GRUP *NILPOTENT* DAN APLIKASINYA DALAM KRIPTOGRAFI (MOR *CRYPTOSYSTEM*)

SKRIPSI

Untuk Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1

Program Studi Matematika

Diajukan oleh:

Erna Fitriana Rohmawati

12610032

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI 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 : Erna Fitriana Rohmawati
NIM : 12610032
Judul Skripsi : Grup Nilpotent dan Aplikasinya dalam Kriptografi (*MOR Cryptosystem*)

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 dimunaqosyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 26 Agustus 2016

Pembimbing I

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

Pembimbing II

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

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/3071/2016

Skripsi/Tugas Akhir dengan judul : Grup *Nilpotent* dan Aplikasinya dalam Kriptografi (MOR *Cryptosystem*)

Yang dipersiapkan dan disusun oleh :
Nama : Erna Fitriana Rohmawati
NIM : 12610032
Telah dimunaqasyahkan pada : 30 Agustus 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

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

Yogyakarta, 2 September 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Erna Fitriana Rohmawati

NIM : 12610032

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi ini merupakan hasil pekerjaan penulis sendiri dan sepanjang pengetahuan penulis tidak berisi materi yang dipublikasikan atau ditulis orang lain, dan atau telah digunakan sebagai persyaratan penyelesaian Tugas Akhir di Perguruan Tinggi lain, kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 26 Agustus 2016

Yang menyatakan,

Erna Fitriana Rohmawati

NIM. 12610032

HALAMAN PERSEMBAHAN

Penelitian ini, penulis persembahkan teruntuk :

- Fakultas Sains dan Teknologi, khususnya jurusan Matematika UIN Sunan Kalijaga Yogyakarta.
- Dosen-dosen pembimbing, Ibu Khurul dan Bapak Zaki yang selalu membimbing dan memberikan inspirasi.
- Bapak dan Ibu tercinta yang selalu mendoakan, mencurahkan kasih sayang serta mendidik penulis sampai detik ini.
- Adek-adekku tercinta Anna dan Afiq, yang selalu memberikn semangat dan senyuman.
- Noor Kholish, S. I.Kom terimakasih semangat yang telah diberikan, semoga Allah SWT menempatkan keridloan dalam setiap perjalanan hidup kita.
- Teman – teman seperjuanganku Helvi, Uun, Laila, Yudi, Dani dan tak lupa teman-teman matematika 2012, terimakasih atas dukungan dan semangatnya.

MOTTO

"*Sukses itu*: 99.99% *kerja keras dan* 0.01% *bakat*"

(Thomas Alfa Edison)

"*Barang siapa menempuh jalan untuk mencari ilmu, Allah akan memudahkan baginya jalan ke surga, sesungguhnya para malaikat menaungkan sayap-sayapnya kepada orang yang menuntut ilmu karena senang terhadap apa yang diperbuat*".

(HR. Muslim)

"*Belajarlah kalian ilmu untuk ketentraman dan ketenangan serta rendah hatilah pada orang yang kamu belajar darinya*"

(HR. At-Tabrani)

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Segala puji bagi Allah SWT yang telah memberikan rahmat, taufik, dan hidayah-Nya, sehingga penulis mampu meyelesaikan penulisan skripsi berjudul *"Grup Nilpotent dan Aplikasinya dalam Kriptografi (MOR Cryptosystem)"* 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.

Penulis menyadari bahwa proses penulisan skripsi ini tidak terlepas dari dukungan, motivasi, kerjasama dan bimbingan dari berbagai pihak. Oleh karena itu, ucapan terimakasih penulis sampaikan kepada:

1. Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Dr. M. Wakhid Musthofa, M.Sc., selaku Ketua Prodi program studi Matematika.
3. Dr. Hj. Khurul Wardati, M.Si., dan M. Zaki Riyanto, S.Si., M.Sc. selaku pembimbing yang telah memberikan ilmu, arahan serta dukungan sehingga penulisan skripsi ini dapat terselesaikan.

4. Bapak dan Ibu ku tercinta yang telah memberikan doa restu dan kasih sayangnya tiada henti untuk penulis dan selalu memprioritaskan pendidikan untuk putri-putrinya.
5. Semua guru dan dosen jurusan matematika untuk arahan dan ilmu yang telah diberikan, serta bimbingan kepada penulis.
6. Noor Kholish,S.I.Kom yang selalu memberikan dukungan penuh, sehingga penelitian ini terselesaikan.
7. Teman-teman Matematika 2012, Helvi, Laila, Uun, Yudi, Dani, serta teman-teman matematika 2011 yang tidak bisa penulis sebutkan satu persatu yang senantiasa menjadi teman dan keluarga dikampus.

Wassalamu'alaikum Wr.Wb

Yogyakarta, 26 Agustus 2016

Penulis,

Erna Fitriana Rohmawati
NIM. 12610032

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ARTI LAMBANG DAN SINGKATAN

$A \times B$: perkalian kartesius dari A dan B

(x, y) : pasangan berurutan dari x, y

xRy : x berelasi R dengan y

$\sim$: ekuivalensi

$[x]$: kelas ekuivalensi yang memuat x

$m|n$: m membagi habis n

$m \nmid n$: m tidak membagi habis n

$\mathbb{Z}$: himpunan bilangan bulat

$\mathbb{Z}^+$: himpunan bilangan bulat positif

$\mathbb{Z}_p$: himpunan bilangan bulat modulo prima

$\mathbb{Z}_p{}^*$: grup penggandaan modulo prima

$a \in G$: a elemen dari G

$b \notin G$: b bukan elemen dari G

$\forall$: untuk setiap (kuantor universal)

$\exists$: terdapat (kuantor eksistensial)

S_n : grup permutasi dari himpunan $\{1,2,\ldots,n \in \mathbb{Z}^+\}$

D_n : grup dihedral dari himpunan dengan $n \geq 3$

$\emptyset$: himpunan kosong

■ : akhir dari suatu pembuktian

$\wedge$: dan

$\vee$: atau

$A \cup B$: A gabungan B, $A \cup B = \{x | x \in A \wedge x \in B\}$

$A \cap B$: A irisan B, $A \cap B = \{y | y \in A \vee y \in B\}$

$\subseteq$: subset (himpunan bagian)

$A \subseteq B$: setiap elemen di A juga merupakan elemen di B

$|G|$: order dari grup G

$\circ(x)$: order dari elemen x

$H \trianglelefteq G$: H subgrup normal dari G

$\Leftrightarrow$ **:** Biimplikasi atau jika dan hanya jika

$\Rightarrow$ **:** "berakibat" atau bukti implikasi kea rah kanan

$\Leftarrow$ **:** bukti implikasi kearah kiri

$< a >$: subgrup yang dibangun oleh elemen a

G/N : grup factor G modulo N

Hg : koset kanan dari H dengan koset representative g

gH : koset kiri dari H dengan koset representative g

$|H|||G|$: order grup H membagi habis order grup G

$\phi: G \to G'$: ϕ suatu pemetaan dari grup G ke grup G'

$[G:H]$: indeks dari H dalam G

$G \cong G'$: G isomorfis dengan G'

$C(a)$: centralizer elemen a

$N_G(H)$: normalizer dari H dalam G

$Z(G)$: center dari G

$Cl(a)$: kelas konjugasi dari a

$Z_n(G)$: center ke-n dari G

$UT(n, G)$: grup matriks upper triangular berukuran $n \times n$ atas grup berhingga G

GRUP *NILPOTENT* DAN APLIKASINYA DALAM KRIPTOGRAFI

(MOR *CRYPTOSYSTEM*)

Oleh: Erna Fitriana Rohmawati

Abstrak

Grup *nilpotent* adalah grup dimana dengan menggunakan *central series* dari grup, sehingga dapat ditemukan suatu indeks, misalkan n, dimana *center* dengan indeks n dari grup tersebut adalah grup itu sendiri. Teorema-teorema dari grup nilpotent akan memunculkan beberapa sifat dan contoh grup *nilpotent*, diantaranya yaitu grup dihedral dan grup matriks *upper triangular* yang merupakan grup *nilpotent*.

Perkembangan teknologi dan komunikasi pada era saat ini sangat pesat sehingga banyak ditemukan adanya interkoneksi antara aljabar dengan ilmu teknologi dan komunikasi. Salah satunya yaitu dalam bidang penyandian pesan. Kenyataanya suatu grup dapat diaplikasikan ke dalam suatu sistem penyandian pesan yang dinamakan kriptografi.

Sistem kriptografi yang dipakai dalam penelitian ini adalah sistem kriptografi MOR dengan automorfisma grup. Sistem kriptografi ini lebih dikenal sebagai generalisasi dari sistem kriptografi ElGamal. Bedanya adalah pada grup yang digunakan. Jika pada sistem kriptografi ElGamal menggunakan grup siklik, sedangkan pada sistem kriptografi MOR menggunakan sebarang grup berhingga yang tidak harus siklik. Keduanya mempunyai kesamaan dalam tingkat keamanannya yaitu berdasarkan masalah logaritma diskrit.

Penelitian ini akan menunjukkan bahwa grup dihedral dan grup matriks upper triangular yang keduanya merupakan grup *nilpotent* nantinya dapat digunakan sebagai aplikasi dalam sistem kriptografi MOR. Kedua grup tersebut akan digunakan dalam proses enkripsi dan dekripsi pada penyandian pesan. Uji coba dan implementasi dari penelitian ini akan menggunakan program MAPLE.

Kata Kunci : grup *nilpotent*, *central series*, grup dihedral, grup matriks *upper triangular*, sistem kriptografi ElGamal, sistem kriptografi MOR, logaritma diskrit.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Ilmu matematika terutama aljabar adalah ilmu penting yang mendasari berbagai ilmu lain, seperti ilmu ekonomi, fisika, kimia, dan lain sebagainya. Aljabar pertama kali diperkenalkan pada era kejayaan Islam oleh Alkhawarizmi yang dikenal sebagai bapak aljabar. Aljabar dalam matematika dapat dikategorikan menjadi beberapa macam yaitu: aljabar dasar, aljabar abstrak, aljabar linear, aljabar universal, dan aljabar komputer.

Salah satu yang dipelajari oleh penulis pada perkuliahan adalah aljabar abstrak. Aljabar abstrak merupakan bidang matematika yang mempelajari struktur aljabar, seperti grup, ring, lapangan (*field*), modul, ruang vektor, dan aljabar lapangan. Salah satu yang dipelajari dari aljabar abstrak adalah teori grup. Grup adalah suatu himpunan tak kosong G yang dilengkapi dengan operasi biner dan memenuhi aksioma-aksioma dalam grup. Materi teori grup yang diperoleh penulis selama perkuliahan adalah mengenai konsep grup, grup permutasi, grup siklik, subgrup, koset, grup faktor, subgrup normal, *center* grup, dan homomorfisma. Sebuah ayat dalam Al-Quran pada surat An-Nur telah terlebih dahulu menjelaskan tentang adanya teori himpunan yang merupakan bagian dari ilmu aljabar abstrak.

وَٱللَّهُ خَلَقَ كُلَّ دَآبَّةٍ مِّن مَّآءٍ ۖ فَمِنْهُم مَّن يَمْشِى عَلَىٰ بَطْنِهِۦ وَمِنْهُم مَّن يَمْشِى عَلَىٰ رِجْلَيْنِ وَمِنْهُم مَّن يَمْشِى عَلَىٰٓ أَرْبَعٍ ۚ يَخْلُقُ ٱللَّهُ مَا يَشَآءُ ۚ إِنَّ ٱللَّهَ عَلَىٰ كُلِّ شَىْءٍ قَدِيرٌ ﴿٤٥﴾

Artinya: "*Dan Allah telah menciptakan semua jenis hewan dari air, maka sebagian dari hewan itu ada yang berjalan di atas perutnya dan sebagian berjalan dengan dua kaki, sedang sebagian (yang lain) berjalan dengan empat kaki. Allah menciptakan apa yang dikehendaki-Nya, sesungguhnya Allah Maha Kuasa atas segala sesuatu*" (QS. An-Nur:45).

Jika suatu grup mempunyai order berhingga maka disebut grup berhingga. Grup berhingga sendiri mencakup dua kategori yaitu grup berhingga komutatif dan grup berhingga non-komutatif. Banyak contoh dari kedua kategori tersebut namun salah satu contoh dari grup berhingga adalah grup *nilpotent* yang membuat penulis tertarik untuk mengkajinya lebih dalam. Salah satu alasan ketertarikan tersebut adalah karena pada saat perkuliahan penulis belum pernah mendapatkan materi tentang grup *nilpotent.*

Materi terkait dengan grup *nilpotent* banyak dikaji pada beberapa literatur. Salah satunya yaitu dari Dummit dan Foote (2004), yang berjudul "*Group Theory*", yang di dalamnya menjelaskan secara rinci grup *nilpotent* dan teorema-teorema dari grup *nilpotent*. Teorema-teorema *nilpotent* ini, akan memunculkan suatu grup yang termasuk dalam grup *nilpotent*. Berdasarkan ketertarikan penulis pada literatur tersebut dan berdasarkan jurnal oleh Ayan Mahalanobis (2005), yang berjudul "*Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Group*", yang menjelaskan tentang adanya aplikasi dari grup *nilpotent* dalam proses penyandian atau lebih dikenal dengan kriptografi. Oleh karena itu, suatu hal yang menarik bagi penulis, jika grup *nilpotent* diaplikasikan dalam

kriptografi pula. Sebelum menjelaskan kriptografi, terlebih dahulu dijelaskan latar belakang penulis menggunakan kriptografi sebagai aplikasi grup *nilpotent.*

Dewasa ini, perkembangan teknologi informasi dan komunikasi sangat pesat sehingga berpengaruh terhadap semua aspek kehidupan manusia, salah satunya dalam proses pengiriman pesan. Seiring dengan kemunculan media-media komunikasi, seperti *gadget* dengan akses internet yang dapat menghubungkan kita dengan setiap orang dimanapun mereka berada. Seiring perkembangan teknologi dan informasi pula, tuntutan akan keamanan atas kerahasiaan pesan informasi juga semakin meningkat. Hal ini dikarenakan lalu lintas informasi yang beredar baik dari media internet ataupun yang lain tidaklah menjamin keamanan.

Berbagai cara telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia. Salah satu cara yang digunakan sekarang adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Berdasarkan hal tersebut, diperlukan adanya ilmu kriptografi yang mempelajari teknik-teknik penyandian suatu pesan dengan algoritma-algoritma tertentu. Sebuah ayat dalam Al-Quran yang menjelaskan terkait dengan ilmu kriptografi dan balasan bagi penyadap yang tertera pada surat Ibrahim ayat 14 yang berbunyi:

وَمَآ أَرۡسَلۡنَا مِن رَّسُولٍ إِلَّا بِلِسَانِ قَوۡمِهِۦ لِيُبَيِّنَ لَهُمۡۖ فَيُضِلُّ ٱللَّهُ مَن يَشَآءُ وَيَهۡدِي مَن يَشَآءُۚ وَهُوَ ٱلۡعَزِيزُ ٱلۡحَكِيمُ ٤

Artinya: “ *Kami tidak mengutus seorang rasul, melainkan dengan bahasa kaumnya, supaya ia dapat memberi penjelasan dengan terang kepada mereka.*

Maka Allah menyesatkan siapa yang Dia kehendaki, dan memberi petunjuk kepada siapa saja yang Dia kehendaki. Dan Dia adalah Tuhan Yang Maha Kuasa lagi Maha Bijaksana" (QS. Ibrahim:14).

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *cryptos* yang berarti rahasia, dan *graphein* yang berarti tulisan. Sehingga kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, Oorcshot, and Vanstone, 1996).

Secara umum, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (Bruce Schneier). Kriptografi memiliki dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan kode dari yang dapat dimengerti (*plainteks*) menjadi sebuah kode yang tidak dimengerti (*cipherteks*), sedangkan proses kebalikannya yaitu mengubah *cipherteks* menjadi *plainteks* disebut dekripsi. Proses enkripsi dan dekripsi membutuhkan suatu kunci rahasia yang harus disepakati oleh kedua pihak yang berkomunikasi.

Salah satu peran kriptografi adalah dalam upaya mengamankan informasi yang bersifat rahasia, baik yang dilakukan secara *off-line* maupun *on-line*. Adanya hal tersebut, hubungan kriptografi dan teknologi informasi adalah pada aplikasinya, yaitu kriptografi bersifat membangun komunikasi yang lebih aman meskipun pada saat tertentu dapat mengurangi kecepatan dalam proses komunikasi.

Suatu skema dalam kriptografi yang dapat digunakan untuk mengatasi masalah pengiriman informasi rahasia tersebut dinamakan protokol perjanjian kunci, yang dalam hal ini diperlukan suatu kunci. Kunci tersebut harus disepakati oleh kedua pihak yang saling bersangkutan dalam pengiriman pesan rahasia karena akan digunakan dalam proses enkripsi dan dekripsi pesan. Ada dua metode algoritma pada kriptografi, yaitu algoritma rahasia dan algoritma kunci.

Metode algoritma rahasia adalah algoritma yang pertama kali dibuat, akan tetapi metode ini tidaklah efisien untuk digunakan dalam komunikasi, sedangkan metode algoritma kunci diciptakan setelah penggunaan metode algoritma rahasia yang mulai dirasa tidak efisien untuk digunakan lagi. Metode ini tidak menumpukan keamanan pada algoritmanya, akan tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Metode algoritma kunci mempunyai tingkat keamanan yang lebih baik dibandingkan dengan algoritma rahasia, hingga sampai sekarang saja algoritma kunci masih digunakan secara luas di internet dan terus dikembangkan untuk memperoleh keamanan yang semakin baik.

Algoritma ElGamal merupakan salah satu dari algoritma kunci yang dikembangkan pertama kali oleh Taher ElGamal pada tahun 1985. Hingga saat ini, algoritma ElGamal masih menjadi metode penyandian, seperti PGP dan GNUPG yang dapat digunakan untuk pengamanan e-mail dan tanda tangan digital. Pada tahun 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard,* sebuah mekanisme penyandian yang berdasar pada algoritma ElGamal. Contoh kecil dari algoritma ElGamal adalah media sosial seperti *Facebook* dan *Wikipedia*.

Sebuah makalah dari Whitfield Diffie dan Martin Hellman yang diterbitkan pada tahun 1976, pertama kali memperkenalkan algoritma kunci publik dengan tingkat keamanan yang didasarkan pada masalah logaritma diskrit pada grup siklik. Metode ini adalah metode pertama untuk menciptakan kunci rahasia yang telah disepakati oleh kedua belah pihak yang saling berkomunikasi dengan jalur yang tidak aman. Konsep yang diperkenalkan oleh Diffie-Hellman tersebut, dalam penelitian ini dikembangkan lebih lanjut yaitu generalisasi ElGamal pada masalah logaritma diskrit dengan struktur aljabar sebarang grup berhingga baik yang komutatif dan non-komutatif agar dapat memberikan keamanan yang lebih.

Sebuah jurnal oleh Ayan Mahalanobis pada tahun 2005 mengembangkan generalisasi dari protokol perjanjian kunci Diffie-Hellman dengan menggunakan grup nilpotent, selanjutnya pada tahun 2006 pula, beliau mengembangkan sistem kriptografi MOR sebagai generalisasi ElGamal yang lebih ringkas pada grup non-komutatif matriks *upper triangular*. Kedua jurnal dari Ayan Mahalanobis ini menunjukkan bahwa grup yang digunakan adalah grup non-komuatif *nilpotent.*

Penelitian ini adalah gabungan dari penelitian yang dilakukan oleh Ayan Mahalanobis yang sama-sama menggunakan sistem kriptografi MOR, yaitu generalisasi dari kriptografi ElGamal yang dapat menggunakan automorfisma semua grup dengan masalah logaritma diskrit. Penamaan sistem kriptografi MOR berasal dari kata automorfisma, hal ini dikarenakan pada algoritmanya menggunakan automorfisma grup. Menarik jika meneliti sistem kriptografi MOR menggunakan automorfisma grup *nilpotent*, lebih eksplisitnya yang digunakan adalah p-grup. Dipilih p-grup karena berdasarkan pada jurnal oleh Adney dan Ti

Yen (1965) yang menjelaskan juga tentang automorfisma dari p-grup dan suatu teorema yang menyebutkan jika setiap p-grup adalah *nilpotent*. Oleh karena itu, menarik bagi penulis untuk menjadikannya contoh dalam aplikasinya pada kriptografi.

1.2 Batasan Masalah

Pembatasan masalah dalam suatu penelitian sangat penting, guna menghindari kesimpangsiuran terhadap objek dari suatu penelitian dan untuk membantu penulis juga agar lebih fokus dan terarah sesuai dengan tema penelitian. Penelitian ini akan membahas grup *nilpotent* secara matematis, dan memfokuskan teorema *nilpotent* yang dikaji hanya berbatas pada pembuktian teorema bahwa setiap p-grup yang non-komutatif adalah grup *nilpotent* dan beberapa teorema terkait dengan p-subgrup sylow adalah subgrup dari grup *nilpotent*.

Penulis juga membatasi algoritma yang digunakan dalam penelitian ini hanya algoritma MOR dalam protokol perjanjian kuncinya dan hanya membatasi grup yang digunakan adalah p-grup non-komutatif secara khusus hanya pada grup dihedral dan matriks *upper triangular* sebagai salah satu contoh dari grup *nilpotent* dalam proses penyandiannya.

1.3 Rumusan Masalah

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

1. Bagaimana konsep matematis mengenai grup *nilpotent* ?

2. Bagaimana algoritma dan perhitungan proses enkripsi-dekripsi pada sistem kriptografi MOR dengan masalah logaritma diskrit atas grup *nilpotent* ?
3. Bagaimana implementasi perhitungan sistem kriptografi MOR dalam proses enkripsi-dekripsi dengan mengunakan program MAPLE ?

1.4 Tujuan Penelitian

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

1. Mengkaji mengenai materi konsep matematis mengenai grup *nilpotent.*
2. Mengkaji tentang materi algoritma dan perhitungan proses enkripsi-dekripsi pada sistem kriptografi MOR dengan masalah logaritma diskrit atas grup *nilpotent*.
3. Mengkaji tentang implementasi perhitungan sistem kriptografi MOR dalam proses enkripsi-dekripsi dengan mengunakan program MAPLE.

1.5 Manfaat Penelitian

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

1. Memberikan pengetahuan tentang grup *nilpotent*.
2. Memberikan solusi tentang pengnggunakan grup *nilpotent* dalam sistem kriptografi MOR.
3. Memberikan referensi tambahan untuk mengembangkan penelitian selanjutnya.

1.6 Tinjauan Pustaka

Banyak refrensi yang membahas mengenai grup terutama grup *nilpotent*, salah satunya adalah dari Dummit dan Foote (2004) dalam bukunya "*Group Theory"* namun hanya terbatas pada definisi dan beberapa teorema terkait dengan grup *nilpotent*. Oleh karena itu, penulis mengambil beberapa teorema dan beberapa contoh terkait grup *nilpotent* untuk melengkapi referensi yaitu dari J.S Milne (2010) dengan bukunya "*Group Theory"* juga. Penelitian ini mengambil beberapa contoh dari teorema terkait *nilpotent*, yaitu pada grup dihedral dan matriks *upper triangular* yang akan digunakan selanjutnya dalam proses penyandian pada algoritma asimetris MOR. Referensi utama pada penelitian ini yang terkait dengan grup *nilpotent* adalah dari Dummit dan Foote (2004) dan J.S Milne (2010) sebagai pelengkap pembuktian pada teorema-teorema dalam pembahasan.

Grup yang digunakan pada penelitian ini adalah automorfisma grup non-komutatif, karena masih sedikit penelitian yang membahas mengenai adanya grup non-komutatif sebagai grup yang digunakan untuk pengamanan pesan rahasia yang berdasarkan masalah logaritma diskrit. Salah satu grup non-komutatif yang mempunyai automorfisma grup adalah grup *nilpotent*, yang lebih eksplisitnya yang akan dibahas pada penelitian ini adalah p -grup yang selanjutnya digunakan dalam aplikasinya pada sistem kriptografi MOR.

Algoritma MOR adalah generalisasi dari algoritma ElGamal namun lebih kompleks grup yang digunakan. Algoritma ElGamal sebenarnya telah dibahas di berbagai buku, jurnal, dan beberapa penelitian yang lain, tetapi tidak banyak yang membahas terkait algoritma ElGamal pada grup non-komutatif. Peneliti

Taher ElGamal (1985) yang berjudul *"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"* yang menjelaskan algoritma Elgamal pada grup komutatif. Skripsi Muhamad Zaki Riyanto (2007) yang berjudul "*Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal atas Grup Pergandaan* $\mathbb{Z}_p^*$*"* juga membahas algoritma ElGamal pada grup komutatif juga. Najib Mubarok (2013) juga mengembangkan algoritma ElGamal dan grup yang digunakan masih menggunakan grup komutatif. Penelitian yang dilakukan oleh Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, dkk (2001) mulai membahas protokol perjanjian kunci pada grup non-komutatif automorfisma dan nantinya di kembangkan oleh In-Sok Lee, Woo-Hwan Kim, dkk (2004) yang memperkenalkan algoritma MOR sebagai generalisasi algoritma ElGamal.

Refrensi utama yang digunakan pada penelitian ini yang terkait dengan proses penyandian adalah jurnal oleh Ayan Mahalanobis (2006) dari pengembangan penelitian sebelumnya yang berjudul "*A simple generalization of ElGamal Cryptosystem to non-abelian groups.* Jurnal tersebut mengkaji tentang pengembangan generalisasi protokol perjanjian kunci ElGamal pada automorfisma grup non-komutatif yang disebut dengan sistem kriptografi MOR.

Perbedaan penelitian ini dengan penelitian sebelumnya adalah pada sistem kriptografi yang digunakan adalah sistem kriptografi MOR yang dapat digunakan untuk semua grup berhingga, untuk lebih lengkapnya akan penulis sajikan pada tabel berikut.

Tabel 1.1 Tinjauan Pustaka

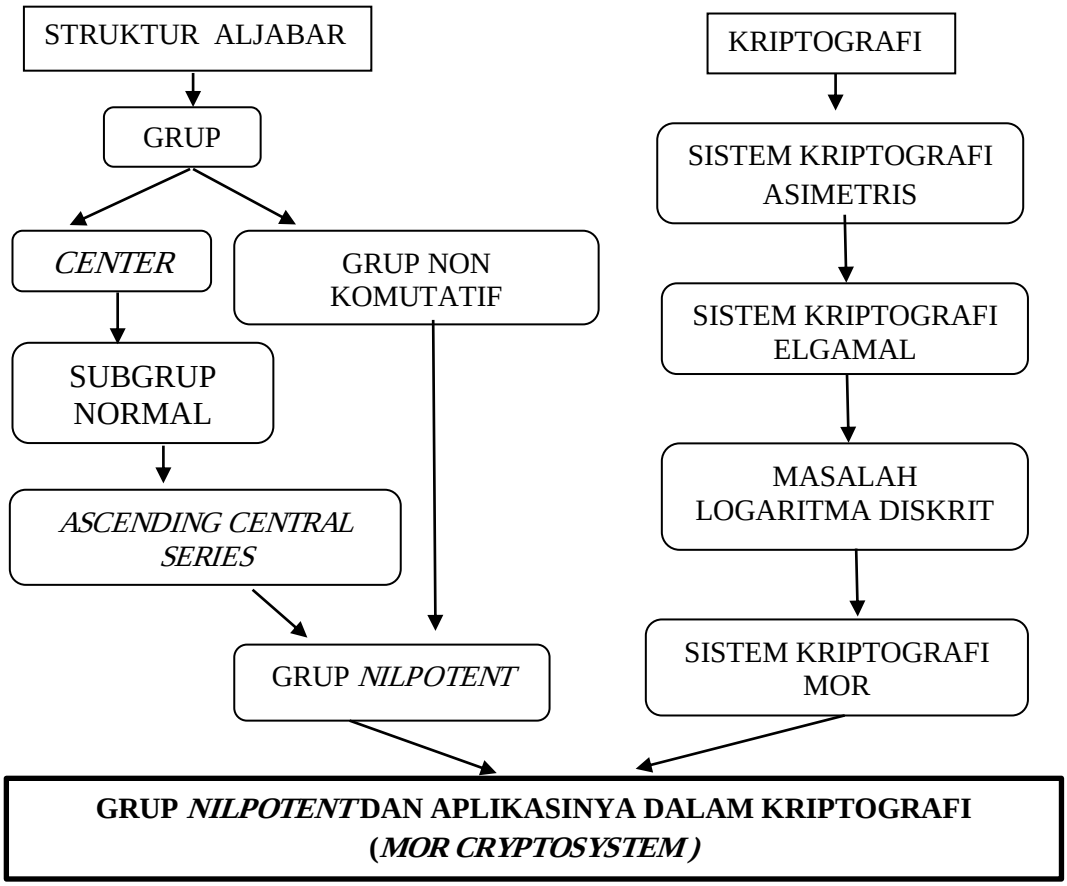
No.	Nama Peneliti	Judul Penelitian	Perbedaan
1.	Taher ElGamal (1985)	*"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"*	Struktur aljabar yang digunakan, yaitu pada grup siklik.
2.	Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, dkk (2001)	*"New Public Key Cryptosystem using Finite Non-Abelian Groups (Automorphism Group)"*	Sruktur aljabar yang digunakan adalah grup automorfisma non-komutatif automorfisma
3.	Ayan Mahalanobis (2005)	*"Diffie-Hellman Key Exchange Protocol, its generalization and Nilpotent Group"*	Sistem kriptografi yang dipakai menggunakan generalisasi algoritma kriptografi Diffie-Hellman
4.	Ayan Mahalanobis (2006)	*"A Simple Generalization of ElGamal Cryptosystem to Non-Abelian Groups"*	Sistem kriptografi yang dipakai menggunakan generalisasi algoritma kriptografi Elgamal secara umum dengan menggunakan matriks *upper triangular* sebagai aplikasinya
5.	Muhamad Zaki Riyanto (2007)	*"Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Elgamal atas Grup Pergandaan* $\mathbb{Z}_p{}^*$*"*	Struktur aljabar yang digunakan, yaitu pada grup $\mathbb{Z}_p{}^*$ (komutatif)

6.	Najib Mubarok (2013)	*"Generalisasi Algoritma Kriptografi ElGamal atas Grup Pergandaan Modulo Polinomial Irreducible dalam Pengamanan Pesan Rahasia"*	Struktur aljabar yang digunakan, yaitu grup komutatif
7.	Erna Fitriana Rohmawati (2016)	*"Grup Nilpotent dan Aplikasinya dalam Kriptografi (MOR Cryptosystem)"*	Peneliti memperkenalkan grup *nilpotent* dan teoremanya sehingga nantinya contoh dari grup tersebut dapat digunakan sebagai aplikasi pada algoritma kriptografi MOR dengan masalah keamanannya pada logaritma diskrit. Peneliti juga menambahkan contoh grup dihedral non-komutatif sebagai salah satu contoh aplikasi pada kriptografinya.

Penyusunan penelitian ini juga dibutuhkan beberapa materi struktur aljabar selain dari Dummit dan Foote (2004) dan J.S Milne (2011) juga dari beberapa literatur yaitu Menezes, Oorschot, dan Vanstone (1996), John B. Fraleigh (2000), Gallian (1990), dan lain-lain. Penelitian ini juga akan ditambahkan sebuah program komputer sederhana dengan menggunakan MAPLE.18 untuk memudahkan proses perhitungan dalam proses enkripsi-dekripsi penyandian.

1.7 Metode Penelitian

Alur penelitian pada penelitian ini, terbagi menjadi dua bagian yaitu struktur aljabar dan kriptografi. Berikut adalah alur penelitian yang penulis kaji dalam penelitian ini.



Gambar 1.1. Alur Penelitian

Penulisan pada penelitian ini juga menggunakan studi literatur yaitu data-data penelitian diambil dari sumber buku, jurnal, *paper*, catatan kuliah, dan informasi dari internet yang berkaitan dengan semua pembahasan mengenai *nilpotent*, algoritma ElGamal, algoritma MOR, dan semua materi pendukung lainnya. Metode penelitian pada penelitian ini mayoritas menggunakan proses induksi, namun ada pula yang menggunakan proses deduksi.

1.8 Sistematika Penulisan

Penulisan pada penelitian ini, terbagi dalam lima bab yang disusun secara runtun

dan sistematis dengan rincian masing-masing bab dijelaskan dengan sistematika penelitian dari penulis secara umum, sebagai berikut :

- BAB I (Pendahuluan): Bab ini membahas mengenai latar belakang, perumusan masalah, batasan masalah, tujuan penulisan tugas akhir, tinjauan

  pustaka, metode penelitian, serta sistematika penelitian.
- BAB II (Landasan Teori): Bab ini membahas mengenai landasan teori yang terdiri dari dasar struktur aljabar dan kriptografi secara umum.
- BAB III (Grup *Nilpotent* dan Aplikasinya dalam Sistem Kriptografi MOR): Bab ini mengenai grup *nilpotent*, teorema grup *nilpotent*, dan contoh aplikasi grup *nilpotent* pada proses penyendian dengan algoritma MOR.
- BAB IV (Implementasi dan Uji Coba Program): Bab ini membahas mengenai implementasi dan uji coba pada progam MAPLE.
- BAB V (Penutup): Bab ini menyampaikan kesimpulan umum yang merupakan jawaban dari rumusan masalah yang terdapat pada BAB I dan saran dari penulis mengenai penelitian yang dilakukan.

BAB V

PENUTUP

5.1 Kesimpulan

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

5.1.1 Grup *nilpotent* adalah jika diberikan suatu central series dinamakan *ascending central series* (*upper central series*), jika terdapat subgrul normal series berikut:

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

dengan $Z_0(G) = \{e\}$, $Z_1(G) = Z(G)$, *jadi* $Z_{i+1}(G)$ adalah subgrup dari G memuat $Z_i(G)$, sehingga jika dibentuk grup faktornya

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)),$$

maka dinamakan *nilpotent*, jika ditemukan suatu $Z_m(G) \leq G$, untuk suatu $m \in \mathbb{Z}^+$.

5.1.2 Teorema-teorema dari grup *nilpotent*, adalah:

5.1.2.1 Setiap p-grup non-komutatif adalah grup *nilpotent*. Misalnya adalah grup dihedral D_n, dengan $n > 3$. Sehingga, setiap p-subgrup sylow adalah subgrup dari grup *nilpotent*.

5.1.2.2 *Direct product* dari grup *nilpotent* adalah *nilpotent*. Sehingga, grup *nilpotent* adalah *direct product* dari subgrup-subgrup sylow.

5.1.3 Aplikasi grup *nilpotent* pada MOR *cryptosystem*

5.1.3.1 Sistem Kriptografi MOR adalah generalisasi dari sistem kriptografi ElGamal bedanya yaitu jika sistem kriptografi ElGamal digunakan pada grup komutatif dan pada sistem kriptografi MOR digunakan pada grup non-komutatif, salah satunya yaitu pada grup *nilpotent*.

5.1.3.2 $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ dari beberapa proses algoritma MOR untuk grup *nilpotent* berdasarkan Definisi 2.2.3.1, $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ untuk grup *nilpotent* pada pembahasan ini. Dimisalkan G grup *nilpotent* dan $g \in G$ dan automorfisma grup $\alpha: G \to G\ isomorfisma$ dengan $\alpha(x) = g^{-1}xg$.

- $\mathcal{P} = G$
- $\mathcal{C} = \{(\gamma(x), \delta) | \gamma: G \to G\ isomorfisma$ dan $\delta \in G\}$
- $\mathcal{K} = \{(K_p, K_s)\}$ dengan

  $K_p = \{(\alpha(x), \beta(x)) | \alpha: G \to G\ isomorfisma$

  dan $\beta: G \to G\ isomorfisma\}$

  dan $K_s \in \mathbb{N}$.
- $\mathcal{E} = \{(\gamma(x), \delta)\}$
- $\mathcal{D} = G$.

5.1.3.2 Keunggulan dari sistem kriptografi MOR seperti sistem kriptografi ElGamal, namun sistem kriptografi MOR lebih luas untuk sebarang grup, tidak hanya untuk grup komutatif, tetapi grup non-komutatif. Salah satu kelebihan dari sistem kriptografi MOR adalah bahwa suatu *plainteks* yang sama akan dienkripsi menjadi *cipherteks* yang berbeda-beda. Hal ini dikarenakan pemilihan bilangan r secara acak. Akan

tetapi, walaupun *cipherteks* yang diperoleh berbeda-beda, tetapi pada proses dekripsi akan diperoleh *plainteks* yang sama

5.2. Saran

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

1.2.1 Penelitian ini hanya membahas gambaran kecil mengenai grup *nilpotent* khususnya p-grup yaitu pada grup dihedral dan grup matriks *upper triangular* non-komutatif. Penelitian selanjutnya, diharapakan dapat memperluas bahasan terkait grup *nilpotent* dan sifat-sifat yang lebih luas dan lebih detail.

1.2.2 Implementasi dari struktur aljabar pada sistem kriptografi pada penelitian ini, hanya membatasi pada sistem kriptografi MOR, sehingga dimungkinkan penelitian lebih mendalam tentang struktur aljabar yang digeneralisasikan pada sistem kriptografi. Penelitian selanjutnya, dapat menggunakan sistem kriptografi lainnya.

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

DAFTAR PUSTAKA

Adkins, William A. 1999. *Algebra an Approach via Module Theory*. USA: Departement of Mathematics. Louisiana State University, Baton Rouge.

Bhattacharya, P. B., S. K. Jain, dan S. R. Nagpaul. 1994. *Basic Abstract Algebra.* Second Edition. Cambridge University Press.

Buchman, Johanes. 2000. *Introduction to Cryptograpy*. USA: Barkey.

Dummit, David S. And Foote,Ricard M. 2004. *Abstract Algebra*. Third Edition. USA: John Wiley & Sons, Inc.

Fraleigh, John B., 2000, *A First Course in Abstract Algebra*, Sixth Edition, USA: Addison-Wesley Publishing Company, Inc.

Gallian, Joseph A. 1990. *Contemporary Abstract Algebra*. Second Edition. Toronto: D.C. Heath Company.

Gilbert, Jimmie dan Linda Gilbert. 2000. *Elements of Modern Algebra*. Fifth Edition. USA: Brook/Cole.

Herstein I. N. 1964. *Topics In Algebra*. Second Edition. Masschusetts: Blaisdell Publishing Company.

In-sok Lee, Woo-hwan Kim, Daesung Kwon, Sangil Nahm, Nam-soek Kwak, And Yoo-jin Baek. 2004. *On The Security Of Mor Public Key Cryptosystem.* asiacrypt 2004 (P. J. Lee, ed.), LNCS, No.3329. Springer-verlag. vol.387-400.

Mahalanobis, Ayan. 2005. *Diffie-hellman Key Exchange Protocol, Its Generalization And Nilpotent Groups*. *Ph.D. Thesis*. Florida Atlantic University. http://eprint.iacr.org/2005/223.

Mahalanobis, Ayan. 2006. *A Simple Generalization Of El-gamal Cryptosystem To Non-abelian Groups*. Departement Of Mathematical Sciences. Stevens

Institute Of Technology, Hoboken, Nj 07030. http://eprint.iacr.org/2006/233.

Malik, D. S., J. N. Mordeson, dan M. K. Sen.1997. *Fundamental of Abstract Algebra.* Singapore: The McGraw-Hill Companies.

Menezes, Oorcshot, And Vanstone. 1996. *Handbook Of Applied Cryptography*. USA: Crc Press Inc.

Milne, J.S. 2011. *Group Theory*. *E-book*. Version 3.10. www.jmilne.org/math.

Myasnikov Alexei, dkk . 2008. *Grup Based Criptoggrafi* . Berlin: Birkhäuser Verlag.

Paar, Christof and Pelzl. 2009. *Understanding Cryptology*. USA: Springer-Verlag New York: Inc.

Raisinghania, M. D. dan R. S. Anggarwal. 1980. *Modern Algebra*. Second Edition. New Delhi: S. Chand&Company Ltd.

Riyanto, M. Zaki. 2007. *Pengamanan Pesan Rahasia menggunakan Algoritma ElGamal atas Grup Pergandaan* $\mathbb{Z}_p^*$. *Skripsi*. Yogyakarta : Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Gadjah Mada.

R. Odoni, V. Varadharajan, And R.Sanders. 1984. *Public Key Distribution In Matrix Rings, Electronic Letters*,vol.293-298.

Seong-hun Paeng, Kil-chan Ha, Ja Heon Kim, Seongtaek Chee, And Choonsik Park. 2001. *New Public Key Cryptosystem Using Finite Non-abelian Groups.* Crypto 2001 (J. Kilian, ed.), LNCS. vol.2139. Springer-verlag,2001,vol.470-485.

Setyawati, Lia. 2012. *Sifat-sifat p-grup dan p-subgrup Sylow*. *Skripsi*. Yogyakarta: Jurusan Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga

Sukirman. 2005. *Pengantar Aljabar Abstrak.* Cetakan Pertama. Malang: Universitas Negri Malang.

Wikipedia. Aljabar. http://id.wikipedia.org/wiki/Aljabar.

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	*
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	▯
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
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

DAFTAR RIWAYAT HIDUP

Nama Lengkap : Erna Fitriana Rohmawati

Tempat, tanggal lahir : Pati, 27 Oktober 1993

Alamat : Ds. Asempapan, RT.03/RW.3, Kec. Trangkil, Kab. Pati, Jawa Tengah

Hp : 0899-961-5000-3

Fakultas/Jurusan : Sains dan Teknologi / Matematika

Email : ernafitri27@gmail.com

Riwayat pendidikan :

TK Uswatun Hasanah	1998-2000
MI Silahul Ulum Pati	2000-2006
Mts. Silahul Ulum Pati	2006-2009
MA. Raudlatul Ulum Pati	2009-2012
UIN Sunan Kalijaga	2012-2016