JISKa, Vol. 2, No. 2, September, 2017, Pp. 115 – 126
ISSN 2527 -5836

APLIKASI ALGORITMA GENETIKA UNTUK MENEBAK KATA KUNCI PADA DEKRIPSI VIGENERE CIPHER TEKS BAHASA INDONESIA

Tsuraya Ats Tsauri [(1)] Nurochman [(2)]
Program Studi Teknik Informatika, Fakultas Sains Dan Teknologi
Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Jl. Marsda Adisucipto, Yogyakarta 55281
e-mail : ayyaa.ats12@gmail.com[(1)] nurochman@uin-suka.ac.id [(2)]

Abstract

Cryptanalysis is the art to solve without key ciphers. Vigenere ciphers is one of the cryptanalysis algorithm. Brute force attack and exhaustive attack is a technique of cryptanalysis vigenere ciphers, but less optimal in result. This research proposes how to solve the secret key (cryptanalysis), using a genetic algorithm on text Indonesian ciphers.

The first step, designing the chromosome that will be the length of the keyword, used is index coincidence(IOC), with IOC in Indonesian is 0.075. The fitness value is obtained by searching the weight, comparing the word decrypted with Indonesian dictionary. There are reproductive processes including crossover, mutation and elitism. In the keyword search process there are several parameters that are crossover probability value, the probability of mutation and the number of population.

This analysis performed five scenarios with different combinations of parameters, number of ciphertext characters and two different keyword types. Testing done as much as 1000 times and produced 467 data that successfully guess the keyword in more or less 60 minutes. After analyzing the results of the research, obtained the optimal parameters with the value of Pc 0.09, Pm 0.3 and Pop_size 20.

Keywords: ***Cryptanalysis, Genetic Algorithm, Vigenere Cipher, Index Coincidence.***

Kriptanalisis adalah seni untuk memecahkan cipher tanpa kunci, berbeda dengan kriptografi yaitu untuk menjaga kerahasian data dengan menyandikan sebuah *plaintext.* Vigenere cipher merupakan salah satu algoritma kriptanalisis. B*rute force attack* dan *exhaustive attack* merupakan teknik dari kriptanalisis vigenere cipher, namun kurang optimal dalam penyelesaianya. Penelitian ini mengusulkan cara pemecahan kunci rahasia (kriptanalisis), menggunakan algoritma genetika pada teks cipher berbahasa Indonesia.

Langkah pertama, merancang kromosom yang akan menjadi panjang kata kunci, metode yang digunakan adalah index coincidence(IOC), dengan nilai IOC teks Berbahasa Indonesia adalah 0.075. Nilai fitness didapatkan dengan melakukan pencarian bobot, yaitu membandingkan kata hasil dekripsi dengan kamus Bahasa Indonesia. Algotitma genetika akan mencari semua kemungkinan kata kunci, dalam proses tersebut terdapat proses reproduksi meliputi crossover, mutasi dan elitisme. Terdapat parameter yang dimasukan dalam proses pencarian kata kunci yaitu nilai probabilitas crossover, probabilitas mutasi dan jumlah populasinya, parameter tersebut yang akan dioptimalkan untuk mendapatkan kata kunci.

Analisis ini dilakukan lima skenario dengan perbedaan beberapa kombinasi parameter, jumlah karakter cipherteks dan dua jenis kata kunci yang berbeda. Pengujian dilakukan sebanyak 1000 kali dan dihasilkan 467 data yang berhasil menebak kata kunci dalam waktu lebih kurang 60 menit. Setelah dilakukan analisis terhadap hasil penelitian, diperoleh parameter yang optimal dengan nilai Pc 0.09, Pm 0.3 dan Pop_size 20.

Kata kunci : Kriptanalisis, Algoritma Genetika, Vigenere Cipher, Index Coincidence

1. PENDAHULUAN

Kriptanalisis merupakan sebuah studi mengenai cipher, ciphertext atau cyrptosystems yang bertujuan menemukan kelemahan dalam sistem penyandian, sehingga memungkinkan untuk

memperoleh plaintext dari ciphertext yang ada, tanpa perlu mengetahui kunci ataupun algoritma pembangun ciphertext tersebut (Hapsari, Perdana, & Risvelina, 2004). Kriptanalisis berawal dari cabang ilmu kriptologi, kriptologi di bagi menjadi dua, kriptografi dan kriptanalisis (Bawono, 2015), antara kriptologi dan kriptanalisis saling bertolak belakang, jika kriptanalisis membongkar untuk memecahkan cipher tanpa kunci, berbeda dengan kriptografi yaitu untuk menjaga kerahasian data dengan menyandikan sebuah plainteks atau teks asli.

Salah satu algoritma kriptografi yaitu vigenere cipher. Kode vigenere termasuk pada kode abjad majemuk, dalam proses enkripsi dan dekripsi menggunakan bujur sangkar vigenere atau tabula recta. Kriptografi ini pernah di pecahkan oleh Babagge dan Kasiski pada pertengahan abad ke 19 (Munir, 2009). Percobaan kriptanalisis menggunakan analisis frekuensi yang dilakukan oleh Babagge memiliki kelemahan terhadap vigenere, ketika ada dua huruf yang sama dalam text kode (cipherteks) belum tentu bisa didekripsikan menjadi dua huruf yang sama pada text aslinya (Plaintext). Sedangkan yang dilakukan oleh Kasiski membantu memecahkan kunci hanya mengetahui berapa jumlah karakter kuncinya (Chiquita, 2013).

Kriptanalisis pada kriptografi vigenere cipher dapat dilakukan dengan mencoba semua kemungkinan yang ada atau biasa disebut dengan brute force attack atau exhaustive attack namun ini dirasa kurang optimal, karena memerlukan waktu yang lama (Hutasoit, 2008). Kriptanalisis vigenere cipher dengan mengimplementasikan algoritma genetika pernah dilakukan namun menggunakan teks cipher berbahasa inggris sebagai objek, dan memberikan hasil yang optimal dibanding algoritma lainnya (Rodriguez, 2015)

Algoritma genetika merupakan salah satu bidang ilmu dari komputasi evolusioner, yang merupakan cabang dari bidang artificial intelligence. Algoritma genetika adalah algoritma pencarian dan pengoptimisasian berdasarkan seleksi alami (Widodo, 2012). Algoritma genetika banyak digunakan untuk menyelesaikan permasalahan sehari hari, contohnya, penjadwalan, TSP (Travelling Salesman Problem) dan banyak lainnya. Dalam penelitian kali ini mengusulkan untuk membangun suatu sistem yang dapat memecahkan kunci rahasia, menggunakan algoritma genetika pada teks cipher berbahasa Indonesia. Dengan menggunakan algoritma genetika sebagai algoritma untuk memecahkan kunci pada kriptanalisis Vigenere Cipher, index coincidence untuk menentukan panjang kata kunci, sistem akan mengenerik segala kemungkinan kombinasi kata yang mungkin untuk cipherteks tersebut.

Penelitian yang dilakukan oleh Rodriguez (2015) mengimplentasikan algoritma genetika dalam kriptanalisis vigenere cipher, penelitian ini dilakukan pada cipherteks yang berasal dari teks Bahasa Inggris. Ditemukan ukuran populasi yang efisien dengan jumlah 20 dan probabilitas mutasi degan nilai 0.01, namun untuk probabilitas crossover memiliki dua kemungkinan 0.6 dan 0.8, dan melakukan kriptanalisis dengan algoritma genetika dipandang lebih cepat dibanding teknik kriptanalisis lainnya (Rodriguez, 2015). Sedangkan Penelitian yang dilakukan Wardoyo dan Nilogiri (2012) melakukan kriptanalisis pada algoritma Vigenere Cipher dengan menggunakan teknik Exhaustive Attack. Exhaustive Attack sama dengan teknik Brute Force Attack yaitu mencari kunci dari semua kemungkinan, kelemahannya proses pencarian kunci yang lama karena menggunakan semua kemungkinana karakter yang ada (Wardoyo & Nilogiri, 2012). Penelitian berikutnya dilakukan oleh Ragheb dan Arumugan (2008), yaitu menerapkan algoritma genetika untuk mencari kunci antipublik poliaphabetic subtitusi cipher, dalam penelitian ini terlebih dahulu mencari panjang kunci untuk dapat mengetahui kunci aslinya. Pada penelitian ini menunjukan bahwa ukuran cipherteks berpengaruh dalam mengembalikan tulisan aslinya, dan algoritma genetika memiliki waktu yang lebih cepat dibandingkan lainnya (Toemeh & Arumugam, 2008).

Pada penelitian ini akan dilakukan yaitu melakukan pembongkaran kata kunci kriptografi vigenere cipher dengan algoritma genetika, perbedaan dengan penelitian yang lain adalah penelitian ini fokus pada plainteks berbahasa Indonesia. Algoritma genetika digunakan untuk mendapatkan kata kuncinya dan untuk menentukan panjang kata kuncinya menggunakan index coincidence. Disamping itu, penelitian ini juga bertujuan untuk mendapatkan nilai parameter optimal dari proses algortima genetika.

2. METODE PENELITIAN

2.1 Studi Pendahuluan

Dalam studi pendahuluan, peneliti mempelajari literatur–literatur yang sudah dilakukan oleh penelitian sebelumnya, yaitu dengan membaca maupun dengan mengambil informasi dari jurnal ilmiah, penelitian yang sudah dilakukan, buku, situs-situs web terpercaya dan forum diskusi lainnya. Setelah dilakukan studi literatur maka didapatkan konsep-konsep tentang kriptanalisis vigenere cipher dan berbagai macam implementasi algoritma genetika. Dari studi literatur yang sudah dilakukan oleh peneliti, penelitian sebelumnya hanya melakukan kriptanalisis dengan metode analisis frekuensi yang menjadi objek dengan menggunakan teks berbahasa Inggris. Algoritma genetika untuk menentukan kata kunci telah dilakukan penelitian sebelumnya dengan menggunakan objek teks bahasa Inggris.

2.2 Pengumpulan Data

Pengambilan data dalam penelitian ini didapatkan dari percobaan plaintext yang telah dienkripsi dengan aplikasi atau sistem enkripsi vigenere cipher. Disiapkan beberapa teks percobaan, kemudian teks diinputkan ke sistem enkripsi yang menghasilkan cipherteks. Cipherteks ini akan menjadi data yang digunakan dalam pembangunan sistem Kriptanalisis Vigenere Cipher dalam Menentukan Kata Kunci dengan Algoritma Genetika.

2.3 Algoritma Genetika

Algoritma genetika merupakan salah satu cabang kecerdasan buatan, dalam penelitian ini sistem yang dikembangan menggunakan metodologi pengembangan sistem algoritma genetika. Berikut adalah metodologi pengembangan sistem:

a. Analisis

Penelitian ini dilakukan untuk mengetahui apakah algoritma genetika dapat di implementasikan untuk membongkar kata kunci dari kriptografi vigenere cipher. Algoritma genetika digunakan untuk mengoptimalisasi kriptanalisis dari vigenere. Objek penelitian ini merupakan cipher text yang didapatkan dari teks bahasa Indonesia tanpa tanda baca dan angka.

b. Desain dan Rancangan Sistem Kriptanalisis

Dalam penelitian ini dilakukan rancangan dan desain dalam proses pembentukan algoritma genetika, sebagai berikut:

- **Rancangan representasi kromosom**
  Kromosom direpresentasikan dalam bentuk non biner. Gen yang terdapat dalam kromosom berbentuk hanya huruf ASCII tanpa tanda baca, yang merupakan kata kunci yang digunakan untuk mengenkripsi cipher yang dimasukan. Panjang kromosom di dasarkan pada rumus analisis frekuensi dalam penentuan panjang kata kunci dari algoritma Vigenere Cipher.
- **Rancangan pembangkitan populasi awal**
  Populasi awal di bangkitkan sejumlah individu yang di inisialisasi, kromosom digenerik secara random dari kombinasi huruf A sampai dengan Z.
- **Rancangan Penentuan Fungsi Fitness**
  Fungsi fitness dirancang untuk mengetahui individu yang memiliki kualitas yang baik dan yang buruk. Setiap individu akan memiliki nilai fitnessnya.
- **Rancangan metode seleksi**
  Dalam penelitian ini seleksi dilakukan untuk mendapatkan solusi dalam memperoleh individu terbaik. Individu yang terseleksi akan melaju pada tahap algoritma genetika selanjutnya.
- **Rancangan reproduksi**
  Ada beberapa metode dalam proses reproduksi, reproduksi dilakukan untuk mendapatkan offspring baru, atau individu baru dalam suatu generasi.
  - Rancangan Metode *Crossover*
    Dalam penelitian ini *crossover* dilakukan dengan menukarkan materi genetik dua individu yang dijadikan sebagai induk menjadi dua individu baru atau offspring.
  - Rancangan Metode Mutasi
    Mutasi dilakukan dengan mambahkan materi genetik baru yang didapatkan secara random, kemudian disisipkan kesuatu individu untuk menjadi individu yang baru.

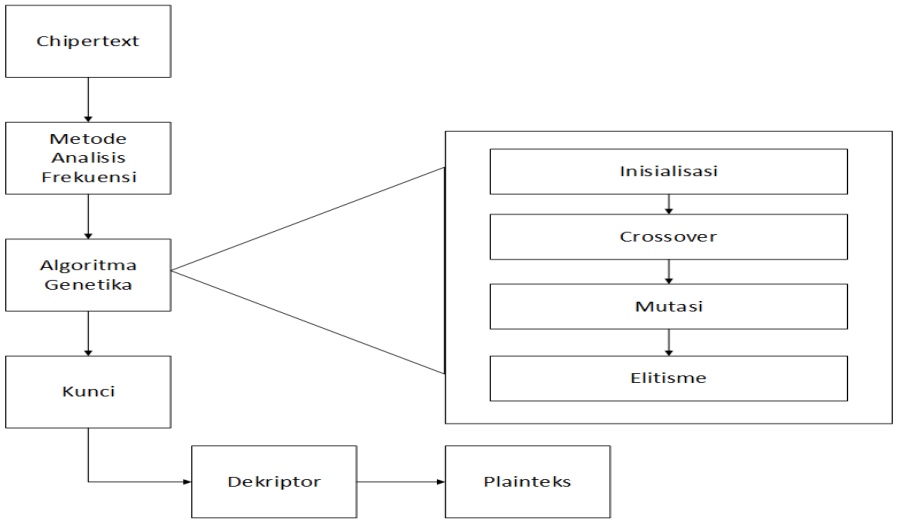
- Rancangan Metode Elitisme
  Elitisme dilakukan untuk mempertahankan individu yang terbaik dalam populasi awal, *crossover* dan mutasi pada generasi tersebut tetap di pertahankan pada generasi selanjutnya.

c. Desain Antarmuka
Interface atau antarmuka dibuat untuk memudahkan pengguna dalam melakukan pemprosesan, dan lebih interaktif dan lebih menarik.

d. Implementasi Sistem Kriptanalisis
Memasuki tahap berikutnya adalah tahap implementasi. Implementasi dilakukan dengan menerapkan tahapan tahapan sebelumnya.

e. Pengujian Sistem Kriptanalisis
Setelah pada tahap implementasi, dilakukan pengujian sistem setelah sistem telah selesai di buat untuk menguji tingkat akurasi dalam sistem, menguji optimasi sistem dalam mnentukan kata kunci, dilakukan pengujian untuk mengetahui parameter yang paling optimal untuk parameter pada algotima genetika sistemnya.

Berikut adalah alur sistem kriptanalisis algoritma vigenere cipher dengan algoritma genetika untuk penentuan kata kunci yang terlihat pada gambar 1:



Gambar 1. **Gambaran Umum Alur Sistem Kriptanalisis**

Alur kerja untuk sistem kriptanalisis vigenere cipher dengan algoritma genetika dalam penentuan kata kunci, adalah sebagai berikut :

1. Input Cipherteks
Cipher yang dimasukan merupakan cipher bersih tanpa adanya tanda baca dan tanpa adanya angka, dikarenakan kriptografi vigenere tidak dapat memproses tanda baca dan angka. Cipher yang di masukan merupakan hasil enkripsi kriptografi vigenere yang sudah dilakukan uji coba. Kemudian, cipher akan diproses untuk mendapatkan kata kunci dan digunakan untuk menebak kata kunci dengan algoritma genetika.

2. Metode Analisis Frekuensi dalam Penentuan Panjang Kunci
Langkah pertama, cipher di proses untuk mendapatkan panjang kata kunci, kata kunci didapatkan dengan metode analisis frekuensi. Panjang kata kunci ini merupakan panjang kromosom yang akan dibuat untuk merepresentasikan kromosom.
3. Proses algoritma genetika

Proses algoritma genetika dilakukan dengan membangkitkan populasi awal yang sudah dirancang kromosomnya, satu individu sesuai dengan panjang kata kunci yang merupakan panjang gennya. Populasi awal akan diproses dengan melakukan seleksi, setelah seleksi di lakukan masuk pada proses crossover untuk mendapatkan individu baru. Individu baru yang terbentuk dari proses crossover kemudian diproses dengan dilakukan mutasi, yaitu menyisipkan materi genetik baru pada kromosom, yang menghasilkan individu baru. Dari hasil populasi awal, crossover dan mutasi dilakukan elitisme untuk mempertahankan individu yang sudah baik agar masuk ke generasi berikutnya. Tiap individu memiliki nilai fitness yang menjadi pembanding baik tidaknya suatu individu. Nilai fitness dihasilkan dari fungsi fitness yang sudah di rancang, fungsi fitness bergantung pada objek penelitian yang dilakukan.

4. Proses Keadaan Berhenti

Penelitian ini akan terus berlanjut hingga berada pada keadaan berhenti, sistem akan berhenti ketika nilai fitness mencapai angka satu. Maka kata tersebut merupakan kata kunci dari cipher yang dimasukan.

3. HASIL DAN PEMBAHASAN

3.1 Pengumpulan Data

Data cipher text yang digunakan diperoleh dari analisis hasil percobaan enkripsi. Dalam penelitian ini teks data asli yang di gunakan untuk pengujian merupakan teks bahasa Indonesia, teks tersebut berupa teks cerita dongeng anak anak berbahasa Indonesia. Yang bersumber dari: http://www.rumahdongeng.com/cerita-anak.php?id=597 yang berjudul gagak dan merak. Data teks yang di dapatkan tidak dapat langsung diolah, data sebelumnya harus di bersihkan dari segala tanda baca dan angka. Data teks asli merupakan teks Bahasa Indonesia yang baik dan benar. Data teks asli yang digunakan adalah sebagai berikut:

```
seekor gagak tinggal di dalam hutan dan merasakan kenikmatan hidup suatu hari
harus melihat angsa ia membatin angsa begitu putih dan dirinya sangat hitam
tentu dia menjadi burung paling bahagia sedunia gagak pun mengatakan
pikirannya kepada angsa lalu angsa bercerita bahwa dirinya merasa ia burung
bahagia sedunia hingga melihat burung kakaktua yang mempunyai dua warna siapa
lebih bahagia merak atau gagak gagak pergi menemui burung kakaktua karena
dipikirnya burung itulah yang paling bahagia ketika mendekati burung kakaktua
lalu burung kakaktua berkata bahwa paling bahagia adalah burung merak hal ini
karena burung merak memiliki banyak warna yang sangat indah gagak pergi
menemui merak di kebun binatang dia melihat ratusan orang berkerumun hanya
demi bisa melihat merak setelah orang orang pergi gagak mendekati merak dia
mengatakan kalau merak adalah burung paling bahagia di planet ini karena semua
orang berdatangan demi bisa melihat keindahannya sedangkan jika mereka melihat
gagak pasti akan segera diusir pergi merak tadinya berpikir bahwa dirinya
adalah burung paling bahagia di muka bumi karena dirinya memiliki kecantikan
dan kesempurnaan pada kenyataan
```

Data yang di rubah kedalam bentuk cipher harus dalam satu paragraf. Enkripsi plainteks menggunakan rumus persamaan (1).

$$Ci = (Pi + Kr)\ mod\ 26 \qquad (1)$$

Dengan :
Ci = cipherteks huruf ke-i
pi = huruf ke-i dalam teks asli
kr = huruf ke-r dalam kunci

Contoh vigenere cipher:
Plaintext : INI ADALAH PESAN RAHASIA
Kunci : LAG ULAGUL AGULA GULAGUL

Kunci disesuaikan dengan plaintext, apabila kunci lebih pendek dari plaintext, maka kunci akan diulang. Adapun proses enkripsi vigenere cipher dapat dilihat pada tabel 1.

Cipherteks : TNO UOARUS PKMLA XUSAYCL

Tabel 1. Proses Enkripsi Vigenere Cipher

		PLAINTEXT																								
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
K	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
U	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
N	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
C	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
I	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Seperti terlihat pada tabel 1 cara menggunakan tabula recta untuk menentukan kode vigenere dapat dilihat diatas, posisi horizontal merupakan text asli dan pada posisi vertical adalah kunci. Yang menjadi cipher adalah perpotongan antara huruf asli dengan huruf kunci.

Data teks ini memiliki banyak karakter sebanyak 1000 karakter apabila di hitung tanpa spasi. Dengan jumlah kata sebanyak 171 kata. Teks asli akan di enkripsi dengan kata kunci. Kata kunci yang dipilih merupakan satu kata dalam kamus bahasa Indonesia. Dalam penelian ini kata kunci yang di pilih merupakan kata “makan” dengan hasil enkripsi sebagai berikut:

```
eeokbd gkgnw tsntsav dv pavaz tudaa pax mrdacaxmn ueaukwagmn riqgp cunfu
raeu hkrhe molvtad aassk in yewbnfix aassk brsidu cgtsh qmn nieunia fmnqag
tidaz fexth pik mrzjkdv nubuas pklvzg laumgsa fqdenvm gkgnw pen zqnqagmkkn
cuksrnznia xqpkdn mnqsn xavu nzgca oqrmeeutk bntwk dvdixyn yebafm ik bhduxg
omhkgvm sodhzik hvzgqa zqlshnf berhzg uaxmkdun kaxg zqmzuakas dhm wkram
ssacm lobvt bkhnsik mrdau agmu qatmk qatmk zeesi weaqmei ogrent wauaxfuk
kndexa qupskvdnia ogrent utelnt yknt bavias bkhnsik krfiua zqnnexmts bhduxg
xmkkkgga vayg berhzg uaxmkdun nebknfa lauia zayunq bntaqin mdklnt berhzg
weemk ray uns kndexa ogrent yebax yewiyuks bnzykk jmrxa lmnq snzgkt vzdkh
tmgkk cqrqi zqnomhu mornw ds krnux bvzadaas dsa zqlshnf rktheax oemnq
brdkorhyux hnzyk dryi lifm molvtad mrdau srfevau arknt arknt bebgv saqax
yexdrwadi zqrkk qua weasadaxmn uaymu weemk kdnxar bhduxg cmlsnt naratua ni
cxaxeg uns kndexa fqmea bdaxg oqrnagmnqaa pewi ousk mrxirag wesnqmhknaka
ceqmnqknz jskn yebexm molvtad gnsau pnets axmn cetqrk dvgssr cqrqi zqrkk
gmdsnlm borcuksr omhga qursnlm anaymh luegnq pnxixg omhkgvm ds mhwa luzu
kkrrza nieunia zqmslvwi uepmndixmn naa wecezbubnnmn zaqm konlmtkaa
```

3.2 Implementasi Algoritma Genetika

3.2.1 Representasi Kromosom

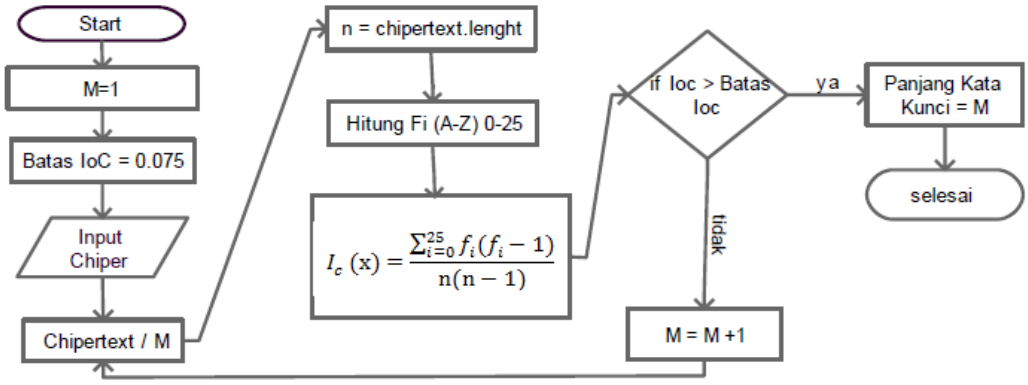
Untuk mengetahui panjang dari sebuah kromosom maka harus diketahui panjang dari sebuah kata kunci. Dalam hal ini algoritma yang digunakan untuk menebak kata kunci menggunakan *index coincidence* yaitu dengan menghitung banyak frekuensi huruf dalam sebuah bagian. Berdasarkan penelitian sebelumnya nilai *index coincidence* teks berbahasa Indonesia yang mengacu pada penelitian Sutanto dan Khudri nilai *index coincidence* adalah 0.078 (Sutanto & Khudri, 2012). Namun setelah dilakukan pengamatan kembali dan analisis terhadap nilai batasan tersebut, didapatkan nilai batas tersebut tidak dapat menebak semua panjang kata kunci dengan benar. Kemudian didapatkan nilai batas index coincidence yaitu 0.075. Nilai tersebut yang akan menjadi batas berhentinya proses algoritma penebakan panjang kata kunci yang akan dilakukan. Nilai index Ioc di dapatkan dengan menggunakan rumus (2).

$$I_c\,(\mathrm{x}) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{\mathrm{n}(\mathrm{n} - 1)} \qquad (2)$$

I_c = *Index coincidence*
f_i = Frekuensi A, B, ……Z
n = Banyak karakter seluruh cipherteks

Adapun teknik dalam *index coincidence* dapat dilakukan sebagai berikut (Bawono, 2015):
1. Hitung masing-masing karakter dalam baris dan kolom.
2. Catat fekuensi tiap urutan huruf.
3. Hitung *index coincidence* tiap kolom dan baris.
4. Hitung rata-rata dari setiap *index coincidence* yang dihasilkan.
5. Hasil dari *index coincidence* yang terbesar merupakan kemungkinan dari panjang kunci dari cipherteks.

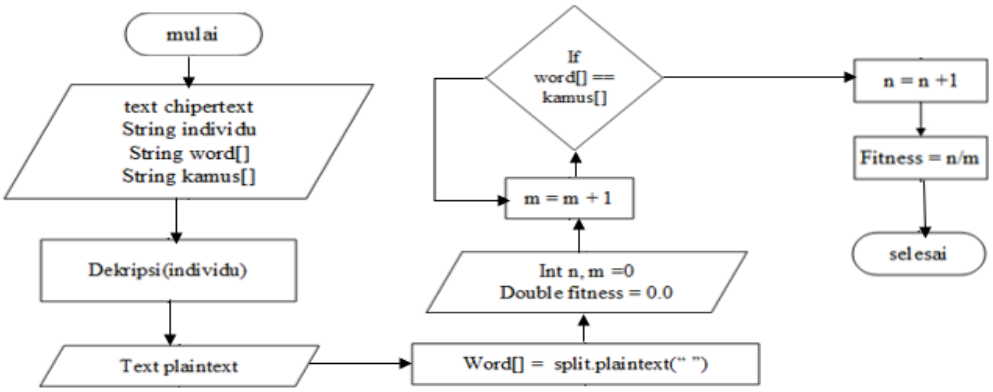
Rancangan diagam alir dalam penentuan panjang kata kunci yang menjadi panjang dari suatu kromosom disajikan pada gambar 2 dibawah ini:



Gambar 2. Diagram Alir Rancangan Penentuan Panjang Kata Kunci

3.2.2 Perhitungan Fungsi Fitness

Fungsi fitness merupakan fungsi yang digunakan untuk mendapatkan nilai fittnes yang menjadi nilai baik buruknya suatu individu. Fungsi fitness dirancang berdasarkan jenis kasus yang di hadapi. Nilai fungsi fitness didapatkan berdasarkan ada atau tidaknya kata hasil dekripsi kata kunci suatu individu pada kamus atau *library* yang sudah di gunakan pada sistem. Fungsi fitness memiliki nilai rentang 0 sampai dengan 1, perancangan fungsi fitness berdasarkan banyaknya kecocokan kata pada kamus Bahasa Indonesia. Berikut digram alir dalam menentukan fungsi fitness disajikan pada gambar 3 dibawah ini:



Gambar 3. Diagram Alir Penetuan Fungsi Fitness

Adapun tahapan dalam menentukan fungsi fitness sebagai berikut:

1. Setiap individu dengan kata yang sudah tergenerik di lakukan proses dekripsi.
2. Kemudian hasil dekripsi berupa plaintext dengan kata kunci dari masing masing individu.
3. Dilakukan pencocokan tiap kata kedalam kamus
4. Apabila kata tersebut ada dalam kamus maka akan memiliki nilai +1 apabila kata tidak ditemukan maka akan bernilai 0
5. Kemudian kata banyak yang benar di jumlahkan di bagi dengan banyak kata keseluruhan
6. Hasil bagi tersebut yang akan di ambil menjadi nilai fitness dari individu tersebut.

3.2.3 Crossover

Proses crossover merupakan proses pertukaran silang materi genetika antara dua individu sebagai induk yang menghasilkan dua individu baru sebagai anak. Pada penelitian ini crossover yang di gunakan adalah crossover uniform. Dengan crossover ini akan menukarkan gen induk 1 dengan gen induk 2 yang di pilih secara acak berdasarkan nilai probabilitas crossover (Pc).

3.2.4 Mutasi

Gen yang di mutasi berdasarkan nilai Probabilitas Mutasi (Pm). Nilai Pm memiliki nilai rentan antara 0 sampai dengan 1. Gen dipilih secara acak, kemudian gen terpilih akan di sisipkan dengan materi Genetik yang baru. Metode Mutasi ini adalah metode Mutasi Uniform.

3.2.5 Elitisme

Elitisme merupakan proses untuk mempertahankan individu yang baik agar tetap bertahan pada generasi selanjutnya. Elistisme yang digunakan yaitu dengan menggabungkan semua individu yang ada pada populasi awal, hasil *crossover* dan hasil mutasi. Jenis elisitme ini dinamakan union yaitu penggabungan.

3.3 Experimen untuk pencarian parameter optimal

Setelah dilakukan tahap implementasi selanjutnya dilakukan Eksperimen untuk menemukan solusi terbaik dari kasus kriptanalisis ini. Solusi terbaik dalam kasus ini merupakan kata kunci yang dipakai untuk mengenkripsi teks asli. Kata kunci ini di modelkan dalam bentuk individu yang memiliki nilai fitness yang mendekati angka 1.

Dalam pengujian sistem yang menggunakan algoritma genetika dalam pemecahaan kata kunciya terdapat beberapa variable bebas yang digunakan untuk mengoptimasi hasil uji. Variable bebas tersebut adalah Pc (probabilitas *crossover*), Pm (propbabilitas mutasi) dan Pop

size atau ukuran jumlah individu dalam satu populasi. Tiga variable bebas tersebut yang akan mempengaruhi hasil individu yang berdampak pada nilai fitness.

Pengujian dilakukan dengan lima kali eksperimen, dengan kriteria tiap ekperimen yang berbeda beda. Adapun yang menjadi perbedaan tiap eksperimen adalah:

1. Ekperimen 1, melakukan pengujian dengan perbedaan variable bebas (parameter) dengan 1000 kombinasi parameter dengan batas waktu +- 60 menit. Pada teks cipher dengan jumlah karakter 1000 karakter yang memiliki kata kunci “makan”. Ditemukan 467 kombinasi parameter dengan modus kombinasi parameter yang menghasilkan hasil terbanyak dan waktu yang paling optimal diantara 1000 kombinasi parameter ditampilkan dalam tabel 2.

Tabel 2. Kombinasi Parameter Terpilih

pm	pc	pop_size
0.09	0.5	12
0.1	0.4	14
0.08	0.2	16
0.07	0.1	18
0.1	0.5	18

2. Eksperimen 2, melakukan pengujian dengan menggunakan paramater yang terdapat dalam tabel 2, terhadap cipher 1000 karakter dengan dua kata kunci yang berbeda, untuk dilakukan perbandingan dan dilakukan sebanyak lima kali tiap parameter. Kata kunci yang digunakan “makan” dan “bintang”. Ditemukan nilai rata rata waktu tercepat adalah dengan parameter ke-4 yaitu Pm 0.07, Pc 0.1 dan Pop_size 18 diperoleh 1807 detik, dengan standar deviasi yaitu 456.4 detik. Sedangkan untuk kata kunci bintang rata rata waktu tercepat dengan Pm 0.08, Pc 0.2 dan Pop_size 16, diperoleh 4286.9 detik, dengan standar deviasi 2516.4 detik.

3. Eksperimen 3, melakukan pengujian dengan menggunakan paramater yang terdapat dalam tabel 2, terhadap cipher 500 karakter dengan dua kata kunci yang berbeda, untuk dilakukan perbandingan dan dilakukan sebanyak lima kali tiap parameter. Kata kunci yang digunakan “makan” dan “bintang”. Ditemukan nilai rata rata waktu tercepat untuk kata kunci makan adalah dengan parameter ke-4 yaitu Pm 0.07, Pc 0.1 dan Pop_size 18 diperoleh 1739.8 detik, dengan standar deviasi yaitu 784.5 detik. Sedangkan, untuk kata kunci bintang, rata rata waktu tercepat dengan Pm 0.08, Pc 0.2 dan Pop_size 16, diperoleh 2221.5 detik, dengan standar deviasi 266.2 detik.

4. Eksperimen 4, melakukan pengujian dengan menggunakan paramater hasil terbanyak pada eksperimen 1 tanpa melihat durasinya yaitu Pm 0.09, Pc 0.3 dan pop_size 20 yang bertujuan untuk mencari durasi rata rata. terhadap cipher 1000 karakter dengan dua kata kunci yang berbeda, untuk dilakukan perbandingan dan dilakukan sebanyak lima kali tiap parameter. Kata kunci yang digunakan “makan” dan “bintang”. Ditemukan nilai rata rata waktu tercepat yang di peroleh untuk kata kunci makan dengan parameter Pm 0.09, Pc 0.3 dan Pop_size 20 adalah 1366.3 detik dan nilai standard deviasi 421.7 detik. Sedangkan untuk kata kunci bintang, rata rata waktu tercepat dengan Pm 0.09, Pc 0.3 dan Pop_size 20, diperoleh 2833.1 detik, dengan standar deviasi 987.5 detik.

5. Eksperimen 5, melakukan pengujian dengan menggunakan paramater hasil terbanyak pada eksperimen 1 tanpa melihat durasinya yaitu Pm 0.09, Pc 0.3 dan pop_size 20 yang bertujuan untuk mencari durasi rata rata. terhadap cipher 500 karakter dengan dua kata kunci yang berbeda, untuk dilakukan perbandingan dan dilakukan sebanyak lima kali tiap parameter. Kata kunci yang digunakan “makan” dan “bintang”. Ditemukan nilai rata rata waktu tercepat yang di peroleh untuk kata kunci makan dengan parameter Pm 0.09, Pc 0.3 dan Pop_size 20 adalah 1737.4 detik dan nilai standard deviasi 582 detik. Sedangkan

untuk kata kunci bintang, rata rata waktu tercepat dengan Pm 0.09, Pc 0.3 dan Pop_size 20, diperoleh 2006.2 detik, dengan standar deviasi 763 detik.

3.4 Perbandingan Eksperimen

Setelah dilakukan percobaan terhadap parameter yang telah ditentukan dengan jumlah karakter yang berbeda dan kata kunci yang berbeda, maka perbandingan kelima eksperimen tersebut disajikan pada tabel 3:

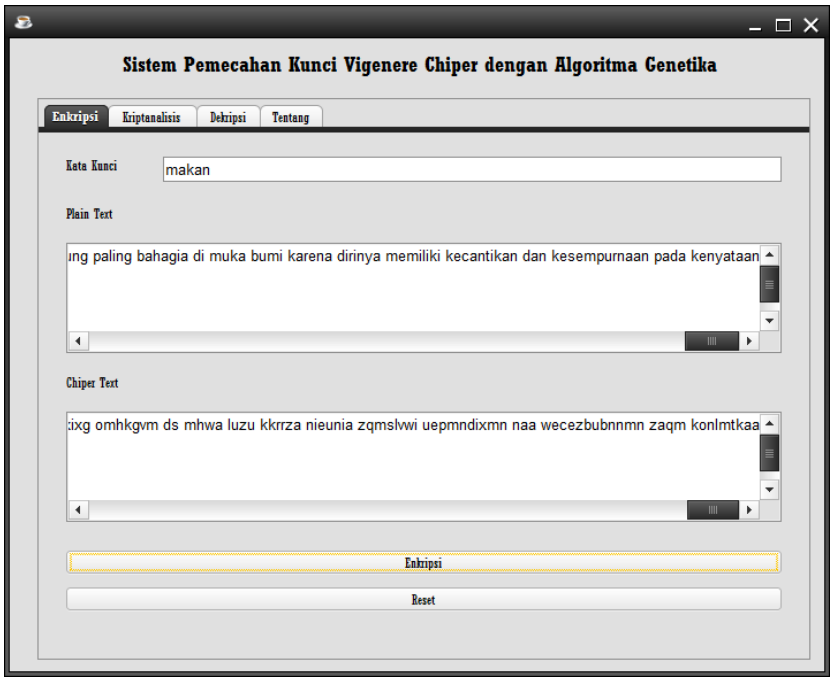
Tabel 3. Hasil perbandingan Eksperimen

pm	Pc	pop_ size	1000 karakter				500 karakter			
			rata-rata		standar deviasi		rata-rata		standar deviasi	
			makan	bintang	makan	bintang	makan	bintang	makan	bintang
0.09	0.7	12	2098.2	9731.9	956.2	10910.9	3917.9	24595.1	2288.4	8335.9
0.1	0.4	14	2325.7	4607.8	850.0	1303.0	1815.9	3514.5	500.0	1577.3
0.08	0.2	16	2338.8	4286.9	667.8	2516.4	3504.9	2221.5	1439.3	266.2
0.07	0.1	18	1807.0	4793.7	456.4	1951.6	1739.8	3616.1	784.5	1253.0
0.1	0.5	18	4084.8	5253.7	662.6	1635.2	2890.0	2664.1	1388.5	1406.0
0.09	0.3	20	1366.3	2833.1	421.7	987.5	1737.4	2006.2	582.0	763.0

Berdasarkan tabel 3, jumlah karakter cipher yang memiliki panjang 1000 karakter memiliki waktu eksekusi yang lebih lama dibanding dengan cipher yang memiliki panjang 500 karakter. Perbedaan kata kunci pun memiliki pengaruh terhadap waktu eksekusi, kata kunci yang lebih panjang memiliki waktu yang lebih lama dibanding dengan kata kunci yang pendek.

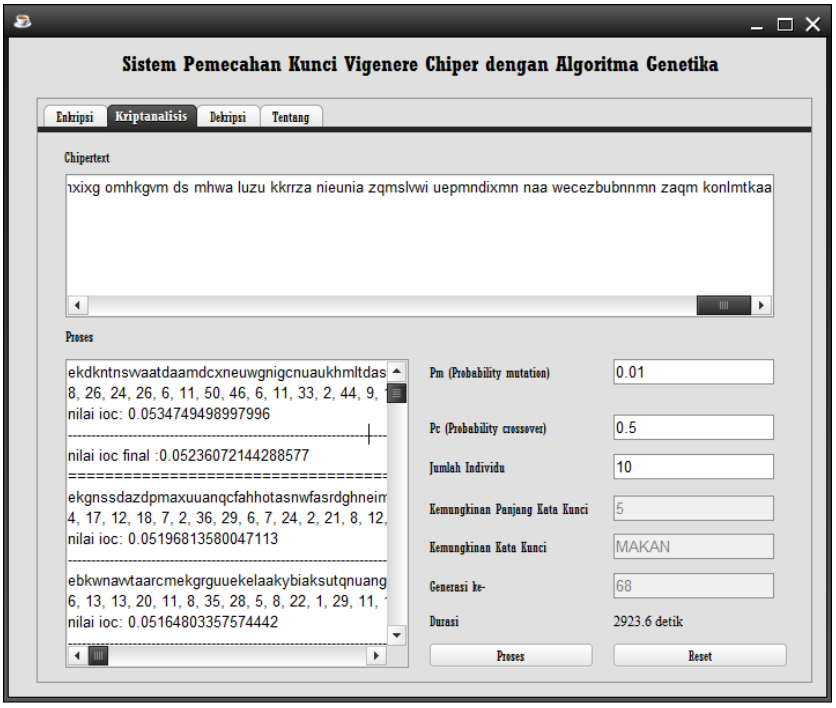
3.5 Tampilan Sistem Kriptanalisis

Adapun hasil implementasi dalam penelitian ini adalah sebagai berikut, sistem dibuat dalam satu tampilan dengan 4 tab untuk mempermudah. Tab pertama halaman enkripsi seperti pada gambar 4, terdapat kolom kata kunci dan plainteks untuk diinputkan, kemudian tombol Enkripsi untuk memproses dan menghasilkan data enkripsi.



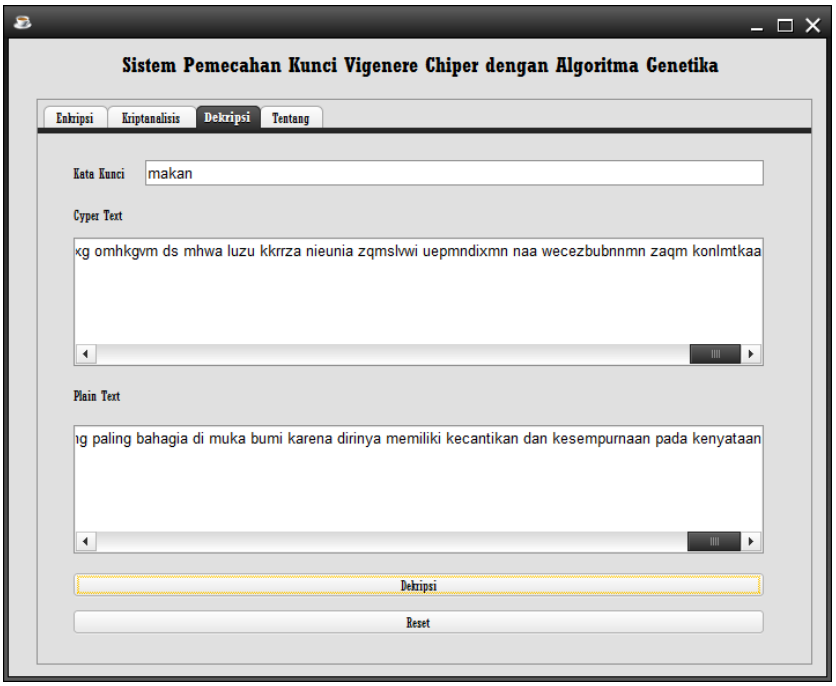
Gambar 4. Tampilan Halaman Enkripsi

Tab kedua yaitu halaman Kriptanalisis, sistem meminta inputan cipher dan tiga parameter yang menjadi variable dalam komputasi Algoritma Genetika. Diantaranya nilai parameter Pm (Probability of Mutasi), Pc (Probability of Crossover) dan Jumlah Individu atau yang biasa disebut Pop_Size. Ditampilkan gambar 5 tampilan kriptanalisis. Kemudian tombol Proses untuk mengeksekusi dan tombol reset untuk hapus data.



Gambar 5. Tampilan Halaman Kriptanalisis

Tab ketiga halaman dekripsi seperti pada gambar 6 dibawah ini, terdapat kolom kata kunci dan ciphertext untuk diinputkan, kemudian tombol dekripsi untuk memproses dan menghasilkan data dekripsi atau plainteks.



Gambar 6. Tampilan Halaman Enkripsi

4 KESIMPULAN

Dari penelitian yang telah dilakukan oleh peneliti dapat di tarik kesimpulan bahwa sistem kriptanalisis ini dapat membongkar kata kunci cipher yang digunakan dengan menghasilkan parameter optimal yaitu Pm 0.09 Pc 0.3 dan Pop_size 20 sebagai syarat untuk melakukan kriptanalisis pada sistem.

Dari penelitian ini dapat membuktikan bahwa metode Algoritma genetika dapat digunakan sebagai alat untuk melakukan kriptanalisis vigenere cipher.

Setelah dilakukan beberapa experimen dalam penelitian ini bahwa Jumlah karakter dan panjang kata kunci menjadi pengaruh terhadap waktu pemprosesan Algoritma Genetika. Dan dalam menentukan panjang kata kunci Nilai *index coincidence* untuk teks Bahasa Indonesia yang digunakan adalah 0.075.

DAFTAR PUSTAKA

Adyaksyah, R., & Irawan, M. I. (2012). Perancangan Sistem Kriptanalisis RSA Menggunakan Jaringan Syaraf Tirua Perceptron. *Jurnal Teknik Pomits* (hal. 1-6). Surabaya: Intitut Teknologi Sepuluh Nopember.

Andana, G. (2014). *Analisis Frekuensi pada Teks Bahasa Indonesia Dan Modifikasi Algoritma Kriptografi Klasik.* Bandung: Institut Teknologi Bandung.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis, Dan Implementasi.* Yogyakarta: Andi.

Bawono, H. R. (2015). *Kriptanalisis Pada Vigenere Cipher.* Yogyakarta: Universitas Sanata Darma.

Chiquita, C. (2013). *Kriptanalisis pada Vigenere Cipher Menggunakan Aplikasi Maple untuk Menerapkan Teknik Signature dan Scrawls.* Bandung: Institut Teknologi Bandung.

Christensen, C. (2015). Dipetik Desember 13, 2016, dari http://www.nku.edu/: http://www.nku.edu/~christensen/1402%20Friedman%20test%202.pdf

Delman, B. (2004). *Genetic algorithms in cryptography.* New York: Rochester Institute of Technology .

Engelbrecht, A. P. (2007). *Computational Intelligence.* Ltd.: John Wiley & Sons.

Hapsari, A., Perdana, R., & Risvelina. (t.thn.). Dipetik Mei 18, 2017, dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Makalah/Makalah07.pdf

Hutasoit, J. T. (2008). *Penerapan Algoritma Backtracking Pada Proses Kriptanalisis terhadap Hasil Enkripsi Vigenere Cipher denganMenggunakan Pendekana Dictonary Attack .* Bandung : Institut Teknologi Bandung.

Munir, R. (2005). *Diktat Kuliah IF5054 Kriptografi.* Bandung: Program Studi Teknik Informatika.

Munir, R. (2006). *Kriptografi.* Bandung: Penerbit Informatika.

Omran, S. S., Al-Khalid, A. S., & Al-Saady, D. M. (2011). A cryptanalytic attack on Vigenère cipher using genetic algorithm. *IEEE Conference on Open System (ICOS2011)*, 6.

Robi, N. M. (2016). *Implementasi Algoritma Genetika untuk Penjadwalan Instruktur Training ICT di UIN Sunan Kalijaga.* Yogyakarta: UIN Sunan Kalijaga.

Rodriguez, J. F. (2015). *Genetic Algorithm For Cryptanalysis on the Vigenere Cipher.* United State: ProQuest LLC.

Schneier, B. (1996). *Aplied Cryptography 2nd.* New York: John wiley and sons.

Sutanto, & Khudri, W. (2012). *Kriptanalisis Algoritma Vigenere Cipher.* Solo: Universitas Sebelas Maret Solo.

Toemeh, R., & Arumugam, S. (2008). Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers. *The International Arab Journal of Information Technology*, 5.

Wardoyo, A. E., & Nilogiri, A. (2012). *Penerapan Teknik Exhaustive Attack pada Proses Kriptanalisis Vigenre Ciphertext Menggunakan Bantuan Kamus Bahasa Indonesia.* Jember: Universitas Muhamadiyah Jember.

Wati, D. A. (2011). *Sistem Kendali Cerdas: Fuzzy Logic Controller, Jaringan Syaraf Tiruan, Algoritma Genetik Dan Algoritma Particle Swarm Aptimization.* Yogyakarta: Graha Ilmu.

Widodo, T. S. (2012). *Komputasi Evolusioner.* Yogyakarta: Graha Ilmu.