PROTOKOL PERTUKARAN KUNCI BERDASARKAN MASALAH DEKOMPOSISI SIMETRIS ATAS RING NON-KOMUTATIF $\boldsymbol{END}(\mathbb{Z}_{\boldsymbol{p}} \times \mathbb{Z}_{\boldsymbol{p}^2})$

Skripsi

Untuk Memenuhi Sebagian Persyaratan

Mencapai Derajat Sarjana S-1

Program Studi Matematika

Diajukan oleh :

Fadhil Andika Rahman

11610002

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2015

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan skripsi
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 : Fadhil Andika Rahman
NIM : 11610002
Judul Skripsi : Protokol Pertukaran Kunci Berdasarkan Masalah Dekomposisi Simetris atas Ring Non-Komutatif *End* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

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 Matamatika.

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

Wassalamu'alaikum wr. wb.

Yogyakarta, 17 April 2015
Pembimbing

Muhammad Zaki Rivanto S.Si., M.Sc.
NIP: 19840113 000000 1 301

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1565/2015

Skripsi/Tugas Akhir dengan judul : Protokol Pertukaran Kunci Berdasarkan Masalah Dekomposisi Simetris Atas Ring Non-Komutatif $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

Yang dipersiapkan dan disusun oleh :

Nama : Fadhil Andika Rahman

NIM : 11610002

Telah dimunaqasyahkan pada : 8 Mei 2015

Nilai Munaqasyah : A

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

TIM MUNAQASYAH :

Ketua Sidang

Muhammad Zaki Riyanto, M.Sc

Penguji I

Dr. Khurul Wardati, M.Si
NIP.19660731 200003 2 001

Penguji II

Pipit Pratiwi Rahayu, M.Sc

Yogyakarta, 5 Juni 2015
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA UIN SUNAN KALIJAGA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA

Dr. Maizer Said Nahdi, M.Si
NIP. 19550427 198403 2 001

SURAT PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini :

Nama	: Fadhil Andika Rahman
NIM	: 11610002
Jurusan	: Matematika
Fakultas	: Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

menyatakan dengan sesungguhnya bahwa dalam skripsi saya ini **tidak terdapat karya serupa yang diajukan untuk memperoleh gelar kesarjanaan disuatu perguruan tinggi lain** dan skripsi saya ini adalah asli karya saya sendiri dan bukan meniru hasil skripsi karya orang lain.

Yogyakarta, 17 April 2015

Yang menyatakan

METERAI TEMPEL

6FC04ADF199981637

6000

ENAM RIBU RUPIAH

Fadhil Andika Rahman

NIM. 11610002

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahan kepada:

- Kampusku tercinta UIN Sunan Kalijaga Yogyakarta.
- Papa, Mama, Kakak, Adek dan Nenekku yang selalu memberikanku semangat, nasehat, motivasi dan doa-doanya serta kasih sayang yang tiada henti.

MOTTO

"Ketika datang sifat malas belajar

dalam diri kita, ingatlah selalu orang tua

yang sedang banting tulang mencari nafkah

untuk membiayai pendidikan kita."

~Fadhil Andika Rahman

"Barangsiapa bersungguh-sungguh,

sesungguhnya kesungguhannya itu adalah

untuk dirinya sendiri."

~(QS Al-Ankabut [29]: 6)

"Tiadanya keyakinanlah yang membuat

orang takut menghadapi tantangan,

dan saya percaya pada diri saya sendiri."

~Muhammad Ali

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillah, segala puji bagi Allah SWT yang telah memberikan rahmat, taufik, dan hidayah-Nya yang tiada henti-hentinya, sehingga penulis dapat menyelesaikan penulisan skripsi berjudul *"Protokol Perjanjian Kunci Berdasarkan Masalah Dekomposisi Simetris atas Ring Non- Komutatif* $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$*"* ini dengan semaksimal mungkin. Sholawat dan salam semoga senantiasa terlimpahkan kepada Nabi Muhammad SAW yang telah membawa umat manusia menuju zaman yang terang benderang dengan kemajuan ilmu pengetahuan dan teknologi seperti saat sekarang ini.

Penulis menyadari bahwa proses penulisan skripsi ini tidak terlepas dari dukungan, motivasi, kerjasama dan bimbingan dari berbagai pihak. Oleh karena itu, iringan doa dan terimakasih penulis sampaikan yang sebesar-besarnya kepada:

1. Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Semua dosen yang telah membagi ilmunya kepada penulis.
3. Bapak M. Zaki Riyanto, M.Sc. selaku pembimbing yang telah bersedia meluangkan waktu untuk bimbingan, arahan serta dukungan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
4. Papa dan Mamaku tercinta, serta kakak dan adikku tersayang yang selalu memberikan semangat, nasehat dan doa-doanya yang tiada henti, sehingga penulis termotivasi untuk mengerjakan skripsi ini dengan giat.

5. Ibu Malahayati, M.Sc selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama kuliah.
6. Aidha Rosel dan juga semua teman-teman matematika angkatan 2011.
7. Semua pihak yang turut membantu penulis hingga selesainya skripsi ini yang tidak dapat penulis sebutkan satu persatu, terima kasih.

Penulis berharap dengan selesainya skripsi ini akan memberikan sesuatu yang bermanfaat bagi semua orang yang membacanya.

Wassalamu'alaikum Wr.Wb

Yogyakarta, 6 Juni 2015

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
SURAT PERNYATAAN KEASLIAN iv
HALAMAN PERSEMBAHAN v
MOTTO vi
KATA PENGANTAR vii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
DAFTAR LAMBANG xiv
ABSTRAK xv
BAB I 1
1.1. Latar Belakang 1
1.2. Batasan Masalah 4
1.3. Rumusan masalah 4
1.4. Tujuan Penelitian 5
1.5. Manfaat Penelitian 5
1.6. Tinjuan Pustaka 6
1.7. Metode penelitian 6
1.8. Sistematika Penulisan 7
BAB II 9
2.1. Kriptografi 9
2.1.1. Definisi Kriptografi 9
2.1.2. Sejarah Kriptografi 10
2.1.3. Algoritma Kriptografi 11
2.1.4. Sistem Kriptografi 12
2.2. Dasar Struktur Aljabar 15

2.2.1. Teori Bilangan 15
2.2.2. Grup 25
2.2.3. Ring 30
2.2.4. Lapangan 34
2.2.5. Ring Matriks 35
2.2.6. Ring Polinomial 36
2.2.7. Homomorfisma ring 36
BAB III 39
3.1. Ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ 39
3.2. Sifat-sifat ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ 42
3.3. Elemen Invers Perkalian di E_p 51
BAB IV 59
4.1. Sejarah protokol pertukaran kunci 59
4.2. Perhitungan Protokol Pertukaran Kunci atas Ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$... 60
4.3. Sandi Hill 66
4.4. Cipher Hill Atas E_p 69
BAB V 73
5.1. Sarana Implementasi 73
5.2. Implementasi Algoritma Protokol Pertukaran Kunci atas Ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ 75
5.3. Uji Coba Program 76
5.3.1. Program Protokol Pertukaran Kunci atas Ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. 77
5.3.2. Program Sandi Hill atas E_p 81
BAB VI 85
6.1. Kesimpulan 85
6.2. Saran 86

DAFTAR GAMBAR

Gambar 1.1 Alur Penelitian 7
Gambar 1.2 Alur Sistematika Penulisan 8
Gambar 2.1 Skema sistem kriptografi simetris 14
Gambar 5.1 Proses input program protokol pertukaran kunci 78
Gambar 5.2 Hasil output program protokol pertukaran kunci 79
Gambar 5.3 Proses input program enkripsi 82
Gambar 5.4 Hasil output program enkripsi 82
Gambar 5.5 Proses Input program Dekripsi 83
Gambar 5.6 Hasil Output program Dekripsi 83

DAFTAR TABEL

Tabel 2.1 Perhitungan menggunakan algoritma Euclide yang diperluas 24
Tabel 4.1 Tabel Alur Pembuatan Kunci 62
Tabel 4.2 Tabel korespondensi karakter dengan bilangan 67
Tabel 5.1 Spesifikasi perangkat keras 73
Tabel 5.2 Spesifikasi perangkat keras 74

DAFTAR LAMPIRAN

Lampiran 1 Program Protokol Pertukaran Kunci 89
Lampiran 2 Program Enkripsi 103
Lampiran 3 Program Dekripsi 105
Lampiran 4 Tabel ASCII 107
Lampiran 5 Proses perhitungan invers kunci rahasia 108

DAFTAR LAMBANG

$\mathbb{N}$	: Himpunan semua bilangan asli.
$\mathbb{Z}$	: Himpunan semua bilangan bulat.
$\mathbb{R}$	: Himpunan semua bilangan real.
$x \in \mathbb{Z}$	: x anggota bilangan bulat.
$A \subseteq X$	: A subset (himpunan bagian) atau sama dengan X.
$\gcd(m, p)$	: Faktor persekutuan terbesar dari m dan p.
$(R, +, .)$	: Ring dengan dua operasi biner, yaitu penjumlahan dan perkalian.
$\mathbb{Z}_p$	: Himpunan bilangan bulat modulo prima p.
$\rightarrow$	: Menuju.
$M_2(\mathbb{R})$	: Matriks ukuran 2×2 atas himpunan bilangan real.
E_p	: Himpunan semua ring matriks ukuran 2×2 dengan baris atas matriks merupakan elemen dari $\mathbb{Z}_p$ dan baris bawah matriks merupakan elemen dari $\mathbb{Z}_{p^2}$.
$End(G)$	: Himpunan semua endomorfisma grup $f: G \rightarrow G$.

ABSTRAK

Pesan rahasia yang dikirim melalui jalur yang tidak aman sangat rentan untuk disadap oleh pihak lain. Kriptografi memberikan solusi untuk menjaga keamanan pesan rahasia tersebut tidak jatuh ketangan pihak lain, melalui proses enkripsi dan dekripsi. Kedua proses ini menggunakan suatu kunci rahasia yang hanya diketahui oleh kedua belah pihak. Walaupun kedua belah pihak tidak dapat bertemu untuk membuat kunci rahasia, tetapi mereka dapat menggunakan protokol pertukaran kunci yang memberikan solusi untuk masalah distribusi kunci.

Protokol pertukaran kunci pertama kali diperkenalkan oleh Diffie-Hellman pada tahun 1976. Protokol ini menggunakan struktur aljabar komutatif dan keamanannya diletakkan pada masalah logaritma diskrit. Adanya ancaman komputer kuantum dimasa depan mengakibatkan protokol yang menggunakan struktur aljabar komutatif ini menjadi kurang aman. Pengembangan protokol pertukaran kunci atas struktur aljabar non-komutatif yang diharapkan mampu menjaga keamanan kunci rahasia.

Protokol pertukaran kunci yang dibahas pada tugas akhir ini menggunakan polinomial atas ring non-komutatif yaitu ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, dengan p adalah bilangan prima. Keamanan protokol pertukaran kunci ini diletakkan pada permasalahan dekomposisi simetris. Protokol ini menggunakan polinomial dengan koefisiennya berupa matriks. Kunci rahasia ini akan sulit diketahui pihak lain, karena harus mengetahui kunci rahasia dan fungsi polinomial yang digunakan oleh kedua belah pihak.

Kata kunci: endomorfisma ring, kriptografi, polinomial, protokol pertukaran kunci, ring non-komutatif.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi sangat penting dalam kehidupan karena dapat membantu manusia dalam penyampaian dan penyebarluasan informasi dengan menggunakan media komunikasi. Sebagaimana hakikat manusia sebagai makhluk sosial yang membutuhkan orang lain, setiap orang kini dapat dengan mudah saling berkomunikasi dengan orang lain di belahan bumi manapun. Jalur komunikasi yang paling sering digunakan adalah jaringan internet. Akan tetapi, internet merupakan jalur komunikasi umum yang dapat dilalui oleh setiap orang, sehinga akan sangat membahayakan apabila informasi yang dirimkan bersifat rahasia.

Pentingnya nilai sebuah informasi yang bersifat rahasia menyebakan informasi hanya boleh diakses oleh orang-orang tertentu. Informasi-informasi yang bersifat rahasia terkadang dikirim melalui jalur yang tidak aman, seperti media sosial, email dan internet. Jalur-jalur yang tidak aman tersebut tentu saja mengundang orang lain yang berkepentingan untuk mendapatkan informasi rahasia tersebut. Dibutuhkan keamanan yang tinggi untuk menjaga informasi tersebut tidak jatuh kepada pihak yang tidak berhak mengetahuinya. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi tersebut (Budi Rahardjo, 2002).

Kriptografi disini berperan untuk memberikan solusi mengenai permasalahan-permasalahan keamanan suatu informasi. Kriptografi merupakan sebuah studi matematika yang berhubungan dengan aspek-aspek keamanan suatu

informasi. Kriptografi menawarkan solusi-solusi dalam mengamankan informasi yang bersifat rahasia yang dikirim melalui jalur yang tidak aman, seperti internet.

Ketika suatu pesan yang dikirim melalui jalur komunikasi yang tidak aman, isi pesan tersebut memiliki kemungkinan untuk disadap. Untuk menjaga isi pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang sulit dimengerti oleh pihak lain. Enkripsi adalah suatu proses penyandian yang melakukan perubahan suatu pesan dari yang dapat dimengerti (plainteks), menjadi kode yang sulit dimengerti (chiperteks). Sedangkan proses kebalikannya, untuk mengubah chiperteks menjadi plainteks memerlukan suatu mekanisme dan kunci tertentu (M. Zaki Riyanto,2007).

Ketika melakukan komunikasi secara rahasia, pihak-pihak yang berkomunikasi harus menyetujui suatu kunci rahasia yang sama. Cara membuat kunci rahasia yang sama walaupun kedua pihak tidak dapat bertemu, digunakan suatu metode yaitu protokol pertukaran kunci. Metode ini membantu kedua belah pihak yang tidak dapat bertemu untuk membuat kunci rahasia. Kunci rahasia tersebut nantinya akan digunakan dalam menyandikan pesan rahasia yang akan dikirim melalui jalur yang tidak aman.

Metode protokol pertukaran kunci pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Diffie dan Hellman memperkenalkan protokol pertukaran kunci menggunakan struktur aljabar komutatif, yaitu grup siklik. Adanya ancaman dari komputer kuantum dimasa depan, membuat protokol dengan struktur aljabar komutatif, seperti masalah logaritma diskrit dan faktorisasi menjadi lemah keamanannya (Peter W. Shor,

1997). Akibatnya beberapa peneliti mulai mengembangkan protokol pertukaran kunci menggunakan struktur aljabar non-komutatif yang diharapkan tingkat kemanannya lebih sulit untuk dipecahkan.

Berdasarkan jurnal CLiment, Navarro dan Tortosa (2012), beberapa peneliti yang telah mengembangkan struktur aljabar non-komutatif untuk protokol pertukaran kunci adalah:

1. I. Anshel, M. Anshel, B. Fisher dan D. Goldfeld (2001) mengembangkan protokol pertukaran kunci dengan tingkat keamanannya diletakkan pada masalah logaritma diskrit untuk automorfisma yang didefinisikan sebagai operasi konjugasi dan kesulitan untuk menemukan elemen konjugasi pada grup non-komutatif berhingga.
2. V. Sphilrain dan A. Ushakov (2006) mengembangkan protokol pertukaran kunci menggunakan suatu grup non-komutatif yang disebut grup Thompson, dimana tingkat keamanannya diletakkan pada permasalahan dekomposisi simetris.
3. B. Hurley dan T. Hurley (2011) mengembangkan protokol pertukaran kunci yang menggunakan grup ring non-komutatif.

CLiment, Navarro dan Tortosa (2012) mengembangkan protokol pertukaran kunci yang menggunakan permasalahan dekomposisi simetris atas ring non-komutatif $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, dengan p adalah bilangan prima. Skripsi ini akan mengkaji protokol yang dikembangkan oleh CLiment, Navarro dan Tortosa (2012) tersebut.

1.2. Batasan Masalah

Pembatasan masalah dalam suatu penelitian sangatlah penting, guna menghindari pembahasan objek yang terlalu meluas dan kesimpangsiuran objek kajian, sehingga lebih membantu penulis untuk lebih fokus dan terarah sesuai dengan tema penelitian. Sesuai latar belakang masalah, skripsi ini akan difokuskan untuk membahas prosedur dalam protokol pertukaran kunci atas ring non-komutatif yaitu ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, dengan p suatu bilangan prima. Tingkat keamanan dari protokol ini diletakkan pada tingkat kesulitan dalam menyelesaikan masalah dekomposisi simetris.

1.3. Rumusan masalah

Berdasarkan latar belakang dan batasan yang telah dipaparkan, maka dirumuskan permasalahan-permasalahan berikut:

1. Bagaimana konsep matematis yang melandasi prosedur protokol pertukaran kunci pada sistem kriptografi simetris?
2. Bagaimana langkah-langkah dan perhitungan dalam memperoleh kunci rahasia menggunakan protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dengan keamanannya diletakkan pada masalah dekomposisi simetris?
3. Bagaimana proses enkripsi dan dekripsi menggunakan sandi Hill atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$?
4. Bagaimana implementasi perhitungan protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dan perhitungan proses enkripsi serta dekripsi

menggunakan sandi Hill atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ pada bahasa pemograman MATLAB?

1.4. Tujuan Penelitian

Tujuan penulis dalam membuat tugas akhir ini adalah:

1. Mengkaji konsep matematis yang melandasi protokol pertukaran kunci.
2. Mengkaji tentang langkah-langkah dan perhitungan matematis dalam memperoleh kunci rahasia menggunakan metode protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.
3. Mengkaji proses perhitungan enkripsi dan dekripsi sandi Hill atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.
4. Membuat algoritma perhitungan protokol atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ pertukaran kunci dan algoritma proses enkripsi serta dekripsi pada sandi Hill atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ pada bahasa pemograman MATLAB.

1.5. Manfaat Penelitian

Beberapa manfaat dari penelitian ini adalah:

1. Memberikan solusi kepada kedua belah pihak yang berkomunikasi secara rahasia untuk mendapatkan kunci yang sama.
2. Memberikan kemudahan dalam perhitungan protokol pertukaran kunci dan proses enkripsi serta dekripsi sandi Hill atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dengan pembuatan bahasa pemograman MATLAB.
3. Sebagai dasar untuk peneliti selanjutnya dalam mengembangkan protokol pertukaran kunci.

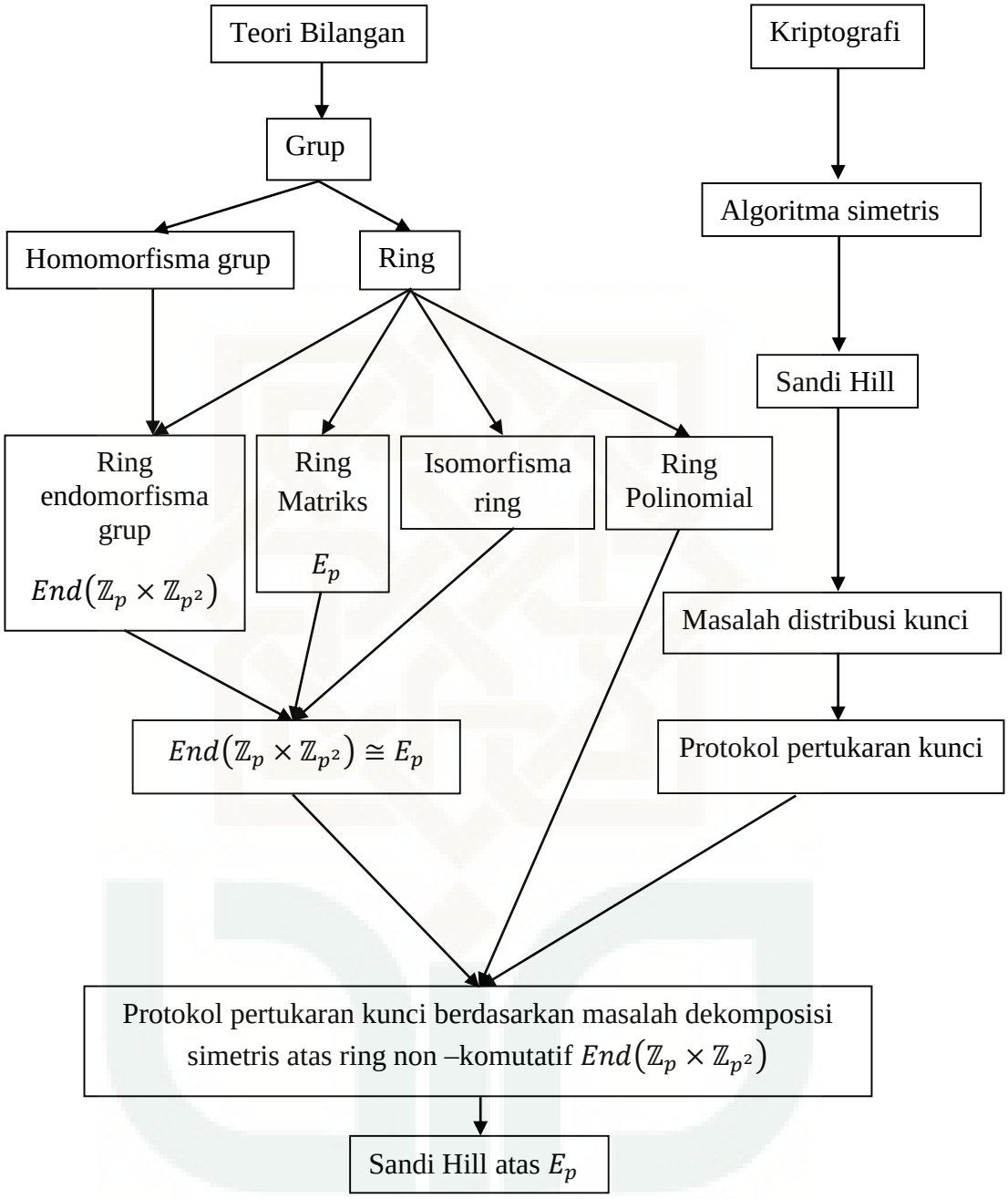
1.6. Tinjuan Pustaka

Referensi utama tugas akhir ini adalah jurnal dari Climent, Navaro dan Tortosa (2012) yang berjudul *Key Exchange Protocol over non-commutative Rings. The Case of* $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Jurnal tersebut memaparkan bahwa protokol pertukaran kunci yang menggunakan polinomial atas ring non-komutatif, tingkat keamanan protokol ini diletakkan pada permasalahan dekomposisi simetris. Contoh ring non-komutatif yang digunakan adalah ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, dengan p merupakan bilangan prima. Protokol ini menggunakan operasi penjumlahan dan perkalian atas $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Referensi lain yang digunakan yaitu jurnal Climent, Navaro dan Tortosa (2010). Di dalam jurnal tersebut, dijelaskan mengenai sifat-sifat, dan operasi penjumlahan, perkalian serta invers pada ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Selanjutnya, pada tugas akhir ini dibutuhkan materi-materi mengenai struktur aljabar dan kriptografi yang diambil dari beberapa buku yaitu, JB. Fraleigh (2003), Menezes, Oorschot dan Vanstone (1996), dan Johanes A. Buchman (2000).

1.7. Metode penelitian

Metode yang digunakan pada penulisan tugas akhir ini menggunakan studi literatur. Penelitian ini dilakukan dengan cara membahas dan menjabarkan materi-materi dan teorema-teorema yang terdapat dalam buku atau jurnal, sehingga hasil akhir yang diharapkan dapat mempermudah pembaca dalam memahami maksud dari isi tugas akhir ini. Adapun langkah-langkah penulis dalam mengerjakan tugas akhir ini adalah:



Gambar 1.1 Alur Penelitian

1.8. Sistematika Penulisan

Dalam penulisan tugas akhir ini, penulis membaginya ke dalam enam bab yang disusun secara runtun dan sistematis dengan rincian masing-masing bab yaitu, BAB I sebagai pendahuluan, BAB II sebagai dasar teori, BAB III tentang

pembahasan ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, BAB IV sebagai pembahasan perhitungan protokol dan sandi hill atas E_p, BAB V sebagai uji coba program dan BAB VI sebagai penutup. Alur sistematika penelitian dari penulis secara umum dapat dijelaskan dalam bagan dibawah ini :

Gambar 1.2 Alur Sistematika Penulisan

BAB VI

PENUTUP

6.1 Kesimpulan

Protokol pertukaran kunci merupakan salah metode dalam kriptografi yang berguna untuk mengatasi masalah distribusi kunci pada sistem kripto kunci simetris. Pada protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ ini diperlukan pemahaman mengenai kriptografi dan beberapa dasar struktur aljabar seperti teori bilangan, grup, ring dan lapangan. Inilah yang melandasi prosedur protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Keamanan dari pembuatan kunci rahasia protokol ini diletakkan pada memecahkan masalah dekomposisi simetris yaitu *Diberikan* $(x, y) \in G \times G$ *dan* $m, n \in \mathbb{Z}$, *masalah dekomposisi simetris adalah masalah untuk menemukan* $z \in G$ *sehingga* $y = z^m x z^n$. Adapun skema perhitungan pembuatan kunci rahasianya adalah, pertama Alice dan Bob menyepakati bilangan prima p dan kunci publik $M, N \in E_p$. Kemudian Alice memilih kunci rahasia $r, s \in \mathbb{N}$ dan $f(X) \in \mathbb{Z}[X]$ dan Bob memilih kunci rahasia $u, v \in \mathbb{N}$ dan $g(X) \in \mathbb{Z}[X]$. Selanjutnya Alice menghitung kunci publiknya $P_A = f(M)^r N f(M)^s$ dan mngirimkannya kepada Bob, begitu juga Bob menghitung kunci publiknya $P_B = g(M)^u N g(M)^v$ dan mengirimkannya kepada Alice. Setelah itu Alice dan Bob menghitung kunci rahasianya yaitu $S_A = f(M)^r P_B f(M)^s$ dan $S_B = g(M)^u P_A g(M)^v$. Diperoleh $S_A = S_B$.

Setelah kunci rahasia didapatkan dari protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, maka kunci rahasia tersebut akan digunakan dalam penyandian pesan rahasia yang akan dikirim melalui jalur yang tidak aman pada sistem keamanan sandi Hill atas E_p. Alurnya yaitu, pertama Alice dan bob menyepakati bilangan prima $p > 256$ dan kunci rahasia yang sama, yaitu $\mathcal{K} = \{ \begin{bmatrix} a & b \\ pc & pu + v \end{bmatrix} \in E_p | a \neq 0, v \neq 0\}$. Selanjutnya, plainteks yang akan dikirim dibagi menjadi masing-masing lima huruf. Huruf-huruf tersebut diubah menjadi angka sesuai tabel ASCII dan membentuk himpunan E_p. Setelah itu Alice melakukan proses enkripsi, yaitu $e_K(M) = MK$, dan mengirimkan hasil cipherteksnya kepada Bob. Setelah cipherteksnya sampai, Bob melakukan proses dekripsi, yaitu $d_K(C) = CK^{-1}$, dan mendapatkan plainteksnya.

Dalam mempermudah perhitungan kunci rahasia dan proses enkripsi serta dekripsi yang sangat rumit dan panjang, dibuat suatu bahasa pemograman menggunakan MATLAB, seperti pada Lampiran 1, 2, dan 3. Pemograman ini akan sangat membantu kedua belah pihak untuk menghitung protokol pertukaran kunci atas ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dan mempermudah dalam melakukakn proses enkripsi dan dekripsi pada sandi Hill atas E_p.

6.2 Saran

Setelah membuat skripsi ini, ada beberapa saran yang ingin penulis sampaikan, diantaranya yaitu:

1. Protokol pertukaran kunci merupakan salah satu cara mengatasi masalah distribusi kunci, diharapkan ada penelitian selanjutnya tentang cara

mengatasi masalah distribusi kunci yang lebih efektif dan mempunyai keamanan yang tinggi.

2. Untuk menjaga keamanan protokol pertukaran kunci atas ring End $(\mathbb{Z}_P \times \mathbb{Z}_{P^2})$ ini, diharapkan menggunakan bilangan prima yang besar dan polinomial dengan pangkat yang juga besar. Semakin besar bilangan prima dan pangkat polinomialnya, semakin tinggi tingkat keamanannya.
3. Program yang sudah penulis buat, terbatas hanya maksimal polinomial pangkat 3. Diharapkan kepada peneliti selanjutya yang ingin meneliti lebih lanjut mengenai masalah ini untuk membuat program dengan pangkat polinomialnya terserah pembuat kunci (pangkat input sendiri), serta menyempurnakan program ini.

DAFTAR PUSTAKA

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

Climent, Navarro, and Tortosa, 2012, *Key Exchange Protocol over Noncommutative Rings. The Case of End* $(\mathbb{Z}_P \times \mathbb{Z}_{P^2})$, Universitat d'Alacant.

Climent, Navarro, and Tortosa, 2010, *On Arithmetic of Endomorphism Ring End* $(\mathbb{Z}_P \times \mathbb{Z}_{P^2})$, Universitat d'Alacant.

Fraleigh, John., 2003, *A First Course in Abstract Algebra* Seventh Edition, Addison-Wesley Publishing Company, Inc., USA.

Joyce, David, 2008, *Introduction to Modern Algebra*, Clark University.

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

Myasnikov, Shpilrain, and Ushakov, 2008, *Group Based Cryptography*, Birkhäuser Verlag, Berlin.

Raharjo, Budi, 2002, *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Infonesia, Bandung.

Riyanto, M. Zaki, 2011, *Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-Komutatif*, prosiding seminar nasional matematika dan pendidikan matematika 2011. Universitas Negeri Yogyakarta.

Shor, Peter W., 1997, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Society for Industrial and Applied Mathematics Philadelphia, PA, USA.

LAMPIRAN

Lampiran 1. Program Protokol Pertukaran Kunci

```
%proses perhitungan protokol pertukaran kunci
clc;
p=input('masukkan bilangan primanya=');
disp('>>>>>masukkan nilai kunci publik M')
M1=input('masukkan nilai a=');
M2=input('masukkan nilai b=');
M3=input('masukkan nilai c=');
M4=input('masukkan nilai d=');
m1=M3/p;
m2=floor(M4/p);
m3=M4-(p*m2);
disp('>>>>>masukkan nilai kunci publik N')
N1=input('masukkan nilai a=');
N2=input('masukkan nilai b=');
N3=input('masukkan nilai c=');
N4=input('masukkan nilai d=');
n1=N3/p;
n2=floor(N4/p);
n3=N4-(p*N2);
disp('>>>>>alice memilih kunci rahasia (r, s) dan fungsi polinomial
f(x)')
r=input('masukkan nilai kunci rahasia r=');
s=input('masukkan nilai kunci rahasia s=');
fprintf('(r, s)= (%1d,%1d)\n', r,s)
A=input('masukkan variabel A=');
```

```
B=input('masukkan variabel B=');
C=input('masukkan variabel C=');
D=input('masukkan variabel D=');
disp('>>>>>bob memilih kunci rahasia (u, v) dan fungsi polinomial
g(x)')
u=input('masukkan nilai kunci rahasia u=');
v=input('masukkan nilai kunci rahasia v=');
fprintf('(u, v)= (%1d,%1d)\n', u,v)
E=input('masukkan variabel E=');
F=input('masukkan variabel F=');
G=input('masukkan variabel G=');
H=input('masukkan variabel H=');
clc;
disp('Diberikan kunci publik:');
fprintf('bilangan primanya=%1d\n',p);
fprintf('M = %1d %3d\n %4d %3d\n', M1,M2,M3,M4);
fprintf('N = %1d %3d\n %5d %3d\n', N1,N2,N3,N4);
fprintf('\n        "TABEL KUNCI RAHASIA"\n');
fprintf('      Alice                    Bob\n');
fprintf('_____________________________________________________
_\n');
fprintf('   (r, s)= (%1d,%1d)', r,s);
fprintf('              (u, v)= (%1d,%1d)\n', u,v);
fprintf('f(x)=%1dx^3 + %1dx^2 + %1dx + %1d', A,B,C,D);
fprintf('    g(x)=%1dx^3 + %1dx^2 + %1dx + %1d\n', E,F,G,H);
fprintf('_____________________________________________________
_\n');
disp('>>>>> alice menghitung kunci publik PA');
```

```
a1=A*1;
b1=A*0;
c1=A*0;
d1=A*1;
e1=c1/p;
f1=floor(d1/p);
g1=d1-(p*f1);
a2= mod ((M1*M1),p);
b2= mod (((M1*M2)+(M2*m3)),p);
c2=p*(mod (((m1*M1)+(m1*m3)),p));
d2=(p*(mod (((m1*M2)+(m2*m3)+(m2*m3)+(floor((m3*m3)/p))),p)))+ mod
((m3*m3),p);
e2=c2/p;
f2=floor(d2/p);
g2=d2-(p*f2);
a20= mod ((a2*M1),p);
b20= mod (((a2*M2)+(b2*m3)),p);
c20=p*(mod (((e2*M1)+(m1*g2)),p));
d20=(p*(mod    (((e2*M2)+(f2*m3)+(m2*g2)+(floor((g2*m3)/p))),p)))+
mod ((g2*m3),p);
e20=c20/p;
f20=floor(d20/p);
g20=d20-(p*f20);
a3= mod ((a1*a20),p);
b3= mod (((a1*b20)+(b1*g20)),p);
c3=p*(mod (((e1*a20)+(e20*g1)),p));
d3=(p*(mod (((e1*b20)+(f1*g20)+(f20*g1)+(floor((g1*g20)/p))),p)))+
mod ((g1*g20),p);
```

```
e3=c3/p;
f3=floor(d3/p);
g3=d3-(p*f3);
a4=B*1;
b4=B*0;
c4=B*0;
d4=B*1;
e4=c4/p;
f4=floor(d4/p);
g4=d4-(p*f4);
a30= mod ((a4*a2),p);
b30= mod (((a4*b2)+(b4*g2)),p);
c30=p*(mod (((e4*a2)+(e2*g4)),p));
d30=(p*(mod    (((e4*b2)+(f4*g2)+(f2*g4)+(floor((g4*g2)/p))),p)))+
mod ((g4*g2),p);
e30=c30/p;
f30=floor(d30/p);
g30=d30-(p*f30);
a6=C*1;
b6=C*0;
c6=C*0;
d6=C*1;
e6=c6/p;
f6=floor(d6/p);
g6=d6-(p*f6);
a5= mod ((a6*M1),p);
b5= mod (((a6*M2)+(b6*m3)),p);
c5=p*(mod(((e6*M1)+(m1*g6)),p));
```

```
d5=(p*(mod (((e6*M2)+(f6*m3)+(m2*g6)+(floor((g6*m3)/p))),p)))+ mod
((g6*m3),p);
e5=c5/p;
f5=floor(d5/p);
g5=d5-(p*f5);
a9=D*1;
b9=D*0;
c9=D*0;
d9=D*1;
e9=c9/p;
f9=floor(d9/p);
g9=d9-(p*f9);
a7= mod ((a3+a30),p);
b7= mod ((b3+b30),p);
c7=p*(mod ((e3+e30),p));
d7=(p*(mod ((f3+f30+(floor((g3+g30)/p))),p)))+ mod ((g3+g30),p);
e7=c7/p;
f7=floor(d7/p);
g7=d7-(p*f7);
a8= mod ((a5+a9),p);
b8= mod ((b5+b9),p);
c8=p*(mod ((e5+e9),p));
d8=(p*(mod ((f5+f9+(floor((g5+g9)/p))),p)))+ mod ((g5+g9),p);
e8=c8/p;
f8=floor(d8/p);
g8=d8-(p*f8);
a(1)= mod ((a7+a8),p);
b(1)= mod ((b7+b8),p);
```

```
c(1)=p*(mod ((e7+e8),p));
d(1)=(p*(mod ((f7+f8+(floor((g7+g8)/p))),p)))+ mod ((g7+g8),p);
e(1)=c(1)/p;
f(1)=floor(d(1)/p);
g(1)=d(1)-(p*f(1));
fprintf('f(M)= %1d %3d\n %7d %3d\n', a(1),b(1),c(1),d(1));
disp(' PA = f(M)^r.N.f(M)^s');
for i=1:r
    a(i+1)= mod ((a(i)*a(1)),p);
    b(i+1)= mod (((a(i)*b(1))+(b(i)*g(1))),p);
    c(i+1)=p*(mod (((e(i)*a(1))+(e(1)*g(i))),p));
    d(i+1)=(p*(mod
(((e(i)*b(1))+(f(i)*g(1))+(f(1)*g(i))+(floor((g(i)*g(1))/p))),p)))
+ mod ((g(i)*g(1)),p);
    e(i+1)=c(i+1)/p;
    f(i+1)=floor(d(i+1)/p) ;
    g(i+1)= d(i+1)-(p*f(i+1));
end;
for i=1:s
    a(i+1)= mod ((a(i)*a(1)),p);
    b(i+1)= mod (((a(i)*b(1))+(b(i)*g(1))),p);
    c(i+1)=p*(mod (((e(i)*a(1))+(e(1)*g(i))),p));
    d(i+1)=(p*(mod
(((e(i)*b(1))+(f(i)*g(1))+(f(1)*g(i))+(floor((g(i)*g(1))/p))),p)))
+ mod ((g(i)*g(1)),p);
    e(i+1)=c(i+1)/p;
    f(i+1)=floor(d(i+1)/p) ;
    g(i+1)= d(i+1)-(p*f(i+1));
```

```
end;
a10= mod ((a(r)*N1),p);
b10= mod (((a(r)*N2)+(b(r)*n3)),p);
c10=p*(mod (((e(r)*N1)+(n1*g(r))),p));
d10=(p*(mod
(((e(r)*N2)+(f(r)*n3)+(n2*g(r))+(floor((g(r)*n3)/p))),p)))+     mod
((g(r)*n3),p);
e10=c10/p;
f10=floor(d10/p);
g10=d10-(p*f10);
a11= mod ((a10*a(s)),p);
b11= mod (((a10*b(s))+(b10*g(s))),p);
c11=p*(mod (((e10* a(s))+( e(s)*g10)),p));
d11=(p*(mod
(((e10*b(s))+(f10*g(s))+(f(s)*g10)+(floor((g10*g(s))/p))),p)))+
mod ((g10*g(s)),p);
e11=c11/p;
f11=floor(d11/p);
g11=d11-(p*f11);
fprintf('PA=%3d %3d\n %5d %3d\n', a11,b11,c11,d11);
disp('dan mengirimkannya kepada Bob');
disp('>>>>> Bob juga menghitung kunci publik PB');
h1=E*1;
x1=E*0;
j1=E*0;
k1=E*1;
l1=j1/p;
z1=floor(k1/p);
```

```
q1=k1-(p*z1);
h2= mod ((M1*M1),p);
x2= mod (((M1*M2)+(M2*m3)),p);
j2=p*(mod (((m1*M1)+(m1*m3)),p));
k2=(p*(mod (((m1*M2)+(m2*m3)+(m2*m3)+(floor((m3*m3)/p))),p)))+ mod
((m3*m3),p);
l2=j2/p;
z2=floor(k2/p);
q2=k2-(p*z2);
h20= mod ((h2*M1),p);
x20= mod (((h2*M2)+(x2*m3)),p);
j20=p*(mod (((l2*M1)+(m1*q2)),p));
k20=(p*(mod    (((l2*M2)+(z2*m3)+(m2*q2)+(floor((q2*m3)/p))),p)))+
mod ((q2*m3),p);
l20=j20/p;
z20=floor(k20/p);
q20=k20-(p*z20);
h3= mod ((h1*h20),p);
x3= mod (((h1*x20)+(x1*q20)),p);
j3=p*(mod (((l1*h20)+(l20*q1)),p));
k3=(p*(mod (((l1*x20)+(z1*q20)+(z20*q1)+(floor((q1*q20)/p))),p)))+
mod ((q1*q20),p);
l3=j3/p;
z3=floor(k3/p);
q3=k3-(p*z3);
h4=F*1;
x4=F*0;
j4=F*0;
```

```
k4=F*1;
l4=j4/p;
z4=floor(k4/p);
q4=k4-(p*z4);
h30= mod ((h4*h2),p);
x30= mod (((h4*x2)+(x4*q2)),p);
j30=p*(mod (((l4*h2)+(l2*q4)),p));
k30=(p*(mod    (((l4*x2)+(z4*q2)+(z2*q4)+(floor((q4*q2)/p))),p)))+
mod ((q4*q2),p);
l30=j30/p;
z30=floor(k30/p);
q30=k30-(p*z30);
h6=G*1;
x6=G*0;
j6=G*0;
k6=G*1;
l6=j6/p;
z6=floor(k6/p);
q6=k6-(p*z6);
h5= mod ((h6*M1),p);
x5= mod (((h6*M2)+(x6*m3)),p);
j5=p*(mod (((l6*M1)+(m1*q6)),p));
k5=(p*(mod (((l6*M2)+(z6*m3)+(m2*q6)+(floor((q6*m3)/p))),p)))+ mod
((q6*m3),p);
l5=j5/p;
z5=floor(k5/p);
q5=k5-(p*z5);
h9=H*1;
```

```
x9=H*0;
j9=H*0;
k9=H*1;
l9=j9/p;
z9=floor(k9/p);
q9=k9-(p*z9);
h7= mod ((h3+h30),p);
x7= mod ((x3+x30),p);
j7=p*(mod ((l3+l30),p));
k7=(p*(mod ((z3+z30+(floor((q3+q30)/p))),p)))+ mod ((q3+q30),p);
l7=j7/p;
z7=floor(k7/p);
q7=k7-(p*z7);
h8= mod ((h5+h9),p);
x8= mod ((x5+x9),p);
j8=p*(mod ((l5+l9),p));
k8=(p*(mod ((z5+z9+(floor((q5+q9)/p))),p)))+ mod ((q5+q9),p);
l8=j8/p;
z8=floor(k8/p);
q8=k8-(p*z8);
h(1)= mod ((h7+h8),p);
x(1)= mod ((x7+x8),p);
j(1)=p*(mod ((l7+l8),p));
k(1)=(p*(mod ((z7+z8+(floor((q7+q8)/p))),p)))+ mod ((q7+q8),p);
l(1)=j(1)/p;
z(1)=floor(k(1)/p);
q(1)=k(1)-(p*z(1));
fprintf('g(M)= %1d %3d\n %7d %3d\n', h(1),x(1),j(1),k(1));
```

```
disp(' PB = g(M)^u.N.g(M)^v');
for i=1:u
    h(i+1)= mod ((h(i)*h(1)),p);
    x(i+1)= mod (((h(i)*x(1))+(x(i)*q(1))),p);
    j(i+1)=p*(mod (((l(i)*h(1))+(l(1)*q(i))),p));
    k(i+1)=(p*(mod
(((l(i)*x(1))+(z(i)*q(1))+(z(1)*q(i))+(floor((q(i)*q(1))/p))),p)))
+ mod ((q(i)*q(1)),p);
    l(i+1)=j(i+1)/p;
    z(i+1)=floor(k(i+1)/p) ;
    q(i+1)=k(i+1)-(p*z(i+1));
end;
for i=1:v
    h(i+1)= mod ((h(i)*h(1)),p);
    x(i+1)= mod (((h(i)*x(1))+(x(i)*q(1))),p);
    j(i+1)=p*(mod (((l(i)*h(1))+(l(1)*q(i))),p));
    k(i+1)=(p*(mod
(((l(i)*x(1))+(z(i)*q(1))+(z(1)*q(i))+(floor((q(i)*q(1))/p))),p)))
+ mod ((q(i)*q(1)),p);
    l(i+1)=j(i+1)/p;
    z(i+1)=floor(k(i+1)/p) ;
    q(i+1)=k(i+1)-(p*z(i+1));
end;
h10= mod ((h(u)*N1),p);
x10= mod (((h(u)*N2)+(x(u)*n3)),p);
j10=p*(mod (((l(u)*N1)+(n1*q(u))),p));
```

```
k10=(p*(mod
(((l(u)*N2)+(z(u)*n3)+(n2*q(u))+(floor((q(u)*n3)/p))),p)))+     mod
((q(u)*n3),p);
l10=j10/p;
z10=floor(k10/p);
q10=k10-(p*z10);
h11= mod ((h10*h(v)),p);
x11= mod (((h10*x(v))+(x10*q(v))),p);
j11=p*(mod (((l10*h(v))+(l(v)*q10)),p));
k11=(p*(mod
(((l10*x(v))+(z10*q(v))+(z(v)*q10)+(floor((q10*q(v))/p))),p)))+
mod ((q10*q(v)),p);
l11=j11/p;
z11=floor(k11/p);
q11=k11-(p*z11);
fprintf('PB=%3d %3d\n %5d %3d\n', h11,x11,j11,k11);
disp('dan mengirimkannya kepada Alice');
disp('>>>>> Alice menghitung kunci rahasia bersamanya SA');
disp('SA=f(M)^r.PB.f(M)^s');
a12= mod ((a(r)*h11),p);
b12= mod (((a(r)*x11)+(b(r)*q11)),p);
c12=p*(mod (((e(r)*h11)+(l11*g(r))),p));
d12=(p*(mod
(((e(r)*x11)+(f(r)*q11)+(z11*g(r))+(floor((g(r)*q11)/p))),p)))+
mod ((g(r)*q11),p);
e12=c12/p;
f12=floor(d12/p);
g12=d12-(p*f12);
```

```
a13= mod ((a12*a(s)),p);
b13= mod (((a12*b(s))+(b12*g(s))),p);
c13=p*(mod (((e12*a(s))+(e(s)*g12)),p));
d13=(p*(mod
(((e12*b(s))+(f12*g(s))+(f(s)*g12)+(floor((g12*g(s))/p))),p)))+
mod ((g12*g(s)),p);
e13=c13/p;
f13=floor(d13/p);
g13=d13-(p*f13);
fprintf('Diperoleh SA=%3d %3d\n %15d %3d\n', a13,b13,c13,d13);
disp('>>>>> Bob menghitung kunci rahasia bersamanya SB');
disp('SB=g(M)^r.PA.g(M)^s');
a14= mod ((h(u)*a11),p);
b14= mod (((h(u)*b11)+(x(u)*g11)),p);
c14=p*(mod (((l(u)*a11)+(e11*q(u))),p));
d14=(p*(mod
(((l(u)*b11)+(z(u)*g11)+(f11*q(u))+(floor((q(u)*g11)/p))),p)))+
mod ((q(u)*g11),p);
e14=c14/p;
f14=floor(d14/p);
g14=d14-(p*f14);
a15= mod ((a14*h(v)),p);
b15= mod (((a14*x(v))+(b14*q(v))),p);
c15=p*(mod (((e14*h(v))+(l(v)*g14)),p));
d15=(p*(mod
(((e14*x(v))+(f14*q(v))+(z(v)*g14)+(floor((g14*q(v))/p))),p)))+
mod ((g14*q(v)),p);
e15=c15/p;
```

```
f15=floor(d15/p);
g15=d15-(p*f15);
fprintf('Diperoleh SB=%3d %3d\n %15d %3d\n', a15,b15,c15,d15);
disp('____________________________________________________________
')
fprintf('"kunci rahasia bersama" --> SA = SB = %3d %3d\n %40d
%3d\n', a13,b13,c13,d13)
disp('____________________________________________________________
')
```

Lampiran 2. Program Enkripsi

```
%proses enkripsi sandi Hill
clc;
disp('"alice mempunyai pesan asli yang akan dijadikan pesan
sandi"');
p=input('masukkan bilangan prima=');
P=input('masukkan 5 huruf plainteks yang akan disandikan=','s');
h=double(P);
disp('"alice mempunyai kunci rahasia"');
k1=input('masukkan entri pertama kunci rahasia=');
k2=input('masukkan entri kedua kunci rahasia=');
k3=input('masukkan entri ketiga kunci rahasia=');
k4=input('masukkan entri keempat kunci rahasia=');
c1=k3/p;
u1=floor(k4/p);
v1= k4-(p*u1);
clc;
fprintf('bilangan prima yang dipilih= %1d\n', p);
fprintf('plainteks yang sudah diubah menjadi angka= %1d %1d %1d
%1d %1d\n',h(1),h(2),h(3),h(4),h(5));
fprintf('kunci rahasia= %1d %3d\n %17d %3d\n', k1,k2,k3,k4);
a=mod((h(1)*k1),p);
b=mod(((h(1)*k2)+(h(2)*v1)),p);
c=p*(mod(((h(3)*k1)+(h(5)*c1)),p));
d=(p*(mod(((h(3)*k2)+(h(4)*v1)+(u1*h(5))+floor((h(5)*v1)/p)),p)))+
mod((h(5)*v1),p);
x=c/p;
y=floor(d/p);
```

```
z= d-(p*y);
C=char('a','b','x','y','z');
fprintf('e(x)=%1d %3d\n %7d %3d\n',a,b,c,d)
fprintf('cipherteks= %1d %1d %1d %1d %1d\n', a,b,x,y,z)
```

Lampiran 3. Program Dekripsi

```
%proses dekripsi sandi Hill
clc;
disp('"Bob mendapatkan pesan sandi dari Alice"');
p=input('masukkan bilangan prima=');
h(1)=input('masukkan huruf cipherteks pertama=');
h(2)=input('masukkan huruf cipherteks kedua=');
h(3)=input('masukkan huruf cipherteks ketiga=');
h(4)=input('masukkan huruf cipherteks keempat=');
h(5)=input('masukkan huruf cipherteks kelima=');
disp('"Bob mempunyai kunci rahasia"');
k1=input('masukkan entri pertama kunci rahasia=');
k2=input('masukkan entri kedua kunci rahasia=');
k3=input('masukkan entri ketiga kunci rahasia=');
k4=input('masukkan entri keempat kunci rahasia=');
c1=k3/p;
u1=floor(k4/p);
v1= k4-(p*u1);
[g1,a2,d1]=gcd(k1,p);
[g2,v2,d2]=gcd(v1,p);
a= mod(a2,p);
b= mod ((-a2*k2*v2),p);
x=p*(mod ((-v2*c1*a2),p));
y=(p*(mod (((c1*a2*k2*(v2^2))-(u1*(v2^2))-
(floor((v1*v2)/p))*v2),p)))+ v2;
c3=x/p;
u3=floor(y/p);
v3= y-(p*u3);
```

```
clc;
fprintf('bilangan prima yang dipilih= %1d\n', p);
fprintf('cipherteksnya= %1d %1d %1d %1d
%1d\n',h(1),h(2),h(3),h(4),h(5));
fprintf('kunci rahasia= %1d %3d\n %17d %3d\n', k1,k2,k3,k4);
a4=mod((h(1)*a),p);
b4=mod(((h(1)*b)+(h(2)*v3)),p);
c4=p*(mod(((h(3)*a)+(h(5)*c3)),p));
d4=(p*(mod(((h(3)*b)+(h(4)*v3)+(u3*h(5))+floor((h(5)*v3)/p)),p)))+
mod((h(5)*v3),p);
x4=c4/p;
y4=floor(d4/p);
z4= d4-(p*y4);
fprintf('d(y)=%1d %3d\n %7d %3d\n',a4,b4,c4,d4);
plainteksnya=char(a4,b4,x4,y4,z4)
```

Lampiran 4. Tabel ASCII

Decimal:	ArtNet:	Hex:	ASCII:
0	0:0	00	NUL
1	0:1	01	SOH
2	0:2	02	STX
3	0:3	03	ETX
4	0:4	04	EOT
5	0:5	05	ENQ
6	0:6	06	ACK
7	0:7	07	BEL
8	0:8	08	BS
9	0:9	09	TAB
10	0:A	0A	LF
11	0:B	0B	VT
12	0:C	0C	FF
13	0:D	0D	CR
14	0:E	0E	SO
15	0:F	0F	SI
16	1:0	10	DLE
17	1:1	11	DC1
18	1:2	12	DC2
19	1:3	13	DC3
20	1:4	14	DC4
21	1:5	15	NAK
22	1:6	16	SYN
23	1:7	17	ETB
24	1:8	18	CAN
25	1:9	19	EM
26	1:A	1A	SUB
27	1:B	1B	ESC
28	1:C	1C	FS
29	1:D	1D	GS
30	1:E	1E	RS
31	1:F	1F	US

Decimal:	ArtNet:	Hex:	ASCII:
32	2:0	20	(space)
33	2:1	21	!
34	2:2	22	"
35	2:3	23	#
36	2:4	24	$
37	2:5	25	%
38	2:6	26	&
39	2:7	27	'
40	2:8	28	(
41	2:9	29	)
42	2:A	2A	*
43	2:B	2B	+
44	2:C	2C	,
45	2:D	2D	-
46	2:E	2E	.
47	2:F	2F	/
48	3:0	30	0
49	3:1	31	1
50	3:2	32	2
51	3:3	33	3
52	3:4	34	4
53	3:5	35	5
54	3:6	36	6
55	3:7	37	7
56	3:8	38	8
57	3:9	39	9
58	3:A	3A	:
59	3:B	3B	;
60	3:C	3C	<
61	3:D	3D	=
62	3:E	3E	>
63	3:F	3F	?

Decimal:	ArtNet:	Hex:	ASCII:
64	4:0	40	@
65	4:1	41	A
66	4:2	42	B
67	4:3	43	C
68	4:4	44	D
69	4:5	45	E
70	4:6	46	F
71	4:7	47	G
72	4:8	48	H
73	4:9	49	I
74	4:A	4A	J
75	4:B	4B	K
76	4:C	4C	L
77	4:D	4D	M
78	4:E	4E	N
79	4:F	4F	O
80	5:0	50	P
81	5:1	51	Q
82	5:2	52	R
83	5:3	53	S
84	5:4	54	T
85	5:5	55	U
86	5:6	56	V
87	5:7	57	W
88	5:8	58	X
89	5:9	59	Y
90	5:A	5A	Z
91	5:B	5B	[
92	5:C	5C	\
93	5:D	5D	]
94	5:E	5E	^
95	5:F	5F	_

Decimal:	ArtNet:	Hex:	ASCII:
96	6:0	60	`
97	6:1	61	a
98	6:2	62	b
99	6:3	63	c
100	6:4	64	d
101	6:5	65	e
102	6:6	66	f
103	6:7	67	g
104	6:8	68	h
105	6:9	69	i
106	6:A	6A	j
107	6:B	6B	k
108	6:C	6C	l
109	6:D	6D	m
110	6:E	6E	n
111	6:F	6F	o
112	7:0	70	p
113	7:1	71	q
114	7:2	72	r
115	7:3	73	s
116	7:4	74	t
117	7:5	75	u
118	7:6	76	v
119	7:7	77	w
120	7:8	78	x
121	7:9	79	y
122	7:A	7A	z
123	7:B	7B	{
124	7:C	7C	|
125	7:D	7D	}
126	7:E	7E	~
127	7:F	7F	DEL

Decimal:	ArtNet:	Hex:	ASCII:
128	8:0	80	€
129	8:1	81	
130	8:2	82	‚
131	8:3	83	ƒ
132	8:4	84	„
133	8:5	85	…
134	8:6	86	†
135	8:7	87	‡
136	8:8	88	ˆ
137	8:9	89	‰
138	8:A	8A	Š
139	8:B	8B	‹
140	8:C	8C	Œ
141	8:D	8D	
142	8:E	8E	Ž
143	8:F	8F	
144	9:0	90	
145	9:1	91	‘
146	9:2	92	’
147	9:3	93	“
148	9:4	94	”
149	9:5	95	•
150	9:6	96	–
151	9:7	97	—
152	9:8	98	˜
153	9:9	99	™
154	9:A	9A	š
155	9:B	9B	›
156	9:C	9C	œ
157	9:D	9D	
158	9:E	9E	ž
159	9:F	9F	

Decimal:	ArtNet:	Hex:	ASCII:
160	A:0	A0	
161	A:1	A1	¡
162	A:2	A2	¢
163	A:3	A3	£
164	A:4	A4	¤
165	A:5	A5	¥
166	A:6	A6	¦
167	A:7	A7	§
168	A:8	A8	¨
169	A:9	A9	©
170	A:A	AA	ª
171	A:B	AB	«
172	A:C	AC	¬
173	A:D	AD	-
174	A:E	AE	®
175	A:F	AF	¯
176	B:0	B0	°
177	B:1	B1	±
178	B:2	B2	²
179	B:3	B3	³
180	B:4	B4	´
181	B:5	B5	µ
182	B:6	B6	¶
183	B:7	B7	·
184	B:8	B8	¸
185	B:9	B9	¹
186	B:A	BA	º
187	B:B	BB	»
188	B:C	BC	¼
189	B:D	BD	½
190	B:E	BE	¾
191	B:F	BF	

Decimal:	ArtNet:	Hex:	ASCII:
192	C:0	C0	À
193	C:1	C1	Á
194	C:2	C2	Â
195	C:3	C3	Ã
196	C:4	C4	Ä
197	C:5	C5	Å
198	C:6	C6	Æ
199	C:7	C7	Ç
200	C:8	C8	È
201	C:9	C9	É
202	C:A	CA	Ê
203	C:B	CB	Ë
204	C:C	CC	Ì
205	C:D	CD	Í
206	C:E	CE	Î
207	C:F	CF	Ï
208	D:0	D0	Ð
209	D:1	D1	Ñ
210	D:2	D2	Ò
211	D:3	D3	Ó
212	D:4	D4	Ô
213	D:5	D5	Õ
214	D:6	D6	Ö
215	D:7	D7	×
216	D:8	D8	Ø
217	D:9	D9	Ù
218	D:A	DA	Ú
219	D:B	DB	Û
220	D:C	DC	Ü
221	D:D	DD	Ý
222	D:E	DE	Þ
223	D:F	DF	

Decimal:	ArtNet:	Hex:	ASCII:
224	E:0	E0	à
225	E:1	E1	á
226	E:2	E2	â
227	E:3	E3	ã
228	E:4	E4	ä
229	E:5	E5	å
230	E:6	E6	æ
231	E:7	E7	ç
232	E:8	E8	è
233	E:9	E9	é
234	E:A	EA	ê
235	E:B	EB	ë
236	E:C	EC	ì
237	E:D	ED	í
238	E:E	EE	î
239	E:F	EF	ï
240	F:0	F0	ð
241	F:1	F1	ñ
242	F:2	F2	ò
243	F:3	F3	ó
244	F:4	F4	ô
245	F:5	F5	õ
246	F:6	F6	ö
247	F:7	F7	÷
248	F:8	F8	ø
249	F:9	F9	ù
250	F:A	FA	ú
251	F:B	FB	û
252	F:C	FC	ü
253	F:D	FD	ý
254	F:E	FE	þ
255	F:F	FF	

Lampiran 5. Proses perhitungan invers kunci rahasia

$$K^{-1} = \begin{bmatrix} 460^{-1} & (-460^{-1}.593.224^{-1}) mod\ 1013 \\ 1013[(-224^{-1}.190.460^{-1}) mod\ 1013] & 1013\left[\left(190.460^{-1}.593.(224^{-1})^2 - 972(224^{-1})^2 - \left\lfloor\frac{224.224^{-1}}{1013}\right\rfloor 224^{-1}\right) mod\ 1013\right] + 224^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} 403 & (-403.593.303) mod\ 1013 \\ 1013[(-303.190.403) mod\ 1013] & 1013\left[\left(190.403.593.(303)^2 - 972(303)^2 - \left\lfloor\frac{224.303}{1013}\right\rfloor 303\right) mod\ 1013\right] + 302 \end{bmatrix}$$

$$= \begin{bmatrix} 403 & 629 \\ 29377 & 1316 \end{bmatrix}$$