Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Grup Unit atas Ring Non-Komutatif $\boldsymbol{End}(\mathbb{Z}_{\boldsymbol{p}} \times \mathbb{Z}_{\boldsymbol{p^2}})$

SKRIPSI

Diajukan Guna Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1
Program Studi Matematika

Diajukan oleh :

Laila Marthatilova

12610004

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2016

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 : Laila Marthatilova
NIM : 12610004
Judul Skripsi : Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Grup Unit 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 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, 13 September 2016

Pembimbing I	Pembimbing II
Dr.Khurul Wardati,M.Si	M. Zaki Riyanto, S.Si., M.Sc
NIP: 19660731 200003 2 001	NIP: 19840113 201503 1 001

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-3863/Un.02/DST/PP.05.3/10/ 2016

Skripsi/Tugas Akhir dengan judul	:	Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Grup Unit atas Ring Non-Komutatif $End\,(\mathbb{Z}_p \times \mathbb{Z}_p)$
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Laila Marthatilova
NIM	:	12610004
Telah dimunaqasyahkan pada	:	28 September 2016
Nilai Munaqasyah	:	A

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

TIM MUNAQASYAH :

Ketua Sidang

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

Penguji I

M. Zaki Riyanto, M.Sc
NIP.19840113 201503 1 001

Penguji II

Malahayati, M.Sc
NIP.19840412 201101 2 010

Yogyakarta, 25 Oktober 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

SURAT PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini :

Nama : Laila Marthatilova

NIM : 12610004

Program Studi : Matematika

Fakultas : Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

menyatakan bahwa tugas akhir dengan judul **"Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Grup Unit atas Ring Non-Komutatif End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$"** merupakan karya sendiri dengan mengacu sesuai daftar pustaka yang terlampir dan tidak terdapat karya serupa yang diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi lain.

Yogyakarta, 13 September 2016

Yang menyatakan

Laila Marthatilova

NIM. 12610004

HALAMAN PERSEMBAHAN

Tugas akhir ini dipersembahkan untuk:

1. Almamater UIN Sunan Kalijaga Yogyakarta khususnya untuk Program Studi Matematika, Fakultas Sains dan Teknologi, tempatku mencari ilmu dan bekal pengetahuan selama kurang lebih 4 tahun ini.
2. Ayah dan Ibu yang tak pernah berhenti berdoa demi kelancaran dan kesuksesan putrinya, yang senantiasa mencurahkan cinta dan kasih sayang, yang selalu mendukung dan memberikan kekuatan serta motivasi untuk terus belajar dan memberikan hasil yang terbaik.
3. Kakakku Lutvia Mathofani dan Adikku Lusy Rizkya Millyartha yang selalu memberikan support dengan penuh perhatian.
4. Keluarga besar Paduan Suara Mahasiswa "Gita Savana" tempatku mendapatkan ilmu baru, pengalaman baru dan keluarga baru.
5. Sahabat-sahabat Matematika 2012, kelompok KKN 155 dan saudari-saudariku kos 8A.

MOTTO

" Allah is the protect of those who have FAITH, He will lead them from the depths of darkness into LIGHT "

(Al – Baqarah ; 257)

"Jika engkau berada di jalan Allah, berlarilah dengan kencang, jika sulit, tetaplah berlari meski hanya berlari-lari kecil, jika engkau merasa lelah, berjalanlah, jika semua itu tak mampu kau lakukan, tetaplah maju meski harus merangkak dan jangan sekalipun berbalik arah"

(Al-Imam As-Syafi'i)

"Tidak ada kata sia-sia dalam kebaikan, meski engkau kehilangan kesempatan yang lain, hanya ikhlas penawar sesal "

(Laila Marthatilova)

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillahirrobbil'alamin, puji syukur kehadirat Allah SWT yang senantiasa mencurahkan segala rahmat, hidayah serta inayah-Nya sehingga penulis dapat menyelesaikan tugas akhir dengan judul **"Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Grup Unit atas Ring Non-Komutatif *End*** $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$**"** dengan maksimal. Tugas akhir ini merupakan salah satu syarat untuk memperoleh gelar sarjana program studi Matematika di Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Penulis mengucapkan terimakasih kepada pihak-pihak yang telah membantu dalam proses penyusunan tugas akhir ini baik berupa dukungan, motivasi, bimbingan serta doa hingga tugas akhir ini dapat terselesaikan. Ucapan terimakasih ini penulis sampaikan kepada :

1. Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Dr. Muhammad Wakhid Mustofa, M.Si selaku Ketua Program Studi Matematika.
3. Muchammad Abrori, S.Si., M.Kom selaku Dosen Penasehat Akademik Matematika 2012.
4. Dr. Khurul Wardati, M.Si dan M. Zaki Riyanto, M.Sc selaku Dosen Pembimbing yang telah memberikan bimbingan serta arahan sehingga tugas akhir ini dapat terselesaikan.

5. Bapak dan Ibu dosen program studi Matematika yang telah memberikan bekal ilmu pengetahuan.
6. Ayah, ibu, kakak serta adikku tersayang yang senantiasa memberi cinta kasih, dukungan dan doa.
7. Keluarga PSM "Gita Savana" yang selalu mendukung dan memberikan semangat.
8. Teman-teman Matematika Angkatan 2012 yang telah belajar bersama-sama selama kurang lebih 4 tahun, serta seluruh teman-teman Matematika Fakultas Sains dan Teknologi baik kakak angkatan maupun adik angkatan yang secara tidak langsung berjuang bersam-sama dalam keilmuan Matematika.
9. Teman-teman kelompok KKN 155 yang telah berbagi pengalaman serta teman- teman KOS 8A yang saling mendukung dan berbagi kenyamanan.
10. Semua pihak yang telah mendukung dalam proses penyusunan tugas akhir ini yang tidak dapat disebutkan satu per satu.

Penulis berharap tugas akhir ini dapat bermanfaat dalam perkembangan ilmu matematika sehingga dapat bermanfaat pula bagi semua orang.

Wassalamu'alaikum Wr.Wb.

Yogyakarta, 13 September 2016

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMBANG

$\mathbb{Z}$	: Himpunan semua bilangan bulat
$\mathbb{Z}_n$	: Himpunan bilangan bulat modulo n, $n \in \mathbb{Z}$
$\mathbb{Z}_p$	: Himpunan bilangan bulat modulo p, p adalah bilangan prima
$\mathbb{Z}_{p^2}$	: Himpunan bilangan bulat modulo p^2, p adalah bilangan prima
$(H \times K)$	: Himpunan pasangan berurutan (h,k), dimana , $h \in H$, dan $k \in K$
$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$	: Himpunan pasangan berurutan (x,y), dimana , $x \in \mathbb{Z}_p$, dan $y \in \mathbb{Z}_{p^2}$
$End(G)$	: Himpunan endomorfisma grup $f: G \to G$
$End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$	: Himpunan endomorfisma grup $f: (\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \to (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$
$b \mid a$	: b habis membagi a
$b \nmid a$	: b tidak habis membagi a
$\lfloor a \rfloor$	: Fungsi *floor* dari a
$a \equiv b (mod\ m)$	: a dan b kongruen modulo m
$gcd(a,b)$	: *Greatest common divisor*/ faktor persekutuan terbesar dari a dan b
$(\mathbb{Z}_p, +)$	: Grup $\mathbb{Z}_p$ dengan operasi penjumlahan modulo p
$o(a)$	: Order elemen a, untuk suatu $a \in G$
$\lvert G \rvert$	: Order grup
$(End(G), +, .)$	: Ring endomorfisma dengan dua operasi biner penjumlahan dan perkalian
u	: Unit
$U(R)$	: Grup unit atas ring R
E_p	: Matriks berukuran 2×2, dimana entri-entri pada baris pertama $\in \mathbb{Z}_p$ dan entri-entri pada baris kedua $\in \mathbb{Z}_{p^2}$
$U(E_p)$	: Grup unit atas ring E_p
$M_n(R)$	: Matriks berukuran $n \times n$ atas ring R

$M_n(\mathbb{Z}_p)$: Matriks berukuran $n \times n$ atas ring $\mathbb{Z}_p$

$det(A)$: Determinan dari matriks A

$M_{ij}(A)$: Minor entri a_{ij}

$cof_{ij}(A)$: Kofaktor entri a_{ij}

$adj(A)$: Adjoin dari A

$GL_n(F)$: Grup matriks invertibel berukuran $n \times n$ atas lapangan F

$GL_2(\mathbb{Z}_p)$: Grup matriks invertibel berukuran 2×2 atas lapangan $\mathbb{Z}_p$

$\mathcal{P}$: Himpunan plainteks

$\mathcal{K}$: Himpunan kunci rahasia

$\mathcal{C}$: Himpunan cipherteks

$e_K(X)$: Enkripsi untuk plainteks X dengan kunci K

$d_K(Y)$: Dekripsi untuk cipherteks Y dengan kunci K

ABSTRAK

Internet termasuk jalur komunikasi umum yang dapat dilalui oleh siapapun, sehingga sangat rawan terhadap penyadapan. Penyadapan tentu saja merugikan bagi pihak yang ingin mengirim pesan rahasia. Kriptografi adalah salah satu cara menjaga pesan rahasia, yaitu dengan proses enkripsi dan dekripsi. Kedua proses tersebut memerlukan kunci rahasia yang disepakati bersama. Namun akan terjadi masalah jika kunci rahasia ditukarkan pada jalur komunikasi yang tidak aman, sehingga diperlukan skema pengamanan kunci rahasia yaitu protokol perjanjian kunci.

Tugas akhir ini membahas protokol perjanjian kunci ring non-komutatif $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ yang terdiri dari endomorfisma-endomorfisma grup $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$. Diberikan ring E_p sebagai matriks representasi dari ring $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dan dibentuk grup unit atas ring E_p yaitu $U(E_p)$. Ring E_p isomorfis dengan ring $End\,(\mathbb{Z}_p \text{ x } \mathbb{Z}_{p^2})$, sehingga $U(E_p)$ dapat disebut sebagai grup unit atas ring $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Keamanan protokol perjanjian kunci ini diletakkan pada masalah konjugasi. Kunci rahasia yang diperoleh digunakan dalam proses enkripsi-dekripsi menggunakan algoritma kriptografi simetris, yaitu kombinasi *playfair cipher* dan *Hill cipher*.

Perhitungan dalam pembuatan kunci rahasia maupun perhitungan dalam proses enkripsi-dekripsi pada grup unit atas ring $End\,(\mathbb{Z}_p \text{ x } \mathbb{Z}_{p^2})$ diuji coba menggunakan program MAPLE 18. Progam ini dirancang untuk menyelesaikan berbagai masalah matematika, sehingga perhitungan-perhitungan tersebut dapat dilakukan dengan lebih mudah.

Kata Kunci: kriptografi, protokol perjanjian kunci, ring non-komutatif, ring endomorfisma, endomorfisma grup, grup unit.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Hakikat manusia adalah makhluk sosial yang membutuhkan komunikasi untuk saling berinteraksi dan menyebarkan pesan. Sebagaimana dijelaskan dalam Al-Quran surat An-Nisaa' ayat 83,

وَإِذَا جَآءَهُمْ أَمْرٌ مِّنَ ٱلْأَمْنِ أَوِ ٱلْخَوْفِ أَذَاعُوا۟ بِهِۦ ۖ وَلَوْ
رَدُّوهُ إِلَى ٱلرَّسُولِ وَإِلَىٰٓ أُو۟لِى ٱلْأَمْرِ مِنْهُمْ لَعَلِمَهُ ٱلَّذِينَ يَسْتَنۢبِطُونَهُۥ
مِنْهُمْ ۗ وَلَوْلَا فَضْلُ ٱللَّهِ عَلَيْكُمْ وَرَحْمَتُهُۥ لَٱتَّبَعْتُمُ ٱلشَّيْطَٰنَ إِلَّا
قَلِيلًا ﴿٨٣﴾

yang artinya, "*Dan apabila datang kepada mereka suatu berita tentang keamanan ataupun ketakutan, mereka lalu menyiarkannya. Dan kalau mereka menyerahkan kepada Rasul dan Ulil Amri di antara mereka, tentulah orang-orang yang ingin mengetahui kebenarannya (akan dapat) mengetahuinya dari mereka (Rasul dan Ulil Amri). Kalau tidaklah karena karunia dan rahmat Allah kepada kamu, tentulah kamu mengikut syaitan, kecuali sebagian kecil saja (di antara kamu)".*

Salah satu media komunikasi adalah media tulis (buku), sebagaimana dijelaskan di dalam Al-Quran surat Al-'Alaq ayat 1-5,

ٱقْرَأْ بِٱسْمِ رَبِّكَ ٱلَّذِى خَلَقَ ﴿١﴾ خَلَقَ ٱلْإِنسَٰنَ مِنْ عَلَقٍ ﴿٢﴾

اقْرَأْ وَرَبُّكَ الْأَكْرَمُ ﴿٣﴾ الَّذِي عَلَّمَ بِالْقَلَمِ ﴿٤﴾

عَلَّمَ الْإِنسَانَ مَا لَمْ يَعْلَمْ ﴿٥﴾

yang artinya, "*Bacalah dengan (menyebut) nama Tuhanmu Yang menciptakan. Dia telah menciptakan manusia dari segumpal darah. Bacalah, dan Tuhanmulah Yang Maha Pemurah. Yang mengajar (manusia) dengan perantara kalam. Dia mengajar kepada manusia apa yang tidak diketahuinya".* Pengertian kalam disini adalah sesuatu yang ditulis seperti dijelaskan pada surat Al-Qalam ayat 1,

نٓ وَالْقَلَمِ وَمَا يَسْطُرُونَ ﴿١﴾

yang artinya, "*Nun, demi kalam dan apa yang mereka tulis".*

Media komunikasi terus berkembang seiring dengan perkembangan arus globalisasi. Salah satunya adalah internet. Sejauh apapun jarak dan perbedaan waktu, komunikasi melalui internet dapat dilakukan dengan mudah dan murah. Namun perlu diwaspadai bahwa internet maupun selular tidak menjamin keamanan dalam berkomunikasi, contohnya adalah adanya resiko penyadapan dimana informasi yang dikirimkan oleh pengirim kepada penerima dapat diketahui oleh pihak lain. Peristiwa penyadapan pernah terjadi di Indonesia pada tahun 2013 yaitu penyadapan informasi militer oleh Australia terhadap Bapak Susilo Bambang Yudhoyono yang saat itu menjabat sebagai Presiden RI.

Penyadapan tentunya sangat merugikan terlebih jika informasi yang disadap merupakan informasi penting atau informasi rahasia. Salah satu solusi untuk

mengatasi keamanan informasi dipelajari dalam ilmu kriptografi. Kriptografi merupakan suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data (Menezes, dkk, 1996: 4). Kriptografi memberikan solusi dalam pengamanan pesan yaitu melalui proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah pesan asli (plainteks) menjadi kode yang sulit dimengerti (cipherteks). Dekripsi adalah proses sebaliknya yaitu mengubah kode yang sulit dimengerti (cipherteks) menjadi pesan asli (plainteks). Kedua proses tersebut memerlukan suatu kunci rahasia yang disepakati bersama. Namun akan terjadi masalah jika kunci rahasia ditukarkan pada jalur yang tidak aman, sehingga diperlukan skema pengamanan kunci rahasia yaitu protokol perjanjian kunci.

Protokol perjanjian kunci pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Protokol perjanjian kunci Diffie-Hellman sudah terkenal luas dan merupakan konsep yang sederhana yaitu didasarkan pada masalah logaritma diskrit pada grup siklik (grup komutatif). Namun protokol dengan struktur aljabar komutatif dinilai masih lemah apalagi adanya ancaman dari komputer kuantum di masa depan, hal ini membuat beberapa peneliti mengembangkan protokol perjanjian kunci dengan menggunakan struktur aljabar non-komutatif, diantaranya adalah :

1. Myasnikov, dkk (2008) menyelidiki suatu masalah konjugasi pada suatu grup non-komutatif.
2. M.Zaki Riyanto (2011) meneliti penggunaan grup non-komutatif ($GL_n(\mathbb{Z}_p)$) yaitu matriks atas lapangan $\mathbb{Z}_p$ dengan p adalah bilangan

prima, dengan keamanan kunci rahasianya diletakkan pada masalah konjugasi.

3. Climent, dkk (2012) mengembangkan protokol perjanjian kunci berdasarkan masalah dekomposisi simetris atas ring-non komutatif $End\ (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ yang kemudian dikaji oleh Fadhil Andika Rahman (2015).
4. Agustin Rahayuningsih (2015) mengembangkan protokol perjanjian kunci berdasarkan masalah konjugasi pada matriks atas lapangan hingga.

Berdasarkan penelitian-penelitian tersebut penulis tertarik menyelesaikan masalah protokol perjanjian kunci berdasarkan masalah konjugasi pada grup unit atas ring $End\ (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

1.2. Batasan Masalah

Batasan masalah dalam suatu penelitian diperlukan agar obyek yang dibahas tidak meluas dan tetap terfokus. Berdasarkan latar belakang masalah di atas, tugas akhir ini akan difokuskan untuk membahas prosedur dalam pembuatan kunci rahasia menggunakan protokol perjanjian kunci berdasarkan masalah konjugasi pada grup unit atas ring non-komutatif $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$. Setelah diperoleh kunci rahasia, penulis akan memberikan contoh proses enkripsi dan dekripsi pesan menggunakan algoritma kriptografi simetris yaitu kombinasi *playfair cipher* dan *Hill cipher*. Diberikan pula perhitungan dalam pembuatan kunci rahasia menggunakan protokol perjanjian kunci dan proses enkripsi-dekripsi menggunakan *Hill cipher* melalui program MAPLE 18.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diuraikan, maka dapat dirumuskan permasalahan sebagai berikut :

1. Bagaimana konsep protokol perjanjian kunci pada kriptografi simetris dan bagaimana konsep aljabar yang melandasinya?
2. Bagaimana cara mendapatkan kunci rahasia menggunakan protokol perjanjian kunci pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ yang keamanannya diletakkan pada masalah konjugasi?
3. Bagaimana proses perhitungan enkripsi dan dekripsi menggunakan kombinasi *playfair cipher* dan *Hill cipher* atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$?
4. Bagaimana perhitungan protokol perjanjian kunci dan proses enkripsi-dekripsi pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dengan menggunakan program MAPLE?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Mengkaji tentang konsep protokol perjanjian kunci pada sistem kriptografi simetris dan konsep aljabar yang melandasinya.
2. Mengkaji tentang cara mendapatkan kunci rahasia menggunakan protokol perjanjian kunci pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ yang keamanannya diletakkan pada masalah konjugasi.
3. Mengkaji proses perhitungan enkripsi dan dekripsi menggunakan *playfair cipher* dan *Hill cipher* atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.

4. Mengkaji perhitungan protokol perjanjian kunci dan proses enkripsi-dekripsi pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dengan menggunakan program MAPLE.

1.5. Manfaat penelitian

Penelitian ini diharapkan dapat memberikan manfaat, diantaranya adalah sebagai berikut :

1. Memberikan pengetahuan tentang pembuatan kunci rahasia dengan menggunakan protokol perjanjian kunci berdasarkan masalah konjugasi pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.
2. Memberikan pengetahuan tentang perhitungan enkripsi dan dekripsi menggunakan kombinasi *playfair cipher* dan *Hill cipher* atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.
3. Memberi kemudahan untuk melakukan perhitungan protokol perjanjian kunci dan proses enkripsi serta dekripsi pada grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dengan menggunakan program MAPLE.

1.6. Tinjauan pustaka

Referensi yang digunakan dalam tugas akhir ini diantaranya adalah jurnal berjudul *Key Exchange Protocol over non-commutative Rings. The Case of* $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ oleh Climent, dkk (2012). Jurnal tersebut memaparkan pembuatan kunci rahasia menggunakan protokol perjanjian kunci atas ring non-komutatif dimana tingkat keamanannya diletakkan pada masalah dekomposisi simetris. Protokol ini menggunakan polinomial atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dengan operasi penjumlahan dan perkalian. Jurnal ini juga pernah dikaji oleh Fadhil

Andika Rahman (2015) dalam tugas akhirnya yang berjudul *Protokol Pertukaran Kunci berdasarkan Masalah Dekomposisi Simetris atas Ring Non-Komutatif* $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.

Selain referensi di atas, penulis juga menggunakan tinjauan pustaka sebuah jurnal berjudul *Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-Komutatif* yang ditulis oleh M.Zaki Riyanto (2011). Jurnal tersebut memperkenalkan pembuatan kunci rahasia dengan menggunakan protokol perjanjian kunci pada grup non-komutatif. Tingkat keamanan pada konsep ini diletakkan pada penyembunyian subgrup komutatif dan masalah konjugasi. Jurnal ini merupakan pengembangan dari protokol perjanjian kunci Diffie-Hellman yang tingkat keamanannya diletakkan pada masalah diskrit atas grup siklik.

Referensi lain yang penulis gunakan untuk menyusun tugas akhir ini yaitu buku-buku tentang Struktur Aljabar. Di antaranya adalah buku yang ditulis oleh Raisinghania, Aggarwal (1980), Buchmann (2000), Clark (2001), Dummit, dkk (2004), Hoffsten, dkk (2000), Menezes, dkk (1996) dan Malik, dkk (2007).

1.7. Metode Penelitian

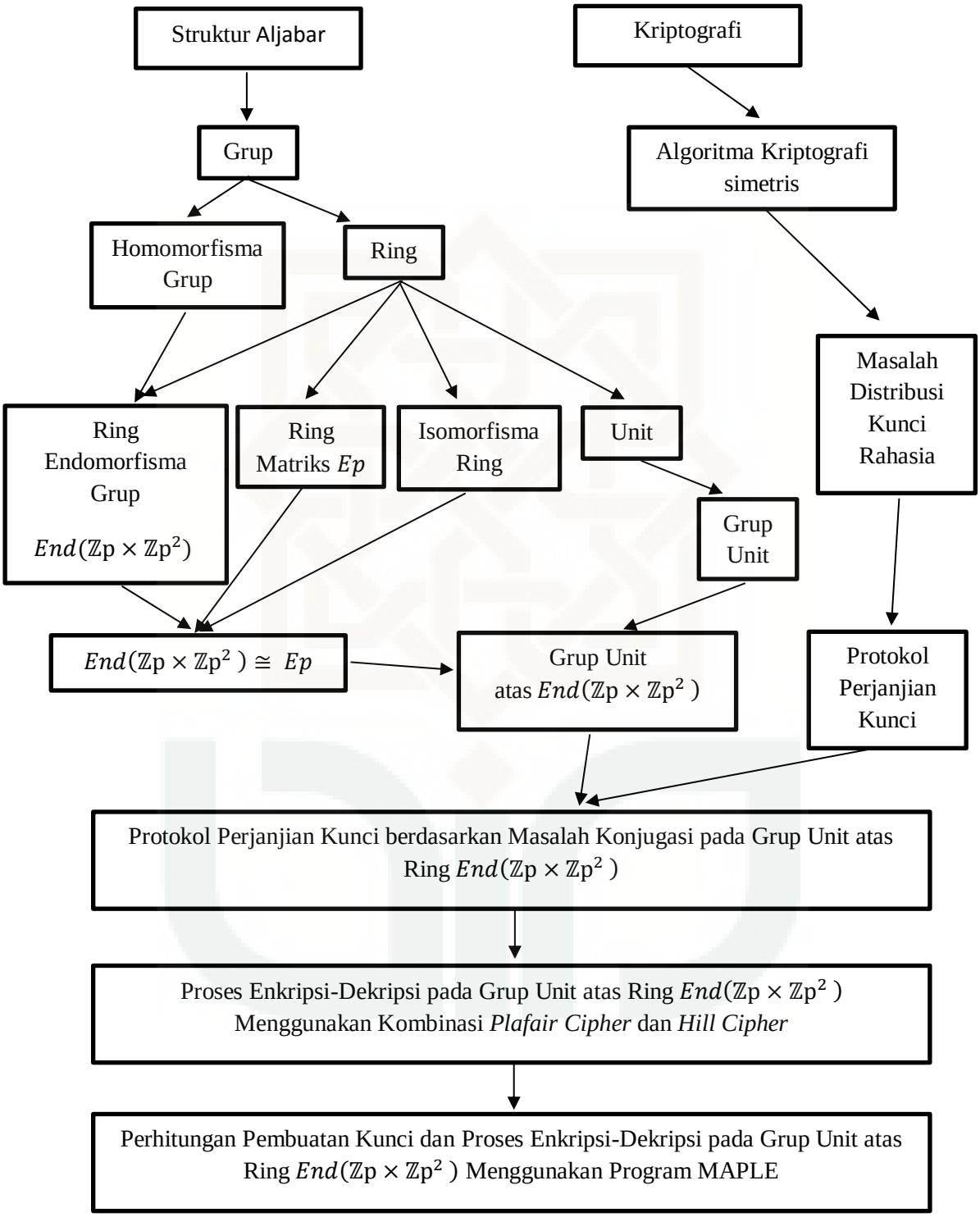
Metode penelitian yang digunakan adalah metode literatur yaitu pengambilan data-data penelitian berupa definisi, teorema dan materi dari referensi buku dan jurnal. Secara umum, protokol perjanjian kunci menggunakan konsep kriptografi dan konsep struktur aljabar yang melandasinya.

Pembahasan awal dari tugas akhir ini adalah konsep kriptografi. Penulis menggunakan kriptografi simetris, dimana untuk proses enkripsi dan dekripsinya menggunakan kunci rahasia yang sama. Permasalahan dari penggunaan kriptografi

simetris pada jalur komunikasi yang tidak aman adalah masalah distribusi kunci rahasia. Solusi untuk mengatasinya yaitu dengan protokol perjanjian kunci. Materi protokol perjanjian kunci yang diberikan antara lain protokol perjanjian kunci Diffie-Hellman, protokol perjanjian kunci berdasarkan masalah konjugasi pada grup non-komutatif $(GL_n(F))$ dan protokol perjanjian kunci berdasarkan masalah konjugasi pada grup unit atas ring non-komutatif $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.

Konsep struktur aljabar diperlukan untuk menjelaskan grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$. Sebelumnya diberikan materi-materi teori bilangan yang berkaitan dengan konsep aljabar yang akan digunakan. Pertama, penulis akan menjelaskan materi tentang grup. Salah satunya adalah pembentukan grup $\mathbb{Z}_p$ x $\mathbb{Z}_{p^2}$ melalui *direct product.* Kemudian penulis menjelaskan materi homomorfisma grup dan ring, hingga terbentuk ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$. Pada materi ring dijelaskan tentang ring matriks E_p yang merupakan matriks representasi dari ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$, isomorfisma ring, unit dan grup unit. Penulis mencari unit pada ring E_p dan membentuk grup unit atas ring E_p. Karena E_p isomorfis dengan ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ maka diperoleh grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$.

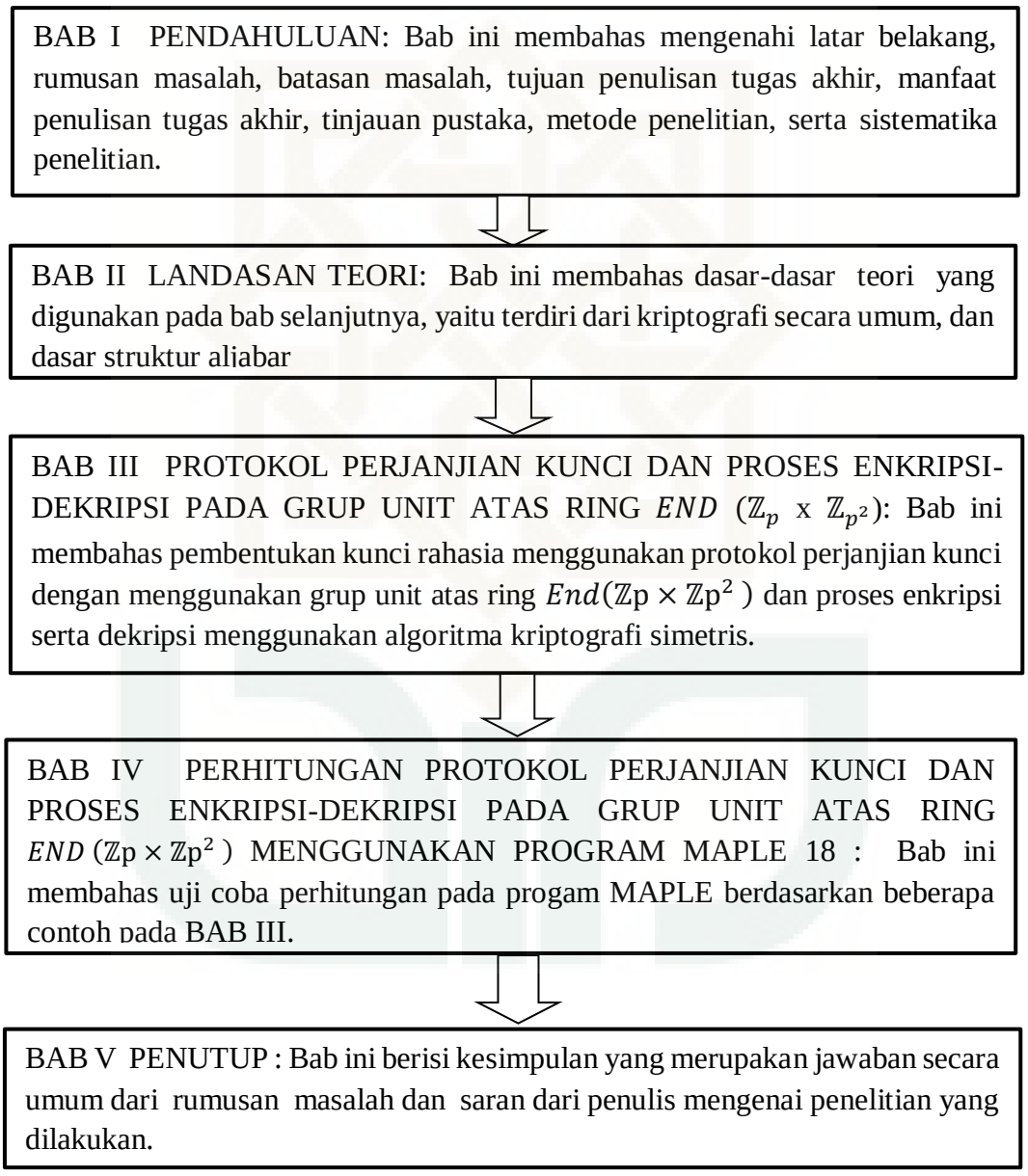
Berdasarkan konsep-konsep yang dijelaskan, penulis akan mengembangkan penelitian dengan mengimplementasikan masalah konjugasi pada protokol perjanjian kunci menggunakan grup unit atas ring $End\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$. Kunci rahasia yang diperoleh kemudian digunakan untuk proses enkripsi-dekripsi menggunakan kombinasi *playfair cipher* dan *Hill cipher.* Gambaran alur penelitian dari tugas akhir ini akan dijelaskan pada bagan sebagai berikut :



Gambar 1.1. Alur Penelitian

1.8. Sistematika Penulisan

Tugas akhir ini dibagi menjadi lima bab yang disusun secara runtun dan sistematis. Berikut ini rincian masing-masing bab yang akan dijelaskan secara umum.



Gambar 1.2. Alur Sistematika Penulisan

BAB V

PENUTUP

5.1. Kesimpulan

Kriptografi simetris memerlukan suatu kunci rahasia yang disepakati bersama. Namun akan terjadi masalah jika kunci rahasia ditukarkan pada jalur komunikasi yang tidak aman, sehingga diperlukan skema pengamanan kunci rahasia yaitu protokol perjanjian kunci. Konsep protokol perjanjian kunci pertama kali diperkenalkan oleh Diffie-Hellman. Dimisalkan pihak-pihak yang berkomunikasi adalah Alice dan Bob. Pertama Alice dan Bob mempublikasikan grup siklik G dan elemen pembangun $g \in G$. Kemudian Alice memilih bilangan $a \in \mathbb{N}$ dan menghitung $A = g^a$ lalu mengirimkannya kepada Bob. Sementara Bob memilih bilangan $b \in \mathbb{N}$ dan menghitung $B = g^b$ lalu mengirimkannya kepada Alice. Selanjutnya Alice dan Bob masing-masing menghitung $A' = B^a$ dan $B' = A^b$ sehingga diperoleh kunci yang sama yaitu K. Secara garis besar konsep aljabar yang melandasi pembentukan kunci rahasia ini adalah materi tentang grup dan ring serta didukung dengan beberapa teori bilangan.

Protokol perjanjian kunci yang dikembangkan pada tugas akhir ini menggunakan ring non-komutatif $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ yaitu terdiri dari endomorfisma-endomorfisma grup $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$. Diberikan ring E_p sebagai matriks representasi dari ring $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ dan dibentuk grup unit atas ring E_p yaitu $U(E_p)$. Diketahui bahwa ring E_p isomorfis dengan ring $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, sehingga $U(E_p)$ dapat disebut sebagai grup unit atas ring $End\,(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Keamanan kunci rahasia pada protokol perjanjian kunci ini akan diletakkan pada masalah konjugasi. Dimisalkan pihak-pihak yang berkomunikasi adalah Alice dan Bob. Pertama Alice dan Bob mempublikasikan $U(E_p)$ dan memilih $W \in U(E_p)$ serta H subgrup komutatif dari $U(E_p)$. Kemudian Alice memilih $A \in H$ dan menghitung $X = A^{-1}WA$ lalu mengirimkan X kepada Bob. Sementara Bob memilih $B \in H$ dan menghitung $Y = B^{-1}WB$ lalu mengirimkan Y kepada Alice. Selanjutnya Alice dan Bob masing-masing menghitung $K_A = A^{-1}YA$ dan $K_B = B^{-1}XB$ sehingga diperoleh kunci rahasia yang sama yaitu $K = K_A = K_B$.

Kunci rahasia yang telah diperoleh kemudian digunakan dalam proses enkripsi dan dekripsi menggunakan kombinasi *playfair cipher* dan *Hill cipher*. Proses enkripsi pertama menggunakan *playfair cipher* yang terdiri dari bebrapa tahap yaitu pemisahan plainteks menjadi digraf, pembentukan tabel kunci, dan enkripsi digraf berdasarkan tabel kunci. Cipherteks yang dihasilkan dari proses ini kemudian dienkripsi kembali menggunakan *Hill cipher*, yaitu menghitung $e_K(P) = PK$ dengan P adalah cipherteks dari proses *playfair cipher* yang telah diubah ke dalam bentuk matriks E_p. Proses dekripsi dilakukan kebalikannya. Pertama cipherteks didekripsi menggunakan *Hill cipher*, yaitu menghitung $d_K(C) = CK^{-1}$ dengan C adalah cipherteks dan K^{-1} adalah invers dari kunci K. Hasil yang diperoleh didekripsi kembali menggunakan *playfair cipher* sehingga diperoleh pesan asli.

Perhitungan dalam pembentukan kunci rahasia menggunakan protokol perjanjian kunci maupun perhitungan dalam proses enkripsi-dekripsi pada grup unit atas ring $End\ (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ diuji coba pada sebuah program komputer yaitu

MAPLE 18. Proses pembentukan kunci rahasia dilakukan sesuai dengan konsep protokol perjanjian kunci. Pertama menginputkan matriks-matriks yang dipublikasikan oleh Alice dan Bob, lalu menghitung kunci rahasia dengan terlebih dahulu mendefinisikan operasi perkalian dan invers pada ring E_p. Hasil yang diperoleh berupa matriks K yang selanjutnya digunakan untuk proses enkripsi-dekripsi. Proses enkripsi-dekripsi yang dilakukan pada MAPLE 18 hanyalah perhitungan matriks pada proses *Hill cipher* saja. Pertama diinputkan matriks P dan K kemudian dihitung $e_K(P) = PK$ dengan terlebih dahulu mendefinisikan operasi perkalian pada E_p. Selanjutnya proses dekripsi yaitu menginputkan matriks C dan menghitung K^{-1}, lalu menghitung $d_K(C) = CK^{-1}$ dengan terlebih dahulu mendefinisikan operasi perkalian pada E_p.

5.2. Saran

Protokol perjanjian kunci yang diperkenalkan oleh Diffie-Hellman didasarkan pada masalah logaritma diskrit pada grup komutatif. Penggunaan grup komutatif dinilai masih lemah karena adanya ancaman komputer kuantum, sehingga diperlukan pengembangan-pengembangan konsep protokol perjanjian kunci menggunakan struktur aljabar non-komutatif.

Tugas akhir ini merupakan salah satu pengembangan protokol perjanjian kunci dengan menggunakan grup unit atas ring non-komutatif yaitu ring $End\ (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Namun penulis belum meneliti tingkat keamanan kunci rahasia yang dihasilkan, sehingga dimungkinkan ada penelitian selanjutnya yang meneliti tingkat keamanan tersebut. Apabila penelitian tersebut berhasil, dan menunjukkan tingkat keamanan kunci rahasia yang baik maka hasil penelitian dari tugas akhir

ini dimungkinkan dapat diimplementasikan dalam media komunikasi sebagai program pengamanan pesan.

Protokol perjanjian kunci adalah skema yang digunakan untuk membuat kunci rahasia pada jalur komunikasi yang tidak aman. Namun akan terjadi masalah jika terdapat pihak ketiga yang berhasil mengetahui kunci rahasia tersebut dan mengirimkan kunci rahasia palsu kepada pihak-pihak yang berkomunikasi. Oleh karena itu, diperlukan sebuah skema untuk memastikan bahwa kunci rahasia yang dikirim adalah benar dari pihak yang berkomunikasi. Skema ini disebut dengan protokol otentikasi kunci. Penulis berharap ada penelitian lanjutan tentang protokol otentikasi kunci menggunakan grup unit atas ring $End\ (\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Penulis menggunakan kombinasi *playfair cipher* dan *Hill cipher* dalam proses enkripsi dan dekripsi pesan. Pengkombinasian dua buah *cipher* atau lebih ditujukan untuk meningkatkan keamanan pesan rahasia. Namun seperti telah dijelaskan pada bab III bahwa *playfair cipher* memiliki beberapa kekurangan, diantaranya adalah *polygram playfair cipher* tidak cukup besar sehingga kurang aman karena hanya menggunakan dua huruf. Selain itu, meski *playfair cipher* sulit dipecahkan dengan menggunakan analisis frekuensi relatif huruf-huruf, namun *playfair cipher* dapat dipecahkan dengan menggunakan analisis yang serupa yaitu dengan pasangan huruf. Oleh karena itu, penelitian pada tugas akhir ini dapat dikembangkan dengan menggunakan algoritma kriptografi yang lain. *Cipher* yang digunakan dapat berupa satu *cipher* atau kombinasi beberapa cipher, dengan harapan dapat ditemukan *cipher* yang lebih efektif dan aman.

Perhitungan dalam pembuatan kunci rahasia maupun perhitungan dalam proses enkripsi-dekripsi telah dilakukan dengan menggunakan program MAPLE 18. Namun penggunaan program ini masih relatif sederhana karena perintah-perintah yang digunakan masih sedikit. Program ini dimungkinkan dapat dikembangkan dengan menggunakan perintah-perintah yang lebih bervariasi.

Demikian saran-saran dari penulis. Semoga tugas akhir ini dapat menjadi inspirasi bagi penelitian-penelitian selanjutnya terutama dalam bidang kriptografi maupun bidang aljabar.

DAFTAR PUSTAKA

Aggarwal, R.S., Raisinghania, M.D., 1980, *Modern Algebra,* Ram Nagar, New Delhi

Ariyus, D., 2008, *Pengantar Ilmu Kriptografi*, Penerbit Andi, Yogyakarta

Brown, W.C., 1993, *Matrices Over Commutative Ring,* Marcel Dekker, Inc, New York, USA

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

Clark, W.E., 2001, *Elementary Abstract Algebra,* University of South Florida

Climent, dkk, 2012, *Key Exchange Protocol over Noncommutative Rings. The Case of* $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, Universitat d'Alacant

Climent, dkk, 2010, *On The Arithmatic of The Endomorphisms Ring* $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, Universitat d'Alacant

Dummit, dkk, 2003, *Abstract Algebra*, Jhon Wiley and Sons, Inc, USA.

Goodman, F.M., 2006, *Algebra Abstract and Concrete,* Semisimple Press, Iowa City, IA

Grillet, P.A., 2006, *Abstract Algebra,* Springer, New York, USA

Hoffsten dkk, 2000, *An Introduction to Mathematical Cryptography,* Springer, USA

Malik, D.S., dkk, 2007, *An Introduction to Abstract Algebra*, USA.

Menezes, dkk, 1996, *Handbook of Applied Cryptography,* CRC Press, Inc., USA.

Myasnikov, dkk, 2008, *Group Based Cryptography*, Birkhauser Verlag, Berlin.

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

LAMPIRAN

Lampiran 1. TABEL ASCII

DEC	OCT	HEX	BIN	CHAR
1	1	1	00000001	
2	2	2	00000010	┐
3	3	3	00000011	└
4	4	4	00000100	┘
5	5	5	00000101	│
6	6	6	00000110	─
7	7	7	00000111	•
8	10	8	00001000	◘
9	11	9	00001001	
10	12	A	00001010	
11	13	B	00001011	♂
12	14	C	00001100	♀
13	15	D	00001101	
14	16	E	00001110	♫
15	17	F	00001111	☼
16	20	10	00010000	┼
17	21	11	00010001	◄
18	22	12	00010010	↕
19	23	13	00010011	‼
20	24	14	00010100	¶
21	25	15	00010101	┴
22	26	16	00010110	┬
23	27	17	00010111	┤
24	30	18	00011000	↑
25	31	19	00011001	├
26	32	1A	00011010	→
27	33	1B	00011011	←
28	34	1C	00011100	
29	35	1D	00011101	
30	36	1E	00011110	
31	37	1F	00011111	
32	40	20	00100000	
33	41	21	00100001	!
34	42	22	00100010	"
35	43	23	00100011	#
36	44	24	00100100	$
37	45	25	00100101	%
38	46	26	00100110	&
39	47	27	00100111	'
40	50	28	00101000	(
41	51	29	00101001	)
42	52	2A	00101010	*

DEC	OCT	HEX	BIN	CHAR
43	53	2B	00101011	+
44	54	2C	00101100	,
45	55	2D	00101101	-
46	56	2E	00101110	.
47	57	2F	00101111	/
48	60	30	00110000	0
49	61	31	00110001	1
50	62	32	00110010	2
51	63	33	00110011	3
52	64	34	00110100	4
53	65	35	00110101	5
54	66	36	00110110	6
55	67	37	00110111	7
56	70	38	00111000	8
57	71	39	00111001	9
58	72	3A	00111010	:
59	73	3B	00111011	;
60	74	3C	00111100	<
61	75	3D	00111101	=
62	76	3E	00111110	>
63	77	3F	00111111	?
64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U

DEC	OCT	HEX	BIN	CHAR
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`
97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y
122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	▯

DEC	OCT	HEX	BIN	CHAR
128	200	80	10000000	€
129	201	81	10000001	
130	202	82	10000010	‚
131	203	83	10000011	ƒ
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž
159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª

DEC	OCT	HEX	BIN	CHAR
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	-
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á
194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Ð
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô

DEC	OCT	HEX	BIN	CHAR
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß
224	340	E0	11100000	à
225	341	E1	11100001	á
226	342	E2	11100010	â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í
238	356	EE	11101110	î
239	357	EF	11101111	ï
240	360	F0	11110000	ð
241	361	F1	11110001	ñ
242	362	F2	11110010	ò
243	363	F3	11110011	ó
244	364	F4	11110100	ô
245	365	F5	11110101	õ
246	366	F6	11110110	ö
247	367	F7	11110111	÷
248	370	F8	11111000	ø
249	371	F9	11111001	ù
250	372	FA	11111010	ú
251	373	FB	11111011	û
252	374	FC	11111100	ü
253	375	FD	11111101	ý
254	376	FE	11111110	þ
255	377	FF	11111111	ÿ

CURRICULUM VITAE

Nama	: Laila Marthatilova
Tempat, tanggal lahir	: Wonogiri, 5 Maret 1994
Jenis Kelamin	: Perempuan
Alamat	: Patuk Kidul, RT 01/RW 03, Ds. Baturetno, Kec. Baturetno, Kab. Wonogiri, Jawa Tengah
No. HP	: +6289520297073
E-mail	: marthatilovalaila@gmail.com

Riwayat Pendidikan

2000-2006	: SD Negeri VI Baturetno
2006-2009	: SMP Negeri I Baturetno
2009-2012	: SMA Negeri I Baturetno
2012-2016	: Prodi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta