SKRIPSI

PENERAPAN TEOREMA DEKOMPOSISI NILAI SINGULAR PADA ENKRIPSI DENGAN *PLAINTEXT* BERUPA KARAKTER AKSARA JAWA PADA *CAESAR, VIGENERE* DAN *AFFINE CIPHER*

MA'RIFAH
15610039

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA

2019

PENERAPAN TEOREMA DEKOMPOSISI NILAI SINGULAR PADA ENKRIPSI DENGAN *PLAINTEXT* BERUPA KARAKTER AKSARA JAWA PADA *CAESAR, VIGENERE* DAN *AFFINE CIPHER*

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

MA'RIFAH

15610039

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

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 : Ma'rifah
NIM : 15610039
Judul Skripsi : Penerapan Teorema Dekomposisi Nilai Singular pada Enkripsi dengan *Plaintext* Berupa Karakter Aksara Jawa pada *Caesar, Vigenere* dan *Affine Cipher*.

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 Program Studi 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, 26 Agustus 2019
Pembimbing

Muhammad Zaki Riyanto, M.Sc.,
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-3737/Un.02/DST/PP.00.9/09/2019

Tugas Akhir dengan judul : PENERAPAN TEOREMA DEKOMPOSISI NILAI SINGULAR PADA ENKRIPSI DENGAN PLAINTEXT BERUPA KARAKTER AKSARA JAWA PADA CAESAR, VIGENERE DAN AFFINE CIPHER

yang dipersiapkan dan disusun oleh:

Nama	: MA`RIFAH
Nomor Induk Mahasiswa	: 15610039
Telah diujikan pada	: Rabu, 04 September 2019
Nilai ujian Tugas Akhir	: A/B

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

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

Penguji I

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

Penguji II

Pipit Pratiwi Rahayu, S.Si., M.Sc.
NIP. 19861208 201503 2 006

Yogyakarta, 04 September 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama : Ma'rifah

NIM : 15610039

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 penilis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya prang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 26 Agustus 2019

Yang Menyatakan

Ma'rifah

Karya sederhana ini saya persembahkan kepada

Kedua orang tua, kakak, adik dan sahabat

Almamater tercinta

Program Studi Matematika

Fakultas Sains dan Teknologi

UIN Sunan Kalijaga Yogyakarta

...يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ۚ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ

"Allah akan meninggikan orang-orang yang beriman diantaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah maha mengetahui apa yang kamu kerjakan."

"Allah will exalt those who believe among you and those who are given some degree of knowledge. And Allah know best what you do."

[illegible]

(QS. Al-Mujadilah:11)

PRAKATA

Syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat, taufiq dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi ini. Penulis menyadari dengan sepenuh hati bahwa dalam penyelesaian penulisan tugas akhir ini benar-benar merupakan pertolongan Allah SWT. Shalawat dan salam semoga selalu tercurahkan kepada Nabi Muhammad SAW sebagai figur teladan dalam dunia pendidikan yang patut ditiru dan diikuti.

Skripsi ini merupakan kajian singkat tentang penerapan teorema dekomposisi nilai singular dalam konsep kriptografi. Penulis menyadari bahwa skripsi ini tidak akan terwujud tanpa adanya bantuan, bimbingan dan dukungan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati saya mengucapkan banyak terimakasih kepada bapak/ibu/sdr:

1. Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberikan pengarahan yang berguna selama penulis menjadi mahasiswa.

2. Dr. M. Wakhid Musthofa, S.Si, M.Si., selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta sekaligus sebagai dosen penasehat akademik, yang telah banyak memberi masukan-masukan, saran dan motivasi serta memberikan dukungan yang berguna bagi penulisan skripsi ini.

3. Muhammad Zaki Riyanto, M.Sc., selaku dosen pembimbing skripsi yang telah mencurahkan perhatian dan kesabarannya dalam meluangkan waktu, tenaga

dan fikiran untuk memberikan bimbingan dan arahan dalam penyusunan dan penyelesaian skripsi ini.

4. Segenap dosen dan karyawan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta, yang telah dengan sabar membimbing dan memberi arahan selama proses penyusunan skripsi ini.

5. Kedua orangtua tercinta, Mahfud dan Munfaridah, yang selalu setia mendengar curahan hati dan selalu memberi motivasi untuk keberhasilan anak tercintanya serta memberi dukungan baik berupa materi maupun nonmateri selama proses perkuliahan hingga selesai.

6. Keluarga besar penulis (Mbak Rahma, Mbak Ina, Mbak Mus, Mas Abib, Mas Upin, Mas Udin, Iban dan Nayla) yang selalu menemani, memotivasi dan mendukung penulis dalam menyelesaikan skripsi ini.

7. Teman-teman kelas matematika angkatan 2015 sekaligus teman-teman seperjuangan konsentrasi aljabar (Fafa, Syakila, Noval, Ismail dan Hambali) yang selalu sabar menemani dan memberi motivasi selama proses penyusunan dan menyelesaikan skripsi ini.

8. Teman-teman anak rantau (Fitri, Fafa, Ana, Alya, Cika, Rani) yang selalu kompak dan semangat dalam menyelesaikan tugas akhir ini.

9. Teman-teman seperjuangan wisma pelangi (Dini, Dewi, Wati, Desi, Elfi, Ica, Lella, Pepy, Ayda dan Putri) yang selalu menghibur dan memberi semangat kepada penulis.

10. Semua pihak yang telah banyak membantu selama ini, yang tidak dapat disebutkan satu persatu tanpa mengurangi rasa hormat.

Semoga semua bantuan, bimbingan dan dukungan semuanya diterima sebagai amal ibadah oleh Allah SWT aamiin.

Yogyakarta, 23 Agustus 2019

Penulis,

Ma'rifah

DAFTAR ISI

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

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

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

HALAMAN PERNYATAAN . . . . . **iv**

HALAMAN PERSEMBAHAN . . . . . **v**

HALAMAN MOTTO . . . . . **vi**

PRAKATA . . . . . **vii**

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

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

DAFTAR GAMBAR . . . . . **xvi**

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

INTISARI . . . . . **xviii**

I PENDAHULUAN **1**

1.1. Latar Belakang Masalah 1

1.2. Rumusan Masalah 3

1.3. Tujuan Penulisan 4

1.4. Manfaat Penulisan 4

1.5. Tinjauan Pustaka 5

1.6. Metode Penelitian 6

1.7. Batasan Masalah 7

1.8. Sistematika Penulisan 8

II DASAR TEORI **10**

2.1. Kriptografi 10

2.1.1. Pengertian Kriptografi 11

2.1.2. Tujuan Kriptografi 11
2.1.3. Istilah Dalam Kriptografi 12
2.1.4. Algoritma Kriptografi 14
2.1.5. Kriptografi Kunci Simetris 16
2.1.6. Algoritma Kriptografi Klasik 17
2.2. *Caesar Cipher* 18
2.2.1. Pengertian *Caesar Cipher* 18
2.2.2. Memecahkan *Caesar Cipher* 23
2.3. *Vigenere Cipher* 25
2.3.1. Pengertian *Vigenere Cipher* 25
2.3.2. Proses Enkripsi *Vigenere Cipher* 26
2.3.3. Proses Dekripsi *Vigenere Cipher* 27
2.3.4. Variasi Pada *Vigenere Cipher* 29
2.4. *Affine Cipher* 30
2.4.1. Pengertian *Affine Cipher* 30
2.4.2. Proses Enkripsi *Affine Cipher* 31
2.4.3. Proses Dekripsi *Affine Cipher* 32
2.5. Matriks 33
2.5.1. Notasi dan Istilah-Istilah Matriks 33
2.5.2. Transpose Matriks 36
2.5.3. Determinan 38
2.5.4. Nilai Eigen dan Vektor Eigen 40
2.5.5. Nilai Singular 42
2.5.6. Matriks Ortogonal 43
2.6. Vektor 44
2.6.1. Norma dan Jarak Suatu Vektor 45
2.6.2. Ruang Vektor 46

2.6.3. Ruang Hasil Kali Dalam 47
2.6.4. Himpunan Orthonormal 49
2.6.5. Proses Gram Schmidt 50
2.7. Dekomposisi Nilai Singular 51
2.7.1. Mencari matriks V berukuran $n \times n$ 52
2.7.2. Mencari matriks U berukuran $m \times m$ 56
2.8. Aksara Jawa 57
2.8.1. Sejarah Aksara Jawa 57
2.8.2. Pengertian Aksara Jawa 61
2.8.3. Pembagian Macam-Macam Aksara Jawa 62
2.8.4. Bentuk Aksara Jawa 67
III PEMBAHASAN 70
3.1. Pengkodean Aksara Jawa 71
3.2. *Caesar Cipher* 73
3.2.1. Pembentukan Teks Pesan dan Kunci berupa Karakter Aksara Jawa 73
3.2.2. Proses Enkripsi 74
3.2.3. Proses Dekripsi 77
3.3. *Vigenere Cipher* 78
3.3.1. Pembentukan Pesan Teks dan Kunci berupa Karakter Aksara Jawa 78
3.3.2. Proses Enkripsi 80
3.3.3. Proses Dekripsi 81
3.4. *Affine Cipher* 82
3.4.1. Pembentukan Teks Pesan dan Kunci berupa Karakter Aksara Jawa 82
3.4.2. Representasi Pesan Teks ke dalam Bentuk Matriks 84

3.4.3. Perhitungan Teorema Dekomposisi Nilai Singular pada Matriks Kunci 85
3.4.4. Mengubah Matriks Kunci dari Hasil SVD 87
3.4.5. Proses Enkripsi 88
3.4.6. Proses Dekripsi 92
IV PENUTUP 96
4.1. Kesimpulan 96
4.2. Saran 97
DAFTAR PUSTAKA 99
CURRICULUM VITAE 101

DAFTAR TABEL

2.1 Contoh Proses ROT3 18
2.2 Huruf Alfabet 19
2.3 Huruf Alfabet ROT3 19
2.4 Contoh *Plaintext* dan *Plaincode* 20
2.5 Contoh Enkripsi *Caesar Cipher* 21
2.6 *Plaintext* dan *Ciphertext* 21
2.7 Contoh Dekripsi *Caesar Cipher* 21
2.8 Tabel frekuensi kemunculan huruf dalam bahasa inggris 22
2.9 Frekuensi Kemunculan Huruf dalam Bahasa Indonesia 23
2.10 Proses Enkripsi Pada *Vigenere Cipher* 28
2.11 Aksara Dasar 68
2.12 Pasangan 68
2.13 Sandangan Bunyi Vokal 69
2.14 Sandangan Penutup Kata 69
2.15 Tanda Baca 69

3.1 Kode Karakter Aksara Jawa 72
3.2 Kode Aksara Jawa dalam Bentuk Latin 73
3.3 *Plaintext* Aksara Jawa dikonversi ke Kode Angka 74
3.4 Aksara Jawa ROT5 75
3.5 Enkripsi pada Caesar Cipher 76
3.6 Dekripsi pada Caesar Cipher 77
3.7 *Plaintext* Aksara Jawa yang Dikonversi ke Bentuk Angka 79
3.8 Kunci Aksara Jawa yang Dikonversi ke Bentuk Angka 79

3.9 Enkripsi pada *Vigenere Cipher* 80
3.10 Dekripsi pada *Vigenere Cipher* 81
3.11 *Plaintext* yang dikonversi ke Bentuk Angka 83
3.12 Kunci Aksara Jawa yang Dikonversi ke Bentuk Angka 83

DAFTAR GAMBAR

1.1 Alur Penelitian 7

2.1 Proses Sandi 15
2.2 Proses Enkripsi Vigenere 26
2.3 Proses Dekripsi Vigenere Cipher 27
2.4 Proses Enkripsi *Affine Cipher* 31
2.5 Proses Dekripsi Affine 32
2.6 Vektor AB 44
2.7 Aksara Pallawa. 58
2.8 Aksara Kawi (Raffles, 1817) 59
2.9 Mata uang menggunakan Aksara Majapahit (Raffles, 1817) 60

DAFTAR LAMBANG

C_i	: $Ciphertext$ ke-i
P_i	: $Plaintext$ ke-i
K_i	: $Keyword$ ke-i
U	: matriks ortogonal berukuran $m \times m$
V	: matriks ortogonal berukuran $n \times n$
$\sum$	:matriks diagonal berukuran $m \times n$, dan semua entrinya bernilai nol kecuali diagonal utamanya
σ	: nilai singular
Y_i	: proses enkripsi pada affine $cipher$
X_i	: proses dekripsi pada affine $cipher$
m	: modulo
$\mathbb{Z}_{26}$	: Bilangan bulat modulo 26
$\mathbb{Z}_{53}$	: Bilangan bulat modulo 53
$\|\|u\|\|$	: Norma dari suatu vektor u
$\mathbb{R}^n$	: Ruang vektor berukuran *n*
$\alpha,\ \beta,\ k$	: Nilai *skalar*

INTISARI

Penerapan Teorema Dekomposisi Nilai Singular pada Enkripsi dengan *Plaintext* Berupa Karakter Aksara Jawa pada *Caesar, Vigenere* dan *Affine Cipher*

Oleh

MA'RIFAH

15610039

Salah satu tujuan kriptografi yaitu menjaga kerahasiaan dan keamanan suatu pesan teks. Pada zaman dahulu salah satu cara untuk menjaga kerahasiaan suatu pesan teks dilakukan dengan menerjemahkan pesan ke dalam bahasa kuno. Pada penelitian ini akan diterapkan konsep yang sama, yakni dengan mengubah pesan teks ke dalam bentuk karakter aksara jawa, agar meningkatkan keamanan dari suatu pesan dan mempersulit orang lain memahami pesan yang akan dikirim kepada penerima pesan. Dalam hal ini, keilmuan matematika terutama di dalam aljabar linear yaitu teorema dekomposisi nilai singular digunakan sebagai metode untuk mencari suatu kunci yang akan digunakan pada proses enkripsi dan dekripsi. Proses enkripsi teks dilakukan dengan memasukkan pesan teks berupa karakter aksara jawa yang telah dikodekan ke dalam bentuk bilangan bulat, kemudian akan digunakan teorema dekomposisi nilai singular atau biasa dikenal *Singular Value Decomposition* (SVD) yang merupakan pokok-pokok dari aljabar linear. Dengan mendefinisikan matriks $A_{m\times n}$ yang selanjutnya akan diterapkan proses perhitungannya pada *caesar cipher, vigenere cipher* dan *affine cipher*, maka akan diperoleh suatu *ciphertext* atau tes sandi. Kemudian dilakukan proses dekripsi dengan membalikkan persamaan pada proses enkripsi untuk memperoleh pesan teks yang asli atau *plaintext*.

Kata Kunci: *SVD*, enkripsi, dekripsi, aksara jawa, *caesar cipher*, *vigenere cipher*, *affine cipher*.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Berkomunikasi satu sama lain merupakan salah satu sifat dasar manusia sejak ada di muka bumi. Bagi manusia komunikasi berfungsi sebagai sarana untuk saling memahami satu sama lain. Salah satu sarana komunikasi manusia yaitu melalui tulisan. Sebuah tulisan berfungsi menyampaikan pesan kepada pembacanya. Pesan sendiri merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya. Pada zaman dahulu cara penulisan pesan dilakukan menggunakan simbol atau gambar yang ditulis di batu, tulang, dinding goa atau yang lain, sedangkan pada zaman teknologi informasi sekarang ini suatu pesan dapat dituliskan pada komputer dengan menggunakan jaringan internet sebagai sarana untuk mengirim pesan.

Proses pengiriman pesan dilakukan menggunakan metode atau cara yang tidak bisa dipahami oleh semua orang guna menjaga kerahasiaan dan keamanan pesan tersebut. Dalam hal ini kriptografi digunakan untuk mengamankan informasi berupa data ataupun pesan teks. Pada zaman dahulu di Amerika, proses pengamanan suatu pesan dilakukan dengan mengubah pesan ke dalam bentuk bahasa kuno amerika, hal tersebut dilakukan untuk tetap menjaga keutuhan dan kerahasiaan suatu pesan. Dalam hal ini, penulis akan menggunakan metode yang sama yaitu mengubah suatu pesan teks ke dalam bentuk karakter aksara jawa. Selain itu, akan digunakan teorema dekomposisi nilai singular sebagai metode untuk mengolah matriks kunci yang selanjutnya akan digunakan untuk

mengenkripsi suatu pesan teks. Hal tersebut berguna untuk meningkatkan keamanan pesan serta menjaga pesan agar tetap utuh dan rahasia.

Pada konsep kriptografi, algoritma kriptografi digunakan untuk mengenkripsi suatu pesan yang dapat menjamin keutuhan dalam proses pengiriman dan penyimpanan pesan sehingga pesan tetap rahasia dan hanya dapat diakses oleh orang tertentu. algoritma kriptografi terdiri dari dua macam yaitu simetri dan asimetri. Algoritma simetri adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan algoritma asimetri adalah algoritma yang menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsi.

Algoritma kunci simetri dalam penelitian ini, akan peneliti terapkan pada *caesar cipher, vegenere cipher* dan *affine cipher*. *Caesar cipher* adalah salah satu teknik kriptografi lama, yaitu teknik subsitusi kode merupakan teknik yang pertama kali digunakan dalam dunia penyandian, dilakukan dengan menggeser karakter ke kanan dari karakter asli. *Vigenere cipher* adalah teknik kriptografi sederhana yang lebih aman. Pengembangan dari metode *caesar cipher*, metode ini menggunakan karakter huruf sebagai kunci enkripsi. Sedangkan *affine cipher* adalah jenis *cpher* substitusi monoalphabetic, dimana setiap huruf dalam alfabet dipetakan dengan numerik yang setara, dienkripsi menggunakan fungsi matematika sederhana dan dikonversi kembali menjadi huruf pada teks pesan.

Dalam memunculkan konteks keilmuan matematika pada penelitian ini, peneliti menggunakan teorema dekomposisi nilai singular sebagai metode untuk mengenkripsi suatu pesan teks. Dekomposisi nilai singular *(Singular Value Decomposition)* atau lebih dikenal sebagai *SVD*, adalah suatu pemfaktoran matriks dengan mengurai suatu matriks ke dalam dua matriks ortogonal U dan V, dan sebuah matriks diagonal S yang berisi faktor skala yang disebut dengan nilai

singular. Dekomposisi nilai singular dari suatu matriks dapat didefinisikan menggunakan persamaan sebagai berikut:

$$A = USV^T$$

Didefinisikan *A* matriks berukuran $m \times n$, *U* adalah matriks ortogonal berukuran $m \times m$, *V* merupakan matriks ortogonal berukuran $n \times n$ dan *S* adalah matriks diagonal dengan dagonal utamanya merupakan nilai singular dari $A^T A$.

Kebudayaan jawa memiliki banyak macam ragam budaya, dalam hal ini peneliti menggunakan salah satu ragam budaya yaitu tulisan aksara jawa. Aksara jawa merupakan salah satu peninggalan budaya yang tak ternilai harganya. Aksara jawa memiliki banyak bentuk aksara, namun hanya beberapa yang peneliti gunakan diantaranya aksara dasar, pasangan, sandangan bunyi vokal, sandangan penutup kata dan tanda baca. Bentuk aksara dan seni pembuatannya pun menjadi suatu peninggalan yang patut untuk dilestarikan. Menulis aksara Jawa berarti sedang merevitalisasi keluhuran untuk kehidupan masa kini dan yang akan datang. Oleh karenanya perlu adanya pelestarian aksara jawa terhadap generasi penerus. Upaya yang dilakukan peneliti yaitu dengan memakai aksara Jawa dalam penulisan teks pesan yang akan dienkripsi pada *caesar cipher, vigenere cipher* dan *affine cipher*.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat dirumuskan beberapa rumusan masalah yaitu:

1. Bagaimana cara mengkodekan karakter aksara Jawa yang selanjutnya dikonversikan ke dalam bentuk matriks?

2. Bagaimana pengaplikasian teorema *SVD* pada proses enkripsi pesan teks?

3. Bagaimana proses enkripsi dan dekripsi pada *caesar cipher, vigenere cipher* dan *affine cipher*?

1.3. Tujuan Penulisan

Sehubungan dengan rumusan masalah di atas, penulis mempunyai tujuan yang hendak dicapai dalam penelitian ini, yaitu:

a. Untuk mengetahui cara mengkodekan karakter aksara Jawa yang selanjutnya dikonversikan ke dalam bentuk matriks.

b. Untuk mengetahui cara pengaplikasian teorema *SVD* pada proses enkripsi pesan teks.

c. Untuk mengetahui proses enkripsi dan dekripsi pada *caesar cipher, vigenere cipher* dan *affine cipher*.

1.4. Manfaat Penulisan

Adapun manfaat penelitian dalam skripsi ini adalah:

a. Memberikan kontribusi dalam kajian kriptografi mengenai salah satu metode yang digunakan yaitu enkripsi teks berupa aksara jawa menggunakan teorema dekomposisi nilai singular.

b. Memberikan pengetahuan tentang cara enkripsi pesan teks sandi berupa karakter aksara Jawa menggunakan teorema dekomposisi nilai singular.

c. Dapat dijadikan sebagai alat belajar mengenai plainteks atau teks sandi berupa karakter aksara Jawa.

1.5. Tinjauan Pustaka

Dalam mendukung penulisan yang lebih komprehensif, maka penulis melakukan pengkajian dari berbagai *literature* atau karya-karya yang memiliki keterkaitan dengan topik yang akan diteliti. Terdapat beberapa karya *literature* yang dijadikan rujukan utama pada penelitian ini. Karya yang digunakanpun beragam, diantaranya: jurnal, paper, makalah dan laporan.

Penulisan skripsi ini terinspirasi dari jurnal yang ditulis oleh Nidhal K. Adil Muhammad dkk (2014) yang berjudul *"Text Encryption Based on Singular Value Decomposition"*. Jurnal ini membahas tentang proses enkripsi teks menggunakan teorema dekomposisi nilai singular. Dalam penelitian tersebut, plainteks ditulis dalam bentuk matriks persegi yang diurutkan berdasarkan rank kolom. Penerapkan teorema dekomposisi nilai singular pada proses enkripsi dilakukan untuk memperoleh teks awal, dengan mengabaikan panjang kunci. Matriks *plaintext* yang berukuran $m \times m$, dikalikan dengan matriks kunci berukuran $m \times n$ sehingga diperoleh matriks kunci yang baru yakni C_1. Kemudian untuk mendapatkan matriks kunci C_2 dengan membalikkan matriks kunci yang baru. Namun pada jurnal ini, penulis hanya memakai metode atau teori yang digunakan oleh Nidhal dkk yakni menerapkan teorema dekomposisi nilai singular pada *affine cipher.*

Kemudian paper yang ditulis oleh Mohammed Abdul-Hamed Jassim Al-Kufi (2016) yang berjudul *Use the Singular Value Decomposition in the Text Encryption with Encryption in Real Number*. Jurnal tersebut membahas tentang menghitung matriks yang tersusun atas *plaintext* yang sudah ditukar dengan bilangan bulat pada proses enkripsi maupun dekripsi. Dalam jurnal ini teorema dekomposisi nilai singular diterapkan pada kunci yang telah ditetapkan. Setelah kunci ditetapkan, akan dibentuk kunci baru yang nantinya akan digunakan untuk

enkripsi teks.

Perbedaan penelitian ini dengan penelitian sebelumnya adalah teks yang digunakan berupa karakter aksara Jawa. Diberikan suatu *plaintext* dan kunci, dengan mengabaikan panjang kunci yang kemudian akan ditukar dengan bilangan bulat sesuai dengan pengkodean karakter aksara Jawa yang telah ditentukan oleh penulis. Kemudian *plaintext* dan kunci tersebut akan digunakan dalam proses enkripsi dan dekripsi pada *caesar cipher, vigenere cipher* dan *affine cipher.* Sedangkan untuk teorema dekomposisi nilai singular hanya diterapkan pada *affine cipher*, dengan melakukan SVD pada matriks kunci berukuran $m \times n$ untuk mencari matriks kunci A dan B yang selanjutnya digunakan untuk proses enkripsi pada *affine cipher* dengan pesan teks berupa karakter aksara Jawa.

Penyusunan penelitian ini juga dibutuhkan beberapa materi dasar dari teorema dekomposisi nilai singular diantaranya tentang matriks dan vektor bersumber dari Howard Anton (1987), Steve J. Leon (2001), Goldberg (1991), Rorres (2002), Gunawan (2009). Kemudian beberapa tentang kriptografi dari Menezes (1996), Dony Ariyus (2008), Rinaldi Munir (2006). Sedangkan untuk materi mengenai aksara Jawa dari Hardjawijana Drusuprapta (2002), Wahyudi Djaja (2008), Raffles (1817), Teguh Budi Sayoga (2004).

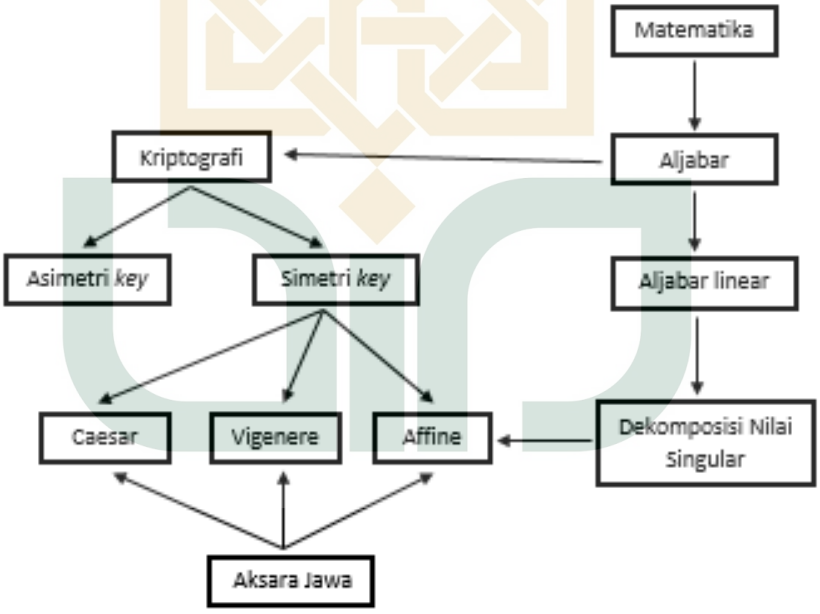
1.6. Metode Penelitian

Metode penelitian yang digunakan adalah metode literatur yaitu pengambilan data-data penelitian dari referensi buku dan jurnal. Secara umum, penerapan teorema dekomposisi nilai singular pada affine *cipher* menggunakan konsep kriptografi dengan teks berupa karakter aksara jawa.

Pembahasan awal dari tugas akhir ini adalah tentang kriptografi. Konsep kriptografi yang diperlukan untuk menerapkan teorema dekomposisi nilai singular

adalah Algoritma kunci simetri, diantaranya pada *caesar cipher, vigenere cipher dan affine cipher.* Teorema dekomposisi nilai singular yang digunakan pada penelitian ini akan diterapkan pada proses enkripsi dan dekripsi pada *affine cipher*, dalam kriptografi akan dilakukan juga pada *caesar dan vigenere cipher*.

Konsep penerapan teorema dekomposisi nilai singular pada *affine cipher* diterapkan pada proses enkripsi dan dekripsi teks. Dalam hal ini, peneliti menggunakan teks berupa karakter aksara jawa yang diterapkan untuk pesan teks , kunci dan teks sandi. Karakter aksara jawa yang dipakai oleh peneliti hanya sebagian saja, diantaranya aksara dasar, aksara pasangan, sandangan bunyi vokal, sandangan penutup kata dan tanda baca. Gambaran alur penelitian dari tugas akhir ini akan dijelaskan pada bagan sebagai berikut:



Gambar 1.1 Alur Penelitian

1.7. Batasan Masalah

Pembatasan masalah dalam suatu penelitian sangat penting, guna menghindari kesimpangsiuran terhadap objek dari suatu penelitian dan untuk

membantu peneliti agar lebih fokus dan terarah sesuai dengan tema penelitian. Penelitian ini akan membahas enkripsi suatu *plaintext* berupa karakter aksara Jawa menggunakan teorema dekomposisi nilai singular. Selanjutnya penggunaan teorema tersebut nantinya akan diterapkan pada proses enkripsi dan dekripsi pada *caesar cipher, vigenere cipher* dan *affine cipher.* Algoritma yang digunakan oleh penulis yakni simetri *key*, dikarenakan pada proses enkripsi maupun dekripsinya menggunakan satu kunci yang sama.

Telah diketahui bahwa karakter aksara jawa terbagi atas beberapa macam aksara yang jika ditotal berjumlah seratus bahkan lebih. Namun agar lebih efisien penulis membatasi karakter aksara jawa yang digunakan dalam penelitian ini, yaitu aksara dasar, aksara pasangan, sandangan bunyi vokal, sandangan penutup kata dan tanda baca.

1.8. Sistematika Penulisan

Agar pembahasan dalam skripsi ini mengarah kepada maksud yang sesuai dengan judul. Penulisan pada penelitian ini, terbagi dalam empat bab yang disusun secara runtun dan sistematis dengan rincian masing-masing bab dijelaskan dengan sistematika penelitian sebagai berikut:

1. BAB I (Pendahuluan): Bab ini membahas mengenai pendahuluan yang terdiri dari sub-sub tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, batasan masalah dan sistematika penulisan.

2. BAB II (Dasar Teori): Bab ini membahas dasar teori yang berisi kajian mengenai teoritis yang berupa: bagian pertama tinjauan tentang kriptografi yang meliputi: sejarah kriptografi, pengertian kriptografi, algoritma yang digunakan dalam kriptografi dan teknik enkripsi dan dekripsi suatu teks.

Bagian kedua tinjauan tentang dekomposisi nilai singular yang meliputi, dasar-dasar yang digunakan dalam dekomposisi nilai singular seperti matriks dan ruang vektor beserta teorema yang digunakan. Kemudian bagian ketiga tinjauan tentang aksara jawa yang meliputi: sejarah aksara jawa, pengertian dan penulisan aksara jawa, dan ketentuan-ketentuan yang ada dalam penulisan aksara jawa.

3. BAB III (Pembahasan): Bab ini menjelaskan pembahasan dalam penelitian ini, yang berisi paparan cara mengenkripsikan suatu plainteks berupa aksara jawa dengan menerapkan teorema dekomposisi nilai singular.
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 untuk perbaikan-perbaikan yang mungkin dapat dilakukan.

BAB IV

PENUTUP

Pada bab ini akan diberikan kesimpulan dan saran-saran yang dapat diambil berdasarkan materi-materi yang telah dibahas pada bab-bab sebelumnya.

4.1. Kesimpulan

Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan skripsi ini adalah :

1. Karakter aksara jawa tidak semuanya digunakan oleh penulis, hanya beberapa saja diantaranya aksara dasar yang berjumlah 20, aksara pasangan yang berjumlah 20, sandangan bunyi vokal yang berjumlah 5, sandangan penutup kata berjumlah 5 dan tanda baca yang berjumlah 3, sehingga keseluruhan berjumlah 53 karakter aksara jawa. Untuk dapat mengkodekan karakter aksara jawa kedalam bentuk bilangan bulat, diperlukan pemahaman mengenai urutan aksara dasar, pasangan, dan sandangan-sandangan. Karakter aksara jawa dikodekan dengan dengan bilangan bulat nol sampai 52. Setelah mengkodekan karakter aksara jawa ke dalam bilangan bulat, selanjutnya *plaintext* yang berisikan deret angka-angka akan dikonversi menjadi suatu matriks berdasarkan rank baris.

2. Dalam mengaplikasikan teorema dekomposisi nilai singular pada proses enkripsi pesan teks, dalam hal ini hanya diterapkan pada *affine cipher*. Sedangkan pada *caesar cipher* dan *vigenere cipher* dengan metode substitusi angka. Hal tersebut juga berlaku sebaliknya pada proses dekripsi.

Penerapan teorema dekomposisi nilai singular berguna untuk meningkatkan keamanan pesan serta dapat menjaga keutuhan suatu pesan teks.

3. *Plaintext* pada *caesar cipher dan vigenere cipher* yang sudah terbentuk ke dalam suatu deret angka-angka akan di enkripsi menggunakan metode substitusi biasa berdasarkan pesan teks dan kunci yang sudah didtentukan sehingga diperoleh *ciphertext*, sedangkan untuk proses dekripsi hanya membalikkan persamaan pada enkripsi untuk memperoleh pesan teks yang asli. *Plaintext* pada *affine cipher* dibentuk menjadi sebuah submatriks untuk mempermudah proses enkripsi. Kunci pada *affine cipher* juga dalam bentuk matriks, kunci A dan B diperoleh dari hasil perhitungan dekomposisi nilai singular pada kunci awal. Enkripsi dilakukan dengan menggunakan persamaan *monoalphabetic* berlaku sebaliknya pada proses dekripsi teks.

4.2. Saran

Setelah membahas dan mengimplementasikan teorema dekomposisi nilai singular pada konsep kriptografi, penulis ingin menyampaikan beberapa saran:

1. Penggunaan karakter aksara jawa harus dimaksimalkan sehingga nantinya dapat memperluas ranah pembelajaran atapun penelitian dalam hal kemanfaatan aksara jawa dalam dunia persandian atau kriptografi. Ketika menggunakan seluruh karakter aksara jawa yang berjumlah 100 karakter diharapkan dapat memberikan pemahaman secara utuh mengenai apa dan bagaimana bentuk aksara, juga dapat melestarikan kebudayaan jawa yang pada zaman sekarang ini sangat jarang digunakan dalam suatu karya keilmuan.

2. Dalam aljabar linear, terutama teorema dekomposisi nilai singular

merupakan perluasan dari materi yang telah dipelajari di bangku perkuliahan yaitu dekomposisi matriks. Penulis berharap pada penelitian-penelitian selanjutnya, penggunaan teorema dekomposisi nilai singular tidak hanya diterapkan pada konsep kriptografi, namun bisa lebih luas dan kompleks pemanfaatannya dalam keilmuan matematika. Seperti contohnya pada keamanan jaringan internet, keamanan jaringan komputer dan sebagainya.

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

Adkins, W. 1992. *Algebra An Approach via Module Theory*. Springer-Verlag New York, Inc. USA.

Anton, Howard. 1987. *Aljabar linear elementer, Edisi Kelima*. Erlangga. Jakarta.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi(Teori, Analisis, dan Implementasi)*. Andi Offset. Yogyakarta.

Ayres, Frank JR. PhD., dan Susila Nyoman. 1994. *Theory and Problems of Matrices-S1-(Metric)*. Erlangga. Jakarta.

Darusuprapta, Hardjawijana, Harjana. 2002, *Pedoman Penulisan Aksara Jawa*. Yogyakarta. Yayasan Pustaka Nusantara.

Djaja, Wahyudi. 2008. *Peninggalan Sejarah di Indonesia*. Klaten. Cempaka Putih.

Goldberg, J. 1991. *Matrix Theory with Aplications*. Mc Graw-Hill Inc. United Stayes of America.

Leon, Steve, J. 2001. *Aljabar Linear dan Aplikasinya, Edisi Kelima*. Erlangga, Jakarta.

Menezes, A. Oorschot, P. van and Vastone. 1996. *Handbook of Applied Cryptography*. CRC Press. New York.

Mohammed Abdul-Hameed, Jassim Al-kufi. 2016. *Use the Singular Values Decomposition in the Text Encryption with Encryption Key Is Real Number*. Jurnal International Journal of Innovative Research in Computer and Communication Engineering. 4(2).

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

Nidhal K., Adil Mohammad. 2014. *Text Encryption Based on Singular Value Decomposition*. Jurnal European Academian Research. Vol II (6).

Raffles, Thomas Stamford. 1817. *The History of Java Volume 2*. London. Black Parbury.

Rorres, Anton. 2002. *Aljabar Linear Elementer Versi Aplikasi Edisi Kedelapan Jilid 1*. Erlangga. Jakarta.

Santosa, R. Gunawan. 2009. *Aljabar Linear Dasar*. ANDI. Yogyakarta.

Sulaiman, Annas Marzuki. 2010. Hanacaraka: Aksara Jawa yang Mulai Ditinggalkan. Makalah. Dikutip dari $https$: $//www.researchgate.net/publication/311268388 - HANACARAKA - AKSARA-JAWA-YANG-MULAI-DITINGGALKAN?enrichId = enrichSource = publicationCoverPdf.$

Sayoga, Teguh Budi. 2004. *Dokumentasi dan Panduan Pemakaian Hanacaraka Truetype Font unruk Perangkat Komputer Berbasis Sistem Operasi Windows*. Makalah. http://hanacaraka.fateback.com/.

$https://id.m.wikipedia.org/wiki/Aksara_Pallawa.$

Curriculum Vitae (CV)

1. Biodata Lengkap

Nama Lengkap : Ma'rifah

Jenis Kelamin : Perempuan

Tempat, Tanggal lahir : Cilacap, 15 September 1997

Alamat Asal : Jl. Kyai Suyuti No. 28 RT 02 RW 13 Karang Sari, Planjan, Kesugihan, Cilacap 53272.

Alamat Tinggal : Wisma Pelangi, Jl. Timoho , gang Wirakarya No. 510 RT 08 RW 08 Sapen, Demangan, Yogyakarta, DIY.

Email : marifah.thamsa156@gmail.com

No. HP : 081391183511

2. Latar Belakang Pendidikan Formal

Jenjang	Nama Sekolah	Tahun
SD	SD Planjan 04	2003-2009
SMP	MTsN Planjan	2009-2012
SMA	MA AL-MA'WA Cilacap	2012-2015
S1	UIN Sunan Kalijaga Saintek/ Matematika	2015-2019