TEKNIK KEAMANAN PESAN MENGGUNAKAN KRIPTOGRAFI DENGAN MODE ELECTRONIC CODE BOOK (ECB) DAN STEGANOGRAFI DENGAN METODE LEAST SIGNIFICANT BIT (LSB)

Hardhian Yuniansyah

Jurusan Teknik Informatika-S1, Fakultas Ilmu Komputer

Universitas Dian Nuswantoro Semarang

Jln. Nakula I no 5-17 Semarang 50131 INDONESIA

111201005370@mhs.dinus.ac.id

Sejalan dengan pesatnya perkembangan teknologi, kebutuhan manusia akan pertukaran informasi cukuplah besar. Oleh karena itu, pengiriman dan penyimpanan pesan memerlukan suatu proses yang mampu menjamin kemanan pesan tersebut dari penyadapan maupun pencurian pesan yang dianggap penting. Untuk menjamin keamanan dari suatu pesan yang akan dikirimkan, dibutuhkan suatu teknik untuk menyandikan ataupun mengacak pesan tersebut. Dengan melakukan proses enkripsi pada pesan yang akan dikirim, Proses ini adalah mengubah pesan asal menjadi pesan rahasia yang acak sehingga tidak dapat dibaca. Selanjutnya, adalah proses dekripsi yaitu mengubah pesan yang acak tadi sehingga dapat dibaca kembali oleh penerima. Dengan cara tadi, pesan asli tidak akan terbaca oleh pihak yang tidak dimaksud, melainkan hanya oleh penerima yang memiliki kunci untuk mendekripsikan pesan tersebut. Salah satu teknik untuk mengamankan pesan yaitu dengan mengimplementasikan kriptografi dengan mode ECB (*Electronic Code Book*). Sebagai contoh penggunaan kriptografi dengan kunci simetri, teknik ini cukup mampu untuk mengamankan informasi termasuk pesan, Sehingga teknik ini dapat digunakan untuk mengamankan pesan. Untuk lebih meningkatkan tingkat keamanan diperlukan teknik penyembunyian pesan ke dalam file yang sering disebut dengan Steganografi. Hal ini untuk mengalihkan perhatian pihak yang tidak berkepentingan untuk mengetahui ini pesan yang ada dalam gambar. Pada hal ini digunakan teknik penyembunyian pesan dengan metode LSB (*Least Significant Bit*). Dengan menggunakan teknik ECB (*Electronic Code Book*) dan LSB (*Least Significant Bit*) dibuatlah program aplikasi yang digunakan untuk melakukan pengamanan pesan sehingga hanya orang-orang tertentu saja yang mengetahui isi pesan.

Kata kunci : electronic code book, least significant bit

Along with the rapid development of technology, the human need for exchange of information large enough. Therefore, delivery and storage of messages requires a process that is capable of guaranteeing the security of the message from eavesdropping and theft are considered important message. To ensure the security of a message to be delivered, we need a technique to encode or scramble the message. By performing encryption on the message to be sent, this process is to change the origin of a message into a random secret message that can not be read. Furthermore, the decryption process is the random change message earlier so it can be read back by the receiver. By the way earlier, the original message will not be read by a person not mentioned, but only by a receiver who has the key to decrypt the message. One

technique for securing messages is to implement cryptographic with ECB mode (Electronic Code Book). For example, the use of cryptography with symmetric keys, this technique is capable enough to secure information including messages, so this technique can be used to secure the message. To further increase the level of security required concealment message into a file that is often referred to as steganography. This is to divert the attention of those who are not interested to know that there is a message in the picture. In this case the message concealment technique used by the method of LSB (Least Significant Bit). By using the technique of the ECB (Electronic Code Book) and LSB (Least Significant Bit) made an application program that is used to secure the message so that only certain people who know the content of the message.

Keywords: electronic code book, the least significant bits

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini sudah sangat pesat dan memberikan pengaruh yang cukup besar bagi kehidupan di masyarakat. Sejalan dengan perkembangan teknologi informasi dan komunikasi yang semakin pesat saat ini maka proses pertukaran data maupun pesan dapat dilakukan dengan mudah dan banyak tersedia media untuk melakukan pertukaran data maupun pesan tersebut antara lain melalui media internet seperti fasilitase-mail, melalui transfer data antar perangkat mobile (handphone, PDA dan flasdisk) maupun dengan teknologi radio frequency (bluethoot, IrDA, GPRS). [1]

Seiring dengan berkembangnya teknologi informasi dan komunikasi muncul sebuah kekhawatiran bagi user tentang keamanan data maupun pesan yang mereka kirimkan, apakah terjadi penyadapan saat proses pengiriman. Dengan itu dibutuhkan suatu teknik untuk pengamanan data maupun pesan guna menghindari penyadapan saat proses pengiriman berlangsung, salah satunya melakukan *enkripsi* pada data maupun pesan menjadi *chiperfile* maupun *chipertext*.

Saat ini kriptografi dapat dijadikan salah satu teknik yang dapat diterapkan untuk pengaman data maupun pesan. Dengan cara melakukan enkripsi pada data maupun pesan menjadi kode-kode tertentu, sehingga hanya orang tertentu saja yang dapat mengerti dari data maupun pesan tersebut setelah mendeskripsinya. Hal ini dirasa cukup aman untuk meminimalisir proses penyadapan maupun pencurian data atau pesan yang kita kirim.

Dalam perkembangan dunia kriptografi sudah tercipta banyak sekali algoritma yang dapat kita aplikasikan untuk mengubah data asli menjadi data yang sudah disandikan. Salah satunya adalah algoritma Electroonic Code Book (EBC) yang termasuk dalam algoritma Block Chiper.

Untuk meningkatkan keamanan dari file yang telah dienkripsi ada baiknya menambahkan teknik lain untuk menyembunyikan file tersebut. Yaitu dengan cara menggabungkan file yang telah dienkrip ke dalam file cover seperti file gambar. Teknik seperti ini disebut *Steganografi*. *Steganografi* merupakan teknik yang cukup baik untuk mengurangi kecurigaan akan adanya file didalamnya, karena pesan yang disisipkan tidak kasat mata. Sehingga pihak yang tidak berkepentingan tidak akan mengetahui pesan yang terdapat pada file cover yang mereka lihat.

Dalam perkembangan teknik Steganografi saat ini, ada beberapa metode yang dapat digunakan untuk penyembunyian file tersebut salah satunya adalah dengan metode *Least Significant Bit (LSB)*.

II. METODE YANG DIUSULKAN

1.1 Tinjauan Studi

Berbagai penelitian yang dilakukan terdahulu, hasil yang menunjukan berbagai

hasil yang didapat tentang penerapan metode ECB (*Electronic Code Book*) dan *Least Significant Bit (LSB).*

Mahmuddin Yunus dan Agus Harjoko, "*Penyembunyian Data pada File video menggunakan metode LSB dan DCT*", mengkombinasikan metode Least Significant Bit (LSB) dan DCT untuk penyembunyian data pada file video.

Basuki Rakhmat dan Muhammad Fairuzabadi, M.kom, "*Steganografi menggunakan metode Least Significant Bit (LSB) dengan kombinasi Algoritma Kriptografi Vignere dan RC4*", mengintegrasikan kriptografi dan steganografi dalam sebuah sistem aplikasi. Pesan teks terlindungi dengan algoritma kriptografi dan tersembunyi dalam sebuah gambar.

Ranto Parluhutan Sitorus, "*Perancangan Aplikasi Pengamanan Data Dengan Menggunakan Algoritma Knapsack*"

Tri Andriyanto dan Dra. D .L Crispina Pardede, "*Studi dan Perbandingan Algoritma IDEA dan Algoritma Blowfish*" Membahas cara kerja algoritma Blowfish dan Penerapannya dalam suatu program aplikasi enkripsi dan dekripsi yang berukuran 128 bit dan mode operasi enkripsi menggunakan *Electronic Code Book* (ECB)

1.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani : "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" aritnya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan didalam 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 lagi maknanya. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudiation.* [2]

Di dalam kriptografi terdapat berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui antara lain:

a. Pesan, Plainteks, dan chiperteks
Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*) atau teks-jelas (*cleartext*). Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb). Pesan yang disimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (*image*), suara/bunyi (*voice*), dan video. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext*) atau kriptogram (*cryptogram*). Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca.[3]
b. Pengirim dan penerima
Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (receiver) adalah entitas yang menerima pesan. Entitas disini dapat berupa orang, kertu kredit, dan sebagainya. Pengirim tentu menginginkan pesan dapat dikirim secara aman, yaitu ia yakin bahwa pihak lain tidak dapat membaca isi pesan yang ia kirim. Solusinya adalah dengan cara menyandikan pesan menjadi cipherteks.

c. Enkripsi dan dekripsi
Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption). Sedangkan proses mengembalikan cipherteks menjadi plainteks dinamakan dekripsi (decryption). Enkripsi dan dekripsi dapat diterapkan baik pada pesan yang dikirim maupun pesan yang tersimpan.
d. Cipher dan kunci
Algoritma kriptografi disebut juga cipher yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi.

1.3 Mode Electronic Code Book (ECB)

Pada mode ini, setiap blok plainteks P_i dienkripsi secara individual dan independen menjadi blok chiperteks C_i. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai

$C_i = E_k (P_i)$

Dan dekripsi sebagai

$P_i = D_k (C_i)$

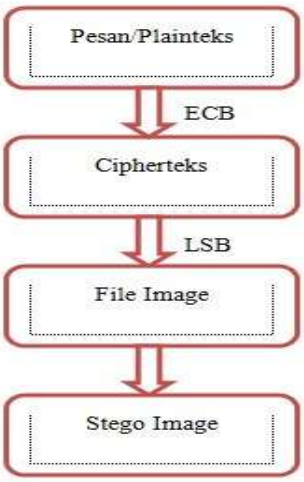
Yang dalam hal ini, *K* adalah kunci dan P*i* dan C*i* masing-masing blok plainteks dan chiperteks ke-*i*. Misalkan enkripsi *m* buah blok plainteks, P_1 ... P_m dan dekripsi *m* buah blok cipherteks, C_1 ... C*m* dengan mode ECB, yang dalam hal ini *E* menyatakan fungsi enkripsi dan D menyatakan yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci K. Istilah "*code book*" di dalam ECB muncul dari fakta bahwa karena blok plainteks yang sama selalu dienkripsi menjadi blok chiperteks yang sama, maka secara teoritis dimungkinkan membuat buku kode plainteks dan chiperteks yang berkoresponden. Namun, semakin besar ukuran blok, semakin besar pula ukuran buku kodenya. Misalkan jika blok berukuran 64 bit, maka buku kode terdiri dari $2^{64} - 1$ buah kode (*entry*), yang berarti selalu besar untuk disimpan. Lagipula, setiap kunci mempunyai buku kode yang berbeda.
Ada kemungkinan panjang plainteks tidak habis dibagi dengan panjang ukuran blok yang ditetapkan (misalnya 64 bit atau lainnya). Hal ini mengakibatkan blok terakhir berukuran lebih pendek daripada blok-blok lainnya. Satu cara untuk mengatasi hal ini adalah dengan *padding*, yaitu menambahkan blok terakhir dengan pola bit yang teratur agar panjangnya sama dengan ukuran blok yang ditetapkan, Misalnya ditambahkan bit 0 semua, atau bit 1 semua, atau bit 0 dan bit 1 berselang seling. Misalkan ukuran blok adalah 64 bit (8 *byte*) dan blok terakhir terdiri dari 24 bit (3 byte). Tambahkan blok terakhir dengan 40 bit (5 *byte*) agar menjadi 64 bit, misalnya dengan menambahkan 4 buah *byte* 0 dan satu buah *byte* angka 5. Setelah dekripsi, hapus 5 *byte* terakhir dari blok dekripsi terakhir.[3]

1.4 Algoritma Least Significant Bit (LSB)

Metode LSB (Least Significant Bit) merupakan metode steganografi yang paling sederhana dan paling mudah diimplementasikan. Untuk menjelaskan metode ini kita menggunakan citra digital sebagai *covertext*. Setiap *pixel* di dalam citra berukuran 1 sampai 3 *byte*. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant bit* atau LSB). Misalnya pada *byte* 11010010, bit 1 yang pertama (digaris bawahi) adalah bit MSB dan bit 0 yang terakhir (digaris bawahi) adalah LSB. Bit yang cocok untuk diganti dengan bit pesan adalah bit LSB, sebab modifikasi hanya mengubah nilai *byte* tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut di dalam gambar memberikan persepsi warna merah, maka perubahan satu bit LSB hanya mengubah persepsi warna merah tidak terlalu berarti. Mata masusia tidak dapat membedakan perubahan yang kecil ini.

1.5 Metode yang Digunakan

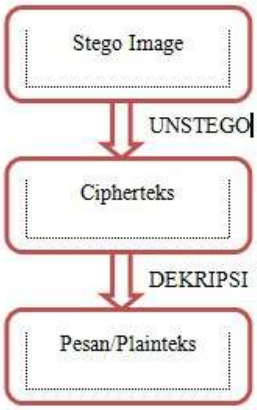
Teknik Kriptografi untuk pengenrkipsian pesan dan Steganografi untuk penyisipan pesan yang sudah dienkripsi ke dalam gambar. Adapun prosedur pengenkripsian dan penyisipan ke dalam file gambar adalah sebagai berikut :



Gambar 2.1 Prosedur Pengenkripsian dan Stego

Berdasarkan gambar diatas, proses enkripsi dan penyisipan menggunakan *Electronic Code Book* (ECB) dan *Least Significant Bit* (LSB). Adapun langkah-langkahnya akan dijelaskan sebagai berikut :

1. Lakukan pengenkripsian pesan/plainteks dengan menggunakan mode Electronic Code Book (ECB) untuk mendapatkan chiperteks.
2. Pilih file gambar/image yang akan digunakan sebagai wadah untuk menampung pesan yang sudah dienkripsi/cipherteks.
3. Lakukan penyisipan cipherteks menggunakan *Least Significant Bit* (LSB)



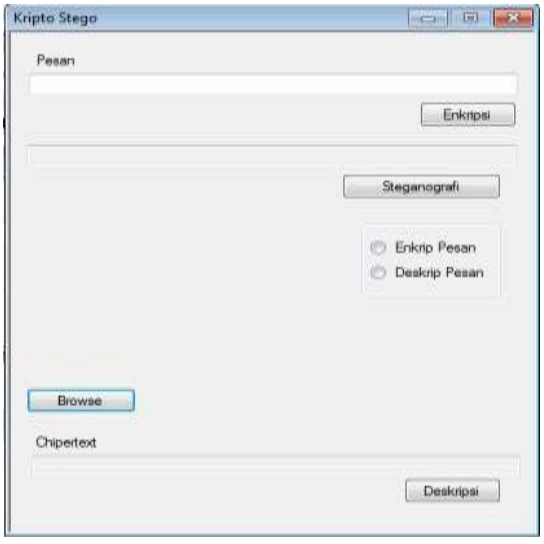
Gambar 2.2 Prosedur Pendekripsian dan Unstego

Berdasarkan gambar diatas, proses Unstego dan Dekripsi menggunakan *Electronic Code Book* (ECB) dan *Least Significant Bit* (LSB). Adapun langkah-langkahnya akan dijelaskan sebagai berikut :

1. Lakukan Unstego pada file Stego Image untuk mendapatkan cipherteks.
2. Dekripsikan kembali cipherteks yang sudah didapat untuk mendapatkan pesan/plainteks.

III. IMPLEMENTASI

Bahasa pemrograman yang digunakan untuk implementasi perangkat lunak ini adalah visual basic. Hasil pemodelan perangkat lunak dapat dilihat pada gambar berikut ini.



Gambar 3.1 Tampilan Awal Program

a. Proses Enkripsi

Proses kriptografi dan steganografi adalah dengan menuliskan pesan yang akan dienkripsi yang ada pada teksbox yang tersedia kemudian klik tombol enkripsi. Setelah itu pilih gambar yang akan kita sisipi cipherteks tadi kemudian pilih Enkrip Pesan

b. Proses Dekripsi

Pilih gambar yang akan didekripsi, pilih Dekrip Pesan, setelah didapatkan cipherteks kemudian klik tombol Dekripsi. Maka didapatkan pesan rahasia tadi.

IV. HASIL DAN PEMBAHASAN

Berikut cara kerja Mode Electronic Code Book (ECB) dengan pesan berupa bilangan hexa yaitu A23A9.[4]

a. Tahap Pertama :
   Pada tahap ini mengubah Pesan atau Plaintext di konversikan ke dalam biner. Dengan cara konversi menggunakan kode ASCII.
   Plaintext : A 2 3 A 9
   Biner : 1010 0010 0011 1010 1001

b. Tahap Kedua :
   Pada tahap ini melakukan pengubahan key atau kunci ke dalam bentuk biner.
   Key : 11
   Biner : 1011

c. Tahap Ketiga :
   Pada tahap ini dilakukan kombinasi antara plaintext dan key dengan menggunakan hubungan XOR.
   Plaintext :1010 0010 0011 1010 1001
   Key :1011 1011 1011 1011 1011
   XOR :0001 1001 1000 0001 0010

d. Tahap Keempat :
   Tahap ini adalah proses yang sangat sederhana yaitu melakukan pergeseran wrapping (siklik) pada tiap blok yang sudah terbagi. Jumlah pergeseran yang dilakukan sebanyak 1 bit ke kiri.
   XOR : 0001 1001 1000 0001 0010
   Geser 1 bit kekiri : 0010 0011 0001 0010 0100

e. Tahap Kelima :
   Pada tahap ini telah didapatkan biner baru yang akan dikonversikan kembali sehingga akan didapatkan ciphertext.
   Geser 1 bit kekiri :0010 0011 0001 0010 0100
   Chipertext :2 3 1 2 4

Bit atau binary digit adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 atau 1. Semua data yang ada pada komputer disimpan ke dalam satuan bit ini, termasuk gambar, suara, ataupun video. Jenis-jenis format pewarnaan di dalam media gambar. Misalkan sebuah data berupa text “secret“, kalau direpresentasikan ke dalam binary kata “secret“ ini menjadi :

Gambar 3.1 Secret Konversi Biner

Character	ASCII value (decimal)	Hexadecimal	Binary
s	115	73	01110011
e	101	65	01100101
c	99	63	01100011
r	114	72	01110010
e	99	63	01100011
t	116	74	01110100

Sesuai dengan namanya, LSB artinya bit yang tidak significant / tidak mempunyai pengaruh yang besar, maka metode ini mengganti nilai bit ke-8 gambar di atas untuk menyisipkan data. Misal sebuah data media yang telah di konfersikan ke biner

00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011

Gambar 3.1 Binary Media

Pada table binary media ini nantinya akan di sisipkan dengan table konversi pesan “secret”

Tabel 3.2 Binary Data

0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	0	0

Table di atas akan disisipkan dengan binary media, sesuai dengan aturan *least significant bit.*

Tabel 3.3 Hasil Penyisipan Sebuah Data atau Pesan

00000000	00000001	00000001	00000001	00000000	00000000	00000001	00000001
00000000	00000001	00000001	00000000	00000000	00000001	00000000	00000001
00000000	00000001	00000001	00000000	00000000	00000000	00000001	00000001
00000000	00000001	00000011	00000011	00000010	00000010	00000011	00000010
00000000	00000001	00000011	00000010	00000010	00000010	00000011	00000011
00000000	00000001	00000011	00000011	00000010	00000011	00000010	00000010

Semakin besar wadah*(cover-image)* yang digunakan untuk penyembunyian pesan maka semakin besar atau banyak pula jumlah karakter yang dapat disembunyikan dan semakin besar teks yang disembunyikan di dalam citra, semakin besar pula kemungkinan teks tersebut rusak akibat manipulasi pada citra penampung.

V. PENUTUP

5.1.Kesimpulan

Dari hasil perancangan dan pembuatan program aplikasi kriptografi dengan Algoritma Blok Chiper ECB (Electronic Code Block) dan Steganografi dengan metode Least Significant Bit (LSB) ini, dapat diambil kesimpulan sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan membuktikan bahwa aplikasi dapat melindungi pesan dan menyembunyikan pesan dengan aman dan tidak menimbulkan kecurigaan terhadap pihak-pihak yang tidak berhak untuk mengetahui isi pesan.
2. Hasil akhir tidak merusak objek penyimpan atau merusak kualitas image yang digunakan secara kasat mata, karena metode ini hanya mengubah bit yang paling tidak berpengaruh pada gambar.
3. Pesan yang terenkripsi dapat tersimpan dengan baik pada file gambar yang berjenis (.jpg, .bmp, .gif)

5.2.Saran

Saran-saran yang berguna pengembangan sistem dan aplikasi ini adalah sebagai berikut :

1. Menemukan algoritma lain untuk bisa tahan terhadap proses editing pada stego-image.
2. Untuk penelitian selanjutnya mungkin dapat mengembangkan aplikasi ini dengan menggunakan file lain seperti file pdf, word maupun mp3 untuk digunakan sebagai file wadah untuk menampung pesan.
3. Aplikasi ini masih dalam bentuk aplikasi desktop, akan lebih baik lagi apabila dikembangkan berbasis mobile.

REFERENCES

[1] Utami, Ema dan Sukrisno, Implementasi Steganografi EoF dengan Gabungan Enkripsi Rijndael, Shift Chiper dan Fungsi Hash, Yogyakarta, 2007

[2] Sadikin, Rifki, Kriptografi Untuk Keamanan Jaringan, Yogyakarta, Andi, 2012

[3] R. Munir, Kriptografi, Bandung: Informatika, 2006

[4] Kurniawan, Yusuf, Kriptografi Keamanan Internet dan Jaringan:Komunikasi, Bandung 2012