632
   R = 120
   G = 2
   B = 0
23. *Pixel* 612
   R = 100
   G = 2
   B = 0

Jika nilai-nilai RGB tersebut dipetakan ke dalam sebuah matriks 5 X 5 dengan warna *Background* hitam, maka diperoleh hasil enkripsi pesan teks "testing metode *Chiper Text* " dalam bentuk citra digital seperti terlihat pada Gambar 3.



Gambar 3. Citra Digital Hasil Enkripsi

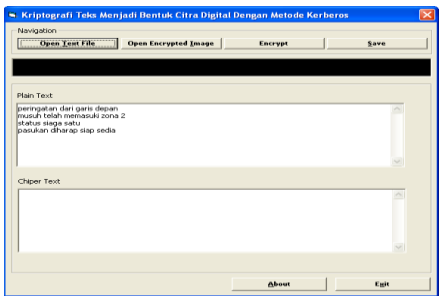
Pengujian Sistem

Setelah mendapatkan hasil tampilan perangkat lunak, selanjutnya dilakukan pengujian terhadap sistem tersebut. Adapun metode pengujian sistem yang penulis lakukan adalah metode *black box* dimana pengujian dibagi dalam beberapa tahapan.

1. Pengujian Proses Enkripsi
   Pengujian proses Enkripsi dilakukan untuk melihat apakah masih terdapat galat (*error*) pada saat proses enkripsi dilakukan pada *Form*

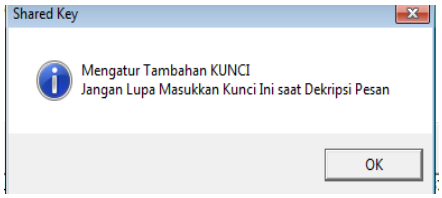
Kerberos. Dalam pengujian ini, dilakukan enrkripsi terhadap sebuah file teks yang berisi pesan sebagai berikut : ”peringatan dari garis depan Musuh telah memasuki zona 2 Status siaga satu Pasukan diharap siap sedia”

Langkah pertama yang dilakukan adalah melakukan *load* terhadap file tersebut dengan menekan tombol Open Text File dan memilih nama file. Hasil yang diperoleh adalah munculnya isi file pada *Text Box* Plain Text, sebagaimana terlihat pada Gambar 4.



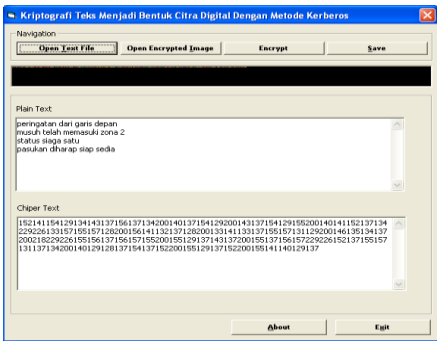
Gambar 4. Hasil Proses *Open File Text*

Selanjutnya, dilakukan penekanan tombol *Encrypt* pada *Form Kerberos*. Hasil yang diperoleh adalah munculnya sebuah pesan yang berisi *Shared Key* yang digunakan dalam proses enkripsi file teks ini, sebagaimana terlihat pada Gambar 5.



Gambar 5. *Shared Key* Proses Enkripsi

Setelah dilakukan penekanan tombol OK pada pesan tersebut, muncul sebuah chiper text pada *Text Box* Chiper Text, yang merupakan hasil proses enkripsi file teks yang diinputkan



Gambar 6. Hasil Proses Enkripsi

Selain *chiper text*, *output* lain yang dihasilkan dari proses enkripsi ini adalah sebuah gambar yang merupakan hasil konversi dari *chiper text* menjadi bentuk *pixel* gambar. Gambar ini kemudian disimpan ke dalam file BMP dengan nama Enkripsi.bmp. Setelah gambar tersimpan, dilakukan pengecekan terhadap isi gambar tersebut. Pengecekan dilakukan dengan menggunakan aplikasi ACDSee Pro, dimana hasilnya seperti terlihat pada Gambar 7.

Gambar 7. Citra Digital Hasil Proses Enkripsi

Pengujian proses Dekripsi dilakukan untuk melihat apakah masih terdapat galat (*error*) pada saat proses dekripsi dilakukan pada Form Kerberos.

Berdasarkan hasil pengujian di atas, dilakukan analisa terhadap kemampuan perangkat lunak dalam melakukan kriptografi teks menjadi bentuk citra digital. Sebagai bahan acuan analisa ini, digunakan hasil pengujian sistem sebelumnya yang dirangkum dalam bentuk tabel, seperti terlihat pada Tabel berikut.

Tabel 1. Hasil Pengujian Sistem

Jenis Pengujian	*Plain Text / Chiper Text*	*Shared Key*	*Cipher Text / Plain Text*
Enkripsi	Peringatan dari garis depan Musuh telah memasuki zona 2 Status siaga satu Pasukan diharap siap sedia	232	152141154129134143137156137134 200140137154129200143137154129 155200140141152137134229226165 157155157128200156141132137128 200133141133137155157131129200 146135134137200218229226187156 137156157155200155129137143137 200155137156157229226184137155 157131137134200140129128137154 137152200155129137152200155141 140129137
Dekripsi	152141154129134143137156171342001401371541292005143171541291552001401411521371342292261651571551571282001561411321371282001331411313715515713112920014613513137200218229226187156137151571552001551291371431372015513715615722922618413715157131137134200140129128137154137152200155129137152200155141140129137	232	peringatan dari garis depan Musuh telah memasuki zona 2 Status siaga satu Pasukan diharap siap sedia
Gambar Hasil Citra Digital			
Dekripsi	152141154129134143137156171342001401371541292005143171541291552001401411521342292261651571551571282015614113213712820013314133171555157131129200146135134137200218229226187156137151571552001551291371431372015513715615722922618413715517131137134200140129128137154137152200155129137152200155141140129137	231	❑j}fahn{na/kn}f/hn}f|/kj❑haBz|zg/{j cng/bjbn|zdf/u`an/=\{n{z|/|fnhn/|n{z_ n|zdna/kfgn}n❑/|fn❑/|jkfn
Gambar Hasil Citra Digital			

KESIMPULAN

1. Cara kerja metode *Kerberos* menggunakan kata kunci dalam bentuk acak sebagai alat autentikasi pada proses dekripsi dan enkripsi.
2. Dengan mengubah nilai ASCII *Chiper text* menjadi bentuk nilai *pixel*, dapat dilakukan konversi *Chiper Text* kemudian di konversi menjadi menjadi bentuk citra digital. Pengubahan *Chiper Text* menjadi bentuk citra digital akan mempersulit proses kriptanalis *Chiper Text* tersebut, karena formatnya telah berubah.
3. Hasil enkripsi yang dihasilkan sistem dalam bentuk numerik, lebih aman dibandingkan hasil enkripsi yang menggunakan karakter alfabet.Hasil enkripsi yang dihasilkan juga dalam bentuk citra digital dengan extensi BMP.

DAFTAR PUSTAKA

[1]Lubis Ali Akbar, Wong Ng Poi, Arfiandi Irfan, Damanik V Immanuel dan Maulana Adithya, 2015, Steganografi Pada Citra Dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher, JSM STMIK Mikroskil. Vol 16 (2) : 125-134. Diakses 09 Juni 2016

[2]Hojabri, K.V. Rao, Innovation in cloud computing : Implementation of Kerberos version5 in cloudcomputing in order to enhance the security issues. Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.452,456, 21-22 Feb. 2013.

[3]C.Neuman, et.al., "The Kerberos Network Authentication Service (V5)," IETF RFC 4120, Juli 2005

[4]Linn, J., Juni 1996, *The Kerberos Version 5 GSS-API Mechanism*, IETF, RFC 1964, diakses 1 Desember 2016.

[5]Aura, Tuomas. *Network Security: Kerberos*[pdf].http://research.microsoft.com/enus/um/people/tuomaura/teaching/network-security kerberos.pdf (diakses tanggal 1 Desember 2016)