APLIKASI PENGAMANAN PESAN DENGAN ALGORITMA ROT 13 DAN STEGANOGRAFI END OF FILE

APPLICATION OF MESSAGE SECURITY USING ROT 13 AND STEGANOGRAPHY END OF FILE

Nidia Enjelita Saragih
Informatika, Fakultas Teknik dan Ilmu Komputer
Universitas Potensi Utama; Jl. KL. Yos Sudarso Km. 6,5 No 3-A Tanjung Mulia
e-mail: **nidia.1924@gmail.com**

Abstrak

Perkembangan teknologi terutama teknologi informasi dan komunikasi membawa dampak baik bagi kehidupan masyarakat, yaitu semakin mudahnya masyarakat saling bertukar informasi. Namun, di saat yang bersamaan kemudahan ini juga mendatangkan masalah baru, yakni kemungkinan seseorang untuk menyadap informasi dan menyalahgunakannya. Untuk mengatasi masalah tersebut digunakanlah teknik kriptografi. Dengan kriptografi, seorang penyadap tidak akan langsung bisa mengakses informasi yag dikirimkan melalui media pengiriman, karena sudah berbeda dengan bentuk pesan aslinya. Ada banyak algoritma yang diperkenalkan dalam bidang ini, salah satunya adalah algoritma ROT 13. Dalam algoritma ini, proses enkripsi dilakukan dengan menambahkan karakter asli dengan 13 karakter di atasnya. Untuk meningkatkan keamanan dalam masa pengiriman sehingga tidak menimbulkan kecurigaan, pesan tersandi bisa disisipkan ke dalam media penampung seperti gambar. Teknik penyisipan ini disebut dengan Steganografi. Salah satu teknik Steganografi yang cukup efektif menyembunyikan teks dalam gambar adalah End Of File.

Kata kunci— Kriptografi, Steganografi, ROT 13, End Of File.

Abstract

The technological development specially information and communication technology bring good impact on public life. They can easily exchange information to each other. However, this bring us a new problem. That someone can hack the information sent and do some missapproriate things. We can implementing Cryptography in solving that issue. So, a hacker have no ability to directly accessing information sent through the media, because it has change to a new form. There's several algorithm we known, one of them is ROT 13. In this algorithm, encription is implemented by adding the character in plaintext with 13 character after it. But, the message we got will be suspiciuos. Therefore, we need to put it in a another media, such as picture.This insertion technique is called Steganography. One the the effective technique of steganography is End Of File.

Keywords—Cryptography, Steganography, ROT 13, End Of File

1. PENDAHULUAN

Pesan yang merupakan aset bernilai yang seharusnya dilindungi agar aman dan tidak bisa diakses selain penerima pesan. Terutama pesan atau data yang berhubungan dengan informasi keamanan ataupun finansial.

Untuk memastikan bahwa pesan sampai dengan aman kepada penerima pesan dibutuhkan teknik untuk mengubah pesan asli yang akan dikirim kepada penerima, menjadi bentuk yang tersandikan. Teknik ini disebut dengan Kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi adalah proses penggunaan berbagai teknik dan atau ilmu dan seni untuk menjaga keamanan pesan,(Fauzi, dkk, 2017 :2).

Dalam kriptografi dikenal beberapa metode yang digunakan untuk mengubah pesan asli menjadi pesan rahasia, salah satunya adalah algoritma ROT13. ROT13 (*Rotate* 13) adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya.

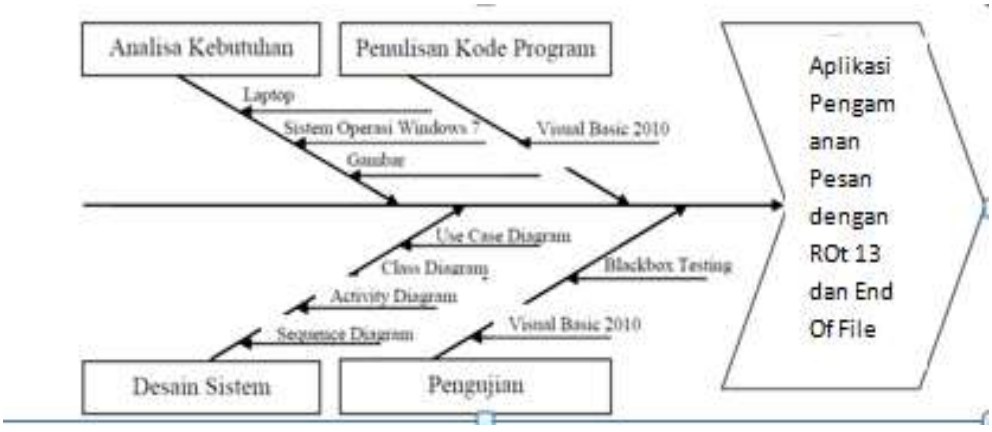
Pesan yang akan dikirim harus disandikan terlebih dahulu dengan menggunakan algoritma ROT 13 sebelum dikirimkan kepada penerima pesan. Masalah berikutnya yang mungkin muncul adalah bahwa dalam masa pengiriman pesan yang sudah dalam bentuk acak ini, sangat rentan menimbulkan kecurigaan yang berujung pada upaya untuk memecahkan plainteks dengan menggunaakan beragam cara. Oleh karena itu, dibutuhkan sebuah teknik tambahan untuk menyembunyikan pesan hasil enkripsi, agar tidak menimbulkan kecurigaan selama masa pengiriman pesan.

Teknik yang bisa digunakan adalah teknik penyisipan atau Steganografi. Dalam teknik steganografi, pesan rahasia disisipkan ke dalam media lain sehingga keberadaan pesan di dalam media tersebut tidak disadari oleh orang lain, selain pengirim dan penerima pesan.

Teknik ini bertujuan untuk menyembunyikan pesan rahasia dalam media digital tertentu sehingga dalam masa pengirimannya, tidak dicurigai oleh penyadap. Dalam penelitian ini, penggunaan steganografi dimaksudkan agar meningkatkan keamanan dari pesan yang akan dikirimkan. Dimana pesan yang sudah tersandikan dengan menggunakan algoritma ROT13, yang bisa saja menimbulkan kecurigaan sebagai sebuah pesan tersandi jika langsung dikirimkan melalui media pengiriman, akan disisipkan terlebih dahulu pada media gambar. Sehingga pengirim seolah seperti mengirimkan file gambar biasa kepada penerima, dan bukan mengirimkan pesan rahasia.

2. METODE PENELITIAN

Berikut adalah fish bone metode penelitian yang digunakan dalam penelitian ini.



Gambar 1. Diagram Fish Bone Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian. Peneliti juga menentukan *software* dan *hardware* yang akan digunakan untuk membuat penelitian. Adapun penentuan analisa kebutuhan, didasarkan kepada studi literatur yang telah dilakukan sebelumnya. Dalam studi literatur, didapatkan konsep-konsep dasar mengenai algoritma yang akan diterapkan dalam penelitian, yaitu sebagaimana yang akan dijelaskan berikut ini.

1.2. Uraian Teoritis

1.2.1.Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi adalah proses penggunaan berbagai teknik dan atau ilmu dan seni untuk menjaga keamanan pesan.

Dengan menggunakan teknik kriptografi, pesan asli yang selanjutnya disebut dengan plainteks akan mengalami perubahan dengan menggunakan proses tertentu sehingga menjadi bentuk yang berbeda dari pesan aslinya. Proses pengubahan ini disebut dengan proses enkripsi. Sementara pesan yang dihasilkan dari proses enkripsi disebut sebagai cipherteks. Cipherteks ini yang kemudian akan dikirimkan kepada penerima pesan. Setelah sampai pada penerima, pesan akan diubah kembali menjadi bentuk asli(plainteks) melalui proses dekripsi. Proses ini bertujuan mengubah cipherteks kembali menjadi plainteks sehingga bisa dipahami maknanya oleh penerima pesan.

1.2.2 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi diklasifikasikan menjadi dua jenis, yaitu :

1. Algoritma klasik. Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher*, *Vigenere Cipher*, dan *Hill Cipher*.
2. *Algoritma Kriptografi Modern*. Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, Contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain.

1.2.3. ROT13

ROT 13 merupakan salah satu algoritma kriptografi yang bekerja menyandikan pesan dengan cara mensubstitusikan sebuah karakter dengan 13 karakter sesudahnya.

Enkrip metode ROT13 menggunakan penjumlahan *ascii plaintext* dengan *ascii* kunci 13 sebagai berikut :

$$\mathrm{Ci} = \mathrm{Pi} + 13 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Keterangan :
Ci = *Ciphertext* hasil enkrip
Pi = *Plaintext* yang akan dienkrip

Dalam penelitian ini, setiap karakter dalam pesan asli terlebih dahulu diubah ke dalam indeks abjad. Kemudian nilai yang didapatkan diterapkan ke dalam persamaan di atas.

Sebagai contoh sebuah pesan berisi kata : "informatika"

Untuk karakter pertama, yakni "i", yang merupakan huruf ke-9 dalam deret abjad. Maka :

$$C(1) = P(1) + 13$$

= 9 + 13
= 22 = v

Untuk karakter kedua, yakni "n", yang merupakan huruf ke-14 dalam deret abjad. Maka :

C(1) = P(1) + 13
= 14 + 13
= 27 mod 26 = 1 = a

Karena nilai 27 sudah lebih besar dari nilai tertinggi pada abjad, yakni sebanyak 26 karakter, maka nilai ini dimodulokan terlebih dahulu dengan 26.

Dengan proses yang sama, dilakukan perhitungan terhadap keseluruhan karakter dalam plainteks, sehingga plainteks berubah menjadi bentuk berikut.

Tabel 1. Enkripsi

Plainteks	Cipherteks
i	v
n	a
f	s
o	b
r	e
m	z
a	n
t	g
i	v
k	x
a	n

Dengan demikian plainteks semula 'informatika' telah diubah menjadi cipherteks 'vasbezngvxn'

Cipherteks ini kemudian akan dikirimkan kepada penerima setelah sebelumnya disisipkan ke dalam media gambar. Setelah sampai pada penerima dan mengalami proses ekstraksi, maka cipherteks harus melalui proses dekripsi untuk bisa kembali menjadi plainteks.

Dekrip metode ROT13 menggunakan pengurangan *ascii ciphertext* dengan *ascii* kunci 13 sebagai berikut :

$$Pi = Ci + 13 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Keterangan :
Ci = *Ciphertext* yang akan didekrip
Pi = *Plaintext* hasil dekrip.

Dari proses enkripsi sebelumnya, dihasilkan cipherteks 'vasbezngvxn' . Terhadap setiap karakter dalam cipherteks di atas, dilakukan proses dekripsi dengan menerapkan persamaan dekripsi pada Rot 13.

Untuk karakter pertama, yakni "v", yang merupakan karakter ke 22 dalam abjad, Maka

P(1) = C(1) - 13
=22 - 13
=9 = i

Untuk karakter kedua, yakni "a", yang merupakan karakter pertama dalam abjad, Maka, terlebih dahulu ditambahkan dengan 26. Karena logika penambahan pada persamaan enkripsi ROT13 tidak memungkinkan penjumlahan dengan konstanta 13 yang menghasilkan nilai 1. Karena

itu nilai ini bisa dipastikan merupakan hasil modulasi dengan nilai abjad tertinggi pada proses enkripsi. Sehingga

$$P(2) = C(1) - 13$$
$$= (1 + 26) - 13$$
$$= 14 = n$$

Dengan proses yang sama, dilakukan perhitungan terhadap keseluruhan karakter dalam cipherteks, sehingga cipherteks berubah menjadi bentuk berikut.

Tabel 2. Dekripsi

Cipherteks	Plainteks
v	i
a	n
s	f
b	o
e	r
z	m
n	a
g	t
v	i
x	k
n	a

Dengan demikian, pesan telah kembali menjadi bentuk aslinya menggunakan persamaan enkripsi dan dekripsi ROT 13.

1.2.4. Steganografi

Steganografi adalah ilmu seni menulis atau menyembunyikan pesan ke dalam sebuah media sehingga keberadaan pesan tidak dapat diketahui atau tidak disadari oleh indera manusia. Teknik ini berfungsi untuk menyamarkan keberadaan pesan selama masa pengiriman sehingga tidak menimbulkan kecurigaan penyadap. Teknik ini memerlukan dua komponen utama yaitu berkas atau media penampung dan pesan yang akan disisipkan.

1.2.5. End Of File (EOF)

Implementasi algoritma EoF dilakukan dalam dua tahapan yaitu encoding dan decoding. Adapun langkah-langkah encoding menggunakan algoritma EoF adalah sebagai berikut :

1. Proses encoding dimulai dengan menghitung nilai pixel yang menjadi objek steganografi dan akan menghasilkan bilangan decimal.
2. Mengubah pesan yang akan disisipkan menjadi bilangan bentuk decimal.
3. Memberi penanda pesan di awal pesan dan di akhir pesan.
4. Menyisipkan pesan di akhir file.
5. Kemudian pixel yang sudah disisipi akan dikompresi ulang dengan palet warna yang baru, untuk menghasilkan berkas yang baru/stegoimage.

2. *Desain Sistem*

Desain sistem dilakukan terhadap sistem, baik dari sisi desain logika sistem maupun desain interface dari aplikasi.

3. *Penulisan Kode Program*

Implementasi program menggunakan bahasa pemrograman Java.

4. *Pengujian*

Pengujian program dilakukan dengan memastikan bahwa program telah berjalan tanpa terjadi eror atau bug. Selain itu pengujian juga dilakukan terhadap gambar hasil penyisipan pesan dan terhadap pesan yang disisipkan, apakah bisa kembali menjadi bentuk semula atau tidak. Jika terjadi kesalahan, sistem akan diperbaiki sehingga memberikan hasil yang diharapkan.

5. *Hasil*

Pada tahapan ini aplikasi akan dianalisa dari sisi ketepatan penerapan algoritma kriptografi maupun steganografi yang diterapkan, juga kelebihan dan kekurangan sistem sehingga bisa ditarik beberapa kesimpulan dan saran yang berkaitan dengan penelitian secara keseluruhan.

3. HASIL DAN PEMBAHASAN

Pembuatan aplikasi Implementasi Algoritma ROT13 Untuk Kerahasiaan Pesan Yang Disisipkan Ke Dalam Gambar Menggunakan Metode End Of File ini, menggunakan bahasa pemrograman Java dengan tampilan sebagai berikut :

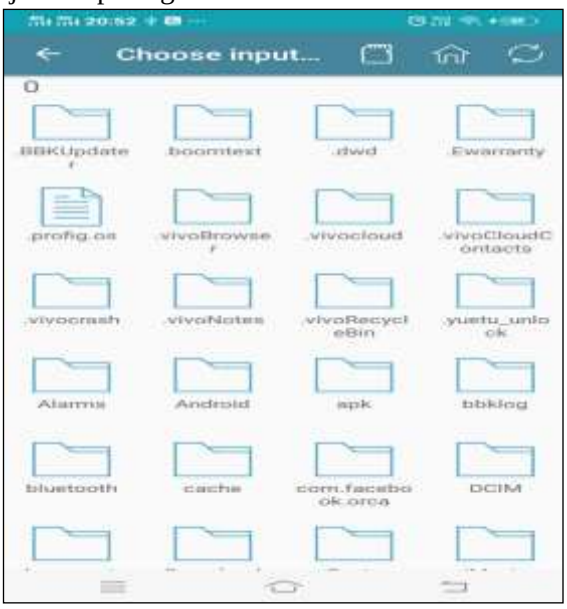
A. Tampilan Form Enkrip dan Embed

Tampilan form enkripsi dan embeded dapat dilihat pada gambar berikut .

Gambar 2. Tampilan enkripsi

B. Tampilan Form choose file

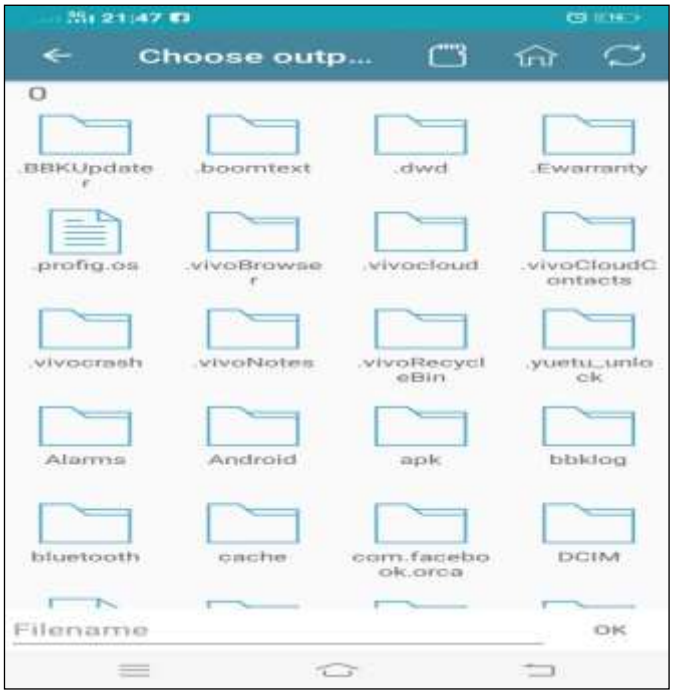
Tampilan pada *form choose file* yang akan muncul saat user diminta untuk memilih file teks dan file gambar, ditunjukkan pada gambar berikut :



Gambar 3. Tampilan Form Choose File

C. Tampilan Form Choose Output

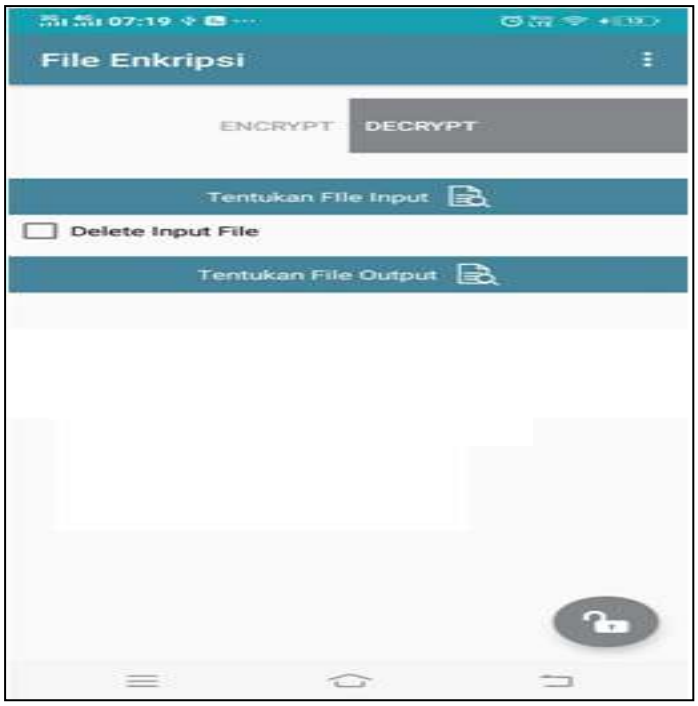
Tampilan pada *form choose output* akan muncul setelah user menekan tombol dengan simbol kunci, dengan tujuan memilih folder tempat menyimpan file gambar hasil embedding (penyisipan) pesan rahasia. Adapun tampilan *choose output* ditunjukkan pada gambar berikut.



Gambar 4. Tampilan choose output

D. Tampilan Form Decrypt

Tampilan pada *form decrypt* , yang berisi fungsi ekstraksi dan dekripsi ditunjukkan pada gambar berikut.



Gambar 5. Tampilan form dekripsi

Pada form di atas, user diminta untuk memilih file input, yaitu file gambar yang sudah disisipi pesan, dengan tampilan persis seperti form *choose file* yang telah dijelaskan sebelumnya. Setelah itu, user akan memilih file output, yaitu tempat menyimpan file text hasil dekripsi. Dengan tampilan form seperti form file *choose ouput* di atas.

Berdasarkan pembahasan di atas, dapat ditentukan beberapa kelebihan dan kekurangan yang dimiliki sistem. Adapun kelebihan sistem yang telah dibuat diantaranya yaitu :

1. Aplikasi yang telah dibuat menggunakan jenis kriptografi simetris sehingga tidak memunculkan persoalan terkait distribusi kunci.
2. Aplikasi yang telah dibuat tidak merusak gambar yang telah disisipkan pesan rahasia.
3. Aplikasi yang telah dibuat menggunakan dua teknik kerahasiaan data yaitu kriptografi dan steganografi sehingga pesan memiliki kerahasiaan data yang kuat.

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :

1. Aplikasi yang telah dibuat hanya dapat menyisipkan pesan ke dalam gambar berformat BMP.
2. Aplikasi yang telah dibuat menghasilkan pesan rahasia yang panjang, sehingga menambah ukuran pada gambar.
3. Aplikasi yang telah dibuat hanya untuk kerahasiaan pesan teks.

4. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, maka kesimpulan yang diperoleh adalah :

1. Algoritma ROT 13 merupakan algoritma yang cukup sederhana untuk dipecahkan, karena itu membutuhkan metode pengamanan tambahan.
2. Metode End Of File cukup efektif digunakan untuk menyisipkan pesan teks ke dalam gambar sebagai media penampung, dimana gambar tidak mengalami banyak perubahan yang bisa terlihat oleh orang yang menerima gambar.

5. SARAN

Setelah mengamati penerapan algoritma *One Time Pad* pada pesan, penulis memiliki beberapa saran untuk menjamin keamanan algoritma tersebut , yaitu :

1. Dibutuhkan fungsi atau algoritma penyandian yang lebih rumit untuk menghasilkan aplikasi pengamanan yang lebih tangguh.
2. Untuk mencegah kecurigaan adanya penyisipan pesan pada gambar, pengguna bisa memilih gambar dengan ukuran yang agak besar. Sehingga bit-bit tambahan di akhir file gambar tidak terlihat jelas.

DAFTAR PUSTAKA

[1] Sinaga, Frisai Anistason dan Mesran. 2017. *Implementasi Algoritma ROT13 dan Algoritma Caesar Cipher dalam Penyandian Text*. Jurnal Pelita Informatika Budi Darma, Volume : XVI,

[2] Murdani, 2017. Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Helman Knapsack. Jurnal Pelita Informatika, Volume 16, Nomor 3, Juli 2017 ISSN 2301-9425 (Media Cetak) Hal: 302-305.

[3] Hidayat, Akik, 2016. Cryptography Asymmetries Merkle-Helman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks. Jatinangor, 27-28 Oktober 2016 ISBN 978-602-72216-1-1.

[4] Fauzi, Rizki Ahmad, 2017. Sistem Informasi Akuntansi (Berbasis Akuntansi). Deepublish, Yogyakarta.

[5] Paryati, 2012. Keamanan Sistem Informasi. UPN Veteran, Yogyakarta.

[6] Juansyah, Andi, 2015. Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-Gps) Dengan Platform Android. Universitas Komputer Indonesia.

[7] Damarullah, Wandy, 2013. Aplikasi Pengenalan Dan Pembelajaran Bahasa Korea (Hangeul) Berbasis Android. Institut Sains & Teknoloi AKPRIND Yogyakarta.

[8] Sumandri, 2017. Seminar Matematika dan Pendidikan Matematika. Universitas Negeri Yogyakarta

[9] Aresta, Redho Maland dkk.2020. Implementasi Multienkripsi ROT 13 pada simbol whatsapp. Journal Of Information System Management, Volume : 2

[10] Hondro, Rivalri Kristianto dan Alwin Fau. 2018 . Perancangan Aplikasi Penyandian Teks Dengan Aldgoritma ROT 13 Dan Triangle Chain Cipher. Jurnal Mahajana Informasi, Volume : 3

[11] Yazid, Muhammad Faisal dan Edy Viktor Haryanto. 2021. Perancangan Aplikasi Penyandian File Teks dengan Menggunakan Algoritma ROT 13 dan Rail Fence Cipher. Voice Of Imformatics, Volume : X

[12] Manullang, Anjur S dkk. 2020. Penyandian Database Menggunakan Metode Base 64 dan Rot 13. Jurnal Mahasiswa Fakultas Teknik Dan Ilmu Komputer, Volume : 1

[13] Hendrik. 2020. Kombinasi Algoritma Huffman dan ROT 13 dalam Pengamanan File Docx. Journal Of Information System Research, Volume : 2

[14] Damanik, Hillman Akhyar dan Merry Anggreini. 2018. Teknik Pengujian Keamanan Data Teks Bertingkat Dengan Metode Steganografi LSB dan Teknik Enkripsi. Jurnal Penelitian Pos dan Informatika, Volume : 8

[15] Darwis, Dedi dan kisworo. 2017. Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File. Jurnal Sistem informasi dan Telematika, Volume : 8

[16] Aulis, Shabila Fitri dan Siti Sauda. 2020. Implementasi Algoritma Steganografi First Of File dan End Of File untuk Penyisipan Pesan Teks Dalam Gambar. Jurnal Nasional Ilmu Komputer, Volume : 2