IMPLEMENTASI MULTI ENKRIPSI ROT 13 PADA SYMBOL WHATSAPP

Redho Maland Aresta [1] **,** *Ero Wahyu Pratomo* [2] **,** *Vicky Geraldino* [3]**,** *Joko Dwi Santoso* [4] **,** *Sri Mulyatun* [5]

[1, 2,3,4] *Teknik Komputer UNIVERSITAS AMIKOM Yogyakarta*
[5] *Sistem Informasi Universitas AMIKOM yogyakarta*
email : redho.a@students.amikom.ac.id [1], *ero.12@students.amikom.ac.id* [2] ,
vicky.dino@students.amikom.ac.id [3] *jds@amikom.ac.id* [4] , *sri.m@amikom.ac.id* [5]

Abstraksi

Kemajuan teknologi membuat berbagai layanan komunikasi tumbuh dengan pesat. Dengan ini memungkinkan ribuan orang melakukan komunikasi melalui jaringan komputer secara global. Di sisi lain terdapat ancaman dalam keamanan data dan informasi. Sistem keamanan data diperlukan untuk melindungi data dan informasi melalui jaringan komunikasi. Untuk menjamin keamanan pesan, data dan infotmasi dalam pertukaran data adalah kriptografi. Kriptografi menggunakan algoritma pengkodean yang mendukung kebutuhan keamanan informasi, yaitu kerahasiaan dan keaslian. Dalam aplikasi kriptografi ini menggunakan metode ROT13, yang merupakan algoritma kritografi klasik yang sudah terpecahkan. Maka dari itu dengan aplikasi kroptografi dengan metode baru, yaitu multi enkripsi ROT13. Multi enkripsi pada ROT13 adalah penggabungan teknik ROT13 dengan kode ASCII yang akan merubah sebuah pesan menjadi symbol. Ini merupakan algoritma kriptografi klasik baru sehingga akan sulit dipecahkan karena menggunakan metode multi enkripsi.

***Kata Kunci* :**
Kriptografi, ROT13, Multi Enkripsi, ASCII, Symbol

Abstract

Advances in technology make various communication services grow rapidly. This allows thousands of people to communicate through computer networks globally. On the other hand there are threats in data and information security. Data security systems are needed to protect data and information through communication networks. To ensure the security of messages, data and information in data exchange is cryptography. Cryptography uses a coding algorithm that supports information security needs, namely confidentiality and authenticity. In this cryptographic application using the ROT13 method, which is a classic criterion algorithm that has been solved. Therefore from the application of kroptography with a new method, namely multi ROT13 encryption. Multi encryption in ROT13 is a combination of ROT13 techniques with ASCII code that will turn a message into a symbol. This is a new classic cryptographic algorithm that will be difficult to solve because it uses a multi-encryption method.

***Keywords* :**
Cryptography, ROT13, Multi Encryption, ASCII, Symbol

Pendahuluan

Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing), artinya “secret writing”. Dahulu kriptografi dapat diartikan ilmu dan seni untuk menjaga keamanan data atau pesan dengan cara menyandikan ke bentuk yang tidak dapat dimengerti lagi artinya.

Dalam perkembangannya, kriptografi tidak hanya diartikan untuk mengenkripsi data ataupun pesan, tetapi juga menjaga keamanan data atau pesan [1].

Perkembangkan teknologi informasi dimasa sekarang mudah untuk melakukan komunikasi dan berbagai informasi. Tetapi dengan kemudahan itu orang lupa bahwa keamanan dan dan privasu data merupakan hal penting dalam komunikasi [2] .

Seiring perkembangan teknologi tersebut, kemudahan dalam mengirimkan informasi memiliki resiko dan dampak buruk yaitu keamanan informasi pada data yang dikirim. Karena tidak sembarang orang bisa mengakses data diantaranya berupa teks yang sudah dipilih karena bersifat rahasia dan umum. Sedangkan aplikasi seperti Whatsapp, BBM, Facebook, tingkat keamanannya rendah [3].

Untuk meminimalisir kekhawatiran tersebut, maka lahirlah kriptografi, yaitu ilmu untuk mengenkripsi dan mendeskripsikan pesan atau membuat pesan menjadi sulit untuk dipahami. Dalam penelitian ini kami mengusulkan menggunakan ROT 13 yaitu menggantikan setiap huruf dengan 13 karakter di depan atu dibelakangnay sesuai dengan Alfabet. Pergeseran k=13 (huruf A diganti dengan N). agar teka-teki dan semacamnya ridak terbaca dengan sekilas [1] Pergeseran karakter pada tabel ASCII dengan menggeser mundur sebanyak 13 karakter[4] .

Tinjauan Pustaka

Setelah melakukan studi dan analisi komprehensif dari beberapa jurnal atau paper tentang deteksi ancaman terhadap keamanan data, kami memeriksa beberapa penelitian dengan teknik yang berbeda. Paper yang pertama mengimplementasikan algoritma ROT 13 dan elgamal untuk enkripsi dan deskripsi pesan rahasia. Aplikasi tersebut dikemas untuk mengamankan data berupa teks agar tidak bisa dibaca secara langsung oleh orang lain atau teks tersebut dirubah menjadi teks bersandi [3].

Paper dengan judul implementasi algoritma ROT 13 dan algoritma caesar chiper dalam penyandian teks merupakan Analisis masalah bertujuan untuk mengidentifikasi permasalahan-permasalahan yang ada pada sistem, dimana aplikasi dibangun meliputi perangkat keras (hardware), perangkat lunak (software) dan pengguna (user).

Analisa perancangan ini akan menganalisis bagaimana pengkombinasian algoritma ROT13 cipher dan caesar cipher pada aplikasi penyandian teks dan bagaimana proses perancanngan aplikasi dalam pengamanan data teks. Selanjutnya untuk paper yang lain MULTI ROT-V13 Cipher, sebuah algoritma kriptografi klasik multi enkripsi. Perbedaan mendasar antara MULTI ROT V-13 dengan algoritma kriptografi klasik lainnya terletak pada penggunaan multi enkripsi menggunakan dua algoritma klasik lain, yaitu ROT13 dan Vigenère. Penggunaan konsep multi enkripsi dengan multi algoritma ini akan mempersulit usaha-usaha kriptanalis untuk memecahkan algoritma ini. Hal ini akan mengakibatkan untuk memperoleh informasi, perlu dilakukan usaha kriptanalisis yang tidak sebanding dengan nilai informasi yang didapat [5].

Metode Penelitian

Konsep Algoritma multi Enkripsi baru ROT13

Setelah mengenali konsep-konsep kriptografi dasar dan pembuatan algoritma ini, akan dilakukan pembahasan mengenai konsep pembahasan mengenai algoritma multi ROT13. Penggunaan multi enkripsi dengan multi algoritma ini akan mempersulit dan menunda para pihak ketiga untuk memecahkan algoritma ini atau pesan rahasia tersebut.

Langkah – langkah pada metode penelitian yang kita lakukan untuk mengenkripsi pada algoritma multi ROT13 adalah sebagai berikut.

1. Secara umum, ROT13 itu adalah pegeseran key 13, sehingga abjad ‘A’ menjadi ‘N’ dan sebaliknya abjad ‘N’ menjadi ‘A’. Misalkan plaintext ‘AKU’. Setelah dilakukanya enkripsi menggunakan ROT13, maka plaintext ‘AKU’ menjadi ‘NXH’.

Table 1. Enkripsi ROT 13

PLAINTEXT	A	K	U
CHIPERTEXT	N	X	H

2. Setiap abjad (A-Z) ataupun (a-z) tersebut di dalamnya terdapat kode ASCII. Jadi, setiap plaintext yang menggunakan huruf kapital kita ubah ke huruf kecil dahulu dengan tujuan untuk mempersingkat reprentasi nilai dari ASCII tersebut. Namun jika plaintextnya menggunakan huruf kecil maka tidak perlu diubah ke huruf kecil lagi.
3. Kemudian hasil dari pesan yang telah di enkripsi menggunakan ROT 13 kita lakukan kembali Pensubtitusian ke dalam bentuk desimal ASCII

Table 1. Subtitusi Chipertext ke ASCII

ASCII CHAR	N	X	H
ASCII DECIMAL	78	88	72

4. Hasil dari diatas akan kita lakukan pengenkripsian kembali dengan melakukan pensubtitusian nilai dari ASCII decimal tersebut ke dalam pengindeksan bentuk kedalam abjad.

Table 2. Subittusi ASCII ke Abjad

Index	Abjad
7	H
8	I
8	I
8	I
7	H
2	C

5. Hasil dari pengenkripsian ke dalam indeks abjad, dilakukan pengenkripsian kembali ke dalam bentuk hexadecimal.

Table 3. Enkripsi Abjad ke Hexadecimal

ASCII CHAR	H	I	I	I	H	C
ASCII HEX	48	49	49	49	48	3

6. Hasil yang telah disubtitusi menggunakan pensubtitusian ASCII character ke bentuk hexadecimal ASCII, kita lakukan kembali

Pensubtitusian pengindeksan bentuk kedalam abjad.

Table 5. Subtitusi ASCII Hexa ke Abjad

4	8	4	9	4	9	4	9	4	8	3
E	I	E	J	E	J	E	J	E	I	D

7. Setelah itu kita akan melakukan Enkripsi kembali menggunakan ROT 13 , disana kita sudah memiliki Plaintext yang baru yaitu : EIEJEJEJEIED. Plaintext yang baru inilah yang akan kita geser sebanyak 13 kali , Maka plaintextnya akan menjadi.

Table 6. Enkripsi ROT 13

E	I	E	J	E	J	E	J	E	I	D

Hasil dari Enkripsi ROT 13

R	V	R	W	R	W	R	W	R	V	Q

Substitusi Monoalfabetik Multi Enkripsi Baru ROT13 ke dalam symbol atau emoticon

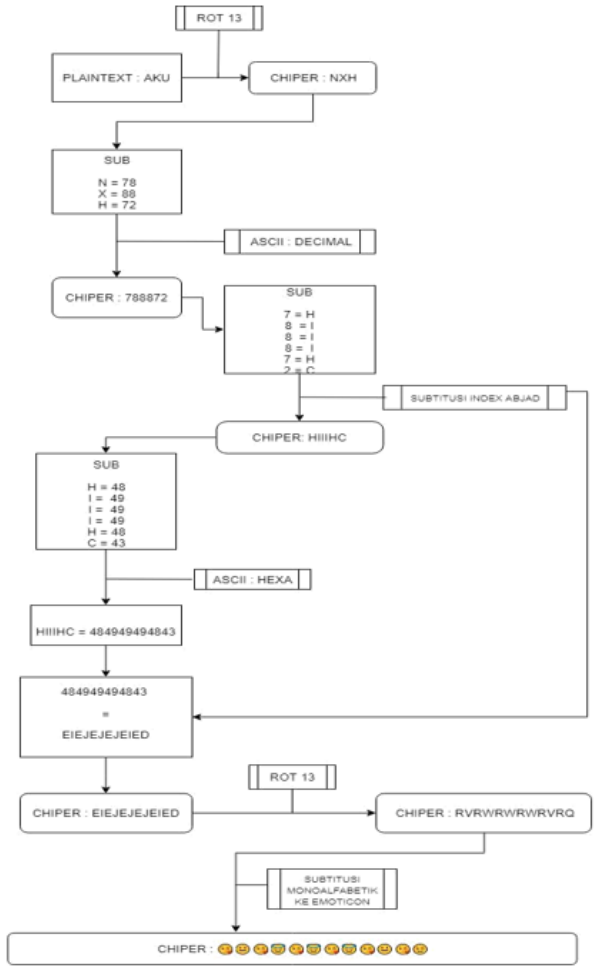
Dalam kriptografi, sandi substitusi adalah jenis metode enkripsi dimana setiap satuan pada teks terang digantikan oleh teks tersandi dengan sistem yang teratur. Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan decrypt.

Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak. Substitusi ROT13 ke emoticon yaitu Perubahan plaintext yang sebelumnya telah di enkripsi dengan metode ROT13 kemudian disempurnakan dengan pengenkripsian dalam bentuk emoticon. Emoticion tersebut akan mewakili dari setiap abjad dari ‘N-A dan n-a’.

Table 7. Contoh Subtitusi ROT 13 ke Emoticon

Abjad	Emoticon
N	😍
O	😣
P	😂
Q	😒
R	😯
S	😹
T	😵
U	😟
V	😐
W	😳
a	😱

Diagram Alur Konsep Algoritma Multi Enkripsi ROT13



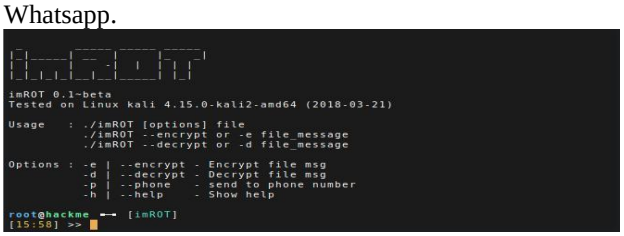
Gambar 1. Diagram Multi Enkripsi ROT 13

Hasil dan Pembahasan

Hasil perancangan akhir dari implentasi diatas , penulis melakukan pembuatan aplikasi Kriptografi yang telah diujikan dengan menggunakan metode Command Line interface (CLI). Aplikasi Kriptografi ini dinamakan imROT.

Tampilan aplikasi tersebut. Aplikasi ini dilakukan pengujian menggunakan distro Kali linux versi 4.15.0-kali2-amd64 (2018-03-21).

Ada beberapa feature aplikasi tersebut yaitu melakukan Enkripsi , Deskripsi dan pengiriman pesan yang telah di Enkripsi ke nomor tujuan melalui Whatsapp.

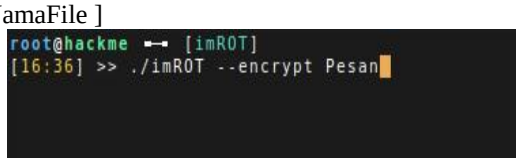


Gambar 2. Tools ImROT

Proses Enkripsi

Gambar 3. Isi Pesan

a. Untuk Melakukan proses Enkripsi kita harus memiliki file yang berisikan sebuah pesan terlebih dahulu.
b. Disini kita memiliki pesan yang berisikan sebuah kalimat yaitu " Cause we were just kids when we fell in love "
c. Kemudian kita jalankan Tools yang bernama imROT dengan memasukan perintah : root@hackme ~ ./imROT –encryption [NamaFile]



Gambar 4. Tools Enkripsi

d. Proses Enkripsi

Gambar 5. Proses Enkripsi

e. Hasil Output

Gambar 6. Hasil dari Tools Multi Enkripsi ROT 13

f. File yang berhasil di Enkripsi akan berada di folder tmp dengan nama file Smile.imROT
g. Pengiriman Hasil Enkripsi ke Social Media
h. Disini social media yang digunakan adalah Whatsapp , karena ditahun ini pengguna Whatsapp sudah semakin meningkat .
Untuk menggunakan metode ini kita menambahkan beberapa options pada Tools tersebut ,dengan menambahkan options –phone yang berfungsi untuk mengirimkan hasil pesan langsung ke nomor tujuan.

Gambar 7. Mengirim Hasil Enkripsi Melalui Aplikasi Whatsapp

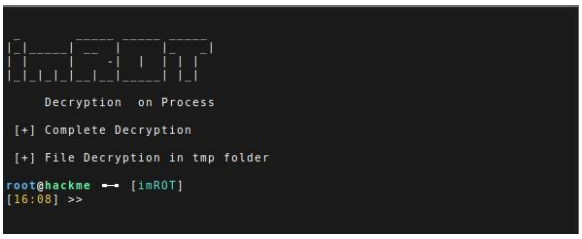
i. Kemudian setelah itu proses Enkripsi akan berjalan dimana pesan yang telah ter Enkripsi akan langsung dialihkan ke whatsapp untuk segera dikirimkan.

Proses Dekripsi

a. Melakukan proses Deskripsi tidak jauh berbeda dengan proses Enkripsi kita cukup menggunakan Options -d atau –decryption [namafile] , dengan mengetikan perintah.

Gambar 8. Tools Dekripsi ROT 13

b. Proses Deskripsi
Aplikasi tersebut akan melakukan proses Deskripsi dimana file yang telah ter Enkripsi berada di lokasi tmp dengan nama file Smile.imROT.



Gambar 9. Tools Dekripsi ROT13

c. Hasil output
Output dari proses Deskripsi akan berada di lokasi tmp folder , dengan nama file imROT.decrypt.

Gambar 10. Hasil Dekripsi Tools

Kesimpulan

Dengan menggunakan Multi Enkripsi ROT 13 pada whatsapp pesan yang disampaikan menjadi lebih terjamin keamananya dan kerahasianya. Proses enkripsi dan dekripsi yang di lakukan sudah berjalan dengan baik.

Daftar Pustaka

[1] R. Rheinadi, Multi ROT-V13 Cipher , Sebuah Algoritma Kriptografi Klasik Multi Enkripsi Baru, 2012.
[2] R. Rahmawati and D. Rahardjo, Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform Dan

Kriptografi AES 128 BIT Pada SMK PGRI 15 Jakarta, J. Tek. Inform. dan Sist. Inf., vol. 2, no. 1, pp. 67–74, 2016.

[3] M. Zainudin Zuhri, Implementasi Algoritma Rot13 Dan Elgamal Untuk Enkripsi Dan Dekripsi Pesan Rahasia, Univ. Nusant. Pgri Kediri, 2018.

[4] C. D. A. N. Root, Analisa implementasi aplikasi keamanan file audio wav dengan menerapkan algoritma beaufort cipher dan root 13, vol. 18, pp. 372–379, 2019.

[5] F. A. Sinaga and Mesran, Implementasi algoritma rot13 dan algoritma caesar chiper dalam penyandian teks, Pelita Inform. Budi Darma, vol. 16, no. Rotate 13, pp. 38–41, 2017.

[6] Safaat, Pemrograman Aplikasi mobile Smartphone dan tablet PC Berbasis Android. Bandung : Informatika, 2012.

[7] Doni, Ariyus, , Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi, Andi, Yogyakarta, 2008.

[8] Andy, Nugroho., Implementasi Algoritma Caesar Chiper ROT13 dan base64 untuk enkripsi dan dekripsi pesan SMS pada handphone berbasis Android,. STMIK AMIKOM YOGYAKARTA, 2012.