JURNAL

IMPLEMENTASI ALGORITMA ROT13 DAN ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PESAN RAHASIA

IMPLEMENTATION OF THE ROT13 AND ELGAMAL ALGORTM OF SECRET MESSAGE TO ENCRYPT AND DECRYPT

Oleh:

M. Zainudin Zuhri

13.1.03.02.0387

Dibimbing oleh :

1. **Ahmad Bagus Setiawan, S.T., M.M., M.Kom.**
2. **Risa Helilintar, M.Kom.**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2018

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2017

Yang bertanda tangan di bawah ini:

Nama Lengkap	: M. Zainudin Zuhri
NPM	: 13.1.03.02.0387
Telepun/HP	: 0856 0887 1713
Alamat Surel (Email)	: zainudin.zuhri812@gmail.com
Judul Artikel	: Implementasi Algoritma ROT13 dan ElGamal untuk Enkripsi dan Dekripsi Pesan Rahasia
Fakultas – Program Studi	: FT – Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jl. K.H Achmad Dahlan No. 76 Kediri

Dengan ini menyatakan bahwa :

a. Artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;

b. Artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila dikemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 9 Agustus 2018
Pembimbing I, Ahmad Bagus Setiawan, S.T., M.M., M.Kom. NIY/NIDN. 1130301117/0703018704	Pembimbing II, Risa Helilintar, M.Kom. NIDN. 0721048402	Penulis, M. Zainudin Zuhri NPM. 13.1.03.02.0387

IMPLEMENTASI ALGORITMA ROT13 DAN ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PESAN RAHASIA

M. Zainudin Zuhri
13.1.03.02.0387
FT – Teknik Informatika
zainudin.zuhri812@gmail.com
Ahmad Bagus Setiawan, S.T., M.M., M.Kom dan Risa Helilintar, M.Kom

UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Penelitian ini bertujuan untuk membangun aplikasi android dengan mengkombinasikan dua algoritma yaitu algoritma ROT13 dan ElGamal. Aplikasi tersebut dikemas untuk mengamankan data berupa teks agar tidak bisa dibaca secara langsung oleh orang lain atau teks tersebut dirubah menjadi teks bersandi. Algoritma ROT13 merupakan *kriptografi klasik* dengan perpaduan menggunakan *teknik kriptografi* dalam menjaga keamanan dan kerahasiaan. Sedangkan, Algoritma ElGamal termasuk *kriptografi modern* mempunyai kelebihan yaitu sulit untuk memecahkan penghitungannya sehingga, kemungkinan untuk diretas sangat minim.

Tahap implementasi diujikan pada dua tahap yaitu pegujian aplikasi *Crypto Text* di *smartphone*, dan pengujian kepada 10 mahasiswa UKM PSHT Universitas Nusantara PGRI Kediri terhadap aplikasi *Crypto Text* melalui angket untuk menilai kelayakan aplikasi tersebut digunakan orang lain. Pengujian aplikasi *Crypto Text* dilakukan pada *smartphone* Oppo A33w Android OS versi 5.1 Lollipop, dan angket yang disediakan untuk penilaian kelayakan terdiri tiga aspek yaitu Tampilan Aplikasi (*Interface*), *Input* Data, dan Kegunaan Aplikasi.

Hasil pengujian aplikasi *Crypto Text* di *smartphone* yaitu dengan kunci yang berbeda, pada proses enkripsi hasil *output*-nya berbeda, dan jika dilakukan *execute* sebanyak dua kali atau lebih maka, hasilnya pun juga berbeda, walaupun teks atau *plaintext*-nya sama. Pada proses enkripsi, *ciphertext* yang di-*insert*-kan dengan *key* yang tidak sama saat proses dekripsi yang terjadi setelah di-*execute* dengan kunci yang berbeda hasilnya tidak dapat terbaca atau tidak sesuai dengan pesan yang dikirim (*plaintext*). Hasil rata-rata persentase penilaian angket kelayakan aplikasi *Crypto Text* adalah 83,75 % dengan kategori sangat layak.

Kata Kunci : Algoritma, ROT13, ElGamal, Enkripsi, Dekripsi, Pesan Rahasia

I. LATAR BELAKANG

Latar Belakang

Banyaknya pengguna internet diera teknologi ini sudah menjadi suatu tuntutan dan kewajiban untuk mendapatkan informasi dan memberikan informasi tanpa bertemu dan tanpa tatap muka. Dampak positif dari perkembangan tersebut adalah semakin mudahnya mengirim informasi tanpa tatap muka, atau tanpa harus mengirimkan surat lewat jasa kurir. Sekarang dengan menggunakan koneksi internet, informasi dapat diterima dengan cepat dan mudah, bahkan tidak hanya informasi berupa teks tetapi, video dan foto bisa dikirim dengan cepat. Seperti aplikasi *Whatsapp*, BBM, *Facebook*, dan lain-lain dapat mengirim informasi dengan koneksi internet.

Kemudahan dalam mengirim informasi dengan koneksi internet, terdapat pula dampak negatif dan resiko, yaitu keamanan informasi atau data yang dikirim. Karena, tidak semua data atau informasi boleh diakses oleh masyarakat umum, beberapa di antaranya pesan berupa teks banyak dipilih masyarakat untuk menyampaikan informasi, dan informasi tersebut ada yang bersifat rahasia dan umum, sedangkan aplikasi *Whatsapp*, BBM, *Facebook*, tingkat keamanannya rendah. *Whatsapp* dapat digandakan dengan satu akun, akun BBM dapat diretas, sehingga dibutuhkan pengaman data berupa teks.

Pengaman data berupa teks yang dapat mendukung aplikasi *smartphone* seperti Whatsapp, BBM, Facebook, Gmail, Yahoo, dan lain-lain yaitu aplikasi yang dibangun menggunakan algoritma. Contohnya aplikasi ROT13 Translator yang tersedia di Play Store. ROT13 adalah program enkripsi sederhana yang terdapat di dalam sistem UNIX. ROT13 menggunakan cipher abjad-tunggal dengan pergeseran k = 13 (jadi, huruf A diganti dengan N, B diganti dengan O, dan seterusnya) (Munir, 2014).

Pada penelitian ini penulis menggunakan *kriptografi klasik* yaitu ROT13 dengan perpaduan menggunakan *teknik kriptografi* dalam menjaga keamanan dan kerahasiaan. *Algoritma* ElGamal termasuk dalam *kriptografi modern* yang menggunakan *plaintext*, *ciphertext* dan kunci untuk melakukan proses *enkripsi* dan *dekripsi* dalam pengamanan data. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan *cipher blok*, yaitu melakukan proses enkripsi pada blok-blok *plaintext* dan menghasilkan blok-blok *ciphertext* yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan (Ifanto, 2009).

Berdasarkan latar belakang di atas maka penulis berusaha untuk mengembangkan sebuah aplikasi yang sesuai dengan harapan tersebut dengan judul "IMPLEMENTASI ALGORITMA ROT13 DAN ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PESAN RAHASIA". Agar nantinya aplikasi ini diharapkan mampu menjaga kerahasiaan data serta memberikan keamanan data dari para penyadap maupun dari pihak-pihak yang tidak bertanggung jawab.

Rumusan Masalah

1. Bagaimana implementasi keamanan data menggunakan metode ROT13 dan kriptografi metode ElGamal untuk mengenkripsi pesan rahasia dalam

menjaga keamanan dan kerahasiaan data?

2. Bagaimana kelayakan aplikasi keamanan data menggunakan metode ROT13 dan kriptografi metode ElGamal untuk mengenkripsi pesan rahasia dalam menjaga keamanan dan kerahasiaan data?

Tujuan Penelitian

1. Mengimplementasikan keamanan data menggunakan metode ROT13 dan kriptografi metode ElGamal untuk mengenkripsi pesan rahasia dalam menjaga keamanan dan kerahasiaan data.
2. Kelayakan aplikasi keamanan data menggunakan metode ROT13 dan kriptografi metode ElGamal untuk mengenkripsi pesan rahasia dalam menjaga keamanan dan kerahasiaan data.

II. METODE

Algoritma ROT13

ROT13 (*Rotate* 13) merupakan perkembangan atau modifikasi dari metode *Caesar Cipher* dalam segi perubahan jumlah geseran dan juga arah geseran. Menurut Frisai, (2017:38) bahwa ROT13 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.

Caesar Cipher ROT13 adalah fungsi yang menggunakan kode Kaisar dengan pergeseran k=13. ROT13 didesain untuk keamanan pada sistem operasi UNIX yang sering digunakan pada forum online, berfungsi untuk menyelubungi isi artikel sehingga hanya orang yang berhak yang dapat membacanya. Sistem enkripsi ROT13 kali ini dengan menggeser maju karakter sebanyak 13 kali, terhitung 1 adalah karakter didepannya, dan pergeseran karakter berdasarkan urutan karakter pada tabel ASCII. Sebagai dekripsinya, dengan menggeser mundur karakter sebanyak 13 kali. (Nugroho, 2012).

Algoritma ElGamal

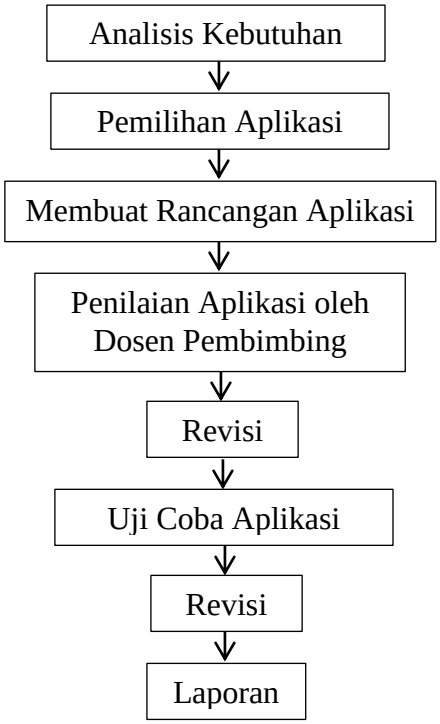
Algoritma *ElGamal* merupakan algoritma dalam *kriptografi* yang termasuk dalam kategori algoritma *asimetris*. Keamanan algoritma *ElGamal* terletak pada kesulitan penghitungan logaritma *diskret* pada bilangan *modulo prima* yang besar sehingga upaya untuk menyelesaikan masalah alogaritma ini menjadi sangat sukar.

Algoritma *ElGamal* mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan. Algoritma ini mempunyai kerugian pada

ciphertext-nya yang mempunyai panjang dua kali lipat dari plainteksnya. Akan tetapi, algoritma ini mempunyai kelebihan pada *enkripsi*. Untuk *plainteks* yang sama, algoritma ini memberikan *ciphertext* yang berbeda (dengan kepastian yang dekat) setiap kali *plainteks* di *enkripsi* (Agrawal, 2013). *Plainteks* di *enkripsi* dalam bentuk bilangan 0 sampai 255 berdasarkan ASCII (*American Standart Code for Information Interchange*)

Prosedur Penelitian

Prosedur penelitian digunakan untuk menggambarkan langkah-langkah kegiatan penelitian dari awal hingga penulisan laporan, agar mendapatkan hasil yang optimal baik aplikasi dan laporan.



Gambar 1 Bagan Prosedur Penelitian

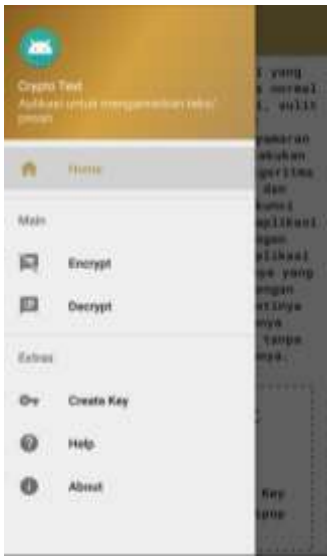
III. HASIL DAN KESIMPULAN

Tampilan Aplikasi

Pada aplikasi ini terdapat lima menu, yakni *Menu Home*, *Menu Encrypt*, *Menu Decrypt*, *Menu Create Key*, *Menu Help* dan *Menu About*. Pada setiap menu tersebut telah disediakan petunjuk pada bagian *layout header*. Berikut ini merupakan tampilan dan fungsi setiap menu yang telah dibangun.

a. Tampilan Menu Utama

Tampilan menu utama yang terdiri dari menu-menu aplikasi tersebut yaitu menu *home*, *encrypt*, *decrypt*, *create key*, *Help*, dan *about*. Detail *interface* aplikasi *Crypto Text* sebagai berikut.



Gambar 2 Tampilan Menu

b. Tampilan Menu *Home*

Setelah dipilih menu *home* disajikan halaman penjelas mengenai *Crypto Text* dan feature aplikasi yang *support*

minimum android lollipop 5.0. Detail tampilan menu *home* sebagai berikut.

Gambar 3 Tampilan Menu *Home*

c. Tampilan Menu *Encrypt*

Pada menu utama terdapat menu *encrypt*, menu *encrypt* merupakan halaman proses enkripsi dimana *plaintext* diubah menjadi *ciphertext*. Detail menu *encrypt* sebagai berikut.

Gambar 4 Tampilan Menu *Encrypt*

Gambar 5 Tampilan Lanjutan Menu *Encrypt*

d. Tampilan Menu *Decrypt*

Kemudian menu *decrypt* merupakan halaman proses dekripsi dimana *ciphertext* diubah menjadi *plaintext* agar pesan yang dikirim dapat dibaca oleh penerima. Detail menu *decrypt* sebagai berikut.

Gambar 6 Tampilan Menu *Decrypt*

Gambar 7 Tampilan Lanjutan Menu *Encrypt*

e. Tampilan Menu *Create Key*

Menu *create key* untuk melalui proses enkripsi dan dekripsi haruslah meng-*Input*-kan *key* agar proses tersebut dapat berjalan, dengan tombol-tombol *on* dan *off* di kolom *setting* ROT13 dan ElGamal yang dapat disesuaikan sesuai kebutuhan.

Gambar 8 Tampilan Menu *Create Key Text*

f. Tampilan Menu *Help*

Menu *Help* merupakan halaman yang berisi tentang penjelasan proses pembuatan kunci, proses enkripsi, proses dekripsi, dan juga menjelaskan tentang algoritma ROT13 dan ElGamal, serta syarat-syarat teks agar bisa melalui proses enkripsi dan dekripsi.

Gambar 9 Tampilan Menu *Help*

g. Tampilan Menu *About*

Menu *about* adalah menu yang berisi tentang keterangan dari aplikasi pesan rahasia *Crypto Text* yaitu versi aplikasi, maksud membuat aplikasi, dan nama pembuat aplikasi pesan rahasia. Tampilan menu *about* sebagai berikut.

Gambar 10 Tampilan Menu *About*

Uji Coba Aplikasi

Uji coba aplikasi dilakukan pada *smartphone* Oppo A33w Android OS versi 5.1 Lollipop. Tabel uji coba proses enkripsi sebagai berikut.

Tabel 1 Tabel Uji Coba Enkripsi

Plaintext	***Key***	***Ciphertext***
Sarjana Teknik Informatika	ROT13 (*on-enable, on-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	156-83-60-269-19-175-136-181-65-270-213-222-330-29-194-43-217-123-283-88-240-254-255-131-187-41-83-261-207-65-70-60-349-166-156-161-272-323-200-322-144-327-317-269-310-274-113-181-319-93-260-29
Sarjana Teknik Informatika	*Create key* ROT13 (*on-enable, off-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	650-448-229-163-529-672-620-628-229-163-650-574-229-163-1-45-620-461-1-114-650-560-529-211-529-476-117-218-620-311-620-41-229-531-650-88-529-158-546-53-1-122-546-83-620-398-650-102-229-239-229-163
Sarjana Teknik Informatika	*Create key* ROT13 (*off-enable, off-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	592-515-357-245-711-498-160-389-273-266-349-292-34-386-543-479-100-181-76-556-234-627-692-131-108-537-479-11-382-630-261-293-541-726-606-553-668-728-19-39-694-710-166-270-494-113-117-156-509-357-731-354

Tabel uji coba proses dekripsi sebagai berikut.

Tabel 2 Tabel Uji Coba Dekripsi

Ciphertext	*Key*	*Plaintext*
156-83-60-269-19-175-136-181-65-270-213-222-330-29-194-43-217-123-283-88-240-254-255-131-187-41-83-261-207-65-70-60-349-166-156-161-272-323-200-322-144-327-317-269-310-274-113-181-319-93-260-29	ROT13 (*on-enable, on-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	Sarjana Teknik Informatika
650-448-229-163-529-672-620-628-229-163-650-574-229-163-1-45-620-461-1-114-650-560-529-211-529-476-117-218-620-311-620-41-229-531-650-88-529-158-546-53-1-122-546-83-620-398-650-102-229-239-229-163	*Create key* ROT13 (*on-enable, off-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	Sarjana Teknik Informatika
592-515-357-245-711-498-160-389-273-266-349-292-34-386-543-479-100-181-76-556-234-627-692-131-108-537-479-11-382-630-261-293-541-726-606-553-668-728-19-39-694-710-166-270-494-113-117-156-509-357-731-354	*Create key* ROT13 (*off-enable, off-reverse mechanism*) ElGamal (*on-enable, on-auto private key, on-auto public key*)	Sarjana Teknik Informatika

Pengujian Aplikasi Melalui Angket

Hasil penghitungan angket penilaian terhadap aplikasi telah dilakukan dengan rumus sebagai berikut.

$$persentase\ kelayakan\ (\%) = \frac{\Sigma\ skor\ total\ (X)}{\Sigma\ skor\ ideal\ (X_i)} \times 100\%$$

Hasil dari perhitungan persentase tersebut dapat dikategorikan menurut skala sebagai berikut.

Tabel 3 Skala Persentase Kelayakan

Rentang	Kategori
100% - 81,26%	Sangat Layak (SL)
81,25% - 62,50%	Layak (L)
62,51% - 43,76%	Tidak Layak (TL)
43,75% - 25%	Sangat Tidak Layak (STL)

Sumber : Riduwan, 2013:41

Pengujian aplikasi dilakukan kepada 10 Mahasiswa UKM PSHT Universitas Nusantara PGRI Kediri melalui angket yang sudah disediakan. Hasil perhitungan angket disajikan dalam bentuk tabel sebagai berikut.

Tabel 4 Perhitungan Persentase Angket

Aspek	**Rata-rata Persentase**	**Kategori**
Tampilan Aplikasi (*Interface*)	78,13 %	Layak
Input Data	85,00 %	Sangat Layak
Kegunaan Aplikasi	89,38 %	Sangat Layak
Total	**83,75 %**	**Sangat Layak**

IV. DAFTAR PUSTAKA

Agrawal, Bhavana dkk. 2013. *Implementation of Various Cryptosystem Using Chaos*. [Online]. Tersedia: http://www.iosrjournals.org/iosr-jce/papers/Vol13-issue4/M01347784.pdf?id=5785. Dalam jurnal IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Vol 13 Issue 4. Diakses [16 September 2017]

Ifanto, Mukhammad. 2009. *Metode Enkripsi dan Dekripsi dengan Menggunakan Algoritma ElGamal*. [Online]. Tersedia: http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2009-2010/Makalah0910/MakalahStrukdis0910-096.pdf. Diakses [18 September 2017].

Munir, Rinaldi. 2014. *Sistem Kriptografi Kunci-Publik*. [Online]. Tersedia: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Sistem%20Kriptografi%20Kunci-Publik.pdf. Diakses [15 September 2017]

Nugroho, Adi. 2009. *Algoritma dan Struktur Data dengan C#*. Yogyakarta: CV. Andi Offset

Riduwan. 2013. *Dasat-dasar Statistika*. Bandung: Alfabeta

Sinaga, Frisai Anistason dan Mesran. 2017. *Implementasi Algoritma ROT13 dan Algoritma Caesar Cipher dalam Penyandian Text*. Dalam jurnal Pelita Informatika Budi Darma, Volume : XVI, Nomor: 1. [Online]. Tersedia: http://stmik-budidarma.ac.id/ejurnal/index.php/pelita/article/download/255/228. Diakses [16 September 2017]