SKRIPSI

MATRIKS ATAS RING BILANGAN BULAT GAUSS DAN PENERAPANNYA PADA KRIPTOGRAFI

MUHAMMAD LUTHFI KAMAL
20106010048

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

2024

MATRIKS ATAS RING BILANGAN BULAT GAUSS DAN PENERAPANNYA PADA KRIPTOGRAFI

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

MUHAMMAD LUTHFI KAMAL

20106010048

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2024

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Muhammad Luthfi Kamal
NIM	: 20106010048
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 29 Februari 2024

Muhammad Luthfi Kamal

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Muhammad Luthfi Kamal
NIM	: 20106010048
Judul Skripsi	: Matriks atas Ring Bilangan Bulat Gauss dan Penerapannya Pada Kriptografi

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

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

Wassalamu'alaikum wr. wb.

Yogyakarta, 29 Februari 2024
Pembimbing I

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

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-439/Un.02/DST/PP.00.9/03/2024

Tugas Akhir dengan judul : Matriks atas Ring Bilangan Bulat Gauss dan Penerapannya pada Kriptografi

yang dipersiapkan dan disusun oleh:

Nama	: MUHAMMAD LUTHFI KAMAL
Nomor Induk Mahasiswa	: 20106010048
Telah diujikan pada	: Kamis, 07 Maret 2024
Nilai ujian Tugas Akhir	: A

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 65f26d2ceb324

Penguji I

Arif Munandar, M.Sc.
SIGNED

Valid ID: 65f3a7d4d2d99

Penguji II

Deddy Rahmadi, M.Sc.
SIGNED

Valid ID: 65f2e16090966

Yogyakarta, 07 Maret 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 65f3df477091a

HALAMAN PERSEMBAHAN

Karya tulis ini dipersembahkan kepada kedua orang tua dan almamater Universitas Islam Negeri Sunan Kalijaga

HALAMAN MOTTO

"Hidup yang tidak dipertaruhkan tidak akan pernah dimenangkan" - Sutan Syahrir

PRAKATA

Allhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT yang telah memberikan segala karuani, rahmat, dan hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Ring atas Bilangan Bulat Gauss dan Penerapannya Pada Kriptografi". Sholawat serta salam senantiasa tercurahkan kepada Baginda Nabi Muhammad SAW yang syafaatnya senantiasa dinantikan oleh umatnya di hari akhir.

Penulis menyadari bahwa dalam penulisan tugas akhir ini terdapat banyak hambatan dan halangan. Namun berkat adanya motivasi, bantuan, bimbingan, dan dorongan dari berbagai pihak, *alhamdulillah* skripsi ini dapat terselesaikan. Oleh karena itu, dengan kerendahan hati penulis mengucapkan terima kasih kepada:

1. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Muchammad Abrori, S.Si., M.Kom., selaku Ketua Program Studi Matematika.
3. Sri Istiyarti Uswatun Chasanah, S.Si., M.Sc., selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama menempuh pendidikan.
4. M. Zaki Riyanto, M.Sc., selaku dosen pembimbing skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.
5. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.

6. Orang tua tercinta, Thoyyibi dan Asti Khoiriyyah yang senantiasa memberikan dukungan, motivasi, dan doa-doa kepada penulis. Pengorbanan dan keikhlasan tanpa batas dari Bapak dan Ibu menjadi sumber kekuatan dalam menyelesaikan tugas akhir ini.
7. Kakak dan adik tercinta, Khoirul Athyabil Anwari dan Irham Jauhari Ahmad yang selalu memberikan dukungan dalam bentuk apapun.
8. Seluruh teman-teman matematika aljabar yang saling mendukung satu sama lain.
9. Teman-teman matematika angkatan 2020 yang telah membersama perkuliahan ini selama kurang lebih 4 tahun.
10. Pihak lain yang berperan dalam pengerjaan skripsi
11. Semua pihak yang tidak bisa penulis sebutkan yang secara langsung maupun tidak langsung membantu terselesaikannya skripsi ini.

Penulis berharap semoga tugas akhir ini dapat memberikan manfaat bagi semua yang membacanya. Penulis juga berharap kritik dan saran yang membangun.

Yogyakarta, 29 Februari 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	:	x anggota himpunan A
$A \setminus B$	:	himpunan A yang tidak memuat himpunan B
$A \subseteq X$	:	A merupakan himpunan bagian (*subset*) atau sama dengan X
$\mathbb{N}$	:	himpunan semua bilangan asli
$\mathbb{Z}$	:	himpunan semua bilangan bulat
$\mathbb{Z}^+$	:	himpunan semua bilangan bulat positif
$\mathbb{Z}_{\geq 0}$	:	himpunan semua bilangan bulat tak negatif
$\mathbb{R}$	:	himpunan semua bilangan real
$\blacksquare$	:	akhir suatu bukti
$\square$	:	akhir suatu contoh
$\rightarrow$	:	menuju
$\sum_{i=1}^{n} a_i$	:	penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_i$	:	perkalian $a_1 \cdot a_2 \cdot \cdots \cdot a_n$
$\mathbb{Z}[i]$	:	himpunan bilangan bulat Gauss
$M_n(\mathbb{Z}[i])$	:	himpunan matriks atas bilangan bulat Gauss
$\mathbb{Z}[i][x]$	:	himpunan polinomial atas bilangan bulat Gauss

INTISARI

MATRIKS ATAS RING BILANGAN BULAT GAUSS DAN PENERAPANNYA PADA KRIPTOGRAFI

Oleh

Muhammad Luthfi Kamal

20106010048

Himpunan bilangan bulat Gauss merupakan himpunan bagian dari himpunan bilangan kompleks. Lebih lanjut, himpunan matriks atas himpunan bilangan bulat Gauss merupakan ring non-komutatif terhadap operasi penjumlahan dan perkalian. Himpunan matriks ini digunakan pada protokol pertukaran kunci sebagai upaya meminimalisir serangan karena protokol pertukaran kunci pada dasarnya menggunakan aljabar komutatif yang letak keamanannya bersandar pada permasalahan logaritma diskrit. Pengembangan protokol pertukaran kunci menghasilkan protokol autentikasi. Protokol autentikasi merupakan proses verifikasi seseorang sebelum mendapatkan hak akses terhadap suatu sistem. Pada tugas akhir ini, akan dibahas protokol pertukaran kunci dan protokol autentikasi menggunakan matriks atas himpunan bilangan bulat Gauss.

Kata kunci : protokol pertukaran kunci, bilangan bulat Gauss, kriptografi, protokol autentikasi.

ABSTRACT

MATRICES OVER RING GAUSSIAN INTEGERS AND ITS APPLICATION ON CRYPTOGRAPHY

By

Muhammad Luthfi Kamal

20106010048

The set of Gauss integers is a subset of the set of complex numbers. Furthermore, the set of matrices over the set of Gauss integers is a non-commutative ring for addition and multiplication operations. This matrix set is used in the key exchange protocol as an effort to minimize attacks because the key exchange protocol basically uses commutative algebra whose security relies on discrete logarithmic problems. The development of the key exchange protocol resulted in the authentication protocol. Authentication protocol is a process of verifying a person before getting access rights to a system. In this final project, examples of key exchange protocols and authentication protocols using matrices over the set of Gauss integers will be given.

Keyword : key exchange protocol, Gaussian integers, cryptography, authentication protocol.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Komunikasi merupakan landasan penting dalam interaksi manusia yang penting dalam menjalin hubungan, menyampaikan gagasan, dan membangun pemahaman bersama. Secara umum komunikasi dibedakan menjadi dua jenis, yaitu verbal dan nonverbal. Komunikasi verbal melibatkan penggunaan kata-kata dan bahasa untuk menyampaikan pesan, sedangkan komunikasi nonverbal meliputi ekspresi wajah, bahasa tubuh, dan intonasi suara. Kedua jenis komunikasi ini saling melengkapi dan menghadirkan dimensi yang lebih kaya dalam proses komunikasi. Pada dasarnya komunikasi melibatkan suatu pesan. Pesan yang akan dilibatkan haruslah pesan yang bersifat valid dan tidak mengandung unsur kebohongan.

Pada awalnya, pesan hanya dapat disampaikan dengan cara dua pihak atau lebih bertemu. Seiring berjalannya waktu, pesan mulai disampaikan menggunakan surat yang dikirim ke pihak penerima yang tidak dapat bertemu secara langsung. Karena terdapat kekurangan surat-menyurat, salah satunya kurang efisien dalam segi waktu, muncul teknologi komunikasi yang memungkin dua atau lebih pihak dapet berkomunikasi. Teknologi berperan penting dalam memperluas cara masyarakat berkomunikasi. Namun, dengan adanya teknologi mengancam keamanan pesan yang disebabkan oleh pihak ketiga. Maka dari itu, perlu adanya suatu konsep untuk mengamankan pesan atau data, salah satunya yaitu kriptografi.

Kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphia*. *Crypto*

berarti rahasia dan *graphia* berarti tulisan. Secara terminologi, kriptografi merupakan suatu ilmu yang digunakan untuk mengamankan suatu pesan yang dikirim oleh suatu pihak ke pihak lain (Ariyus et al.,2008). Sedangkan dipandang dari konsep matematika, kriptografi merupakan ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data (Menezes et al.,2018).

Pesatnya perkembangan kriptografi dimulai pada tahun 1970-an ketika kunci publik atau kriptografi asimetris diperkenalkan. Pada tahun 1976, Diffie dan Hellman memperkenalkan konsep kriptografi asimetris atau kunci public dalam artikelnya yang berjudul *"New Directions in Cryptography"* (Diffie & Hellman,1976). Selain itu mereka memperkenalkan metode pertukaran kunci yang dikenal sebagai protokol pertukaran kunci Diffie-Hellman. Protokol ini menggunakan konsep matematika yaitu struktur aljabar komutatif yang letak keamanannya bergantung pada masalah logaritma diskrit.

Peter W. Shor mempublikasikan sebuah artikel pada tahun 1993 yang berjudul *"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"*. Artikel tersebut menjelaskan bahwa jika komputer kuantum berhasil diwujudkan, maka masalah faktorisasi prima dan masalah logaritma diskrit dapat diselesaikan (Shor, 1997). Hal ini dapat mengancam keamanan pada protokol pertukaran kunci. Oleh karena itu, diperlukan protokol pertukaran kunci yang memiliki tingkat keamanan yang diantisipasi tinggi terhadap potensi serangan dari komputer kuantum.

Seiring berjalannya waktu, sejumlah penelitian mulai dikembangkan untuk mewujudkan suatu protokol pertukaran kunci yang dianggap aman terhadap seranga n komputer kuantum. Salah satunya adalah protokol pertukaran kunci yang

dikenal dengan nama protokol Stickel. Protokol ini menggunakan struktur aljabar nonkomutatif (Stickel,2005). Selain protokol Stickel, Joan-Josep Climent dalam artikelnya yang berjudul *"Cryptanalysis of The CFVZ Cryptosystem"* juga memperkenalkan protokol pertukaran kunci berbasis matriks (Climent et al.,2007). Konsep protokol tersebut akan digunakan dalam modifikasi protokol pertukaran kunci dan autentikasi menggunakan matriks atas bilangan bulat Gauss.

1.2. Batasan Masalah

Penelitian ini dibatasi pada matriks atas himpunan bilangan bulat Gauss. Matriks tersebut akan digunakan pada modifikasi protokol pertukaran kunci Diffe-Hellman dan protokol autentikasi.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diuraikan sebelumnya, maka dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana konsep bilangan bulat Gauss?
2. Bagaimana konsep matriks atas himpunan bilangan bulat Gauss?
3. Bagaimana protokol pertukaran kunci menggunakan matriks atas himpunan bilangan bulat Gauss?
4. Bagaimana protokol autentikasi menggunakan matriks atas himpunan bilangan bulat Gauss?

1.4. Tujuan Penelitian

Berdasarkan beberapa rumusan masalah sebelumnya, maka diperoleh tujuan penelitian sebagai berikut:

1. Mempelajari konsep bilangan bulat Gauss.
2. Mempelajari konsep matriks atas bilangan bulat Gauss.
3. Mengetahui protokol pertukaran kunci menggunakan matriks atas himpunan bilangan bulat Gauss.
4. Mengetahui protokol autentikasi menggunakan matriks atas himpunan bilangan bulat Gauss.

1.5. Manfaat Penelitian

Berdasarkan rumusan masalah dan tujuan penelitian yang telah diuraikan sebelumnya, maka diperoleh beberapa manfaat penelitian sebagai berikut:

1. Memberikan pengetahuan tentang konsep matriks atas bilangan bulat Gauss.
2. Memberikan pengetahuan konsep protokol pertukaran kunci Climent.
3. Memberikan pengetahuan konsep protokol autentikasi yang didasari oleh protokol pertukaran kunci Climent.
4. Memberikan pengetahuan tentang konsep prokol pertukaran kunci dan autentikasi dengan menggunakan matriks atas bilangan bulat Gauss.

1.6. Tinjauan Pustaka

Konsep pertukaran kunci pertama kali diperkenalkan oleh Diffie dan Hellman dalam publikasinya yang berjudul *"New Directions in Cryptography"*. Pada artikel tersebut, dibahas tentang kriptografi asimetris. Diffie dan Hellman menggunakan aljabar komutatif yang letak keamanannya terletak pada logaritma diskrit. Pada tahun 2005, Stickel melalui publikasinya yang berjudul *"A New Method for*

Exchanging Secret Keys" memperkenalkan konsep protokol pertukaran kunci Stickel. Stickel menggunakan konsep struktur aljabar non-komutatif dalam penelitiannya. Stickel memilih konsep tersebut karena adanya ancaman komputer kuantum yang dapat memecahkan logaritma diskrit dengan cepat.

Seiring berjalannya waktu, pada tahun 2013, Joan-Josep Climent, Pedro R. Navarro B, dan Leandro Tortosa memperkenalkan suatu konsep protokol pertukaran kunci atas ring non-komutatif. Mereka memperkenalkan konsep tersebut pada publikasinya yang berjudul *"Key exchange protocols over noncommutative rings."*. Climent, Navarro, dan Tortosa menggunakan $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ sebagai studi kasus dalam publikasi tersebut.

Konsep protokol yang diperkenalkan oleh Climent dkk. juga digunakan pada artikel yang berjudul *"Key Exchange Protocol With Gaussian Integer Matrice"*. Artikel tersebut diterbitkan pada tahun 2016 yang ditulis oleh B.P.Tripathi dan Shruti Nathani. Tripathi dan Shruti menggunakan matriks atas bilangan bulat Gauss pada studi kasus tersebut. Konsep dasar struktur bilangan bulat Gauss dan matriks atas bilangan bulat Gauss menggunakan artikel dari publikasi berjudul *"RSA in extensions of the ring of integers"* yang ditulis oleh Alessia Pina pada tahun 2017.

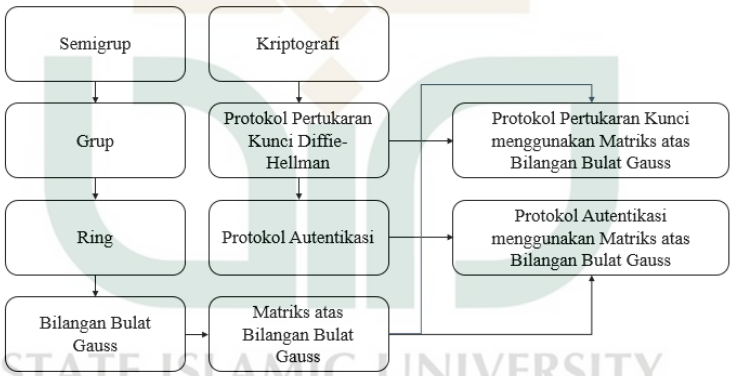
1.7. Metode Penelitian

Metode penelitian yang digunakan pada penulisan tugas akhir ini ialah studi literatur. Metode ini dilakukan dengan sejumlah buku, artikel, karya ilmiah atau majalah yang berkaitan dengan masalah dan tujuan penelitian (Danial & Wasriah,2009). Penulis menggunakan metode ini dengan menghimpunan konsep bilangan bulat Gauss dan protokol pertukaran kunci.

Pembahasan dimulai dengan membahas tentang struktur aljabar, meliput se-

migrup, grup, ring, daerah integral, dan daerah Euclid. Konsep tersebut akan digunakan dalam konsep bilangan bulat Gauss dan matriks atas bilangan bulat Gauss. Pembahasan selanjutnya akan diuraikan tentang konsep bilangan bulat Gauss dan matriks bilangan bulat Gauss, meliputi definisi, sifat, dan operasi yang berlaku.

Pembahasan selanjutnya akan dijelaskan tentang kriptografi yang meliputi definisi, sejarah, dan sistem kriptografi. Setelah pembahasan tentang kriptografi, akan dijelaskan pula konsep protokol pertukaran kunci Diffie-Hellman. Protokol tersebut akan dimodifikasi dengan menggunakan matriks atas himpunan bilangan bulat Gauss. Kunci yang telah dibentuk dari protokol tersebut, akan digunakan dalam proses enkripsi dan dekripsi. Skema penelitian akan ditunjukkan pada gambar di bawah ini.



Gambar 1.1 Skema Metode Penelitian

1.8. Sistematika Penulisan

Penelitian ini disusun dengan merujuk pada urutan sistematika penulisan yang dijelaskan sebagai berikut:

1. Bab 1 : Pendahuluan

   Bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penilitian, tinjauan pustaka, dan sistematika

penulisan.

2. Bab 2 : Dasar Teori

   Bab ini membahas tentang dasar-dasar teori yang mendasari protokol pertukaran kunci dan protokol autentikasi. Dasar-dasar teori tersebut meliputi teori bilangan dan struktur aljabar.

3. Bab 3 : Ring Bilangan Bulat Gauss

   Bab ini membahas tentang konsep bilangan bulat Gauss dan matriks atas himpunan bilangan bulat Gauss. Selanjutnya berdasarkan konsep tersebut akan dibahas juga sifat-sifat dan operasi-operasi yang berlaku.

4. Bab 4 : Protokol Pertukaran Kunci dan Protokol Autentikasi Menggunakan Matriks atas Himpunan Bilangan Bulat Gauss

   Bab ini akan membahas protokol pertukaran kunci yang diawali dengan membahas tentang kriptografi, sejarah kriptografi, dan sistem kriptografi. Adapun sistem kriptografi yang dibahas adalah pertukaran kunci Diffie-Hellman dan protokol autentikasi. Kunci yang diperoleh dari protokol pertukarakan kunci akan digunakan dalam enkripsi dan dekripsi pesan menggunakan sistem kriptografi Vigenere.

BAB V

PENUTUP

Pada bab ini akan diberikan beberapa kesimpulan dan saran dari penulis tentang tugas akhir ini.

5.1. Kesimpulan

Beberapa kesimpulan pada tugas akhir ini yang dapat diambil oleh penulis sebagai berikut:

1. Himpunan bilangan bulat Gauss $\mathbb{Z}[i]$ merupakan daerah integral terhadap operasi penjumlahan dan perkalian pada $\mathbb{Z}$. Lebih lanjut, daerah integral $(\mathbb{Z}[i], +, \cdot)$ merupakan daerah daerah Euclid terhadap fungsi valuasi norm pada himpunan bilangan bulat Gauss $\mathbb{Z}[i]$.

2. Himpunan matriks atas bilangan bulat Gauss $M_n(\mathbb{Z}[i])$ merupakan ring dengan elemen satuan terhadap operasi penjumlahan dan perkalian matriks.

3. Skema protokol pertukaran kunci menggunakan matriks atas bilangan bulat Gauss dimulai dengan menyepakati $f(x) \in \mathbb{Z}[i][x]$ dan dua matriks $A, B \in M_k(\mathbb{Z}[i])$. Langkah selanjutnya

   (a) Alice memilih secara rahasia $m, n \in \mathbb{N}$ dan menghitung

   $$P_A = f(A)^m B f(A)^n$$

   .

(b) Alice mengirim P_A kepada Bob.

(c) Bob memilih secara rahasia $r, s \in \mathbb{N}$ dan menghitung

$$P_B = f(A)^r B f(A)^s.$$

(d) Bob mengirim P_B kepada Alice.

(e) Alice menghitung $K_A = f(A)^m P_B f(A)^n$.

(f) Bob menghitung $K_B = f(A)^r P_A f(A)^s$.

4. Skema protokol autentikasi menggunakan matriks atas bilangan bulat Gauss dimulai dengan menyepakati $f(x) \in \mathbb{Z}[i][x]$ dan dua matriks $A, B \in M_n(\mathbb{Z}[i])$. Langkah selanjutnya

(a) Alice memilih secara bilangan asli $m, n \in \mathbb{N}$ dan menghitung $P_A = f(A)^m B f(A)^n$.

(b) Alice mengirim P_A kepada Bob.

(c) Bob menerima P_A dari Alice dan memilih secara rahasia $r, s \in \mathbb{N}$.

(d) Bob menghitung $P_B = f(A)^r B f(A)^s$ dan mengirim P_B kepada Alice sebagai tantangan.

(e) Alice menerima P_B dari Bob dan menghitung $P = f(A)^m P_B f(A)^n$. Kemudian, Alice mengirim P kepada Bob sebagai bentuk respon.

(f) Bob menerima P dan memverifikasi apakah $f(A)^r P_A f(A)^s = P$.

5.2. Saran

Beberapa saran yang penulis sampaikan setelah menyelesaikan penulisan tugas akhir, yaitu:

1. Pada penelitian selanjutnya, bisa dibahas tentang struktur aljabar pada bilangan bulat Gauss.

2. Penelitian selanjutnya bisa dibahas tentang analisis serangan terhadap protokol pertukaran kunci dan protokol autentikasi menggunakan matriks atas bilangan bulat Gauss.

3. Penelitian selanjutnya dapat mengembangkan sistem kriptografi lainnya menggunakan bilangan bulat Gauss.

DAFTAR PUSTAKA

Ariyus, D. et al. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

Beachy, J. A. & Blair, W. D. (2019). *Abstract algebra*. Waveland Press.

Brown, J. W. & Churchill, R. V. (2009). *Complex variables and applications*. McGraw-Hill,.

Climent, J.-J., Gorla, E., & Rosenthal, J. (2007). Cryptanalysis of the cfvz cryptosystem. *Advances in Mathematics of Communications*, 1(1):1–11.

Danial, E. & Wasriah, N. (2009). Metode penulisan karya ilmiah. *Bandung: Laboraturium Pendidikan Kewarganegaraan*.

Diffie, W. & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

Gallian, J. A. (2015). *Contemporary Abstract Algebra*. Cengage Learning.

Malik, D., Mordeson, J. N., & Sen, M. (2007). *Introduction to Abstract Algebra*. Citeseer.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

Pina, A. (2017). Rsa in extensions of the ring of integers. `https://api.semanticscholar.org/CorpusID:41408577`.

Rosen, K. H. (2011). *Elementary number theory*. Pearson Education London.

Rudhito, M. A. (2020). *Aljabar max-plus dan penerapannya*. Sanata Dharma University Press.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Stickel, E. (2005). A new method for exchanging secret keys. In *Third International Conference on Information Technology and Applications (ICITA'05)*, volume 2, pages 426–430.

Stinson, D. R. & Paterson, M. B. (2008). *Cryptography: Theory and Practice*. CRC Press.