ANALISIS KRIPTOGRAFI SANDI *VIGENERE* TEKS ARAB MENGGUNAKAN METODE KASISKI DAN ALGORITMA GENETIKA

Skripsi

Untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S-1

Program Studi Matematika

Diajukan oleh :

ISMIATUL KHUSNA

13610047

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2017

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi/Tugas akhir
Lamp :-

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Ismiatul Khusna
NIM	: 13610047
Judul Skripsi	: Analisis Kriptografi Sandi Vigenere Teks Arab Menggunakan Metode Kasiski dan Algoritma Genetika

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam bidang matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 20 September 2017

Pembimbing I	Pembimbing II
Muchammad Abrori, S.Si., M.Kom.	Muhamad Zaki Riyanto, M.Sc.
NIP. 19720423 199903 1 003	NIP. 19840113 201503 1 001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2596/Un.02/DST/PP.00.9/11/2017

Tugas Akhir dengan judul : Analisis Kriptografi Sandi Vigenere Teks Arab Menggunakan Metode Kasiski dan Algoritma Genetika

yang dipersiapkan dan disusun oleh:

Nama : ISMIATUL KHUSNA
Nomor Induk Mahasiswa : 13610047
Telah diujikan pada : Kamis, 12 Oktober 2017
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muchammad Abrori, S.Si., M.Kom
NIP. 19720423 199903 1 003

Penguji I

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

Penguji II

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
NIP. 19800402 200501 1 003

Yogyakarta, 12 Oktober 2017
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
D E K A N

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001

SURAT PERNYATAAN KEASLIAN

Yang bertandatangan di bawah ini:

Nama	: Ismiatul Khusna
NIM	: 13610047
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 31 Juli 2017

Yang Menyatakan

METERAI TEMPEL
F0D42AEF483733189
6000
ENAM RIBU RUPIAH

Ismiatul Khusna

MOTTO

"dan bahwa manusia hanya memperoleh apa yang telah diusahakannya"

(Q.S An-Najm : 39)

"Wahai orang-orang yang beriman ! jika kamu menolong (agama) Allah, niscaya Dia akan menolongmu dan meneguhkan kedudukanmu"

(Q.S Muhammad : 7)

HALAMAN PERSEMBAHAN

Karya ini penulis persembahkan untuk :

Ayah, Ibu dan adik tercinta

dan

Keluarga besar Matematika 2013 UIN sunan Kalijaga Yogyakarta

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat dan hidayah-Nya, sehingga skripsi yang berjudul **ANALISIS KRIPTOGRAFI SANDI *VIGENERE* TEKS ARAB MENGGUNAKAN METODE KASISKI DAN ALGORITMA GENETIKA** dapat terselesaikan guna memenuhi syarat memperoleh gelar kesarjanaan di Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

Shalawat dan salam senantiasa tercurahkan kepada Nabi Besar Muhammad SAW, yang membawa umat manusia dari zaman kegelapan menuju zaman yang terang benderang dengan kemajuan ilmu pengetahuan dan teknologi. Penulis menyadari skripsi ini tidak akan selesai tanpa motivasi, bantuan, bimbingan, dan arahan dari berbagai pihak. Oleh karena itu, dengan kerendahan hati penulis mengucapkan terimakasih kepada :

1. Bapak Dr. Murtono, M.Si, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak Dr. M. Wakhid Musthofa, M.Sc, selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

3. Bapak M. Abrori, S.Si, M.Kom, dan Bapak M. Zaki Riyanto, S.Si, M.Sc, selaku pembimbing yang telah meluangkan waktu, tenaga dan pikiran untuk memberikan bimbingan kepada penulis dalam penyelesaian penelitian ini.
4. Bapak Muchtarom, Ibu Sunarti, dan Ulfia Khasanah, serta seluruh keluarga yang telah memberikan dukungan baik moril maupun materil selama penulis menimba ilmu di Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
5. Teman-teman seperjuangan: Lisda Meilinda, Nur Fauziyah, Engla Fitri, Fitri Alfianti, Linda Mustika, Zhovana Khasanah, Riski Ryan Hardiansyah, Tri Anton Saputro, Hilal Hambali, Arif Suwanda, Agung Kurniawan, Alifatun Nasyrochah, Nani Maryani, Ina Riyati, Achmad Yusron, Idrokuttafkiroh, Dita, Alpiyah, yang selalu memberikan keceriaan kepada penulis.
6. Sahabat-sahabatku: Farah Bidara, Khalida Urfiyya, Aabidah Ummu Aziizah, Niken Fatma Putri yang selalu memberi semangat kepada penulis.
7. Teman-teman pengabdian PPIQ, terimakasih atas bantuannya dalam segala hal.
8. Keluarga besar Matematika angkatan 2013 UIN Sunan Kalijaga Yogyakarta yang selalu membantu dan memberikan dukungan kepada penulis selama ini.
9. Serta semua pihak yang tidak dapat penulis sebutkan satu persatu atas bantuan secara langsung maupun tidak langsung sehingga skripsi ini bisa terselesaikan dengan baik.

Semoga Allah memberikan balasan kepada mereka dengan sebaik-baiknya balasan. Penulis menyadari bahwa skripsi ini masih terdapat kekurangan, untuk itu penulis mengharapkan saran, dan kritik yang membangun untuk perbaikan skripsi ini. Penulis berharap semoga skripsi ini dapat bermanfaat bagi pembaca.

Yogyakarta, 26 September 2017

Penulis

Ismiatul Khusna

NIM. 13610047

DAFTAR ISI

HALAMAN JUDUL ..... **i**

HALAMAN PERSETUJUAN SKRIPSI ..... **ii**

HALAMAN PENGESAHAN ..... **iii**

HALAMAN PERNYATAAN KEASLIAN SKRIPSI ..... **iv**

HALAMAN MOTTO ..... **v**

HALAMAN PERSEMBAHAN ..... **vi**

KATA PENGANTAR ..... **vii**

DAFTAR ISI ..... **x**

DAFTAR GAMBAR ..... **xiii**

DAFTAR TABEL ..... **xiv**

DAFTAR LAMBANG ..... **xvii**

ABSTRAK ..... **xviii**

BAB I PENDAHULUAN **1**

1.1 Latar Belakang Masalah 1

1.2 Batasan Masalah 3

1.3 Rumusan Masalah 4

1.4 Tujuan Penelitian 4

1.5 Manfaat Penelitian 5

1.6 Tinjauan Pustaka 5

1.7 Metode Penelitian 7

1.8 Sistematika Penulisan 10

BAB II DASAR TEORI 11

2.1 Kriptografi 11

2.1.1 Definisi Kriptografi 11

2.1.2 Sejarah Kriptografi 12

2.1.3 Algoritma Kriprografi 15

2.1.4 Macam-macam Algoritma Kriptografi 15

2.1.5 Algoritma Kriptografi Klasik 17

2.1.6 Sandi *Vigenere* (*Vigenere Cipher*) 18

2.1.7 Analisis Frekuensi Huruf Arab 22

2.1.8 Sandi *Vigenere* Teks Arab 24

2.2 Analisis Kriptografi 26

2.2.1 Analisis Kriptografi Sandi *Vigenere* 28

2.2.2 Contoh Analisis Kriptografi Sandi *Vigenere* 34

2.3 Algoritma Genetika 44

2.3.1 Latar Belakang Algoritma Genetika 44

2.3.2 Definisi Algoritma Genetika 45

2.3.3 Struktur Dasar Algoritma Genetika 47

2.3.4 Parameter Dalam Algoritma Genetika 49

2.3.5 Komponen Utama Algoritma Genetika 51

2.3.6 Operator-operator Algoritma Genetika 53

2.3.7 Nilai *Fitness* (nilai kelayakan) 61

BAB III PEMBAHASAN 62

3.1 Analisis Kriptografi dengan Metode Kasiski 62

3.1.1 Analisis Kriptografi Teks Arab dengan Metode Kasiski..... 64

3.2 Fungsi *Fitness* 72

3.3 Analisis Kriptografi Menggunakan Algoritma Genetika 72

3.3.1 Analisis Kriptografi Teks Arab menggunakan

Algoritma Genetika. 76

3.4 Pencarian Kata Kunci dengan *Mutual Index Coincidence* 98

BAB IV PENUTUP 111

4.1 Kesimpulan 111

4.2 Saran 112

DAFTAR PUSTAKA 114

DAFTAR GAMBAR

Gambar 1.1 Alur Penelitian 9

Gambar 2.1 Algoritma Simetri 16

Gambar 3.1 *Flowchart* Metode Kasisiki 63

Gambar 3.2 *Flowchart* Algoritma Genetika 75

DAFTAR TABEL

Tabel 2.1 *Vigenere* Angka 20

Tabel 2.2 Contoh enkripsi sandi *Vigenere* 20

Tabel 2.3 Contoh dekripsi sandi *Vigenere* 21

Tabel 2.4 Frekuensi relatif huruf Arab 22

Tabel 2.5 *Vigenere* Angka (Arab) 25

Tabel 2.6 Contoh enkripsi sandi *Vigenere* (Arab) 25

Tabel 2.7 Frekuensi huruf dalam teks Bahasa Inggris 30

Tabel 2.8 Contoh *index of coincidence* 31

Tabel 2.9 3-gram perulangan *ciphertext* 35

Tabel 2.10 *Indices of coincidence* variasi beberapa kunci 35

Tabel 2.11 Frekuensi s_1 untuk panjang kunci 7 36

Tabel 2.12 Frekuensi s_2 untuk panjang kunci 7 37

Tabel 2.13 Nilai *mutual index coincidence* huruf A-M 40

Tabel 2.14 Nilai *mutual index coincidence* huruf N-Z 41

Tabel 2.15 Nilai *indices of coincidence* lebih dari 0,065
dan relasi 2 *string* (i, j) 42

Tabel 2.16 Dekripsi menggunakan kunci **AFZHBKP** 43

Tabel 2.17 Contoh Pengkodean Biner 51

Tabel 2.18 Contoh Pengkodean Permutasi 52

Tabel 2.19 Contoh Pengkodean *Integer* 52

Tabel 2.20 Contoh Pengkodean *Real* 52

Tabel 2.21 Ilustrasi Proses Rekombinasi 56

Tabel 2.22 Contoh Rekombinasi satu titik 56

Tabel 2.23 Contoh Rekombinasi dua titik 57

Tabel 2.24 Contoh Rekombinasi Seragam 58

Tabel 2.25 Ilustrasi *Order Crossover* 59

Tabel 2.26 Contoh *Swap Mutation* 60

Tabel 2.27 Contoh *Scramble Mutation* 60

Tabel 2.28 Contoh *Shift Mutation* 61

Tabel 3.1 3-gram kemunculan huruf *ciphertext* 64

Tabel 3.2 Frekuensi huruf baris ke-1 66

Tabel 3.3 Frekuensi huruf baris ke-2 67

Tabel 3.4 Frekuensi huruf baris ke-3 68

Tabel 3.5 Frekuensi huruf baris ke-4 69

Tabel 3.6 Frekuensi huruf baris ke-5 70

Tabel 3.7 Nilai Indco panjang kunci 5 71

Tabel 3.8 Nilai Indco beberapa variasi panjang kunci 71

Tabel 3.9 Populasi awal 77

Tabel 3.10 Hasil dekripsi menggunakan 10 kunci awal 78

Tabel 3.11 Frekuensi relatif huruf hasil dekripsi kunci ke-1 79

Tabel 3.12 Frekuensi relatif huruf hasil dekripsi kunci ke-2 82

Tabel 3.13 Seleksi Roda *Roulette* 87

Tabel 3.14 Rekombinasi satu titik 90

Tabel 3.15 Rekombinasi kromosom satu titik 91

Tabel 3.16 Hasil rekombinasi satu titik 91

Tabel 3.17 Pembangkitan bilangan acak 93

Tabel 3.18 Mutasi Kromosom 94

Tabel 3.19 Kromosom hasil mutasi 94

Tabel 3.20 Kromosom-kromosom baru 95

Tabel 3.21 Nilai *fitness* panjang kunci 5 96

Tabel 3.22 Nilai *fitness* beberapa asumsi panjang kunci 98

Tabel 3.23 Nilai *mutual index coincidence* huruf ج – ء 99

Tabel 3.24 Nilai *mutual index coincidence* huruf ظ – ح 100

Tabel 3.25 Nilai *mutual index coincidence* huruf ي – ع 101

Tabel 3.26 Relasi pergeseran hasil MutIndCo 102

Tabel 3.27 Hasil dekripsi menggunakan kunci ك ه ب إ ء 104

DAFTAR LAMBANG

C_i	: *Ciphertext* ke-*i*
P_i	: P*laintext* ke-*i*
K_i	: *Keyword* ke-*i*
IndCo(s)	: Nilai *index coincidence* pada *string s*
F_i	: Frekuensi huruf ke-*i*
MutIndCo(s, t)	: Nilai mutual *index coincidence string s* dan *t*
σ	: Jumlah pergeseran huruf
$\mathbb{Z}_{36}$	: Bilangan bulat modulo 36
$\mathbb{Z}_{26}$	: Bilangan bulat modulo 26
P_c	: Peluang *Crossover*
P_m	: Peluang Mutasi
A	: Huruf Arab
K	: Frekuensi relatif huruf Arab ke-*i*
D	: Frekuensi relatif Huruf hasil dekripsi
u	: *Unigram*
α	: Bobot *unigram*
β_i	: Nilai *mutual index coincidence* blok ke-*i*
β_j	: Nilai *mutual index coincidence* blok ke-*j*

ANALISIS KRIPTOGRAFI SANDI V*IGENERE* TEKS ARAB

MENGGUNAKAN METODE KASISKI DAN ALGORITMA GENETIKA

Oleh :
Ismiatul Khusna
13610047

ABSTRAK

Analisis kriptografi atau kriptoanalisis merupakan ilmu untuk memecahkan sistem kriptografi. Analisis kriptografi dengan pendekatan matematika pertama kali dilakukan oleh Al Kindi menggunakan analisis frekuensi huruf. Salah satu sistem kriptografi yang bergantung pada analisis frekuensi adalah sandi *Vigenere*. Sandi *Vigenere* merupakan metode menyandikan teks *alphabet* menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. Pemecahan sandi *Vigenere* berhasil dilakukan pertama kali oleh Kasiski yang dikenal dengan metode Kasiski.

Dalam penelitian ini, akan dibahas mengenai analisis kriptografi sebuah teks Arab yang telah dienkripsi dengan Sandi *Vigenere* menggunakan metode Kasiski dan metode baru yaitu Algoritma Genetika. Metode Kasiski dan algoritma genetika digunakan untuk mencari panjang kunci dari *ciphertext*, dengan mencari jarak dari kriptogram berulang dalam *ciphertext* pada metode Kasiski dan membandingkan nilai *fitness* pada algoritma genetika untuk beberapa asumsi panjang kunci.

Perhitungan frekuensi huruf-huruf Arab diperoleh dari teks pada Al-Qur.an. Analisis kriptografi berhasil dilakukan dengan metode Kasiski maupun algoritma genetika untuk sebuah *ciphertext* dengan panjang 145, diperoleh panjang kunci yaitu 5. Setelah diperoleh panjang kunci, dicari kata kunci menggunakan *mutual index coinceidence.* Hasil dekripsi menunjukkan sebuah teks dalam Al-Qur'an, yaitu Surat Al-Fatihah ayat 1-7.

Kata kunci : *Algoritma Genetika, Analisis Kriptografi, Dekripsi, Enkripsi, Metode Kasiski, Panjang Kunci, Sandi Vigenere, Teks Arab.*

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kriptografi adalah cabang dari kriptologi yang bertujuan menjadikan pesan tidak dimengerti oleh pembaca lain (selain penerima pesan). Kriptoanalisis atau analisis kriptografi merupakan ilmu untuk memecahkan sistem kriptografi.

Analisis kriptografi dengan pendekatan matematika pertama kali dicetuskan oleh ilmuwan muslim pada abad ke-9 zaman kekhalifahan Abbasiyah, yaitu Abu Yusuf Ya'qub Al Kindi atau dikenal dengan Al-Kindi. Al-Kindi merupakan ahli filsafat pertama muslim dan juga merupakan matematikawan muslim. Salah satu karyanya dalam bidang matematika adalah buku tentang kriptoanalisis dengan judul "*Risaala Fii Istihrag Al Mu'amma*". Buku ini membahas tentang teknik-teknik pemecahan sebuah pesan yang bekerja atas analisis frekuensi huruf.

Sejarah lain mencatat, pada abad ke-17 ratu Skotlandia yaitu ratu Mary dijatuhi hukuman pancung, setelah surat rahasia (berisi rencana pembunuhan ratu Elizabeth I) dari ratu Mary untuk rakyat Skotlandia berhasil ditemukan dan dipecahkan oleh tentara Ratu Elizabeth I.

Dalam kriptografi ada beberapa algoritma untuk mengamankan pesan atau data salah satunya adalah sandi *Vigenere*. Sandi *Vigenere* dipublikasikan pertama kali oleh Blaise de Vigenere pada zaman pemerintahan Prancis Henry III pada abad 16 tahun 1586, dan tidak terpecahkan selama 300 tahun (Alqahtani, 2013). Sandi

Vigenere adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. (Hidayat, 2012)

Sandi *Vigenere* pertama kali berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19 yang dikenal dengan uji Kasiski atau metode Kasiski. Metode Kasiski digunakan untuk menemukan panjang kunci dari teks tersandi, kemudian membagi pesan menjadi beberapa substitusi kriptogram sederhana (Toemeh, 2008). Metode Kasiski diperkuat dengan metode lain yang disebut dengan *index coincidence*, yang sangat bergantung pada analisis frekuensi. Data atau teks yang dapat dibaca atau dimengerti tanpa syarat tertentu atau terkode dinamakan *plaintext* atau teks asli. Metode menyembunyikan teks asli dalam sebuah kode disebut enkripsi. Teks asli yang telah terenkripsi atau terkode sehingga tidak dapat dibaca atau dimengerti disebut *ciphertext*. Proses mengubah *ciphertext* menjadi teks asli dinamakan dekripsi. Algoritma yang digunakan untuk proses enkripsi disebut *cipher*.

Menurut (Toemeh, 2008) analisis kriptografi sandi *Vigenere* dapat dilakukan dengan metode optimasi, yang dikenal dengan algoritma genetika. Pada penelitian tersebut, algoritma genetika digunakan untuk mencari panjang kunci pada sebuah teks yang dienkripsi menggunakan sandi *Vigenere* dalam teks bahasa Inggris. Penelitian yang sama dilakukan oleh (Omran, 2011), dengan menggunakan algoritma genetika untuk memecahkan sandi *Vigenere* dalam teks bahasa Inggris. Dalam penelitian tersebut, Toemeh dan Omran menggunakan teks bahasa Inggris sebagai *ciphertext*, sedangkan pemecahan sandi *Vigenere* dapat dilakukan pada bahasa lainnya dengan frekuensi dari bahasa tersebut sudah diketahui. Oleh karena itu, pada penelitian ini

pemecahan sandi *Vigenere* dikembangkan untuk menyelesaikan *ciphertext* dalam bahasa Arab.

Algoritma genetika pertama kali diperkenalkan oleh John Holland (1975), terinspirasi oleh teori evolusi Darwin yang menyatakan bahwa individu-individu yang mempunyai karakteristik yang bagus (menurut kriteria tertentu) akan mempunyai kemungkinan untuk bertahan hidup lebih besar dan berproduksi dan menurunkan karakteristiknya kepada keturunan-keturunannya. Ide utama dari algoritma genetika adalah memodelkan proses evolusi alami menggunakan warisan genetika seperti yang diumumkan oleh Darwin. Proses pencarian penyelesaian atau proses terpilihnya sebuah penyelesaian dalam algoritma ini berlangsung sama seperti terpilihnya individu untuk bertahan hidup dalam proses evolusi. (Zukhri, 2014)

Penelitian ini akan membahas pemecahan sandi *Vigenere* teks bahasa Arab, dengan pencarian panjang kunci dilakukan menggunakan metode Kasiski dan algoritma genetika, dan membandingkan hasil analisis kriptografi menggunakan kedua metode tersebut. Kata kunci diperoleh menggunakan *Mutual Index Coincidence.*

1.2 Batasan Masalah

Pembatasan masalah dalam suatu penelitian sangat penting, guna menghindari kesimpangsiuran terhadap objek dari suatu penelitian dan untuk membantu penulis agar lebih fokus dan terarah sesuai dengan tema penelitian. Penelitian ini akan membahas pemecahan sebuah *ciphertext* bahasa Arab yang telah dienkripsi menggunakan sandi *Vigenere*. Pemecahan sandi *Vigenere* dilakukan dengan pencarian panjang kunci dari *ciphertext* menggunakan algoritma genetika dan metode

Kasiski, dengan frekuensi kejadian huruf Arab diambil dari teks pada Al-Qur'an.

Penulis juga membatasi algoritma yang digunakan dalam penelitian ini adalah algoritma kriptografi dan algortima genetika untuk pemecahan sandi *Vigenere*. Pencarian panjang kunci dalam algoritma genetika adalah dengan membandingkan nilai *fitness* beberapa asumsi panjang kunci. Pencarian kata kunci akan dilakukan dengan *Mutual Index Coincidence* yang sangat bergantung pada analisis frekuensi huruf Arab.

1.3 Rumusan Masalah

Berdasarkan pada latar belakang yang telah dipaparkan di atas, maka dirumuskan permasalahan-permasalahan sebagai berikut :

1. Bagaimana langkah-langkah pencarian panjang kunci pada teks Arab yang telah dienkripsi menggunakan sandi *Vigenere* dengan metode Kasiski ?
2. Bagaimana langkah-langkah pencarian panjang kunci pada teks Arab yang telah dienkripsi menggunakan sandi *Vigenere* dengan algoritma genetika ?
3. Bagaimana proses pencarian kata kunci setelah diperoleh panjang kunci untuk cipherteks Arab yang telah dienkripsi menggunakan sandi *Vigenere* ?

1.4 Tujuan Penelitian

Suatu penelitian harus mempunyai tujuan dalam penelitiannya, sehingga tujuan penulis dalam penelitian ini adalah sebagai berikut :

1. Mengetahui langkah-langkah pencarian panjang kunci pada teks Arab yang dienkripsi dengan sandi *Vigenere* menggunakan metode Kasiski.

2. Mengetahui langkah-langkah pencarian panjang kunci pada teks Arab yang dienkripsi dengan sandi *Vigenere* menggunakan Algoritma Genetika.
3. Mengetahui proses pencarian kata kunci pada sebuah *ciphertext* Arab setelah diperoleh panjang kuncinya.

1.5 Manfaat Penelitian

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka penulis dapat mengambil manfaat penelitian yaitu :

1. Memberikan solusi yaitu penemuan panjang kunci pada teks Arab yang telah dienkripsi menggunakan sandi *Vigenere* dengan metode Kasiski.
2. Memberikan solusi yaitu penemuan panjang kunci pada teks Arab dengan metode baru, yaitu algoritma genetika.
3. Memberikan kontribusi dalam dunia kriptografi, khususnya kriptoanalisis bahwa sebuah *ciphertext* Arab dapat diperoleh panjang kuncinya menggunakan metode baru, yaitu algoritma genetika.

1.6 Tinjauan Pustaka

Banyak referensi yang membahas tentang analisis kriptografi teks Arab. Seperti yang telah dijelaskan sebelumnya bahwa kriptoanalisis merupakan proses pemecahan sistem kriptografi atau *cipher*. Penulisan skripsi ini terinspirasi dari paper yang ditulis oleh Rokaia Shalal Habeeb (2016) yang berjudul "*Arabic Text Cryptanalysis Using Genetic Algorithm*". Jurnal tersebut membahas tentang proses analisis kriptografi teks Arab menggunakan algoritma genetika, dengan panjang kunci

diketahui. Dalam penelitian tersebut, beberapa variasi kunci dibangkitkan pada algoritma genetika dengan panjang masing-masing (5, 10, dan 20 huruf) dengan panjang *ciphertex*t yang berbeda-beda (400, 600, dan 1000 huruf). *Ciphertext* yang digunakan telah dienkripsi menggunakan sandi *Vigenere*. Algoritma genetika digunakan untuk mencari kunci sebenarnya dari beberapa variasi kunci sebelumnya. Algoritma genetika berhasil 100% melakukan dekripsi pada *ciphertext* ketika panjang kunci yang digunakan adalah 5, dengan panjang *ciphertext* 600 dan 1000 huruf.

Kemudian paper yang ditulis oleh S.S Omran, A.s. Al-Khalid, dan D.M. Al-Saady (2011) yang berjudul "*A Cryptanalytic Attack on Vigenere Cipher Using Genetic Algorithm*". Jurnal tersebut membahas tentang menghitung teknik koinsiden untuk menemukan panjang kunci, kemudian diaplikasikan pada algoritma genetika untuk memecahkan sandi *Vigenere* atas teks Bahasa Inggris. Fungsi *fitness* dalam jurnal ini hanya berdasarkan atas frekuensi *monogram*, dengan hasil semua huruf kunci berhasil diperoleh, namun panjang *ciphertext* tidak disebutkan.

Jurnal yang ditulis oleh Ragheb Toemeh dan Subbanagounder Arumugam (2006) dengan judul "*Applying Genetic Algortihms for searching Key-Space of Polyalphabetic Substitution Ciphers*". Jurnal ini membahas tentang aplikasi algoritma genetika untuk analisis kriptografi sandi *Vigenere* pada teks Bahasa Inggris, algoritma genetika digunakan untuk menduga panjang kunci, kemudian mencari kunci yang benar.

Aleksey Gorodilov dan Vladimir Morozenko (2008) dalam jurnal yang berjudul "*Genetic Algorithm For Finding the Key's Length and Cryptanalysis of the*

Permutation Cipher", membahas tentang pencarian kunci rahasia pada sandi permutasi blok. Dalam jurnal ini, kunci yang digunakan adalah permutasi dari beberapa bilangan asli. Algoritma genetika digunakan untuk proses kriptoanalisis.

Perbedaan penelitian ini dengan penelitian sebelumnya adalah teks yang digunakan adalah Bahasa Arab, kemudian setelah dibangkitkan beberapa variasi asumsi panjang kunci pada algoritma genetika, akan dicari panjang kunci yang sebenarnya berdasarkan nilai *fitness* yang dihasilkan dari masing-masing variasi panjang kunci. Pencarian panjang kunci juga dilakukan dengan metode Kasiski. Setelah panjang kunci ditemukan, akan dicari kata kunci dengan *mutual index coinsidence* berdasarkan frekuensi relatif huruf Arab.

Penyusunan penelitian ini juga dibutuhkan beberapa materi dasar dari algoritma genetika yang diambil dari Kusumadewi (2003), Suyanto (2005), S.N. Sivanandam dan S.N. Deepa (2007), Entin (2010), dan Zainudin Zukhri (2014). Kemudian beberapa tentang kriptografi dari Menezes (1996), Bruce Schneier (1996), Buchmann (2000), Dony Ariyus (2008), dan Jeffery Hoffstein (2008)

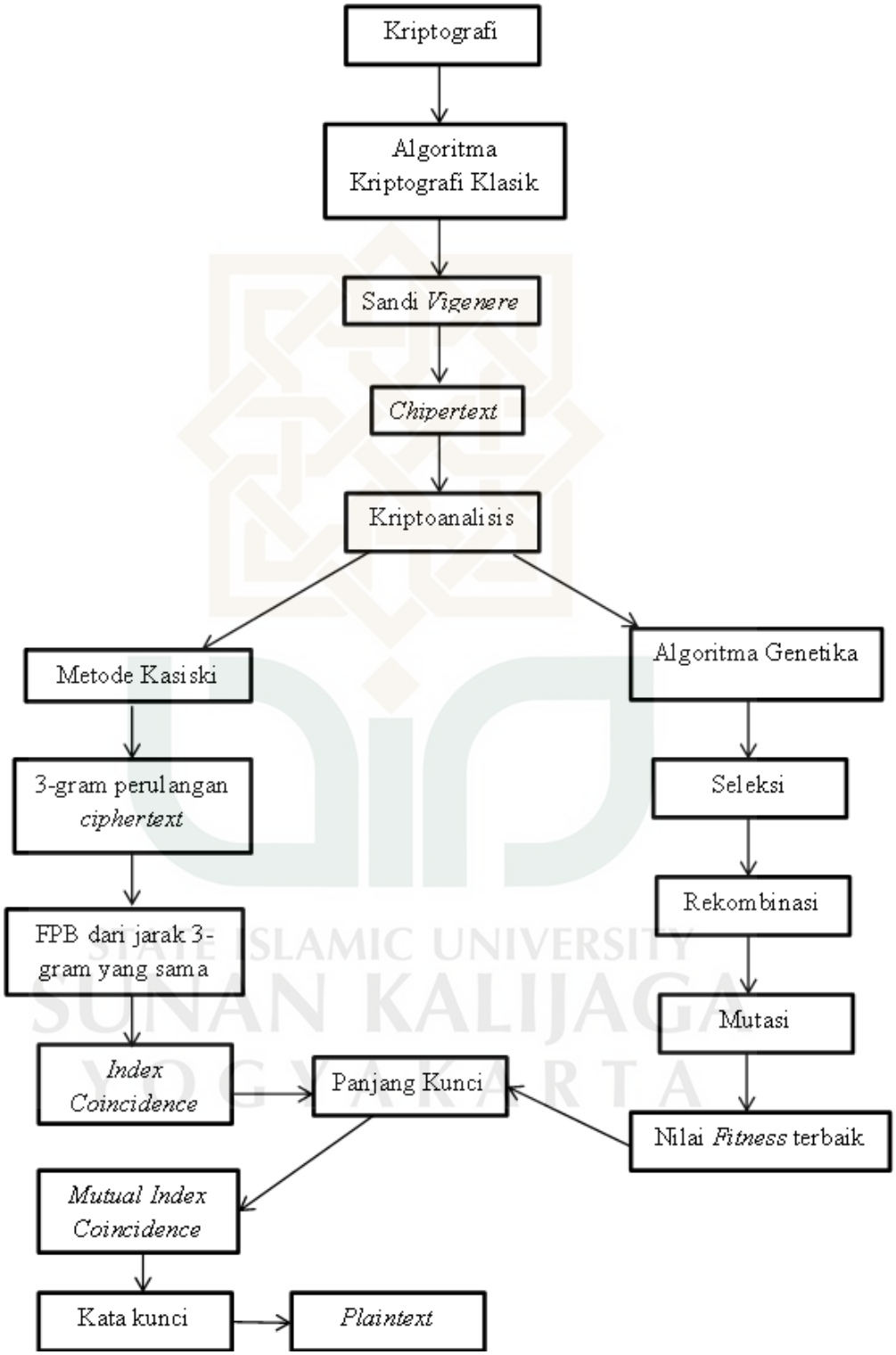
1.7 Metode Penelitian

Metode penelitian yang digunakan adalah metode literatur yaitu pengambilan data-data penelitian dari referensi buku dan jurnal. Secara umum, analisis kriptografi teks Arab menggunakan algoritma genetika menggunakan konsep kriptografi dan algoritma optimasi.

Pembahasan awal dari tugas akhir ini adalah tentang kriptografi. Konsep

kriptografi yang diperlukan untuk analisis kriptografi teks Arab adalah diantaranya pertama algoritma kriptografi klasik, salah satu contoh kriptografi klasik adalah sandi *Vigenere*. Teks Arab yang digunakan pada penelitian ini akan dienkripsi dengan sandi *Vigenere*. Kedua analisis kriptografi sandi *Vigenere*, dalam kriptografi akan dilakukan dengan metode Kasiski, dengan langkah awal adalah penemuan panjang kunci, dilanjutkan dengan mencari kata kunci menggunakan tes *mutual index coincidence* yang bekerja atas frekuensi relatif Huruf Arab (*Hijaiyyah*).

Konsep algoritma genetika diperlukan untuk analisis kriptografi teks Arab yang dienkripsi dengan sandi *Vigenere*. Pemecahan sebuah sandi *Vigenere* dilakukan dengan mencari panjang kunci pada *ciphertext*. Pencarian panjang kunci pada algoritma genetika dilakukan dengan menghitung nilai *fitness* dari beberapa asumsi panjang kunci. Beberapa operator genetika seperti seleksi, rekombinasi, dan mutasi diperlukan untuk memperoleh nilai *fitness*. Gambaran alur penelitian dari tugas akhir ini akan dijelaskan pada bagan sebagai berikut :



Gambar 1.1 Alur Penelitian

1.8 Sistematika Penulisan

Penulisan pada penelitian ini, terbagi dalam empat bab yang disusun secara runtun dan sistematis dengan rincian masing-masing bab dijelaskan dengan sistematika penelitian dari penulis secara umum, sebagai berikut :

1. BAB I (Pendahuluan): Bab ini membahas mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, tinjauan pustaka, metode penelitian dan sistematika penulisan.
2. BAB II (Dasar Teori): Bab ini membahas mengenai dasar teori pada penelitian ini, yaitu kriptografi dan algoritma genetika secara umum.
3. BAB III (Pembahasan): Bab ini membahas tentang analisis kriptografi teks Arab dengan metode Kasiski dan diaplikasikan pada algoritma genetika.
4. BAB IV (Penutup): Bab ini menyampaikan kesimpulan umum yang merupakan jawaban dari rumusan masalah yang terdapat pada BAB I dan saran dari penulis mengenai penelitian yang dilakukan.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pada hasil studi literatur yang telah penulis jabarkan pada bab pembahasan sebelumnya, maka dapat disimpulkan menjadi poin-poin di bawah ini :

1. Ada beberapa langkah dalam pencarian panjang kunci dengan metode Kasiski, yaitu menemukan kriptogram berulang yang terdapat pada *ciphertext*, (dalam penelitian digunakan 3-gram), menghitung jarak antar kriptogram berulang, menghitung semua faktor pembagi dari jarak tersebut, menentukan irisan dari himpunan faktor pembagi, nilai yang muncul dalam irisan tersebut merupakan panjang kunci. Perhitungan metode Kasiski dilanjutkan dengan perhitungan *index coincidence* dari beberapa variasi panjang kunci.
2. Langkah-langkah pencarian panjang kunci menggunakan algoritma genetika yaitu : menentukan parameter, inisialisasi populasi, membangkitkan populasi (*n* kromosom), evaluasi kromosom (dekripsi), menghitung nilai *fitness* dari hasil dekripsi, seleksi dengan Roda *Roulette*, rekombinasi dengan *single point crossover*, mutasi dengan *swap mutation*, dekripsi pesan menggunakan kunci-kunci baru (kromosom), menghitung nilai *fitness*, urutkan nilai *fitness* berdasarkan nilai terbaik, membandingkan nilai *fitness* beberapa panjang kunci, nilai terbaik merupakan panjang kunci.

3. Setelah diperoleh panjang kunci, langkah selanjutnya adalah mencari kata kunci. Dengan menggunakan *mutual index coincidence*, diperoleh nilai-nilai yang ditunjukkan pada tabel **3.23**. Diperoleh kata kunci (0, 4, 7, 32, 28) dari persamaan pada tabel **3.24**. Jika diganti dengan huruf Arab maka diperoleh kata kunci ك ه ب إ ء. Selanjutnya dekripsi pesan dengan kunci ك ه ب إ ء dengan metode geser. Pada pergeseran ke-28, diperoleh kata kunci ص ع ي ه ك dan hasil dekripsi menunjukkan bahwa teks tersebut merupakan surat Al-Fatihah ayat 1-7.

4.2 Saran

Berdasarkan penelitian yang telah penulis lakukan, maka dapat disampaikan beberapa saran sebagai berikut :

1. Penelitian ini hanya membahas pemecahan *ciphertext* Arab yang telah dienkripsi menggunakan sandi *Vigenere*, salah satu algoritma kriptografi klasik. Penelitian selanjutnya, diharapkan dapat menggunakan algoritma kriptografi asimetris atau modern yang lebih baik sistem keamanannya, dengan teks bahasa Arab atau teks bahasa lainnya untuk proses analisis kriptografi.
2. Pada penelitian ini proses pencarian kunci menggunakan algoritma genetika hanya dilakukan secara manual. Diharapkan untuk penelitian selanjutnya, dapat menggunakan program atau *software* sebagai alat agar diperoleh hasil dengan lebih cepat dan akurat.

Demikian saran-saran yang dapat penulis sampaikan. Semoga skripsi ini dapat menjadi inspirasi bagi penelitian-penelitian selanjutnya khususnya di bidang kriptografi dan matematika terapan pada umumnya.

DAFTAR PUSTAKA

Alqahtani, Yahya, P. Kuppuswamy, dan S. Shah. 2014. *New Innovation of Arabic Language Encryption Technique Using New Symmetric Key Algorithm*. International Journal of Advances in Engineering and Technology, vol. 7, pp. 30-37.

Ariyus, Dony. 2008. *Pengantar Ilmu KRIPTOGRAFI : Teori, Analisis, dan Implementasi*. Yogyakarta : ANDI.

Buchmann, J. A. 2000. *Introduction to Cryptography*. USA : Springer-Verlag New York, Inc.

Bhakti, Zeni Fera. 2008. *Kriptoanalisis RSA dengan Kurva Elliptik*. Skripsi S1. Yogyakarta : UIN Sunan Kalijaga

Chamidah, Noor. 2012. *Penerapan Algoritma Genetika dan Algoritma DIJKSTRA Untuk Menyelesaikan Shortest Path Problem*. Skripsi S1. Yogyakarta : UIN Sunan Kalijaga

Chasanah, Sakinatul. 2011. *Aplikasi Algoritma Gentika Untuk Menyelesaikan Masalah Traveling Salesman Problem (TSP)*. Skripsi S1. Yogyakarta : UIN Sunan Kalijaga

Entin. 2010. Kecerdasan Buatan (Bab 7 Algoritma Genetika). Politeknik Elektronika Negeri Surabaya. Surabaya.

Gorodilov, Aleksey dan V. Morozenko. 2008. *Genetic Algorithm for Finding the Key's Length and Cryptanalysis of the Permutation Cipher*. Internatioanl Journal "Information Theories and Applications", vol. 15.

Habeeb, R. Shalal. 2016. *Arabic Text Cryptanalysis Using Genetic Algorithm*. Iraq J. Electrical and Electronic Engineering, vol. 12, No.2.

Hoffstein, Jeffery, J. Pipher, dan J. H. Silverman. 2008. *Introduction to Mathematical Cryptography*. USA : Springer Science and Bussines Media, LLC.

Kusumadewi, S. 2003. *Artificial Intelligence : Teknik dan Aplikasinya*. Yogyakarta : Graha Ilmu.

Menezes, Oorschot, dan Vanstone. 1996. *Handbook of Applied Cryptography*. USA : CRC Press, Inc.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika

Prodi Studi Teknik Informatika. 2006. Pengantar Algoritma Genetika. Yogyakarta : UIN Sunan Kalijaga.

Schneier, Bruce. 1996. *Applied Cryptography, Second Edition : Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, Inc.

S. N. Sivanandam dan S.N. Deepa. 2008. *Introduction to Genetic Algorithms*. Springer-Verlag Berlin Heidelberg.

S. S Omran, A. S. Al-Khalid, dan D. M. Al-Saady. 2011. *A Cryptanalytic Attack on Vigenere Cipher Using Genetic Algorithm*. In Open Systems (ICOS), IEEE Conference, pp. 59-64.

Suyanto. 2005. *Algoritma Genetika dalam MATLAB*. Yogyakarta : ANDI.

Toemeh, Ragheb dan S. Arumugam. 2008. *Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers*. International Arab Journal of Information Technology, vol. 5, pp. 87-91.

Zukhri, Zainudin. 2014. Algoritma Genetika : *Metode Komputasi Evalusioner Untuk Menyelesaikan Masalah Optimasi*. Yogyakarta : ANDI

DAFTAR RIWAYAT HIDUP

A. Data Pribadi

Nama	: Ismiatul Khusna
Tempat, Tanggal, Lahir	: Pulau Burung, 26 September 1995
Umur	: 22 Tahun
Alamat	: Jl. Pendidikan Parit 02, Pulau Burung, Indragiri Hilir, Riau
Jenis Kelamin	: Perempuan
No. Handphone	: 082221498985
Status	: Belum Menikah
Email	: husnaelkholil75@gmail.com

B. Riwayat Pendidikan

1. TK Mutiara Hati Pulau Burung
2. SD Mutiara Hati Pulau Burung
3. Mts Darul Hikmah Pekanbaru
4. MA Ibnul Qoyyim Putri Yogyakarta
5. Universitas Islam Negeri Sunan Kalijaga Yogyakarta