SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 1 Nomor 1, Oktober 2016
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Penyandian Kunci Dengan Optimasi Menggunakan Algoritma Genetika Pada Kunci Enkripsi Kriptografi Hill Cipher

Muhammad Iqbal Nahwi
Universitas Sumatera Utara
iqbalnahwi@gmail.com

Abstrak — *Hill Cipher* merupakan salah satu algoritma kriptografi kunci simetris. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi Karena menggunakan matriks sebagai kunci, *Hill Cipher* merupakan algoritma kriptografi kunci simetris yang sulit dipecahkan, karena teknik kriptanalisis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini. adapun Kriptografi *Hill Chiper* saat ini telah banyak digunakan untuk mengatasi permasalahan yang terkait dengan pengamanan suatu kunci. Adapun dalam proses Salah satu permasalahannya dalam bidang optimasi algoritma genetika ini dapat diterapkan pada berbagai bidang tertuntu didalam hal ini algoritma genetika dapat diterapkan untuk mengoptimasi suatu permasalahan yang ingin diselesaikan pada suatu penyajian kunci pada kriptografi *hill chiper*, dimana tujuan dari algortima genetika ini akan memberikan hasil yang lebih optimal didalam mendapatkan kunci pada kriptografi *hill chiper*, Untuk itu penulis menggunakan algoritma genetika sebagai pengoptimasian sehingga akan diperoleh hasil yang baik didalam menetukan suatu kunci yang lebih baik dan dengan Algoritma Genetika akan menghasilkan hasil yang terbaik didalam memberikan penyajian kunci.

Kata Kunci — *Hill Chiper, kriptografi, Kunci, Simetris, Matriks, Optimasi, Algotima Genetika*.

I. PENDAHULUAN

Perlindungan dalam suatu sistem sangat penting untuk berbagai keperluan dalam hal suatu interaksi berbagai bidang, dalam hal ini sangat dianjurkan suatu sistem yang lebih baik dalam pengaman sehingga akan tercipta suatu keyakinan yang baik dalam melaksanakan pekerjaan didalam sistem yang akan dijalani, maka akan memberikan kepercayaan yang baik dalam perlindungan suatu kerahasian data dari tindakan kejahatan.

Salah satu Dengan ada nya beberapa kendala dalam distribusi kunci belum dilakukan secara maksimal dalam penyandian kunci enkripsi Algoritma Genetika dapat digunakan sebagai menyelesaikan masalah Optimasi yang kompleks pada proses enkripsi dengan menggunakan Algoritma Genetika dapat meningkatan penyajian kunci sehingga lebih baik.

Berdasarkan beberapa uraian di atas penelitian ini mencoba untuk mengoptimasi kunci pada *Hill chiper* dengan menggunakan algoritma genetika dalam penyajian suatu kunci didalam *Hill chiper* sehingga kriptanalis tidak begitu mudah dalam upaya pemecahan kunci *Hill chiper* dan tidak dapat dikembalikan dalam memecahkan kunci yang telah digabungkan dengan metode genetika dan maka akan menghasilkan metode penyajian kunci yang lebih baik didalam menyajikan kunci enkripsi terhadap kriptgrafi *Hill chiper*. Dimana algoritma kriptografi Hill Chiper yang cukup baik didalam penyajian kunci namun bukan berarti tidak memiliki kelemahan didalam penyajian kunci maka diperlukan suatu optimasi penyajian kunci tersebut dalam pembangkit bilangan diperlukan suatu pembangkit bilangan random yang aman dan sulit diperoleh didalam penyajian kunci *Hill chiper*, maka dengan itu diperlukan algoritma genetika didalam mengoptimasi kunci enkripsi sehingga akan semakin sulit didalam pemecahan penyandian kunci. Sehingga dapat digunakan sebagai menyelesaikan masalah optimasi yang kompleks dalam menentukan suatu kunci yang lebih baik didalam menentukan keamanan penyandian suatu kunci.

II. TINJAUAN PUSTAKA

A. Algoritma Genetika

Algoritma Genetika adalah menyimpulkan komputasi berbasis evolusi. dimana manfaatnya adalah membuat suatu perangkat keras bisa melakukan metode algoritma untuk suatu konsep yang sama dengan perubahan alam. salah satu seorang ahli dibidang komputer Holland menekankan perubahan dari nilai yang terdapat dari suatu string dan mengubah menjadi bilangan bit, dan holland memaparkan metode algoritma tersebut konsep perubahan alam. dimana tahanpan algoritma genetika ini diceritakan oleh holland salah satu tahapan yang tersusun dalam bentuk kumpulan sebuah kromosom dimanipulasi sehingga berubah bentuk menjadi kumpulan yang baruhal suatu interaksi berbagai bidang [11].

e-ISSN : 2541-2019
p-ISSN : 2541-044X

B. *Probabilitas Seleksi*

Bagian ini membicarakan bagaimana probabilitas seleksi untuk setiap chromosome. Dalam prosedur seleksi perbandingan, probabilitas seleksi dari sebuah chromosome sebanding denganfitness value yang dimilikinya [5]. Contoh dalam generasi awal, dimana ada sebuah kecenderungan untuk sebuah super chromosome kecil akan mendominasi proses seleksi. Dalam generasi selanjutnya ketika populasi secara besar berkumpul, kompetisi diantara chromosome kurang kuat dan pencarian random tingkah laku akan muncul. Scaling dan ranking mechanism diharapkan dapat mengurangi masalah ini. Metode scaling membuat peta mentah nilai fungsi obyektif menjadi beberapa nilai real positif, dan probabilitas survival untuk setiap chromosome menurut nilai itu. Matode ranking menganggap nilai aktual fungsi obyektif dan menggunakan ranking dari chromosome sebagai pengganti untuk menentukan probabilitas survival. Proses seleksi adalah proses pemilihan chromosome. Setelah chromosome itu terpilih maka chromosome itu langsung akan menjadi chromosome awal pada generasi yang baru. Dengan kata lain setelah melewati proses seleksi itu maka akan berganti ke generasi baru. Proses seleksi yang umum digunakan adalah dengan menggunakan Roulette Wheel Selection[14].

C. *Algoritma Kriptografi*

Definisi yang digunakan di dalam buku 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 di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudation[10].

D. *Enkripsi*

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi bisa diartikan dengan chiper atau kode, di mana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan[14].

E. *Dekripsi*

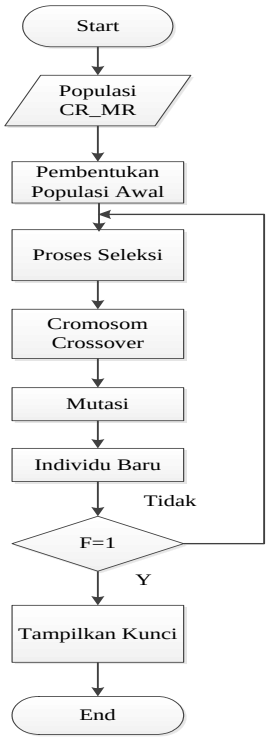
Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak kebentuk file aslinya *dengan menggunakan kunci atau kode*[12].

III. ANALISIS DAN PERANCANGAN

Dalam bagian ini penulis akan menjelaskan rancangan dari sistem komunikasi yang akan dibangun.

A. *Rancangan Topologi*

Dalam tahap penelitian ini untuk memahami proses pemakaian algoritma genetika dalam mencari optimasi kunci enkripsi pada Hill chiper dengan menggunakan algoritma genetika maka apa bila kunci yang dikembalikan tidak sesuai kunci yang telah di enkripsi dengan menggunakan algoritma genetika maka kunci tersebut tidak akan kembali dan apabila kunci yang telah sesuai dengan nilai yang terdapat pada metode tersebut maka secara otomatis kunci yang sudah dioptimasi menggunakan algoritma genetika maka akan kembali sesuai dengan kunci yang telah di enkripsi dengan itu akan diketahui dimana pencarian kunci yang lebih optimal untuk proses enkripsi tersebut.



Gambar 1. Rancangan *Flowchart* untuk optimasi kunci Enkripsi pada *Hill chiper* dengan menggunakan algoritma genetika.

Pada tahap proses diatas akan diseleksi populasi yang layak dijadikan sebagai populasi awal kromosom setelah didapat populasi yang layak maka maka akan dibentuk kembali awal sehingga akan di seleksi kembali menggunakan *crossover* dimana proses ini untuk memilih individu - individu yang akan dipilih untuk proses persilangan mutasi. Adapun fungsi Proses ini bertujuan untuk memotong dan memperoleh calon induk yang baik didalam algoritma genetika tersebut. Induk yang baik akan menghasilkan keturunan yang baik. Maka nilai fitness inilah yang nantinya akan digunakan sebagai populasi awal pada generasi berikutnya apa bila tidak ditemukan atau nilai F = 0 maka akan di terjadi lagi proses seleksi, penyilangan (*crossover*) dan mutasi sehingga akan samapai ditemukan pada generasi selanjut nya nilai F = 1 maka akan diperoleh individu baru setelah itu akan diproleh kunci yang siap ditampilkan.

IV. IMPLEMENTASI SISTEM

Pada bagian ini, penulis akan menjabarkan analisis dari hasil pengujian yang telah dijabarkan pada bagian sebelumnya ke dalam bentuk aplikasi perangkat lunak. Perangkat lunak yang dibangun dengan menggunakan bahasa pemrograman Visual Basic. Kemudian dengan menggunakan perangkat lunak tersebut, maka penulis akan mengoptimasi beberapa kunci yang layak menjadi suatu kunci yang bisa dipakai untuk mengenkripsi kunci Hill chiper dengan menggunakan algoritma genetika. Dari hasil optimasi tersebut akan menghasilkan suatu kunci yang didapat layak dijadikan sebagai kunci dengan penerapan menggunakan algoritma genetika.

A. Pengujian Populasi

Dimana pengujian pertama ini akan menggukan 9 kromosom dengan menggunakan percobaan 0-255 sebagai populasi.

Tabel 1. Populasi

Jumlah Populasi 0-255							
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87
88	89	90	91	92	93	94	95

Jumlah Populasi 0-255							
96	97	98	99	100	101	102	103
104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151
152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167
168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183
184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199
200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215
216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231
232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247
248	249	250	251	252	253	254	255

Maka dari pengujian nilai populasi 1- 9 akan didapat kromosom sebagai berikut:

Kromosom 1	F = 43
Kromosom 2	F = 118
Kromosom 3	F = 49
Kromosom 4	F = 199
Kromosom 5	F = 37
Kromosom 6	F = 59
Kromosom 7	F = 219
Kromosom 8	F = 61
Kromosom 9	F = 55

B. Pengujian Menggunakan Seleksi Roulette Wheel

Tabel 2. Individu

Nomor Individu	1	2	3	4	5	6	7	8	9
Nilai Probabilitas (Fk)	43	118	49	199	37	59	219	61	55

Kemudian akan dihitung total fitness dengan pada tabel diatas diatas berikut pengujian $(\sum fk)$sebagai total fitness :

= 43 + 118 + 49 + 199 + 37 + 59 + 219 + 61 + 55 = 840

Tabel 3. Hasil Seleksi Roulette Wheel

Nomor Individu	1	2	3	4	5	6	7	8	9
Nilai Fitness (FCK)	43	118	49	199	37	59	219	61	5
Probabilitas(PK)	0.0512	0.1405	0.0583	0.2369	0.044	0.0702	0.2607	0.0726	0.0

Dari hasil pengujian menggunalkan seleksi roulate wheel yang dapat dilihat pada tabel 4.13 di atas didapat nialai probabilitas dapat kita lihat kalau kromosom ke empat dan kromosom ke tujuh yang mempunyai fitness paling besar dari sembilan kromosom tersebut mempunyai probabilitas untuk terpilih pada generasi selanjutnya lebih besar dari kromosom lainnya. Untuk proses pengujian seleksi selanjut nya kita gunakan roulette wheel, setelah itu kita harus mencari dahulu nilai kumulatif.

Tabel 4. Hasil Optimasi

Jumlah Individu	1	2	3	4	5	6	7	8	9	Generasi
Kromosom 1	233	176	238	90	238	211	221	75	67	32
Kromosom 2	31	232	232	232	21	232	3	3	3	35
Kromosom 3	7	178	153	68	7	186	68	196	173	4
Kromosom 4	115	161	95	41	43	174	98	51	115	16
Kromosom 5	41	48	48	41	43	43	48	48	43	57
Kromosom 6	7	44	27	102	27	205	27	27	7	27
Kromosom 7	72	155	3	119	135	65	41	227	188	5
Kromosom 8	45	45	172	77	226	114	62	45	139	11
Kromosom 9	19	70	164	19	60	19	254	19	70	52

Dapat dilihat hasil optimasi Pada tabel 4 diatas

C. Enkripsi Pada Hill Chiper

Pada tahapan ini, proses enkripsi dilakukan adapun kunci yang akan di enkripsi ialah hasil dari pengujian menggunakan genetika ialah sebagai berikut :

Tabel 5. Tabel Kunci Enkripsi

Enkripsi	233	176	238
	90	238	211
	221	75	67

Adapun tahap pengujian selanjutnya ialah pada Hill chiper dimana percobaan pertama *plaintext* yang digunakan "TEKNIKXXX". *Plaintext* tersebut akan diubah kedalam bentuk desimal. Berikut hasil pengubahan kedalam bentuk desimal 84, 69, 75, 78, 73, 75, 88, 88 dan 88. Kemudian lakukan pengujian berikutnya dengan menggunakan persamaan berikut **Enkripsi = K.P mod 256.**

D. Deskripsi Pada Hill Chiper

Pada pengujian kedua pada deskripsi, Chipertext yang didekripsi adalah "y¨}Eë|Èh8". Kemudian Chipertext ini diubah kedalam bilangan desimal. Hasil pengubahan dalam bilangan desimal adalah 84, 69, 75, 78, 73, 75, 88,

88 dan 88. Kunci yang digunakan kunci sama seperti pada saat enkripsi. Kemudian lakukan proses XOR untuk mendapatkan pesan aslinya. Dari hasil pengujian, maka didapat :

Tabel 6. Tabel Kunci Deskriptif

Deskripsi	121	170	204
	153	133	161
	232	173	190

Pada pengujian penghitungan diatas menunjukkan hasilnya deskripsi benar .Dengan plaintext ”TEKNIKXXX” dienkripsi dengan hasilnya adalah “y¨}Eë|Èh8”. Setelah itu dideskripsi Hasil pengubahan dalam bilangan desimal adalah 84, 69, 75, 78, 73, 75, 88, 88 dan 88.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil perancangan dan uji coba maka menghasilkan kesimpulan, kesimpulan yang penulis berikan dapat disimpulkan sebagai berikut :

1. Adapun algoritma genetika dapat memberikan solusi untuk pencarian nilai dalam sebuah masalah optimasi untuk penyandian kunci Hill Chiper.
2. Didalam pencarian kunci enkripsi pada Hill Chiper dilakukan dengan proses seleksi alam dimana induk yang terbaiklah yang akan dijadikan sehingga akan lebih baik didalam menentukan parameter yang terdapat pada algoritma genetika .
3. Didalam menentukan suatu penyandian kunci adapun tahapan proses yaitu dengan menggunakan Seleksi, Crossover dan Mutasi didalam solusi pengoptimalan kunci tesebut.
4. Hill Chiper adalah algoritma kriptografi klasik yang sangat kuat dilihat dari segi keamanannya dan Algoritma genetika menggunakan cara kerja berdasarkan pada seleksi alam sehingga sangat baik metode ini dipadukan untuk menyelesaian masalah optimasi dan penyandian kunci.

B. Saran

Penyusun menyarankan untuk pengembangan agar selanjutnya algoritma genetika ini bisa disandingkan dengan algoritma lain untuk menyelesaikan suatu permasalah didalam mengoptimal suatu kasus tertentu dan Teknik ini terbukti efektif dalam penyelesaian beberapa masalah optimasi dan algoritma genetika ini juga bisa memberikan penyelesaian Traveling Salesman Problem didalam penyelesaian optimasi adapun fungsi matematis di algoritma genetika ini menyatakan kualitas dari sebuah penyelesaian pada suatu masalah tertentu.

REFERENSI

[1] Chipperfield, A., Fleming, P., Pohlheim, H., dan Fonseca, C. 2005. Genetic Algorithm TOOLBOX For Use with MATLAB. User’s Guide Ver.1.2. Department of Automatic Control and Systems Engineering, University of Sheffield.
[2] Goldberg, D., & Richardson, J. (1987). Genetik Algorithms With Sharing For Multimodal Function Optimization. In Proccedings Of the Second International Conference on Genetic Algorithms, 148-154 San Mateo, CA. Morgan Kaufmann.
[3] Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. STIMIK Budi Dharma.
[4] Hermawanto, Denny. 2007. Algoritma Genetika dan Contoh Aplikasinya. (Online) denny-optimasi.doc (7 September 2014).
[5] Konar, Amit. 2005. Computational Intelligence Principles, Techniques, and Applications. Springer: Calcutta, India.
[6] Kuhn, Matthias, Thomas Severin and Horst Salzwedel. 2013. Variable Mutation Rate at Genetic Algorithms: Introduction of Chromosome Fitness in Connection with Multi-Chromosome Representation. International Journal of Computer Application (IJCA)72(1):31-38.
[7] Kumar, Rakesh and Jyotishree. 2012. Blending Roulette Wheel Selection & Rank Selection in Genetic Algorithms, International Journal of Machine Learning and Computing2(4): 365-370.
[8] Mitchel, Mielanie. 1999. An Introduction to Genetic Algorithm. IT Press: Massachusets.
[9] Munawar, m. (2012). Perancangan algoritma sistem keamanan data menggunakan metode kriptografi asimetris. Jurnal komputer dan informatika, 1(1).
[10] Munir, R. 2006. Kriptografi. Informatika: Bandung.
[11] Negnevitsky, Michael. 2005. Artificial Intteligence-A Guide to Intelligent Systems. Addison Wesley: Edinburg.
[12] Picek, Stjepan, Jakobovic, Domagoj and Gloub, Marin. 2013. On the Recombination Operator in The Real-Code Genetic Algorithms, 2013 IEEE Congress on Evolutionary Computation, pp. 3103-3110.
[13] Promono Andy dan Sujjada Alun,"Implementasi Algoritma Hill chiper Sebagai media Steganografi Mengggunakan Metode LSB", 2009.
[14] Rabunal, Juan R. and Dorado, Julian. 2006. Artificial Neural Networks in Real-Life Applications, Ideal Group Publishing: Hershey, United States of America
[15] Reeves, Colin R and Rowe, Jonathan E. 2003. Genetic Algorithms : Principles and Perpectives - A Guide to GA Theory. Kluwer Academic Publishers: New York.

e-ISSN : 2541-2019
p-ISSN : 2541-044X

[16] Rifki Sadikin.Kriptografi untuk Keamanan Jaringan. Yogyakarta. Andi. 2012.
[17] Taiwo, Oloruntoyin Sefiu, Olukehinde Olutosin Mayowa and Kolapo Bukola Ruka. 2013. Application of Genetic Algorithm to Solve Traveling Salesman Problem. International Journal of Advance Research (IJOAR)1(4): 27-46.
[18] Widyanarko, A. 2008. Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya. Institut Teknologi Bandung.
[19] Wijaya,Rosyidah Jayanti.2007. http:// supriyanto. Fisika.ui.edu/ matkom1.pdf.