SKRIPSI

PENGAMANAN PESAN RAHASIA MENGGUNAKAN SANDI HILL DENGAN KUNCI PERLUASAN DESIMAL SEBUAH BILANGAN IRASIONAL

NUR LAYLA FAIZATI
14610028

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

2019

PENGAMANAN PESAN RAHASIA MENGGUNAKAN SANDI HILL DENGAN KUNCI PERLUASAN DESIMAL SEBUAH BILANGAN IRASIONAL

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

NUR LAYLA FAIZATI

14610028

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 : Nur Layla Faizati
NIM : 14610028
Judul Skripsi : Pengamanan Pesan Rahasia Menggunakan Sandi Hill dengan Kunci Perluasan Desimal Sebuah Bilangan Irasional

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 dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 08 Februari 2019
Pembimbing

Muhamad Zaki Riyanto, S.Si., 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-606/Un.02/DST/PP.00.9/02/2019

Tugas Akhir dengan judul : PENGAMANAN PESAN RAHASIA MENGGUNAKAN SANDI HILL DENGAN KUNCI PERLUASAN DESIMAL SEBUAH BILANGAN IRASIONAL

yang dipersiapkan dan disusun oleh:

Nama : NUR LAYLA FAIZATI
Nomor Induk Mahasiswa : 14610028
Telah diujikan pada : Jumat, 15 Februari 2019
Nilai ujian Tugas Akhir : A-

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

Sugiyanto, S.Si., M.Si
NIP. 19800505 200801 1 028

Yogyakarta, 15 Februari 2019
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 bertanda tangan di bawah ini:

Nama : Nur Layla Faizati

NIM : 14610028

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 atau saduran 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, 11 Februari 2019

Yang Menyatakan

Nur Layla Faizati

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan untuk:

Bapak Sapardi dan almh. Ibu Partimah, yang selalu membimbing penulis dalam menjalani hari-hari.

Kakak dan Adik-adikku, yang selalu mendukung perjuangan penulis.

MOTTO

Tak apa terlambat daripada tidak sama sekali.

Tetapi akan lebih baik jika tepat waktu!

KATA PENGANTAR

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat serta hidayat-Nya sehingga penulis dapat menyelesaikan penelitian ini. Tak lupa sholawat serta salam penulis haturkan kepada junjungan Nabi Agung Muhammad SAW. yang telah membawa kita menuju jalan yang terang seperti saat ini.

Dalam proses penyusunan skripsi ini, penulis telah banyak mendapat bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Rektor dan Dekan Fakultas Sains dan Teknologi Universita Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak M. Wahid Mustofa, M.Sc. Dan Bapak Moh. Farhan Qudratullah, M.Sc., Selaku Ketua dan Sekretaris Program Studi Matematika, serta segenap dosen dan staf Fakultas Sains dan Tekhnologi UIN Sunan Kalijaga.
3. Bapak Muhamad Zaki Riyanto, S. Si., M. Sc. selaku dosen pembimbing skripsi yang selalu membimbing dan mengingatkan penulis untuk segera menyelesaikan skripsi ini. Terima kasih atas bimbingannya selama ini.
4. Ibu Malahayati, M. Sc. selaku dosen penasihat akademik yang selalu mengingatkan anak-anaknya untuk segera lulus.
5. Bapak Muchammad Abrori, S.Si., M.Kom dan Bapak Sugiyanto, S.Si., M.Si., selaku penguji I dan penguji II.

6. Bapak, yang selalu mendukung penulis dalam meraih cita-cita dan selalu mengingatkan untuk segera lulus kulih. *Maafkan anakmu ini, pak. Yang tidak segera lulus.*

7. Mbakku Shofiyatun Nadia yang selalu memberikan dukungan demi kelangsungan hidup. *You're my best old sister I ever have*. Serta adik-adikku Muhammad Abdul Aziz dan Anisatun Mukarramah yang menghiasi hidup penulis.

8. Teman-teman Matematika 2014, terima kasih kebersamaan, dukungan dan semangatnya. Terkhusus untuk Anita, Yayuk, Mahe, Uyun, Shoba, Yanto, Ani, Esta, Ifa, Dihan dan teman-teman yang telah mendahului munaqosah, terima kasih semangatnya.

9. Dua sahabatku yang selalu musuhan Maryam dan Khotmi, yang selalu bertanya *"Kapan Wisuda"* terima kasih atas motivasi dan semangatnya selama ini. Maaf Khotmi, mendahuluimu.

10. Sahabatku Annisa Fitriana Islamiati yang sama-sama berjuang untuk mendapatkan ACC, terima kasih telah mengantar-jemputku selama ini.

11. Teman-teman KKN Bojong 2, Mendut, Mungkid Magelang, Imam, Awal, Alvin, Putri, Umay, Dian, Wulan, Mega, Ummi, yang telah memberi warna dalam menjalani KKN di Bojong 2.

12. *Kamu*, yang selalu ada dan memotivasi penulis agar cepat lulus. *Terima kasih telah membersamai.*

13. Teman-teman Zeviner khususnya Yuni, Laily, Khotmi, dan yang lainnya yang selalu memotivasi penulis agar cepat lulus. Terima kasih motivasinya.

14. Beberapa pihak yang tidak dapat penulis sebutkan satu-persatu.

Penulis sangat menyadari bahwa penelitian ini masih banyak sekali kekurangan dan kesalahan. Oleh karena itu, kritik dan saran yang membangun untuk menyempurnakan penelitian ini akan sangat penulis nantikan. Kritik saran tersebut dapat disampaikan melalui email nlaylafaizati@yahoo.co.id. Semoga karya sederhana ini dapat bermafaat bagi pembaca.

Yogyakarta, 8 Februari 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$\in$	: elemen atau anggota
$a\|b$	: bilangan a membagi b
$\|a\|$	: modulus a
a^{-1}	: invers dari a
A^T	: transpose dari A
A^H	: transpose konjugat dari A
$\oplus$	: penjumalah yang didefinisikan
$\odot$	: pergandaan yang didefinisikan
$\mathbf{0}$	: elemen identitas pada penjumlahan
$\|\|u\|\|$	: norma dari u
$d(u, v)$	: jarak antara vektor u dan v
$\langle u, v \rangle$	: hasilkali dalam vektor u dan v
$\mathbb{C}$	: himpunan semua bilangan kompleks
$\mathbb{R}$	: himpunan semua bilangan real
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{Z}_p$	: himpunan semua sisa pembagian bilangan bulat modulo p, dengan p prima
${}_2F_1(x, y; z; 1)$	: fungsi hipergeometrik biasa
V	: ruang vektor V
F	: lapangan
F^n	: himpunan vektor dengan panjang n atas lapangan

$a \equiv b \pmod{m}$	: a kongruen b modulo m
$M_{m\times n}(\mathbb{Z})$	: himpunan semua matriks berordo $m \times n$ dengan entri bilangan bulat
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \cdots + a_n$
$\Gamma(n)$	: fungsi gamma dari n
$B(m,n)$	: fungsi beta dari m dan n
$n!$	: n factorial
$\perp$	: ortogonal/tegak lurus
$\blacksquare$	: akhir suatu bukti

INTISARI

Pengamanan Pesan Rahasia Menggunakan Sandi Hill Dengan Kunci Perluasan Desimal Sebuah Bilangan Irasional

Oleh

NUR LAYLA FAIZATI

14610028

Salah satu cara yang digunakan untuk melindungi kerahasiaan pesan adalah kriptografi. Dalam kriptografi dikenal istilah enkripsi dan dekripsi. Enkripsi adalah proses menyembunyikan pesan rahasia menjadi pesan yang tidak terbaca yang disebut cipherteks. Sebaliknya dekripsi adalah proses mengubah cipherteks menjadi pesan semula sehingga dapat dimengerti isinya. Sistem kriptografi Sandi Hill merupakan sebuah metode enkripsi-dekripsi yang prosesnya dilakukan menggunakan operasi perkalian dengan kunci berupa matriks persegi. Proses dekripsi dapat dilakukan dengan mengalikan cipherteks menggunakan invers dari matriks kunci.

Pada penelitian ini dikembangkan sistem kriptografi sandi Hill menggunakan kunci berupa matriks yang tidak persegi. Dalam proses dekripsinya digunakan konsep matriks invers semu (*pseudo invers*).

Matriks kunci dapat dihasilkan melalui konsep posisi desimal dari suatu bilangan irasional. Pada penelitian ini, bilangan irasional yang digunakan adalah π. Posisi desimal ke-i, t didapat dari penjumlahan bilangan asli acak dengan fungsi hipergeometrik dengan modulo suatu bilangan prima. Setelah mendapatkan posisi desimal, selanjutnya dibentuk matriks kunci yang digunakan untuk mengenkripsi pesan menggunakan oeprasi perkalian matriks modulo. Untuk mendekripsi pesan, digunakan invers-semu matriks, hal ini dikarenakan matriks kunci bukan merupakan matriks persegi.

Kata kunci : kriptografi, sandi Hill, fungsi hipergeometrik, bilangan irasional, invers semu

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan teknologi. Semakin berkembangnya teknologi informasi di era modern ini tidak menutup kemungkinan bahwa keamanan informasi juga terjaga. Kemudahan dalam mengirim dan menerima pesan menggunakan media elektonik tentunya memiliki sisi rentan terhadap penyadapan, apalagi menggunakan jaringan internet yang tidak diketahui tingkat keamanannya. Tingkat keamanan yang rendah ini dapat dimanfaatkan oleh pihak-pihak yang haus akan informasi rahasia. Misalnya informasi yang bersifat rahasia seperti data-data rahasia kemiliteran, perbankan, data-data rahasia perusahaan dan data-data lainnya akan bahaya jika sampai pada tangan penyadap. Di sinilah peran kriptografi sebagai sebuah studi matematika yang berhubungan dengan aspek-aspek keamanan data atau informasi untuk menawarkan solusi pengamanan data rahasia yang dikirim melaui suatu jalur yang tidak aman seperti jaringan internet maupun seluler.

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yaitu kriptologi. Kriptografi menggunakan persamaan matematis untuk mengenkripsi dan mendekripsi data. Teknik ini digunakan untuk mengubah data ke dalam kode-kode tertentu dengan tujuan informasi yang disimpan tidak dapat dibaca oleh siapapun kecuali orang-orang yang berhak. Dengan adanya kriptografi, kita dapat mengirimkan berbagai pesan rahasia melalui jaringan komunikasi dengan aman. Kriptografi sudah digunakan sejak jaman mesir kuno dan terus berkembang hingga saat

ini. Pada mulanya, sistem kriptogafi sangat sederhana sehingga mudah dipecahkan. Salah satu sistem kriptografi klasik yaitu sistem kriptografi Sandi Hill. Sandi Hill pertama kali diperkenalkan oleh Lester S. Hill pada tahun 1929 M dalam jurnal *The American Mathematic Monthly*. Sandi Hill juga merupakan sistem kriptografi dengan kunci simetri atau kunci rahasia (*private key*). Mulanya, kunci dari sandi Hill hanya berupa matriks persegi dan non-singular yang mempunyai invers. Seiring perkembangan zaman, sandi Hill diperluas sehingga kuncinya dapat berupa matriks persegi panjang (matriks $m \times n$) dan singular dengan syarat tertentu. Dengan menggunakan invers semu (*pseudo inverse/ Moore-Penrose Inverse*) kita dapat mencari invers matriks non persegi untuk mendekripsi pesan.

Untuk lebih memperumit dalam pendekripsian pesan, digunakan digit desimal bilangan irasional. Digunakannya digit bilangan irasional karena bilangan irasional merupakan bilangan yang tidak dapat dibentuk menjadi pecahan sehingaa bilangan irasional memiliki banyak sekali bilangan dibelakang koma. Selain itu, desimal bilangan irasional tidak memiliki pola tertentu sehingga sulit untuk mendapatkan bilangan mana yang digunakan. Skripsi ini akan membahas bagaimana mencari posisi bilangan irasional sehingga dapat digunakan sebagai kunci dari algoritma sandi Hill. Selanjutnya, dengan kunci tersebut dapat digunakan untuk mengenkripsi dan mendekripsi agar pesan yang kita kirimkan dengan jaringan komunikasi terjaga keamanannya.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, maka dirumuskan permasalahan-permasalah sebagai berikut:

a. Bagaimana cara mencari posisi desimal sebuah bilangan irasional sehingga dapat digunakan sebagai kunci sandi Hill?

b. Bagaimana cara mengenkripsi plainteks menjadi cipherteks menggunakan kunci dari perluasan desimal sebuah bilangan irasional?

c. Bagaimana cara mencari invers semu matriks kunci dan mendekripsi pesan rahasia menggunakan invers semu matriks kunci tersebut?

1.3. Tujuan Penulisan

Tujuan dari penelitian ini adalah:

a. Mengetahui cara mencari posisi desimal bilangan irasional sehingga dapat digunakan sebagai kunci dari algoritma sandi Hill.

b. Mengetahui bagaimana mengenkripsi pesan rahasia menggunakan algoritma sandi hill dengan kunci perluasan desimal sebuah bilangan irasional.

c. Mengetahui bagaimana mencari invers matriks kunci dan mendeskripsikan cipherteks yang dienkripsi menggunakan algoritma sandi Hill dengan invers semu matriks kunci tersebut.

1.4. Manfaat Penulisan

Hasil dari penulisan tugas akhir ini diharapkan memberikan manfaat sebagai berikut:

a. Memberikan kontribusi dalam kajian kriptografi mengenai salah satu kunci yang digunakan dalam algoritma sandi Hill yaitu kunci dari perluasan desimal bilangan irasional.

b. Memberikan kontribusi dalam kajian aljabar dan kriptografi tentang landasan matematis dan penggunaan invers semu (*pseudo inverse*).

c. Sebagai dasar untuk penelitian selanjutnya dalam dunia aljabar dan kriptografi.

1.5. Tinjauan Pustaka

Penelitian ini berawal dari jurnal yang ditulis oleh M.K. Viswanath dan M. Ranjith Kumar pada tahun 2015 dengan judul *"A Secure Cryptosystem Using the Decimal of An Irrational Number"*. Jurnal tersebut menjelaskan mengenai algoritma sandi Hill menggunakan kunci perluasan desimal bilangan irrasional *e* yang posisi dimulainya digit pembentuk kunci dicari dengan menggunakan fungsi hipergeometrik.

Selanjutnya, penulisan penelitian ini juga mengacu pada skripsi yang ditulis oleh Ikhwanudin Achmad (2007) yang berjudul "Aplikasi Invers Matriks Tergeneralisasi pada Cipher Hill". Skripsi ini membahas mengenai invers matriks tergeneralisasi dan penerapannya pada sandi Hill. Skripsi ini memberikan gambaran bagaimana mencari invers sebarang matriks, kemudian invers matriks tersebut digunakan sebagai kunci untuk mendekripsi pesan rahasia yang tersandi menjadi plainteks. Selain itu, penulis juga membuat program menggunakan software Octave. Perbedaan dengan penelitian penulis adalah tidak digunakannya desimal bilangan irasional dalam pembentukan kunci.

Skripsi Okta Arfiyanta (2013), Mahasiswa Matematika UIN Sunan kalijaga yang berjudul "Invers Semu (*Pseudo-Inverse*) dalam Sistem Persamaan Linear" juga digunakan sebagai tinjauan pustaka dalam penulisan skripsi ini. Skripsi Okta Arfiyanta menjelaskan mengenai teori-teori dalam invers semu dan pengaplikasiannya dalam sistem persamaan linear. Sedangkan penelitian ini menerapkan invers semu dalam sandi Hill.

Selanjutnya, buku yang digunakan untuk penulisan skripsi ini mengacu pada buku karya Jack L. Goldberg yang berjudul *"Matrix Theory with Application"*. buku ini membahas mengenai dasar-dasar aljabar linear, dekomposisi matriks, invers semu, serta perintah-perintah dalam software Matlab. Buku ini digunakan dalam

pembuktian dasar-dasar aljabar dan dekomposisi nilai singular.

Selain tinjauan pustaka di atas, penulis juga menggunakan buku-buku maupun jurnal-jurnal lain sebagai referensi pelengkap guna menunjang penulisan skripsi ini.

Tabel 1.1 Tinjauan Pustaka yang Digunakan

No.	Pengarang	Judul	Pembahasan
1.	M.K. Viswanat & M.R. Kumar (2015)	*A Secure Cryptosystem Using the Decimal Expantion of An Irational Number*	Sistem Kriptografi dengan kunci digit desimal bilangan irasional
2.	Ikhwanuddin Achmad (2007)	Aplikasi Invers Matriks Tergeneralisasi pada Cipher Hill	Perluasan Cipher Hill dengan matriks non-persegi
3.	Okta Arfiyanta(2013)	Invers Semu *(Pseudo-Inverse) dalam Sistem Persamaan Linear*	Penerapan Invers semu untuk mencari solusi dari persamaan linear
4.	Jack L. Goldberg (1992)	*Matrix Theory with Applications*	Aljabar linear elementer, Invers semu dan penerapan dalam matlab

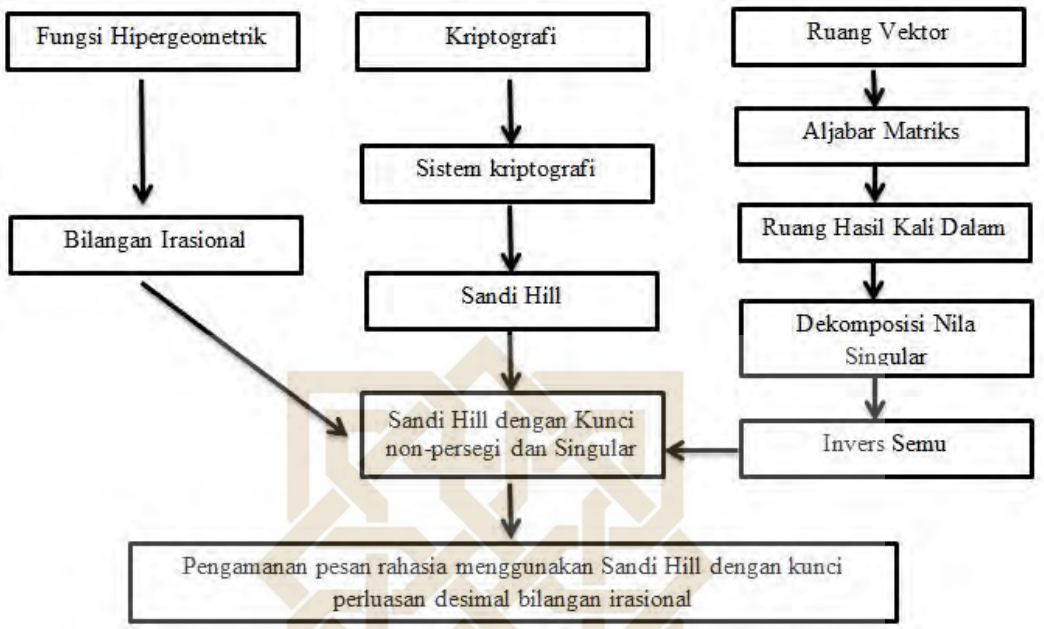
1.6. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah dengan studi literatur, yaitu dengan membahas dan menjabarkan konsep-konsep yang sudah ada dalam bentuk literatur. Baik dalam bentuk buku-buku referensi, maupun bahan-bahan berbentuk jurnal yang diperoleh dari perpustakaan maupun dari intenet. Secara umum pembahasan mengenai pengamanan pesan rahasia menggunakan sandi

Hill dengan kunci perluasan desimal bilangan irasional terdiri dari kriptografi dan Aljabar linear.

Pembahsan awal dari penulisan skripsi ini bermula dari kriptografi, dan lebih khususnya pada kriptografi kunci simetris yaitu sandi hill. Materi ini akan membantu dalam pengaplikasian pada bab-bab yang akan dibahas selanjutnya. Sedangkan pembahasan mengenai aljabar linear bermula dari ruang vektor, subruang vektor, kombinasi linear, bebas linear, basis, dan dimensi yang pembahasannya saling berkaitan satu sama lain. Dari pembahasan tersebut digunakan untuk menghitung rank matriks yang dibahas pada subbab selanjutnya. Materi selanjutnya mengenai Aljabar matriks akan digunakan dalam pembahasan dekomposisi nilai singular yang akan digunakan dalam menentukan ketunggalan invers semu pada subbab setelahnya.

Selain pembahasan mengenai kriptografi dan aljabar linear, terdapat pembahsan mengenai bilangan irasional yang desimalnya akan digunakan dalam pengaplikasian pada pembahasan penulisan skripsi ini. Untuk menentukan letak desimal yang akan digunakan menggunakan fungsi hipergeometrik.



Gambar 1.1 Skema Alur Penelitian

1.7. Sistematika Penulisan

Penulisan laporan penelitian ini dibagi menjadi empat bab dengan sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah yang diambil, rumusan masalah, tujuan penulisan, manfaat penulisan, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

BAB 2 DASAR TEORI

Bab ini menjelaskan mengenai teori-teori yang digunakan dalam dasar pembahasan. Diantaranya adalah bilangan bulat, algoritma euclide, vektor dan matriks, ruang vektor, kombinasi linear dan bebas linear, basis dan dimensi, aljabar matriks, hasilkali dalam, proses Gram-Schmidt, dekoposisi nilai singular, kriptografi, sandi hill, tanda tangan digital, fungsi hipergeometrik, dan bilangan irasional.

BAB 3 PEMBAHASAN

Bab ini menjelaskan mengenai algoritma yang digunakan dalam mengenkripsi dan mendekripsi pesan rahsia menggunakan sandi hill dan perluasan desimal bilangan irasional beserta contohnya dan program matlab.

BAB 4 PENUTUP

Bab ini berisi tentang kesimpulan-kesimpulan yang dapat diambil dari penulisan laporan penelitian ini dan berisi saran-saran.

BAB IV

PENUTUP

Berdasarkan pembahasan mengenai pembentukan kunci algoritma sandi hill dengan perluasan desimal bilangan irasional, diperoleh kesimpulan sebagai berikut:

4.1. Kesimpulan

Berdasarkan hasil studi literatur yang telah penulis lakukan mengenai pengaman pesan rahasia menggunakan sandi hill dengan kunci perluasan desimal sebuah bilngan irasional, diperoleh kesimpulan sebagai berikut:

1. Posisi dimulainya digit dari perluasan desimal bilangan irasional yang digunakan untuk membangkitkan kunci dapat dicari dengan menggunakan penjumlahan bilangan bulat acak α_0 dan fungsi hipergeometrik ${}_2F_1(x, y; z; 1)$, yaitu $\beta_{i,t} \equiv \alpha_0 + {}_2F_1(x, y; z; 1) \pmod{p}$, dengan p adalah bilangan prima.

2. Untuk mengenkripsi pesan rahasia menggunakan sandi hill dengan perluasan desimal bilangan irasional menggunakan

   $$C \equiv KP \pmod{N}$$

   dengan:

   $C =$ cipherteks (pesan rahasia)

   $K =$ matriks kunci

   $P =$ plainteks (pesan asli).

3. Dengan menggunakan sifat dari invers semu $A^+ = (A^T A)^{-1} A^T$ dapat diperoleh invers dari matriks kunci sehingga pesan dapat didekripsi dengan invers

dari matriks kunci.

Selanjutnya, untuk mendekripsi pesan menggunakan rumus sebagai berikut

$$P \equiv K^{+}C \pmod{N}$$

dengan

$P =$ plainteks (pesan asli)

$K^{+} =$ invers semu matriks kunci

$C =$ cipherteks (pesan rahasia).

4.2. Saran

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

1. Penelitian ini hanya membahas mengenai kunci sandi Hill yang menggunakan perluasan desimal sebuah bilangan irasional, oleh karena itu sandi Hill juga dapat dikembangkan dengan menggunakan kunci selain dari perluasan desimal bilangan irasional.

2. Kegunaan invers semu tidak hanya digunakan dalam mencari invers matriks kunci dari sandi Hill, tetapi juga dalam bidang lain dalam matematika terapan, statistika dan yang lainnya. Dalam penelitian selanjutnya dapat dikembangkan mengenai penerapan invers semu.

3. Program dalam penelitian ini sangat sederhana sehingga untuk penelitian selanjutnya dapat dikembangan program interaktif.

DAFTAR PUSTAKA

Achmad, Ikhwanudin.2007.*Aplikasi Invers Martiks Tergeneralisasi pada Cipher Hill*.Skripsi. Yogyakarta:Jurusan Matematika Fakultas MIPA UGM.

Adiwijaya. 2014. *Aplikasi Matriks dan Ruang Vektor*. Yogyakarta: Graha Ilmu.

Anton, H. 2000. *Elementary Linear Algebra*, Eight Edition. New York: John Wiley and Sons, Inc.

Arfiyanta, Okta.2013. *Invers Semu (Pseudo-Inverse) dalam Sistem Persamaan Lenear*. Skripsi. Yogyakarta: Program Studi Matematika Fakultas SAINTEK.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi: Teori Analisis dan Implemetasi*. Yogyakarta: CV. Andi OFFSET.

Bailey, W. N. 1964. *Generalized Hypergeometric Series*. New York: Stechert-Hafner Service Agency, Inc.

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

Dutka, Jacques. 1984. *The Early History of the Hypergeometric Function*. USA: Springer-JSTOR, Inc.

Goldberg, J.L. 1991. *Matrix Theory with Applications*. New York: Mc. Grow-Hill, inc.

Hernawati, Kuswari. 2016. *Implementasi Cipher Hill pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler*. Jurnal. Yogyakarta: FMIPA UNY.

Irawan, Wahyu Henky, DKK. 2014. *Pengantar Teori Bilangan*. Malang:UIN-MALIKI PRESS.

Leon, Steven J.2001.*Aljabar Linear dan Apikasinya, Edisi Kelima*. Jakarta: Erlangga.

Malik, D.S. 2007. *Introduction to Abstract Algebra*. USA: *Scientific Word*.

Safi'i, Muhtar.2013. *Aplikasi Invers Semu (Pseudoinverse) dengan Metode Greville's pada Analisis Regresi Linear Berganda*. Skripsi. Yogyakarta:Program Studi Matematika Fakultas SAINTEK.

Sadikin, Rifki. 2008. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*, Yogyakarta: CV. Andi OFFSET.

Setyaningsih, Emy. 2015. *Kriptografi dan Implementasinya Menggunakan MATLAB*. Yogyakarta: CV. Andi OFFSET.

Sulistiyani, Oktavia, Dkk. 2016. *Kajian Fungsi Hipergeometrik dan Fungsi Hipeergeometrik Konfluen Serta Aplikasinya dalam Menentukan Solusi Persamaan Diferensial Biasa Orde Dua*. Jurnal Matematika. Fakultas Sains dan Teknik Universitas Nusa Cendana.

Viswanath, M.K. and Kumar, M. Ranjith. 2015. *A Secure Cryptosystem Using the Decimal Expantion of an Irrational Number*. http://dx.doi.org/10.12988/ams.2015.56450

LAMPIRAN A

SKRIP PROGRAM MATLAB

1. Program untuk Mencari Adjoin di Modulo n

```
function AD=adj(A)
%=======================================================
%PROGRAM UNTUK MENCARI ADJOIN(A)
%NUR LAYLA FAIZATI
%FAKULTAS SAINS DAN TEKHNOLOGI
%=======================================================
N=input('Masukkan lagi modulo N=');
[m,n]=size(A);
AD=[];
if m~=n, return, end
for i=1:n
    for j=1:n
        AD(i,j)=mod((-1)^(i+j)*det(A([1:i-1 i+1:n],[1:j-1 j
            +1:n])),N);
    end
end
AD=AD';
```

2. Program Mencari Invers Bilangan bulat modulo n

```
function y=invmod(d,p);
%=======================================================
%PROGRAM UNTUK MENCARI INVERS MODULO N
%NUR LAYLA FAIZATI
```

```
%PROGRAM STUDI MATEMATIKA FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================================
p0=p;
d0=d;
t0=0;
t=1;
q=floor(p0/d0);
r=p0-q*d0;
while r>0;
    temp=t0-q*t;
    if (temp>=0),
        temp=mod(temp,p);
    end;
    if (temp<0),
        temp=p-(mod(-temp,p));
    end;
    t0=t;
    t=temp;
    p0=d0;
    d0=r;
    q=floor(p0/d0);
    r=p0-q*d0;
end;
if d0~=1,
    y=[];
    disp('No Invers');
else
    y=mod(t,p);
end;
```

3. Program untuk Mencari Invers Semu

```
function X=pseudoinverse(K)
%=========================================
%PROGRAM UNTUK MENCARI PSEUDOINVERSE
%NUR LAYLA FAIZATI
%FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================
N=input('Masukkan nilai modulo N=');
K=input('Masukkan matriks kunci K=');
[k,l]=size(K);
if k>l
    A=K'*K;
else
    A=K*K';
end
determinan=round(mod(det(A),N));
d=determinan;
y=invmod(d,N);
AD=adj(A);
invers=mod(y*AD,N);
if k>l
    X=mod(invers*K',N);
else
    X=mod(K'*invers,N);
end
```

4. Program Mencari Posisi Digit yang Digunakan

```
function Bit=posisidigit(B)
%=========================================================
%PROGRAM UNTUK MENCARI POSISI DESIMAL YANG DIGUNAKAN
%NUR LAYLA FAIZATI
```

```
%PROGRAM STUDI MATEMATIKA FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================================
aa=input('Masukkan bilangan prima kecil , a=');
bb=input('masukkan bilangan prima<a , b=');
t=input('Masukkan jam pengiriman (misal jam 13.47, maka
      masukkan 13), t=');
u=input('Masukkan berapa kali saling berkomunikasi , i=');
s=aa*bb;
p=s+t;
q=10*((aa+bb)/2)+((aa-bb)/2+t);
r=p+q+u;
w=r-1;
x=(r-p-q)-1;
y=(r-p)-1;
z=(r-q)-1;
a=1;
for i=1:w;
    a=a*i;
end
b=1;
for j=1:x;
    b=b*j;
end
c=1;
for k=1:y;
    c=c*k;
end
d=1;
for l=1:z;
    d=d*l;
end
```

```
F=(a*b)/(c*d);
a0=input('Masukkan sebarang bilangan bulat , a0=');
pp=input('Masukkan bilangan prima besar tdk lebih dari 12
    digit p=');
Bit=floor(mod(a0+F,pp));
fprintf('\n\n');
disp(['Jadi , bilangan irasional yang digunakan dimulai dari
    digit ke-',num2str(Bit)])
```

5. Program Untuk Mengenkripsi Pesan

```
%=========================================
%PROGRAM UNTUK MENGENKRIPSI PESAN
%NUR LAYLA FAIZATI
%FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================
K=input('Masukkan matriks kunci K=');
P=input('Masukkan matriks plainteks P=');
N=input('Masukkan nilai modulo N=');
C=mod(K*P,N)
```


6. Program Untuk Mendekripsi Pesan

```
%=========================================
%PROGRAM UNTUK MENDEKRIPSI PESAN
%NUR LAYLA FAIZATI
%FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================
C=input('Masukkan matriks cipherteks C=');
N=input('Masukkan nilai modulo N=');
X=pseudoinverse;
P=mod(X*C,N)
```

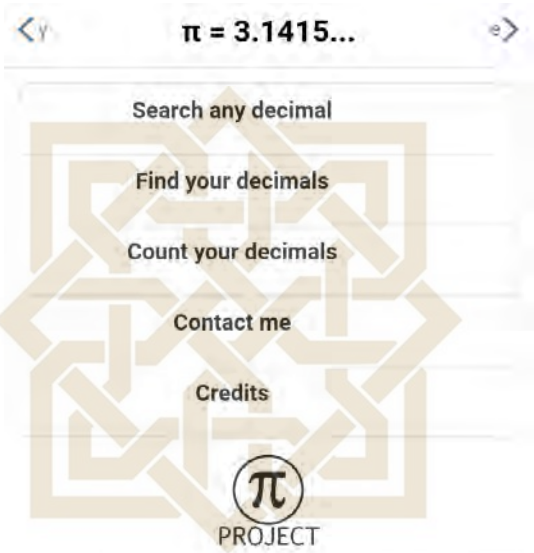
7. Program Enkripsi dan Dekripsi

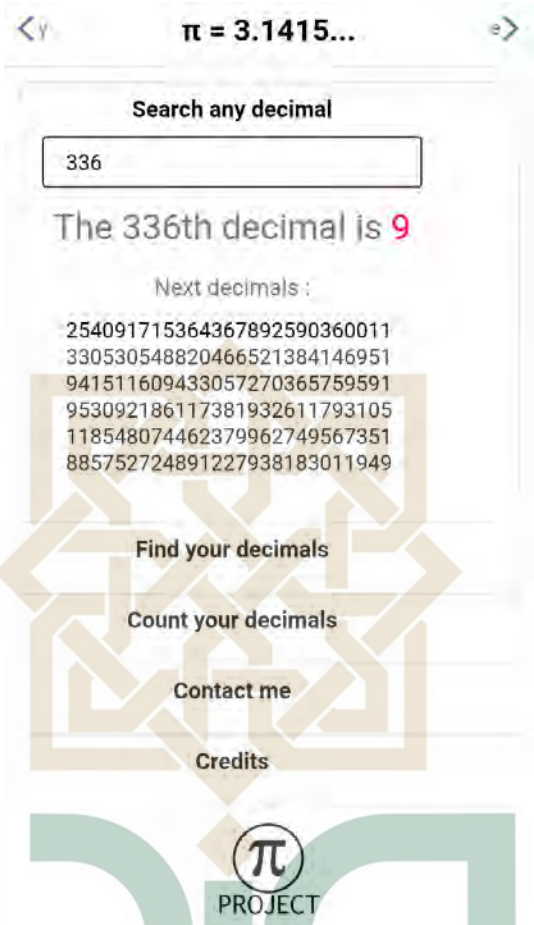
```
%=========================================================
%PROGRAM UNTUK MENCARI POSISI DESIMAL YANG DIGUNAKAN
%NUR LAYLA FAIZATI
%PROGRAM STUDI MATEMATIKA FAKULTAS SAINS DAN TEKHNOLOGI
%=========================================================
clc;
disp('=================================================')
disp('Enkripsi dan Dekripsi dengan Perluasan Desimal')
disp('--------------------NUR LAYLA FAIZATI--------------------')
disp('-----------PROGRAM STUDI MATEMATIKA-----------')
disp('----------FAKULTAS SAINS DAN TEKHNOLOGI----------')
disp('=================================================')
B=[];C=[];P=[];
tekan;
pilihan=0;
while pilihan ~=4
    clc;
    disp('Menu Program')
    disp('1. Mencari Posisi Desimal')
    disp('2. Mengenkripsi Pesan')
    disp('3. Mendekripsi Pesan')
    disp('9. Keluar')
    pilihan=input('Silahkan masukkan pilihan : ');

    switch pilihan
        case 1
            disp('1')
            B=posisidigitt
            tekan;
        case 2
```

```
31              disp('2')
32              enkripsi
33              tekan;
34          case 3
35              disp('3')
36              dekripsi
37              tekan;
38          case 9
39              clc;
40              disp('Thank you');
41              break;
42          otherwise
43              disp('Tidak ada dalam pilihan'); tekan;
44      end
45  end
```

```
1  function tekan;
2  disp('Tekan apa saja untuk lanjutkan');
3  pause;
4  end
```

APLIKASI *DECIMALS SEARCH*





RIWAYAT HIDUP

A. Data Pribadi

Nama	:	Nur Layla Faizati
Tempat, Tanggal Lahir	:	Bantul, 10 April 1996
Jenis Kelamin	:	Perempuan
Alamat	:	Menden RT 02, Dk Babadan, Bantul, Bantul, Yogyakarta, 55711
Agama	:	Islam
Status	:	Belum Menikah
No. HP	:	085743780460
E-mail	:	nlaylafaizati@yahoo.co.id

B. Riwayat Pendidikan

SD Muhammadiyah Bantul Kota	(2002 – 2008)
MTs. Ibnul Qoyyim Putri	(2008 – 2011)
MA Ibnul Qoyyim Putri	(2011 – 2014)
UIN Sunan Kalijaga	(2014 – 2019)