APLIKASI BASIS GRÖBNER PADA KRIPTOGRAFI KUNCI PUBLIK MULTIVARIAT

SKRIPSI

OLEH
FIRDAUS MASITHA
NIM. 19610033

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2024

APLIKASI BASIS GRÖBNER PADA KRIPTOGRAFI KUNCI PUBLIK MULTIVARIAT

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
FIRDAUS MASITHA
NIM. 19610033

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2024

APLIKASI BASIS GRÖBNER PADA KRIPTOGRAFI KUNCI PUBLIK MULTIVARIAT

SKRIPSI

Oleh
FIRDAUS MASITHA
NIM. 19610033

Telah Disetujui Untuk Diuji

Malang, 20 November 2024

Dosen Pembimbing I	Dosen Pembimbing II
Intan Nisfulaila, M.Si	Erna Herawati, M.Pd
NIP. 19900215 201903 2 015	NIPPPK. 19760723 202321 2 006

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

APLIKASI BASIS GRÖBNER PADA KRIPTOGRAFI KUNCI PUBLIK MULTIVARIAT

SKRIPSI

Oleh
FIRDAUS MASITHA
NIM. 19610033

Telah Dipertahankan di Depan Dewan Penguji Seminar Hasil Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Mengukuti Sidang Skripsi

Tanggal 19 Desember 2024

Ketua Penguji	: Hisyam Fahmi, M.Kom	.....
Anggota Penguji 1	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji 2	: Intan Nisfulaila, M.Si	.....
Anggota Penguji 3	: Erna Herawati, M.Pd	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

Nama	: Firdaus Masitha
NIM	: 19610033
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Aplikasi Basis Gröbner pada Kriptografi Kunci Publik Multivariat

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 19 Desember 2024

Yang Membuat Pernyataan,

Firdaus Masitha
NIM. 19610033

MOTO

“Kunci perjalanan panjang adalah memulai dan kunci keberhasilan adalah tidak berhenti”

PERSEMBAHAN

Dengan penuh rasa syukur, skripsi ini penulis persembahkan untuk: Ayahanda Solichan yang selalu menjadi teladan dalam keteguhan, kerja keras, dan doa tanpa henti dan Ibunda Suliati yang dengan kasih sayang dan pengorbanan tak terhingga, selalu mendukung setiap langkah penulis. Adik-adik penulis yang senantiasa menemani dan memberikan semangat kepada penulis.

KATA PENGANTAR

Segala puji bagi Allah SWT. yang telah melimpahkan rahmat, taufik, serta hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Aplikasi Basis Gröbner pada Kriptografi Kunci Publik Multivariat" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat serta salam senantiasa tercurahkan kepada Nabi Muhammad SAW. yang telah menuntun manusia dari jalan gelap gulita menuju jalan terang benderang yaitu agama Islam.

Pada penyusunan skripsi ini, penulis mendapatkan banyak bimbingan dan arahan dari berbagai pihak. Untuk itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. H. M. Zainuddin, M.A, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Hj. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Intan Nisfulaila, M.Si, selaku dosen pembimbing I yang telah memberikan arahan, nasihat, motivasi serta ilmu yang sangat bermanfaat bagi penulis.
5. Erna Herawati, M.Pd, selaku dosen pembimbing II yang telah memberikan arahan, nasihat, serta berbagi ilmunya kepada penulis.
6. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim yang telah memberikan pengalaman serta ilmu yang tak ternilai harganya.
7. Ayah (Solichan) dan Ibu (Suliati), serta adik-adik yang telah memberikan dukungan, semangat, serta cintanya kepada penulis.
8. Seluruh mahasiswa Universitas Islam Negeri Maulana Malik Ibrahim Malang Program Studi Matematika angkatan 2019 yang senantiasa membantu dari awal perkuliahan hingga akhir.

9. Semua pihak yang telah membantu kelancaran penulisan skripsi, baik bantuan moril maupun materil.

Penulis berharap skripsi ini bisa memberikan manfaat kepada penulis maupun pembaca serta memberikan dampak yang baik untuk semua pihak.

Malang, 24 Desember 2024

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRAK

Masitha, Firdaus. 2024. **Aplikasi Basis Gröbner pada Kriptografi Kunci Publik Multivariat**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (1) Intan Nisfulaila, M.Si., (2) Erna Herawati, M.Pd.

Kata Kunci: Kriptografi, Persamaan Polinomial, Basis Gröbner, Kriptanalisis

Kriptografi memiliki peran yang sangat penting dalam keamanan informasi. Kriptografi kunci publik multivariat merupakan salah satu jenis kriptografi berbasis sistem persamaan polinomial pada lapangan berhingga. Penelitian ini membahas konstruksi kriptografi kunci publik multivariat pada lapangan berhingga yang melibatkan pembentukan kunci melalui transformasi affine dan sistem persamaan polinomial. Basis Gröbner dapat diterapkan untuk menyelesaikan persamaan polinomial dengan cara menyederhanakan polinomial. Proses ini berguna untuk mengevaluasi keamanan sistem kriptografi melalui kriptanalisis. Hasil penelitian menunjukkan bahwa keberhasilan kriptanalisis menggunakan basis Gröbner bergantung pada struktur dan kompleksitas polinomial serta transformasi affine yang digunakan pada kriptografi.

ABSTRACT

Masitha, Firdaus. 2024. **Application of Gröbner Basis in Multivariate Public Key Cryptography**. Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (1) Intan Nisfulaila, M.Si., (2) Erna Herawati, M.Pd.

Keywords: Cryptography, Polynomial Equations, Gröbner Basis, Cryptanalysis.

Cryptography plays a crucial role in information security. Multivariate public key cryptography is a type of cryptography based on systems of polynomial equations over finite fields. This research discusses the construction of multivariate public key cryptography over the finite field involving key generation through affine transformations and polynomial equation systems. Gröbner bases can be applied to solve polynomial equations by simplifying the polynomials. This process is useful for evaluating the security of cryptographic systems through cryptanalysis. The results of this study indicate that the success of cryptanalysis using Gröbner bases depends on the structure and complexity of the polynomials and the affine transformations used in the cryptography.

مستخلص البحث

مسيته، فردوس.٢٠٢٤. **تطبيق أساس *Gröbner* في التشفير بالمفتاح العام متعدد المتغيرات**. البحث الجامعي. قسم الرياضيات .كلية العلوم والتكنولوجيا . جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرفة الاولى: اينتان نصف الليلة الماجستيرة، المشرفة الثانية: إيرنا هيرواتي الماجستيرة

كلمات المفتاحية: التشفير، نظام المعادلات متعددة الحدود، أساس *Gröbner*، التحليل الشفري

التشفير له دورٌ مهمٌ جدًا في أمن المعلومات. يُعدُّ التشفير بالمفتاح العام متعدد المتغيرات أحد أنواع التشفير القائم على نظام المعادلات متعددة الحدود في الحقل المنتهي. ناقشت هذه الدراسة بناء التشفير بالمفتاح العام متعدد المتغيرات في الحقل المنتهي والذي يتضمن تكوين المفتاح من خلال تركيب التحويلات *affine* ونظام المعادلات متعددة الحدود. يمكن تطبيق أساس *Gröbner* لحل المعادلات متعددة الحدود من خلال تبسيطها. تُعدُّ هذه العملية مفيدة في تقييم أمان الأنظمة التشفيرية عبر التحليل الشفري. أظهرت نتائج البحث أن نجاح التحليل الشفري باستخدام أساس *Gröbner* يعتمد على هيكلية وتعقيد المعادلات متعددة الحدود، بالإضافة إلى التحويلات *affine* المستخدمة في التشفير.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Aljabar adalah salah satu bagian matematika yang memuat manipulasi pada simbol abstrak serta operasi aritmatika. Aljabar memuat konsep persamaan, sistem bilangan, serta simbol yang digunakan untuk menyampaikan dan memanipulasi pernyataan matematika. Aljabar abstrak merupakan bagian dari ilmu aljabar yaitu suatu himpunan tak kosong yang memenuhi aksioma-aksioma tertentu dengan satu atau lebih operasi. Aljabar abstrak atau struktur aljabar membahas beberapa teori, di antaranya himpunan, grup, ring, daerah hasil, dan lapangan (Gallian, 2017).

Basis Gröbner adalah teori yang diperkenalkan oleh Bruno Buchberger pada tahun 1965, yang berfokus pada pemecahan masalah teoritis terkait ideal dalam ring polinomial serta pencarian solusi untuk sistem persamaan polinomial (Mencinger, 2013). Ring adalah himpunan dengan dua operasi, yakni penjumlahan dan perkalian, yang memenuhi sifat-sifat tertentu. Ring yang digunakan pada basis Gröbner adalah ring polinomial, yaitu ring yang elemen-elemennya berupa polinomial dan memungkinkan operasi dengan banyak variabel. Algoritma basis Gröbner kemudian dikembangkan untuk menangani berbagai masalah dalam aljabar komutatif dan aljabar geometri, seperti keanggotaan ideal, dekomposisi ideal, dan konversi representasi parametrik dalam penyelesaian sistem persamaan polinomial. Saat ini, teori basis Gröbner telah diterapkan secara luas di berbagai bidang keilmuan lainnya, seperti mekanika, biologi, kimia, robotika, statistika, teori pengkodean, dan kriptografi.

Salah satu aplikasi penting basis Gröbner yang selalu berkembang yaitu pada keamanan informasi dan kriptografi. Keamanan informasi memastikan perlindungan informasi dari akses yang tidak diinginkan dan kriptografi adalah ilmu yang digunakan untuk melindungi data agar tidak dapat dibaca oleh pihak yang tidak diinginkan. Informasi harus selalu dilindungi agar tidak digunakan untuk tujuan yang negatif. Salah satu keamanan informasi adalah terkait dengan privasi. Privasi merupakan hal-hal yang bersifat pribadi yang tidak seharusnya diketahui dan dicampuri orang lain. Keamanan informasi disebutkan dalam Al-Qur'an. pada QS. An-Nur ayat 27:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ (٢٧)

Artinya:

"*Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat".* (QS. An-Nur/24: 27)

Larangan untuk memasuki rumah milik orang lain tanpa izin dari pemilik rumah disebutkan pada surat An-Nur ayat 27. Rumah dapat diibaratkan sebagai privasi seseorang yang tidak dapat dilihat dan dipakai tanpa seizin pemiliknya (Soediro, 2018). Privasi setiap orang tidak dapat diketahui oleh sembarang orang. Jika privasi diketahui orang yang tidak baik maka bisa membahayakan diri pemilik privasi. Oleh karena itu menjaga privasi diri sangat penting untuk dilakukan. Hal ini dapat dilakukan dengan usaha untuk melindungi informasi.

Salah satu cara untuk melindungi informasi adalah membuat agar informasi tersebut tidak dapat dibaca oleh sembarang orang melalui kriptografi. Kriptografi merupakan ilmu yang membahas teknik sehubungan dengan aspek keamanan informasi atau data (Mukhtar, 2018). Kriptografi sering dikenal sebagai ilmu atau

seni enkripsi pesan. Awalnya kriptografi hanya digunakan pada politik dan militer, namun saat ini kriptografi menjadi elemen yang penting dalam komunikasi sehari-hari. Saat ini teknik kriptografi juga digunakan dalam kontrol akses pada website seperti *e-mail* dan *online banking* serta terkait autentikasi dan integritas data yang disebarkan melalui internet (Ding et al., 2016).

Kriptografi merupakan salah satu contoh bidang dimana penerapan basis Gröbner dapat dilakukan. Hal ini dikarenakan basis Gröbner adalah metode yang efektif dalam menyelesaikan sistem persamaan multivariat orde tinggi (Zhao et al., 2017). Pada kriptografi beberapa skema kripto dapat dijelaskan menggunakan sistem persamaan polinomial dengan parameter rahasia sebagai variabel. Hal ini memungkinkan untuk menyusun himpunan dalam ring polinomial, mendeskripsikan dan menghitung himpunan pembangun sehingga dapat mempelajari struktur ideal dan melakukan komputasi ideal. Selanjutnya Aljabar kriptanalisis menghasilkan penyelesaian sistem polinomial sehingga plainteks dapat diketahui.

Salah satu jenis sistem kriptografi adalah kriptografi kunci publik. Kriptografi ini menggunakan pasangan kunci publik dan kunci privat. Hal ini memungkinkan keamanan yang lebih kuat untuk menghindari terbukanya pesan rahasia. Permasalahan matematika yang sulit dipecahkan menjamin keamanan pada sistem ini. Sistem kunci publik multivariat adalah sistem kunci publik pada ring polinomial multivariat atas lapangan hingga. Keamanan kunci publik multivariat terletak pada penyelesaian sistem persamaan multivariat pada lapangan hingga.

Keamanan kriptografi harus selalu ditingkatkan agar pesan yang disampaikan tidak dapat dibuka oleh pihak lain. Salah satu cara untuk mengevaluasi

tingkat keamanan adalah kriptanalisis. Kriptanalisis adalah ilmu yang digunakan untuk memecahkan kriptografi. Kunci yang digunakan untuk dekripsi data tidak didapatkan secara langsung tetapi akan melalui proses lain pada kriptanalisis.

Penelitian sebelumnya (Zhao et al., 2017) membahas tentang aljabar kriptanalisis dari AES-256 yang menggunakan basis Gröbner. Pada penelitian ini diperkenalkan tranformasi linier dan persamaan linier multivariat dari AES-26 kemudian basis Gröbner digunakan dengan cara mengganti *term order* dan urutan variabel. Penelitian lain (Kara & Yayla, 2022) membahas tentang serangan basis Gröbner pada tiga kunci simetris berbeda yaitu JARVIS-like ciphers, MiMC, dan GMiMCerf.. Pada penelitian Sistem Kunci Publik Multivariat pada artikel (Riyanto, 2010) dijelaskan sistem kunci publik multivariat yang keamanannya bergantung pada sulitnya penyelesaian sistem persamaan polinomial yang dibentuk. Sehingga evaluasi keamanan dapat dilakukan dengan menyelesaikan sistem persamaan polinomial tersebut.

Berdasarkan penelitian sebelumnya, dapat dipahami bahwa basis Gröbner menjadi salah satu teori penting yang dapat diterapkan pada kriptografi untuk berbagai keamanan informasi. Sehingga peneliti tertarik untuk membahas bagaimana basis Gröbner dapat diterapkan pada kriptografi kunci publik multivariat. Salah satu jenis kriptografi yang melibatkan sistem persamaan polinomial di dalamnya. Hal ini sesuai dengan salah satu kegunaan basis Gröbner adalah dapat membantu mempermudah pencarian solusi persamaan polinomial. Oleh karena itu judul penelitian ini adalah "Aplikasi Basis Gröbner pada Kriptografi Kunci Publik Multivariat".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah pada penelitian ini adalah

1. Bagaimana konstruksi sistem kriptografi kunci publik multivariat?
2. Bagaimana aplikasi basis Gröbner pada kriptanalisis kriptografi kunci publik multivariat?

1.3 Tujuan Penelitian

Tujuan dari penelitian berdasarkan rumusan masalah yang telah dibuat adalah

1. Mengetahui konstruksi sistem kriptografi kunci publik multivariat.
2. Menerapkan basis Gröbner pada kriptanalisis kriptografi kunci publik multivariat.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat bagi pihak-pihak yang terkait, di antaranya:

1. Penulis

   Meningkatkan pengetahuan matematika khususnya pada istilah matematika dalam basis Gröbner dan aplikasinya pada kriptanalisis.

2. Lembaga

   Menjadi bahan pustaka yang dapat digunakan dalam penyelesaian masalah lain sehingga menambah jangkauan pengetahuan penelitian.

3. Pembaca

   Menambah pengetahuan terkait aplikasi basis Gröbner pada kriptanalisis sehingga memunculkan ide baru dalam teori ini.

1.5 Batasan Masalah

Penelitian ini berfokus pada aplikasi basis Gröbner pada kriptografi kunci publik multivariat pada lapangan berhingga dengan dua elemen atau $GF(2)$.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Ring

Ring adalah himpunan yang dilengkapi oleh dua operasi biner penjumlahan dan perkalian. Beberapa himpunan yang termasuk di dalamnya adalah himpunan bilangan bulat, himpunan bilangan riil, matriks, dan polinomial. Definisi dan sifat-sifat dari ring akan dijelaskan pada definisi berikut.

Definisi 2.1

Misalkan R merupakan suatu himpunan tak kosong yang dilengkapi dengan operasi biner berupa penjumlahan $(+)$ dan perkalian $(\cdot)$ sehingga untuk setiap $r_1, r_2, r_3 \in R$ berlaku beberapa sifat:

1. Penjumlahan pada R bersifat komutatif, yaitu $r_1 + r_2 = r_2 + r_1$.
2. Operasi penjumlahan pada R bersifat asosiatif, yaitu $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$.
3. Terdapat elemen identitas $0 \in R$ sehingga $r_1 + 0 = r_1$.
4. Untuk setiap $r_1 \in R$ terdapat $-r_1$ sedemikian sehingga $r_1 + (-r_1) = 0$.
5. Operasi perkalian $(\cdot)$ pada R bersifat asosiatif yaitu $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$.
6. Pada operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ di R berlaku sifat distributif kiri, yaitu $r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$ dan distributif kanan, yaitu $(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3)$ (Gallian, 2017).

Contoh ring yaitu himpunan bilangan bulat genap dengan notasi $2\mathbb{Z}$ yang dilengkapi dua operasi penjumlahan dan perkalian, serta himpunan matriks

berukuran 2×2 yang dilengkapi operasi penjumlahan dan perkalian yang entri-entrinya merupakan bilangan real.

$$M_{2\times 2}(\mathbb{R}) = A = \left\{ A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} | a_{ij} \in \mathbb{R}, i, j = 1, 2 \right\}$$

Sifat-sifat yang telah disebutkan merupakan syarat yang harus dipenuhi agar himpunan dengan dua operasi biner dapat disebut sebagai ring. Beberapa ring memiliki istilah khusus karena mempunyai sifat yang tidak selalu dimiliki oleh ring. Beberapa ring tersebut akan dijelaskan pada definisi berikut (Wahyuni et al., 2016).

Definisi 2.2

Diberikan suatu ring dengan operasi penjumlahan dan perkalian $(R, +, \cdot)$, maka dapat didefinisikan;

1. Ring R merupakan ring komutatif jika operasi perkalian pada R bersifat komutatif, yaitu $\forall r, s \in R$ berlaku $rs = sr$.
2. Ring R merupakan ring identitas jika ring R memiliki elemen identitas terhadap perkalian, yaitu $\exists 1_R$ sedemikian sehingga $\forall r \in R$ berlaku $r1_R = 1_R r = r$.
3. Ring R merupakan ring komutatif dengan elemen identitas jika R adalah ring komutatif yang memiliki elemen identitas terhadap perkalian.
4. Ring R disebut sebagai ring hasil bagi jika memiliki elemen identitas terhadap perkalian dan setiap elemen tak nolnya memiliki invers terhadap perkalian, yaitu $\forall r \in R$ dengan $r \neq 0$ terdapat $r^{-1} \in R$ sehingga $rr^{-1} = r^{-1}r = 1_R$. Ring hasil bagi dengan sifat komutatif dapat disebut juga sebagai lapangan. Contoh ring hasil bagi yaitu misalkan diberikan ring $\mathbb{Z}$ adalah bilangan bulat yang dilengkapi operasi penjumlahan dan perkalian. $\mathbb{Z}/6\mathbb{Z}$ merupakan contoh ring hasil bagi yang terdiri dari himpunan bilangan bulat modulo 6.

$$\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}.$$

Definisi 2.3

Lapangan adalah suatu ring komutatif dengan elemen identitas perkalian yang setiap elemen tak nolnya merupakan invers perkalian, yaitu $\forall u \in R$ dengan $u \neq 0$ terdapat $u^{-1} \in R$ sehingga $uu^{-1} = u^{-1}u = 1_R$ (Rasiman et al., 2018).

Suatu lapangan berhingga dengan q elemen biasa dinotasikan sebagai $GF(q)$ dan disebut sebagai lapangan berhingga atau biasa disebut sebagai Galois *fields*. Lapangan berhingga sangat berguna untuk menerjemahkan data komputer ke dalam bentuk biner. Bentuk biner pada data komputer merupakan kombinasi dua angka yaitu 0 dan 1. Dua angka ini merupakan elemen dari lapangan berhingga yaitu $GF(2)$. Beberapa contoh lapangan yaitu; ring himpunan bilangan bulat ($\mathbb{Z}, +, \cdot$), himpunan bilangan riil $(\mathbb{R}, +, \cdot)$ dan himpunan bilangan kompleks $(\mathbb{C}, +, \cdot)$ (Rasiman et al., 2018).

Definisi 2.4

Lapangan berhingga atau lapangan Galois merupakan lapangan yang memiliki elemen yang jumlahnya berhingga. Elemen-elemen dari lapangan Galois $GF(q)$ atau bisa juga dinotasikan $GF(p^n)$ dapat didefinisikan sebagai

$$GF(p^n) = \{0,1,2, \dots, p^n - 1\}$$

dimana $p \in \mathbb{P}$ dan $n \in \mathbb{Z}^+$ dan p merupakan karakteristik dari lapangan (Benvenuto, 2012). $\mathbb{P}$ adalah himpunan bilangan prima, yang berarti elemen-elemen di dalamnya adalah bilangan bulat positif yang hanya memiliki dua pembagi, yaitu 1 dan dirinya sendiriKarakteristik ring R didefinisikan sebagai bilangan bulat positif p terkecil sedemikian sehingga $px = 0$ untuk setiap $x \in R$ (Gilbert & Gilbert, 2013).

Contoh:

$GF(5) = (0,1,2,3,4,5)$ merupakan lapangan yang terdiri dari lima elemen yang masing-masing merupakan polinomial berderajat nol.

$$GF(2^3) = \{0,1,2,3,4,5,6,7\}$$

$GF(2^3)$ merupakan lapangan yang terdiri dari delapan elemen yang masing-masing elemen adalah polinomial dengan derajat terbesarnya adalah 2.

Hasil operasi penjumlahan dan perkalian berbeda tergantung lapangan yang digunakan. Berikut merupakan tabel hasil operasi penjumlahan pengurangan dan perkalian pada $GF(2)$.

Tabel 2.1 Hasil Operasi Penjumlahan pada $\boldsymbol{GF(2)}$

+	1	0
1	0	1
0	1	0

Tabel 2.2 Hasil Operasi Pengurangan pada $\boldsymbol{GF(2)}$

−	1	0
1	0	1
0	1	0

Tabel 2.3 Hasil Operasi Perkalian pada $\boldsymbol{GF(2)}$

×	1	0
1	1	0
0	0	0

Definisi 2.5

Monomial pada $x_1, \dots, x_n$ dapat dituliskan dalam bentuk $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$. Semua pangkat $\alpha_1, \dots, \alpha_n$ merupakan bilangan bulat positif. Penjumlahan semua pangkat dihasilkan dari penjumlahan $\alpha_1 + \cdots + \alpha_n$ (Cox et al., 2015).

Penjumlahan dari beberapa monomial akan membentuk polinomial. Polinomial merupakan jumlah monomial yang terbatas dan semua variabel memiliki derajat bilangan bulat positif. Contoh monomial adalah x^3y^3 dan $2x^3y^2z$.

Definisi 2.6

Polinomial dengan variabel $x_1, \dots, x_n$ dengan koefisien anggota lapangan k adalah kombinasi linier hingga dari monomial. Bentuk umum polinomial adalah

$$f = \sum_i a_i x^i,\ a_n \in k, i = 1, \dots, n.$$

Himpunan dari semua polinomial dengan variabel $x_1, \dots, x_n$ dan koefisien di k dinyatakan sebagai $k[x_1, \dots, x_n]$ sehingga polinomial dengan satu variabel (x) , dua variabel (x, y), dan tiga variabel(x, y, z) dapat dinyatakan berturut-turut sebagai $k[x], k[x, y], k[x, y, z]$. Misalkan $f = \sum_i a_i x^i$ adalah polinomial pada $k[x_1, \dots, x_n]$ maka

1. a_α disebut sebagai koefisien dari monomial x^i,
2. $a_\alpha \neq 0$ menunjukkan bahwa $a_i x^i$ adalah polinomial,
3. Derajat total dari $f \neq 0$ atau bisa ditulis sebagai deg(f), merupakan nilai maksimum dari $|\alpha|$ sehingga koefisien a_i bukanlah nol (Cox et al., 2015).

Berikut merupakan contoh polinomial:

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2.$$

Selanjutnya akan didefinisikan ring dari polinomial atas suatu ring R. Misalkan diberikan suatu ring komutatif R maka himpunan

$$R[x] = \{a_0x^0 + a_1x^1 + \cdots + a_nx^n | a_i \in R, n \in \mathbb{Z}^+\}$$

disebut sebagai ring dari polinomial atas R pada x (Gallian, 2017).

Definisi 2.7

Misalkan R adalah ring komutatif dengan elemen identitas. Untuk setiap

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

dan

$$g(x) = \sum_{i=0}^{m} b_i x^i$$

pada ring R, maka didefinisikan operasi penjumlahan dan perkalian pada $R[x]$ di bawah ini:

1. Operasi Penjumlahan

$$f(x) + g(x) = \sum_{\alpha=0}^{k} (a_i + b_i)x^i,$$

di mana k adalah bilangan bulat terbesar dari n dan m.

2. Operasi Perkalian

$$\sum_{\alpha=0}^{n+m} (ab)_i x^i.$$

(Gilbert & Gilbert, 2013).

Definisi 2.8 Algoritma Pembagian

Misalkan $f(x)$ dan $g(x)$ adalah polinomial dengan koefisien bilangan riil sehingga $g(x) \neq 0$. Maka terdapat polinomial $q(x)$ dan $r(x)$ sedemikian sehingga

$$f(x) = g(x)q(x) + r(x)$$

Polinomial $q(x)$ merupakan hasil bagi sedangkan $r(x)$ merupakan sisa pembagian. Derajat sisa pembagian $r(x)$ akan selalu lebih kecil dari derajat hasil bagi $g(x)$. Berikut merupakan contoh pembagian $f = x^4 + x + 1$ oleh $g = x^2 + 1$ menghasilkan sisa pembagian $r = x + 2$. Sesuai definisi dapat dilihat bahwa derajat r kurang dari derajat g.

Pembagian polinomial akan lebih rumit dilakukan ketika bekerja pada polinomial yang lebih dari satu variabel. Diperlukan istilah-istilah untuk membuat urutan polinomial variabel(Adams & Loustaunau, 1994).

Definisi 2.9

Monomial ordering merupakan semua hubungan $>$ pada himpunan monomial x^{α}, $\alpha \in \mathbb{N}$, yang memenuhi:

1. $>$ merupakan order total pada $\mathbb{N}$
2. Jika $\alpha > \beta$ dan $\gamma \in \mathbb{N}$, maka $\alpha + \gamma > \beta + \gamma$
3. $>$ adalah *well-ordering* pada $\mathbb{N}$. Setiap himpunan bagian tak kosong dari $\mathbb{N}$ memiliki elemen terkecil di bawah $>$, dengan kata lain jika $A \subseteq \mathbb{Z}^n = \emptyset$ maka terdapat $\alpha \in A$ sedemikian sehingga $\beta > \alpha$. $\forall \beta \neq \alpha$ di A.

Setiap order monomial bergantung pada order variabel yang telah ditentukan. Suatu monomial akan mempunyai urutan yang berbeda tergantung kepada jenis order yang digunakan. Urutan monomial pada suatu polinomial yang sama akan berbeda jika jenis order yang digunakan berbeda. Berikut merupakan jenis-jenis order monomial:

1. *Lexicographical Order (lex)*

   Misalkan $\alpha = (\alpha_1, \dots, \alpha_n)$ dan $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}$. Jika $\alpha - \beta > 0$ atau menghasilkan bilangan positif maka $\alpha >_{lex} \beta$, sehingga $x^{\alpha} >_{lex} x^{\beta}$.

   Contoh:

   $(1, 2, 0) >_{lex} (0, 3, 4)$ karena $\alpha - \beta = (1, -1, -4)$.

   $(3, 2, 4) >_{lex} (3, 2, 1)$ karena $\alpha - \beta = (0, 0, 3)$.

2. *Degree Lexicographical Order (deglex)*

   Misalkan $\alpha = (\alpha_1, \dots, \alpha_n)$ dan $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}$. $\alpha >_{deglex} \beta$ jika $|\alpha| > |\beta|$ atau $|\alpha| = |\beta|$ dan $|\alpha| >_{lex} |\beta|$. Urutan *deglex* memutuskan urutan dengan menggunakan derajat total, kemudian menggunakan order *lex*.

   Contoh:

   $(1, 2, 3) >_{deglex} (3, 2, 0)$ karena $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.

   $(1, 2,4) >_{deglex} (1, 1, 5)$ karena$|(1, 2, 4)| = |1, 1, 5|$

   kemudian menggunakan order *lex* diperoleh $(1, 2, 4) >_{lex} (1, 1, 5)$.

3. *Degree Reverse Lexicographical Order (degrevlex)*

   Misalkan $\alpha = (\alpha_1, \dots, \alpha_n)$ dan $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}$. Maka $\alpha >_{degrevlex} \beta$ jika $|\alpha| > |\beta|$ atau $|\alpha| = |\beta|$ dan elemen paling kanan atau derajat dari variabel terbesar $\alpha - \beta < 0$ (Cox et al., 2015).

   Contoh:

   $(4, 7, 1) > (4, 2, 3)$ karena $|(4, 7, 1)| = 12 > |4, 2, 3| = 9$.

   $(1, 5, 2) > (4, 1, 3)$ karena $|1, 5, 2| = |4, 1, 3|$ dan $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$.

Contoh:

Diberikan polinomial $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$, maka;

Menggunakan order *lex* diperoleh

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$$

Menggunakan order *deglex* diperoleh

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$$

Menggunakan order *degrevlex* diperoleh

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

Definisi 2.10

Misalkan $f = \sum_\alpha a_\alpha x^\alpha$ adalah polinomial tak nol pada $k[x_1, \dots, x_n]$ yang dapat ditulis sebagai $f = a_1x^{\alpha_1} + a_2x^{\alpha_2} + \cdots + a_rx^{\alpha_r}$ dengan $a_i \in k - \{0\}, x^{\alpha_i} \in \mathbb{T}^n$, dan $x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_r}$, maka

1. *Power Product* utama (*leading power)*

$$LP(f) = x^{\alpha_1}$$

2. Koefisien utama (*leading coefficient)*

$$LC(f) = a_1$$

3. Suku utama (*leading term)*

$$LT(f) = LC(f) \cdot LP(f) = a_1x^{\alpha_1}$$

(Noviani et al., 2013).

Diberikan contoh dari pembagian polinomial berikut:

Misalkan $f = x^2 + xy + 1$ dengan $g = xy - x$ sebagai pembagi polinomial menggunakan urutan lex.

Suku utama f adalah x^2 sedangkan suku utama g adalah xy. Dapat disimpulkan bahwa f tidak dapat dibagi dengan g jika bekerja pada polinomial satu variabel. Akan tetapi pada polinomial multivariabel hal ini dapat dilakukan karena suku

kedua f masih dapat dibagi oleh suku utama g. Dengan mengabaikan suku utama dari f maka operasi dapat dilakukan sebagai berikut.

$$xy - x \quad \sqrt{\begin{array}{r} 1 \\ \hline x^2 + xy + 1 \\ xy - x \\ \hline x^2 + x + 1 \end{array}}$$

Hasil pembagian $q = 1$ dan sisa pembagiannya adalah $x^2 + x + 1$. Pada kasus ini pembagian dapat dilakukan tetapi hasil pembagian tidak sesuai dengan algoritma pembagian polinomial di mana derajat sisa lebih besar dibanding derajat hasil bagi.

Berdasarkan contoh dapat disimpulkan bahwa terdapat dua langkah dalam membagi polinomial multivariabel f dengan polinomial multivariabel g yaitu:

1. Memilih order monomial yang akan digunakan.
2. Membagi suku pada f menggunakan suku utama g sampai tidak ada lagi suku pada g yang dapat terbagi oleh suku utama g (Cox et al., 2015).

Suatu polinomial f dapat dibagi dengan himpunan polinomial $F = \{f_1, \dots, f_n\}$, kemudian dapat ditulis $f = \sum_i^n q_i f_i + r$ dimana q_i menunjukkan hasil bagi dan r adalah sisa pembagian. Diberikan contoh sebagai berikut:

Misalkan $F = \{f_1, f_2\}$ dimana $f_1 = xy - 1$, $f_2 = y^2 - 1$, kemudian $f = xy^2 - y^3 + x^2 - 1$. Jika pembagian polinomial dilakukan dengan membagi polinomial f dengan f_1 kemudian f_2 menggunakan order lex maka diperoleh:

$$xy - 1 \quad \sqrt{\begin{array}{r} y \\ \hline xy^2 - y^3 + x^2 - 1 \\ xy^2 - y \\ \hline -y^3 + x^2 + y - 1 \end{array}}$$

$$y^2-1 \quad \begin{array}{r} -y \\ \hline -y^3+x^2+y-1 \\ -y^3+y \\ \hline x^2-1 \end{array}$$

$f = q_1 f_1 + q_2 f_2 + r$

$r = x^2 - 1$

$q_1 = y,\ q_2 = -y$

Selanjutnya ketika urutan pembagian diubah menjadi f_2 kemudian f_1. Sisa pembagian dengan f_2 sudah tidak bisa dibagi dengan f_1 dengan perhitungan berikut:

$$y^2-1 \quad \begin{array}{r} x-y \\ \hline xy^2-y^3+x^2-1 \\ xy^2-x \\ \hline -y^3+x^2+x-1 \\ -y^3+y \\ \hline x^2+x-y-1 \end{array}$$

$f = q_1 f_1 + q_2 f_2 + r$

$r = x^2 + x - y - 1$

$q_1 = 0,\ q_2 = x - y$

Sisa pembagian yang dihasilkan tidak tunggal atau berbeda tergantung urutan pembagian sehingga tidak dapat dikatakan bahwa sisa pembagiannya akan menghasilkan 0. Untuk mendapatkan sisa pembagian yang tunggal untuk berbagai urutan atau order yang digunakan, selanjutnya diberikan dasar-dasar teori basis Gröbner.

2.1.2 Basis Gröbner

Basis Gröbner dan algoritma Buchberger diperkenalkan pertama kali pada tahun 1965 oleh Bruno Buchberger. Pada aljabar komputer, basis Gröbner

merupakan himpunan pembangkit dari ideal pada ring polinomial satu variabel dan multivariabel (Das & Reza, 2018). Beberapa istilah serta teorema perlu dipahami dan dibuktikan agar dapat memahami konsep basis Gröbner. Berikut ini akan didefinisikan beberapa definisi serta teorema yang akan digunakan.

Definisi 2.11

Misalkan R adalah ring dan $I \subseteq R$. Himpunan I adalah ideal jika memenuhi $\forall\, r \in R$ dan $a \in I$, maka $r \cdot a \in I$ dan $a \cdot r \in I$ (Cox et al., 2015).

Contoh ideal yaitu $\{0_R\}$ dan R yang merupakan ideal untuk setiap ring R dan himpunan bilangan bulat genap adalah ideal dari ring R.

Definisi 2.12

Suatu ring disebut sebagai ring Noetherian jika setiap ideal $I \in R$ dihasilkan secara berhingga. $I = \langle f_1, \dots, f_s \rangle$, sedemikian sehingga $f_i \in R$ untuk $i = 1, \dots, s$.

Berikut merupakan contoh ring Notherian:

Lapangan k merupakan ideal yang dibangun secara berhingga (*finitely generated)* ($k = \langle 1 \rangle$). Ideal dari k yang lain adalah $\langle 0 \rangle$. Keduanya merupakan ideal utama yang dihasilkan secara berhingga. Oleh karena itu $k[x_1]$ adalah Notherian ketika k merupakan lapangan.

Basis Gröbner dari ideal I merupakan himpunan pembangun dari I. Misalkan $I \subset k[x_1, \dots, x_n]$ merupakan ideal. Misalkan $LT(I)$ merupakan himpunan suku utama dari elemen-elemen pada I, maka

$$LT(I) = \{cx^{\alpha}\}$$

$$LT(f) = cx^{\alpha}, f \in I$$

$\langle LT(I) \rangle$ merupakan ideal pembangun dari elemen $LT(I)$ (Cox et al., 2015).

Definisi 2.13

Himpunan polinomial tak nol $G = \{g_1, \dots, g_t\} \in I$ merupakan basis Gröbner jika

$$\langle LT(g_1), \dots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Suatu himpunan $\{g_1, \dots, g_t\}$ dikatakan sebagai basis Gröbner dari I jika dan hanya jika suku utama dari sebarang elemen di I terbagi oleh salah satu elemen $LT(g_i)$ karena ideal $\langle LT(I)\rangle$ dihasilkan oleh $LT(g_i)$. Selanjutnya untuk menghitung basis Gröbner diperlukan definisi untuk Polinomial-S (Cox et al., 2015).

Definisi 2.14

1. Misalkan monomial utama dari polinomial f dan g adalah

   $$LM(f) = \prod_{i=1}^{n} x_i^{\alpha_i}, LM(g) = \prod_{i=1}^{n} x_i^{\beta_i}$$

   maka x^{γ} merupakan LCM (*least common multiple)* dari $LM(f)$ dan $LM(g)$, jika $\gamma = (\gamma_1, \dots, \gamma_n)$ sedemikian sehingga $\gamma_i = \max(\alpha_i.\beta_i)$ untuk setiap i.

2. Polinomial-S dari f dan g merupakan kombinasi dengan definisi:

   $$S(f,g) = \frac{x^{\gamma}}{LT(f)} \cdot f - \frac{x^{\gamma}}{LT(g)} \cdot g$$

   Perhatikan bahwa Polinomial-S dibangun dengan mengeliminasi suku utama f dan g dan selalu memiliki suku utama yang lebih kecil dari f dan g (Cox et al., 2015).

Berikut merupakan contoh perhitungan polinomial-S:

Misalkan $F = \{f_1, f_2\}$ dimana $f_1 = xy - 1$ dan $f_2 = y^2 - 1$ menggunakan order *lex* maka

$$LM(f_1) = xy \text{ dan } LM(f_2) = y^2$$

LCM dari $LM(f_1)$ dan $LM(f_2)$ adalah

$$x^{\gamma} = xy^2$$

Oleh karena itu

$$S(f_1, f_2) = \frac{xy^2}{xy} f_1 - \frac{xy^2}{y^2} f_2 = yf -_1 xf_2$$

$$= y(xy - 1) - x(y^2 - 1) = x - y$$

Algoritma Buchberger

Algoritma buchberger merupakan algoritma yang dapat digunakan untuk membentuk basis Gröbner dari $I = (f_1. \ldots . f_m)$ (Adams & Loustaunau, 1994)

Algoritma buchberger merupakan alat yang digunakan untuk menghitung basis Gröbner dari ideal pada ring polinomial. Basis Gröbner mempermudah pencarian solusi sistem persamaan polinomial dan analisis ideal. Masukan dari algoritma Buchberger merupakan polinomial-polinomial pada $k[x_1, \ldots, x_n]$ yang digunakan untuk membentuk ideal $I = \langle f_1, \ldots, f_s \rangle$.

Algoritma Buchberger

Input: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ dimana $f_i \neq 0$, untuk $1 \leq i \leq s$

Output: $G = \{g_1, \ldots, g_n\}$, basis Gröbner dari $I = \langle f_1, \ldots, f_s \rangle$.

Initialization: $G \coloneqq F, \mathcal{G} \coloneqq \left\{ \{f_i, f_j\} \middle| f_i \neq f_j \in G \right\}$

While $\mathcal{G} \neq \emptyset$ ***do***

Pilih sebarang $\{f, g\} \in \mathcal{G}$

$\mathcal{G} \coloneqq \mathcal{G} - \{\{f, g\}\}$

$S(f, g) \overset{G}{\rightarrow}_+ h$

If $h \neq 0$ ***then***

$\mathcal{G} \coloneqq \mathcal{G} \cup \{\{u.h\} | \forall u \in G$

$G \coloneqq G \cup \{h\}$

return G

Berikut merupakan contoh penerapan algoritma Buchberger:

Misalkan $f_1 = y^2 + yx + x^2$, $f_2 = y + x$, dan $f_3 = y \in \mathbb{Q}[x, y]$. Selanjutnya dihitung basis Gröbner untuk $I = \langle f_1, f_2, f_3 \rangle$ dengan menggunakan order *lex* dan $y > x$.

Initialization**:** $G \coloneqq \{f_1, f_2, f_3\}$

$\mathcal{G} \coloneqq \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$

Menggunakan perulangan WHILE pertama

$\mathcal{G} \coloneqq \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$S(f_1, f_2) = x^2$

$f_4 \coloneqq x^2$

$\mathcal{G} \coloneqq \{\{f_1, f_3\}, \{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G \coloneqq \{f_1, f_2, f_3, f_4\}$

Menggunakan perulangan WHILE kedua

$\mathcal{G} \coloneqq \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(\{f_1, f_3) \xrightarrow{G}_{+} 0$

Menggunakan perulangan WHILE ketiga

$\mathcal{G} \coloneqq \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_2, f_3) = x$

$f_5 = x$

$\mathcal{G} \coloneqq \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$G \coloneqq \{f_1, f_2, f_3, f_4, f_5\}$

Menggunakan perulangan WHILE keempat

$\mathcal{G} \coloneqq \{\{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(\{f_1, f_3) \xrightarrow{G}_+ 0$

Menggunakan perulangan WHILE kelima

$\mathcal{G} \coloneqq \{\{f_3, f_4\}, \{f_1, f_5\}, \{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$

$S(\{f_1, f_3) \xrightarrow{G}_+ 0$

Perulangan menggunakan WHILE pada contoh ini akan menghasilkan polinomial S yang tereduksi ke nol untuk perulangan selanjutnya, sehingga $\{f_1, f_2, f_3, f_4, f_5\}$ adalah basis Gröbner untuk $\langle f_1, f_2, f_3 \rangle$

Definisi 2.15

Basis Gröbner tereduksi untuk himpunan polinomial F adalah basis Gröbner G dari F sedemikian sehingga:

1. Koefisien utamanya adalah 1 untuk semua $p \in G$.
2. Untuk semua $p \in G$, tidak ada suku p yang habis dibagi oleh suku utama q, untuk setiap $q \in G - \{p\}$ (Cox et al., 2015).

Algoritma untuk menghitung basis Gröbner tereduksi

Input: $F = \{f_1, \dots, f_s\}$

Output: $G = \{g_1, \dots, g_n\}$ basis Gröbner tereduksi dari F

Method:

Pilih order monomial

Nilai awal $G \coloneqq F$

Ulangi $\mathcal{G} \coloneqq G$

Pilih sebarang $\{f, g\}, f \neq g \in \mathcal{G}$, selanjutnya cari Polinomial-S $S(p, q)$

bagi $S(p, q)$ dengan himpunan polinomial di $\mathcal{G}$

Jika $S \neq 0$ maka $G \coloneqq G \cup \{S\}$

Bagi setiap $f \in G$ dengan $G - \{f\}$ untuk mendapatkan f'. Jika $f' \neq 0$, perlu mengganti f dengan f' di G. Jika $f' = 0$ maka $G = G - \{p\}$.

Sampai $G = \mathcal{G}$

Contoh perhitungan basis Gröbner tereduksi:

Misalkan $F = \{f_1, f_2\}$ dimana $f_1 = xy - 1$, $f_2 = y^2 - 1$, kemudian $f = xy^2 - y^3 + x^2 - 1$. Hitunglah basis Gröbner tereduksi dari ideal yang dihasilkan oleh F dan menggunakan order *lex*.

Pertama, basis Gröbner $G = F$. Selanjutnya menghitung $S(f_1, f_2)$ dan diperoleh $S(f_1, f_2) = x - y$. Misalkan $f_3 = S(f_1, f_2)$ sisa pembagian f_3 oleh G adalah f_3. Karena $f_3 \neq 0$ maka dengan langkah ketiga f_3 ditambahkan pada G sehingga $G = \{f_1, f_2, f_3\}$. Selanjutnya sisa pembagian adalah 0 ketika f_1 dibagi oleh $\{f_2, f_3\}$ maka $G = \{f_2, f_3\}$. Kemudian polinomial-polinomial tidak dapat dihilangkan dari G dan kembali ke awal perulangan dengan $G = \{f_2, f_3\}$.

Pada Langkah pertama, $f_4 = S(f_2, f_3) = y^3 - x$ memiliki sisa pembagian nol ketika dibagi oleh G. Perulangan dapat dihentikan dan basis Gröbner tereduksi yang dihasilkan adalah

$$G = \{x - y, y^2 - 1\}.$$

2.1.3 Penyelesaian Sistem Persamaan Polinomial

Teori eliminasi sering digunakan untuk memecahkan suatu sistem persamaan. Tujuan dari eliminasi adalah mencari salah satu nilai variabel dengan menghilangkan variabel yang lain. Setelah salah satu variabel ditemukan maka variabel dikembalikan pada persamaan untuk mencari nilai variabel yang lain. Salah satu penerapan basis Gröbner yaitu pada teori eliminasi. Teori eliminasi digunakan untuk mencari solusi sistem persamaan polinomial.

Definisi 2.16

Diberikan $I = \langle f_1, \dots, f_s \rangle$ adalah ideal pada $k[x_1, \dots, x_n]$. Eliminasi l pada ideal I_l didefinisikan sebagai $I_l = I \cap k[x_{l+1}, \dots, x_n]$ (Guevara, 2016).

Teorema 2.17 (Teorema Eliminasi)

Misalkan $I \subset k[x_1, \dots, x_n]$ adalah ideal dan G merupakan basis Gröbner dari I order monomial dengan eliminasi l. Maka untuk setiap $0 \leq l \leq n$, himpunan

$$G_l = G \cap k[x_{l+1}, \dots, x_n]$$

adalah basis Gröbner dari eliminasi l dari ideal I (Cox et al., 2015).

Bukti:

Diketahui bahwa $G_l \subset I_l$ sehingga untuk membuktikan bahwa G_l adalah basis Gröbner perlu dibuktikan bahwa $\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$. Jelas bahwa $\langle LT(G_l) \rangle \subset \langle LT(I_l) \rangle$. Untuk membuktikan bahwa $\langle LT(I_l) \rangle \subset \langle LT(G_l) \rangle$ perlu diperlihatkan bahwa jika $f \in I$ maka $LT(f)$ dapat dibagi oleh $LT(g)$ untuk setiap $g \in G_l$. Karena $f \in I$ dan G adalah basis Gröbner dari I, $LT(f)$ dapat dibagi oleh $g \in G$. Tetapi karena $f \in I_l$ berarti $LT(g)$ hanya melibatkan variabel $x_{l+1}, \dots, x_n$. Jadi, order monomial bertipe eliminasi l. $g \in k[x_{l+1}, \dots, x_n]$. ■

Contoh mencari solusi sistem persamaan polinomial:

$$x^2 + y + z = 1,$$

$$x + y^2 + z = 1,$$

$$x + y + z^2 = 1,$$

$$x^2 + y^2 + z^2 = 1.$$

Jawab:

$$F = \{x^2 + y + z = 1, x + y^2 + z = 1, x + y + z^2 = 1, x^2 + y^2 + z^2 = 1\}$$

$$I = \langle x^2 + y + z = 1, x + y^2 + z = 1, x + y + z^2 = 1, x^2 + y^2 + z^2 = 1\rangle.$$

Basis Gröbner tereduksi G dari I dengan order lex $x > y > z$ adalah

$$G = \{z^2 - z, 2yz + z^4 + z^2 - 2z,\ y^2 - y - z^2 + z, x + y + z^2 - 1\}$$

Menggunakan teorema eliminasi basis Gröbner dari ideal eliminasi I_1 dan I_2 maka diperoleh;

$$G_1 = G \cap k[y, z] = (z^2 -\ z, 2yz + z^4 + z^2 - 2z,\ y^2 - y - z^2 + z)$$

$$G_2 = G \cap k[y, z] = (z^2 - z).$$

Basis Gröbner dari I_2 hanya memiliki satu variabel sehingga I_2 dihasilkan dari satu elemen. Selanjutnya dapat dilakukan subtitusi mundur untuk menyelesaikan sistem persamaan yang didefinisikan oleh G_2. Langkah-langkah berikutnya adalah

1. Menyelesaikan $z^2 - z = 0$ sehingga $z = 0$ atau $z = 1$.
2. Menyelesaikan persamaan yang didefinisikan oleh polinomial pada himpunan $G_2 - G_1$ yaitu

   $$2yz + z^4 + z^2 - 2z = 0$$

   $$y^2 - y - z^2 + z = 0.$$

   Ketika $z = 0$ maka $y = 0$ atau $y = 1$ namun ketika $z = 1$ maka $y = 0$.

3. Menyelesaikan persamaan yang didefinisikan oleh polinomial pada himpunan $G - G_1$ yaitu

$$x + y + z^2 - 1 = 0,$$

Subtitusi $y = 0$ dan $z = 0$ pada persaman maka menghasilkan nilai $x = 1$.

Subtitusi $y = 1$ dan $z = 0$ pada persaman maka menghasilkan nilai $x = 0$.

Subtitusi $y = 0$ dan $z = 1$ pada persaman maka menghasilkan nilai $x = 0$.

Sehingga diperoleh solusi dari sistem persamaan adalah

$$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

2.1.4 Sistem Kriptografi

Kriptografi dikenal sebagai ilmu untuk mengamankan pesan. Pada awalnya Ilmu memiliki tujuan yang penting pada dunia politik dan militer. Namun akhir-akhir ini kriptografi sangat dibutuhkan pada komunikasi sehari-hari. Kriptografi digunakan dalam mengamankan pesan dan kontrol akses pada *website* untuk keperluan keaslian dan integritas data yang dikirim melalui internet (Ding et al., 2016).

Kriptografi memiliki suatu sistem yang di dalamnya terdapat kumpulan aturan untuk melakukan enkripsi dan dekripsi pesan. Sistem kriptografi dibagi menjadi dua macam yaitu sistem kriptografi kunci rahasia dan sistem kriptorrafi kunci publik (Riyanto, 2010).

1. Sistem Kriptografi Kunci Rahasia

   Sistem kriptografi kunci rahasia biasa disebut juga sebagai sistem kriptografi simetris. Sistem kriptografi ini menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi. Pengirim dan penerima pesan memerlukan kesepakatan suatu kunci sebelum komunikasi dilakukan.

Keamanan kunci merupakan hal yang harus selalu diperhatikan. Jika terjadi kebocoran kunci maka pihak yang tidak diinginkan bisa melakukan enkripsi dan dekripsi pada pesan yang dikirimkan. oleh karena itu jalur yang digunakan dalam pertukaran kunci haruslah aman atau harus melalui orang yang sangat dipercaya.

2. Sistem Kriptografi Kunci Publik

Sistem kriptografi kunci publik atau asimetris menggunakan dua jenis kunci dalam enkripsi dan dekripsi pesan. Kunci tersebut biasa disebut sebagai kunci publik atau kunci rahasia. Enkripsi pesan dilakukan menggunakan kunci publik sedangkan dekripsi pesan dilakukan dengan menggunakan kunci rahasia. Kunci rahasia merupakan kunci yang hanya diketahui oleh pihak tertentu sedangkan kunci publik dapat diketahui semua pihak karena bersifat umum. Terdapat beberapa hal yang harus terpenuhi dalam algoritma asimetris, yaitu:

a. Penerima B merupakan pihak yang harus membuat pasangan kunci, baik itu kunci publik atau kunci rahasia.
b. Pengirim A melakukan enkripsi pesan menggunakan kunci publik sehingga menghasilkan cipherteks $c = e_{K_{pB}}(x)$.
c. Dekripsi pesan dilakukan oleh penerima menggunakan kunci privat dan menghasilkan plainteks asli

$$d_{K_{pB}}\left[e_{K_{pB}}(x)\right] = d_{K_{pB}}(c) = x.$$

d. Pihak lain hanya mengetahui kunci publik sehingga kesulitan unntuk mengetahui kunci rahasia dan isi pesan x yang dikirimkan.

2.1.5 Sistem Kriptografi Kunci Publik Multivariat

Sistem kriptografi kunci publik multivariat merupakan kriptografi yang pemetaan enkripsinya adalah pemetaan $F : K^n \rightarrow K^m$, yaitu

$$F(x_1, \dots, x_n) = (f_1, \dots, f_m)$$

Langkah pertama pada konstruksi sistem ini adalah membentuk suatu pemetaan $F : K^n \rightarrow K^m$ sehingga dua kondisi berikut ini terpenuhi.

1. $F(x_1, \dots, x_n) = (f_1, \dots, f_m)$, $f_i \in K(x_1, \dots, x_n)$.
2. Persamaan $F(x_1, \dots, x_n) = (y''_1, \dots, y'_m)$ dapat diselesaikan atau dapat dihitung prapeta dari $(y''_1, \dots, y'_m)$. Prapeta pada pemetaan haruslah tunggal karena akan digunakan untuk enkripsi. Prapeta dapat dituliskan sebagai $F^{-1}(y''_1, \dots, y'_m)$.

Selanjutnya pemetaan F dikontruksi dengan komposisi tiga pemetaan berikut:

$$F = S \circ F \circ T,$$

S dan T adalah pemetaan $K^n \rightarrow K^m$. Keduanya juga merupakan transformasi affine invertibel. Yang dipilih secara acak Transformasi affine invertibel adalah penggabungan antara transformasi linier dan translasi serta memiliki sifat invertibilitas (memiliki invers). Misalkan T adalah transformasi affine, maka T dapat didefinisikan:

$$T(x) = Ax + b.$$

A merrupakan matriks persegi dengan ukuran $n \times n$ yang merupakan transformasi linier sedangkan b adalah vektor translasi yang biasanya berukuran $n \times 1$. Selanjutnya, dapat diketahui bahwa kunci publik berjumlah m polinomial dalam F

dan lapangan berhingga K. Kemudian kunci rahasianya adalah pemetaan S dan T. Kunci publik yang digunakan dapat dinyatakan sebagai

$$(f_1, \dots, f_m) = S(F(T(x_1, \dots, x_n))). \quad (2.1)$$

Dekripsi cipherteks $Y' = (y'_1, \dots, y'_m)$ dilakukan dengan menentukan solusi persamaan $F(x_1, \dots, x_n) = Y'$. Dekripsi chipherteks dilakukan dengan:

1. Menyatakan cipherteks pada bentuk biner yang sesuai.
2. Menggunakan kunci privat yang telah ditentukan.
3. Melakukan tranformasi balik dari transformasi sebelumnya.

Berikut merupakan contoh penerapan enkripsi dan dekripsi kriptografi kunci publik multivariat. Tahap pertama yang dilakukan adalah menentukan kunci publik dan kunci privat yang akan digunakan. Misalkan digunakan lapangan berhingga GF(2) dengan dimensi 2. Selanjutnya ditentukan polinomial $F = (f_1, f_2)$ sebagai berikut:

$$f_1 = x_1 + x_2,$$

$$f_2 = x_1 \cdot x_2.$$

Kemudian, transformasi affine invertibel yang akan digunakan;

$$S(x_1, x_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2.2)$$

$$T(x_1, x_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (2.3)$$

Kunci publik yang digunakan dapat diperoleh dari komposisi pemetaan polinomial dan transformasi invertibel pada persamaan (2.2) dan (2.3).

$$y = T \circ F \circ S$$

$$(p_1, p_2) = T(F(S(x_1, x_2)))$$

$$= T(F(x_1 + 1, x_2))$$

$$= T((x_1 + 1) + x_2, (x_1 + 1) \cdot x_2)$$

$$= T(x_1 + x_2 + 1, x_1x_2 + x_2)$$

$$= T(x_1 + x_2 + 1, x_1x_2 + x_2)$$

$$= ((x_1 + x_2 + 1) + 1, (x_1x_2 + x_2) + 1)$$

$$= (x_1 + x_2, x_1x_2 + x_2 + 1)$$

Sehingga diperoleh:

$p_1 = x_1 + x_2$

$p_2 = x_1x_2 + x_2 + 1$

Misalkan plainteks yang akan dienkripsi adalah (1,1) maka dapat diperoleh perhitungan cipherteks berikut:

$Y = y'_1, y'_2$

$= F(1,1)$

$= (p_1(1,1), p_2(1,1))$

$= (0,1)$

Selanjutnya, tahap dekripsi dapat dilakukan menggunakan kunci rahasia yang telah dibentuk. Kunci tersebut adalah transformasi affine S persamaan 1 dan T pada persamaan 2. Perhitungan yang dilakukan menggunakan invers dari kunci privat tersebut. S dan T merupakan invers itu sendiri karena dilakukan pada GF(2). Sehingga diperoleh plainteks melalui perhitungan berikut:

$Y_1 = T(Y)$

$= T(0,1)$

$= (0,1) + (1,1)$

$= (1,0)$

$$Y_2 = S(Y_1)$$
$$= S(1,0)$$
$$= (0,1) + (1,0)$$
$$= (1,1)$$

2.2 Kajian Integrasi Topik dengan Al-Qur'an/Hadits

Al-Qur'an dan hadits menjadi sumber pedoman hidup bagi umat Islam. Pembahasan segala aspek kehidupan terdapat di dalam Al-Qur'an. Mulai urusan ibadah sampai urusan bermasyarakat. Sumber pedoman tersebut menjadi rujukan dalam mengatur kehidupan. Sebagaimana Allah SWT. berfirman dalam surat An-Nisa' ayat 59 (Kementrian Agama RI, 2019):

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اَطِيْعُوا اللّٰهَ وَاَطِيْعُوا الرَّسُوْلَ وَاُولِى الْاَمْرِ مِنْكُمْ فَاِنْ تَنَازَعْتُمْ فِيْ شَيْءٍ فَرُدُّوْهُ اِلَى اللّٰهِ وَالرَّسُوْلِ اِنْ كُنْتُمْ تُؤْمِنُوْنَ بِاللّٰهِ وَالْيَوْمِ الْاٰخِرِ ذٰلِكَ خَيْرٌ وَّاَحْسَنُ تَأْوِيْلًا (٥٩)

Artinya:
"*Wahai orang-orang yang beriman, taatilah Allah dan taatilah Rasul (Muhammad), dan Ulil Amri (pemegang kekuasaan) di antara kamu. Kemudian, jika kamu berbeda pendapat tentang sesuatu, maka kembalikanlah kepada Allah (Al-Qur'an) dan Rasul (sunnahnya), jika kamu beriman kepada Allah dan hari kemudian. Yang demikian itu lebih utama (bagimu) dan lebih baik akibatnya".* (QS An-Nisa':59).

Salah satu hal yang diatur dalam Al-Qur'an adalah tentang amanah. Amanah dalam hal ini berarti sesuatu yang harus dijaga dan tidak boleh diingkari. Amanah memiliki hubungan dengan keamanan informasi. Beberapa informasi hanya dapat diberikan kepada orang yang telah diberi amanah untuk dapat menggunakannya dengan baik dan tidak membahayakan pemilik informasi. Allah SWT. berfirman dalam surat An-Nisa' ayat 58 (Kementrian Agama RI, 2019):

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا (٥٨)

Artinya:
"*Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah m emberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat"*. (QS An-Nisa': 58)

Ayat 58 surat An-Nisa menjelaskan bahwa Allah SWT. memerintahkan agar umat Islam senantiasa menyampaikan amanah pada orang yang berhak menerimanya. Hal ini sesuai dengan salah satu fungsi kriptografi yaitu agar pesan yang disampaikan hanya diterima oleh orang yang berhak atau orang yang dituju. Berdasarkan tafsir Al-Misbah amanah merupakan suatu hal yang diserahkan kepada pihak lain agar dipelihara dan dapat dikembalikan bila diminta oleh pemiliknya. Amanah hanya diberikan kepada orang yang memang dapat dipercaya oleh pemberi untuk dapat memelihara apa yang diberikan (Amiruddin, 2021).

Keamanan merupakan salah satu masalah yang banyak dibahas dalam agama Islam. Beberapa kisah tentang keamanan disebutkan pada Al-Qur'an yang menegaskan bahwa masalah keamanan adalah salah satu hal yang harus diperhatikan. Contoh kisah tentang keamanan informasi adalah kisah Nabi Sulaiman AS. yang terdapat pada QS An-Naml ayat 21-30 sebagai berikut (Kementrian Agama RI, 2019):

لَاُعَذِّبَنَّهٗ عَذَابًا شَدِيْدًا اَوْ لَاَاْذْبَحَنَّهٗٓ اَوْ لَيَأْتِيَنِّيْ بِسُلْطٰنٍ مُّبِيْنٍ(٢١) فَمَكَثَ غَيْرَ بَعِيْدٍ فَقَالَ اَحَطْتُّ بِمَا لَمْ تُحِطْ بِهٖ وَجِئْتُكَ مِنْ سَبَاٍ بِنَبَاٍ يَّقِيْنٍ (٢٢) اِنِّيْ وَجَدْتُّ امْرَاَةً تَمْلِكُهُمْ وَاُوْتِيَتْ مِنْ كُلِّ شَيْءٍ وَّلَهَا عَرْشٌ عَظِيْمٌ (٢٣) وَجَدْتُّهَا وَقَوْمَهَا يَسْجُدُوْنَ لِلشَّمْسِ مِنْ دُوْنِ اللّٰهِ وَزَيَّنَ لَهُمُ الشَّيْطٰنُ اَعْمَالَهُمْ فَصَدَّهُمْ عَنِ السَّبِيْلِ فَهُمْ لَا يَهْتَدُوْنَ (٢٤) اَلَّا يَسْجُدُوْا لِلّٰهِ الَّذِيْ يُخْرِجُ الْخَبْءَ فِى السَّمٰوٰتِ وَالْاَرْضِ وَيَعْلَمُ مَا تُخْفُوْنَ وَمَا تُعْلِنُوْنَ (٢٥) اَللّٰهُ لَآ اِلٰهَ اِلَّا هُوَ رَبُّ الْعَرْشِ الْعَظِيْمِ (٢٦) قَالَ سَنَنْظُرُ اَصَدَقْتَ اَمْ كُنْتَ مِنَ الْكٰذِبِيْنَ (٢٧) اِذْهَبْ بِّكِتٰبِيْ هٰذَا فَاَلْقِهْ اِلَيْهِمْ ثُمَّ تَوَلَّ عَنْهُمْ فَانْظُرْ مَاذَا يَرْجِعُوْنَ (٢٨) قَالَتْ يٰٓاَيُّهَا الْمَلَؤُا اِنِّيْٓ اُلْقِيَ اِلَيَّ كِتٰبٌ كَرِيْمٌ (٢٩) اِنَّهٗ مِنْ سُلَيْمٰنَ وَاِنَّهٗ بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ (٣٠)

Artinya:
"*Pasti akan kuhukum ia dengan hukuman yang berat atau kusembelih ia, kecuali jika ia datang kepadaku dengan alasan yang jelas. Maka tidak lama kemudian (datanglah Hud-hud), lalu ia berkata, "Aku telah mengetahui sesuatu yang belum engkau ketahui. Aku datang kepadamu dari negeri Saba' membawa suatu berita yang meyakinkan. Sungguh, kudapati ada seorang perempuan yang memerintah mereka, dan dia dianugerahi segala sesuatu serta memiliki singgasana yang besar. Aku (burung Hud) dapati dia dan kaumnya menyembah matahari, bukan kepada Allah; dan setan telah menjadikan terasa indah bagi mereka perbuatan-perbuatan (buruk) mereka, sehingga menghalangi mereka dari jalan (Allah), maka mereka tidak mendapat petunjuk. Mereka (juga) tidak menyembah Allah yang mengeluarkan apa yang terpendam di langit dan di bumi dan yang mengetahui apa yang kamu sembunyikan dan yang kamu nyatakan. Allah, tidak ada tuhan melainkan Dia, Tuhan yang mempunyai 'Arsy yang agung." Dia (Sulaiman) berkata, "Akan kami lihat, apa kamu benar, atau termasuk yang berdusta. Pergilah dengan (membawa) suratku ini, lalu jatuhkanlah kepada mereka, kemudian berpalinglah dari mereka, lalu perhatikanlah apa yang mereka bicarakan." Dia (Balqis) berkata, "Wahai para pembesar! Sesungguhnya telah disampaikan kepadaku sebuah surat yang mulia." Sesungguhnya (surat) itu dari Sulaiman yang isinya, "Dengan nama Allah Yang Maha Pengasih, Maha Penyayang."*(QS An-Naml:21-30)

Surat An-Naml ayat 21-30 memuat kisah burung Hud-hud yang menyampaikan berita tentang negeri yang dipimpin oleh seorang wanita kepada Nabi Sulaiman AS. Ratu negeri tersebut bernama Ratu Balqis dan negeri yang dipimpin bernama negeri Saba. Kekayaan negeri tersebut sangat melimpah sehingga memiliki istana yang sangat megah. Setelah mendengar berita tentang negeri Saba, Nabi Sulaiman segera mengirimkan pesan kepada Ratu Balqis untuk memastikan kebenarannya. Surat tersebut disampaikan oleh burung Hud-hud kepada Ratu Balqis untuk menjamin keamanan informasi yang ada dalam surat tersebut tetap terjaga. Dari kisah ini dapat dilihat bahwa konsep keamanan pesan ternyata telah diterapkan mulai zaman Nabi Sulaiman AS. kemudian pengujian kebenaran pada informasi yang dibawa oleh burung hud-hud juga sesuai dengan konsep uji validitas terhadap informasi (Soediro, 2018).

Kriptografi memiliki tujuan untuk merahasiakan informasi sehingga tidak diketahui pihak yang tidak diinginkan. Menjaga rahasia sangat dianjurkan dalam agama Islam. Salah satunya dasar dianjurkannya menjaga rahasia disebutkan pada Hadits Shahih Bukhori berikut (AL-Albani, 2008):

عَنْ أَنَسَ بْنَ مَالِكٍ قَالَ: أَسَرَّ إِلَيَّ النَّبِيُّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ سِرًّا فَمَا أَخْبَرْتُ بِهِ أَحَدًا بَعْدَهُ وَلَقَدْ سَأَلَتْنِي أُمُّ سُلَيْمٍ فَمَا أَخْبَرْتُهَا بِهِ (رواه البخاري)

Artinya:
*"Anas bin Malik berkata:"Nabi SAW. membicarakan pembicaraan rahasia kepadaku. Aku sama sekali tidak memberitahukan pembicaraan rahasia tersebut kepada seorang pun setelah kematian beliau. Ummu Sulaim pernah bertanya kepadaku tentang hal itu, namun aku sama sekali tidak mau memberitahukannya kepadanya."(*HR Bukhori)

Menjaga rahasia orang lain yang diketahui menjadi kewajiban bagi yang mengetahui karena tidak sembarang orang yang dapat mengetahuinya. Informasi rahasia atau privasi dapat diberikan kepada orang yang dapat dipercaya atas izin pemilik informasi. Izin atas informasi atau privasi terdapat pada Al-Qur'an yaitu surat An-Nur ayat 28 (Kementrian Agama RI, 2019):

فَاِنْ لَّمْ تَجِدُوْا فِيْهَآ اَحَدًا فَلَا تَدْخُلُوْهَا حَتّٰى يُؤْذَنَ لَكُمْ وَاِنْ قِيْلَ لَكُمُ ارْجِعُوْا فَارْجِعُوْا هُوَ اَزْكٰى لَكُمْ ۗوَاللّٰهُ بِمَا تَعْمَلُوْنَ عَلِيْمٌ (٢٨)

Artinya:
"Dan jika kamu tidak menemui seorang pun di dalamnya, maka janganlah kamu masuk sebelum kamu mendapat izin. Dan jika dikatakan kepadamu, "Kembalilah!" Maka (hendaklah) kamu kembali. Itu lebih suci bagimu, dan Allah Maha Mengetahui apa yang kamu kerjakan.."(QS An-Nur: 28)

Ayat ini juga menegaskan bahwa mengakses informasi tanpa izin pemilik informasi tidak diperbolehkan. Selain disebutkan dalam Al-Qur'an akses terhadap informasi atau privasi seseorang oleh orang yang tidak bertanggung jawab dapat menimbulkan kerugian bagi pemilik informasi. Pemberian izin terhadap informasi rahasia atau privasi sama seperti menyingkap tirai atau tabir yang melindunginya. Hal ini terdapat pada Hadits Shahih Muslim berikut (Al-Mundziri, 2020):

عَنْ ابْنَ مَسْعُودٍ يَقُولُ قَالَ لِي رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِذْنُكَ عَلَيَّ أَنْ يُرْفَعَ الْحِجَابُ وَأَنْ تَسْتَمِعَ سِوَادِي حَتَّى أَنْهَاكَ (رواه مسلم)

Artinya:
"Dari Ibnu Mas'ud ra, dia berkata; Rasulullah shallallahu 'alaihi wasallam berkata kepada saya; "izinmu kepadaku adalah apabila tirai diangkat dan kamu akan mendengar rahasiaku hingga aku melarang mu." (HR Muslim).

Nabi Muhammad SAW. selalu mengajarkan umatnya untuk memiliki sikap saling menghargai, menghormati, serta menyayangi sesama manusia. Salah satu caranya adalah saling menjaga privasi dan tidak mengganggu serta menyalahgunakannya. Rasulullah SAW. bersabda dalam Hadits Shahih Bukhari sebagai berikut (Al-Bayan, 2008):

حَدَّثَنَا أَبُو الْيَمَانِ أَخْبَرَنَا شُعَيْبٌ حَدَّثَنَا أَبُو الزِّنَادِ أَنَّ الْأَعْرَجَ حَدَّثَهُ أَنَّهُ سَمِعَ أَبَا هُرَيْرَةَ يَقُولُ إِنَّهُ سَمِعَ رَسُولَ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ يَقُولُ لَوْ اطَّلَعَ فِي بَيْتِكَ أَحَدٌ وَلَمْ تَأْذَنْ لَهُ خَذَفْتَهُ بِحَصَاةٍ فَفَقَأْتَ عَيْنَهُ مَا كَانَ عَلَيْكَ مِنْ جُنَاحٍ (رواه البخاري)

Artinya:
"*Telah menceritakan kepada kami [Abul yaman] telah mengabarkan kepada kami [Syu'aib] telah menceritakan kepada kami [Abu Az Zanad], bahwasanya [Al A'raj] menceritakan kepadanya, bahwa [Abu Hurairah] berkata; dirinya mendengar Rasulullah shallallahu 'alaihi wasallam bersabda: "Jika seseorang mengintip rumahmu padahal kamu tidak mengizinkannya, lalu kamu melemparnya dengan batu sehingga membutakan matanya, kamu tidak mendapat dosa karenanya".*
"(HR Bukhori)

Hadits-hadits tentang keamanan informasi menegaskan bahwa informasi pribadi adalah hak setiap pribadi. Karena itu, usaha untuk melindunginya juga merupakan hak pribadi dan sangat dianjurkan. Perlindungan informasi pribadi dilakukan agar tercipta rasa aman, damai, dan saling menghargai satu sama lain (Angriani, 2021).

2.3 Kajian Topik Dengan Teori Pendukung

Penelitian aplikasi basis Gröbner pada kriptanalisis didukung oleh beberapa teori. Kriptografi kunci publik merupakan salah satu teori yang mendukungnya. Kriptografi kunci publik merupakan kriptografi yang menggunakan dua jenis kunci yaitu kunci publik dan kunci rahasia. Sistem yang digunakan adalah kriptografi kunci publik multivariat yang merupakan kriptografi dengan pemetaan enkripsinya adalah pemetaan $F : K^n \rightarrow K^m$. Himpunan K merupakan lapangan berhingga. Pembangkitan kunci menjadi tahap awal penelitian dengan pemilihan kunci yang digunakan. Kemudian dilanjutkan tahap Enkripsi dan dekripsi sebelum melakukan evaluasi keamanan kriptografi melalui kriptanalisis. Teori lain yang mendukung penelitian ini adalah beberapa teori aljabar seperti ring, lapangan, dan ideal. Teori ini menjadi dasar teori sebelum memahami teori basis Gröbner yang akan digunakan.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Metode yang digunakan pada penelitan ini adalah metode kualitatif. Metode kualitatif berupa studi literatur atau studi pustaka. Sumber yang digunakan berasal dari beberapa artikel jurnal dan buku yang memuat informasi mengenai basis Gröbner, kriptografi, dan kriptanalisis.

3.2 Tahapan Penelitian

Penelitian aplikasi basis Gröbner pada kriptanalisis dilakukan pada kriptografi kunci publik multivariat. Penelitian terdiri dari empat tahap yaitu tahap pembangkitan kunci, tahap enkripsi, tahap dekripsi, dan tahap kriptanalisis. Berikut adalah beberapa langkah yang digunakan pada setiap tahap penelitian:

1. Pembangkitan Kunci

   Tahap pembangkitan kunci adalah tahap memilih kunci privat dan menghitung kunci publik yang akan digunakan. Langkah-langkah pembangkitan kunci adalah:

   a. Membentuk kunci privat yang akan digunakan yaitu memilih polinomial multivariat $f(x_1, x_2, \ldots, x_n)$. Pemilihan polinomial dapat didasarkan pada hasil perhitungan basis Gröbner dari sistem polinomial. Sistem polinomial yang baik akan membuat sistem kriptografi sulit untuk dipecahkan.
   b. Menentukan transformasi affine yang akan digunakan. Transformasi affine yang digunakan terdiri dari dua trnsformasi S dan T.

c. Menentukan kunci publik dan kunci privat berdasarkan polinomial dan transformasi affine. Kunci publik yang digunakan merupakan hasil komposisi sistem polinomial dan transformasi affine $S \circ F \circ T$.

2. Enkripsi plainteks kriptografi kunci publik multivariat.

Enkripsi plainteks pada kriptografi kunci publik multivariat dimulai dengan menentukan kunci publik dan kunci rahasia oleh orang yang akan menerima pesan. Langkah-langkah pada enkripsi:

a. Menentukan pesan yang akan dienkripsi.
b. Mengubah pesan ke dalam bentuk biner.
c. Enkripsi pesan menggunakan polinomial dari kunci publik sehingga $c = P(x)$ dimana P merupakan transformasi polinomial.

2. Dekripsi cipherteks kriptografi kunci publik multivariat.

Penerima pesan dapat melakukan dekripsi pesan dengan melakukan perhitungan menggunakan kunci rahasia yang hanya diketahui penerima pesan. Langkah dekripsi pesan adalah sebagai berikut:

a. Memastikan bahwa cipherteks dalam bentuk biner.
b. Menyatakan kunci privat yang digunakan untuk menemukan plainteks.
c. Melakukan transformasi balik menjadi $T^{-1} \circ F \circ S^{-1}$. Basis Gröbner dapat dimanfaatkan sebagai alat yang dapat mempermudah pencarian solusi sistem persamaan polinomial yang dihasilkan pada trasformasi.

3. Kriptanalisis menggunakan basis Gröbner.

Basis Gröbner digunakan untuk mencari solusi sistem persamaan polinomial. Tahap kriptanalisis menggunakan basis Gröbner dilakukan untuk mengetahui apakah basis Gröbner dapat memecahkan cipherteks kriptografi

kunci publik multivariat dengan tepat. Langkah-langkah yang digunakan untuk mencari solusi sistem persamaan adalah sebagai berikut:

a. Menyatakan sistem persamaan yang akan dicari solusinya. Sistem persamaan ini merupakan hasil dari operasi kunci publik dengan cipherteks yang dihasilkan.
b. Melakukan perhitungan basis Gröbner sehingga dihasilkan basis Gröbner dari sistem persamaan polinomial menggunakan library Sympy pada Python.
c. Mencari solusi basis Gröbner yang telah dihasilkan agar didapatkan plainteks yang digunakan.
d. Analisis hasil dilakukan untuk mengidentifikasi hasil perhitungan yang sesuai dengan plainteks yang digunakan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Pembangkitan Kunci Kriptografi Kunci Publik Multivariat

Pembangkitan kunci adalah langkah awal pada kriptografi kunci publik multivariat. Kunci privat dan kunci publik didefinisikan untuk keamanan kriptografi. Tahap ini merupakan tahap pemilihan lapangan, polinomial, serta pemetaan yang akan menjadi kunci privat (Riyanto, 2010). Pembangkitan kunci dilakukan oleh pihak penerima pesan dengan menentukan kunci privat dan kunci publik yang digunakan. Hal ini dilakukan agar kunci privat tetap aman dan hanya diketahui oleh penerima pesan.

Pemilihan polinomial adalah langkah penting dalam pembangkitan kunci karena mempengaruhi tingkat keamanan kriptografi. Pemilihan polinomial dapat dilakukan menggunakan beberapa langkah pemilihan polinomial(Ding et al., 2016):

1. Pemilihan Lapangan Berhingga

   Lapangan yang akan digunakan adalah lapangan berhingga $GF(p)$, dimana p adalah bilangan prima atau hasil pangkatnya. Pemilihan lapangan yang digunakan akan menentukan koefisien polinomial yang digunakan. Misalnya dipilih lapangan berhingga $GF(2)$, maka koefisien yang digunakan terdiri dari dua angka yaitu 0 dan 1.

2. Pemilihan Derajat dan Variabel

   Penentuan derajat dan variabel yang digunakan akan menentukan tingkat keamanan kriptografi. Semakin besar derajat dan variabel yang digunakan maka keamanan kriptografi akan semakin baik. Banyaknya variabel akan menentukan panjang bit plainteks yang dapat dienkripsi sekaligus.

3. Pembentukan polinomial secara acak.

   Pembentukan polinomial secara acak dilakukan dengan memilih koefisien pada lapangan berhingga yang telah ditentukan. Polinomial yang dihasilkan adalah kombinasi variabel dan derajat yang telah ditentukan.

4. Evaluasi keamanan

   Pemilihan polinomial yang akan digunakan dapat dievaluasi terlebih dahulu menggunakan basis Gröbner. Evaluasi dapat dilakukan dengan membandingkan basis Gröbner dari sistem persamaan polinomial. Misalkan akan dicari basis Gröbner dari dua sistem polinomial berikut:

   a. Sistem persamaan pertama

      Misalkan lapangan berhingga yang digunakan pada persamaan pertama adalah $GF(2)$ sehingga koefisiennya adalah 0 dan 1. Derajat polinomialnya adalah 2 dan terdiri dari 4 variabel. Berikut contoh sistem polinomial pertama yang dapat dibentuk:

$$f_1 = x_1x_2 + x_3,$$
$$f_2 = x_2x_3 + x_4,$$
$$f_3 = x_1 + x_3x_4,$$
$$f_4 = x_2 + x_1x_4.$$

   b. Sistem persamaan kedua:

      Misalkan lapangan berhingga yang digunakan pada persamaan kedua adalah $GF(2)$. Kemudian ditentukan derajat polinomialnya adalah 5 dan terdiri dari 4 variabel. Berikut contoh sistem polinomial kedua yang dapat dibentuk:

$$f_1 = x_1^5 + x_2^4 x_3 + x_4^2 + x_4 + 1,$$

$$f_2 = x_1^3 x_2^2 + x_2^4 + x_3^5 + 1,$$

$$f_3 = x_2^3 x_3^2 + x_3 x_4^4,$$

$$f_4 = x_1^5 + x_4^3.$$

Perhitungan basis Gröbner dimulai dengan menentukan pasangan yang dapat dibentuk dari sistem persamaan polinomial. Selanjutnya, dihitung polinomial-S dari setiap pasangan. Proses ini merupakan proses yang rumit karena melibatkan operasi matematis yang kompleks seperti pembagian polinomial yang memiliki tingkat kerumitan yang tinggi terutama jika variabel dan derajat yang digunakan tinggi. Oleh karena itu, perhitungannya dapat menggunakan alat bantu seperti menggunakan library Sympy pada Python dan Singular CAS. Berikut merupakan hasil perhitungan basis Gröbner menggunakan Python dan singular CAS pada masing-masing sistem persamaan:

```python
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x3
f2 = x2*x3 + x4
f3 = x1 + x3*x4
f4 = x2 + x1*x4


# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x4**3
x2 + x4**4
x3 + x4**2
x4**6 + x4
```

Gambar 4.1 Perhitungan Basis Gröbner pada Sistem Persamaan Pertama

```
                     SINGULAR                                 /  Development
 A Computer Algebra System for Polynomial Computations       /   version 4.3.1
                                                           0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann     \   Jun 2022
FB Mathematik der Universitaet, D-67653 Kaiserslautern        \
> // Definisikan ring dengan lapangan GF(2) dan 4 variabel x1, x2, x3, x4
ring R = 2, (x1, x2, x3, x4), lp;
> poly f1 = x1^5 + x2^4*x3 + x4^2 + 1;
poly f2 = x1^3*x2^2 + x2^4 + x3^5 + 1;
poly f3 = x2^3*x3^2 + x3*x4^4;
poly f4 = x1^5 + x4^3;
> ideal I = f1, f2, f3, f4;
> ideal G = groebner(I);
> print("Jumlah basis Grobner: ");
print(size(G));
Jumlah basis Grobner:
5
> print("Basis Grobner yang dihasilkan:");
print(G);
Basis Grobner yang dihasilkan:
x4^483+x4^482+x4^480+x4^448+x4^444+x4^440+x4^428+x4^424+x4^416+x4^400+x4^396+x4^
392+x4^384+x4^343+x4^342+x4^340+x4^339+x4^338+x4^336+x4^335+x4^334+x4^332+x4^323
+x4^322+x4^320+x4^319+x4^318+x4^316+x4^315+x4^314+x4^312+x4^311+x4^310+x4^307+x4
^305+x4^302+x4^297+x4^295+x4^293+x4^292+x4^290+x4^288+x4^286+x4^284+x4^283+x4^28
2+x4^281+x4^279+x4^277+x4^276+x4^275+x4^274+x4^273+x4^264+x4^259+x4^257+x4^255+x
4^252+x4^249+x4^248+x4^246+x4^245+x4^244+x4^242+x4^240+x4^238+x4^236+x4^233+x4^2
30+x4^229+x4^227+x4^224+x4^223+x4^220+x4^219+x4^218+x4^217+x4^216+x4^215+x4^213+
x4^212+x4^209+x4^207+x4^206+x4^204+x4^203+x4^202+x4^199+x4^198+x4^196+x4^195+x4^
193+x4^192+x4^190+x4^185+x4^184+x4^183+x4^181+x4^180+x4^179+x4^178+x4^177+x4^176
+x4^175+x4^174+x4^171+x4^170+x4^168+x4^163+x4^162+x4^156+x4^152+x4^144+x4^135+x4
^134+x4^132+x4^131+x4^130+x4^127+x4^126+x4^124+x4^116+x4^114+x4^113+x4^112+x4^11
0+x4^107+x4^106+x4^105+x4^104+x4^103+x4^101+x4^100+x4^98+x4^96+x4^95+x4^89+x4^88
+x4^87+x4^85+x4^84+x4^81+x4^80+x4^72+x4^67+x4^65+x4^63+x4^60+x4^57+x4^56+x4^55+x
4^53+x4^52+x4^49+x4^44+x4^32+x4^28+x4^24+x4^16+1,
```

Gambar 4.2 Perhitungan Basis Gröbner pada Sistem Persamaan Kedua

Basis Gröbner dari sistem persamaan polinomial pertama terdiri dari 4 polinomial dengan derajat tertinggi 6, sedangkan basis Gröbner pada himpunan kedua lebih rumit yaitu 5 polinomial dengan derajat tertingginya adalah 483. Kedua basis Gröbner yang dihasilkan menunjukkan bahwa sistem polinomial kedua memiliki tingkat keamanan yang lebih tinggi dari polinomial pertama. Proses perhitungannya pun lebih lama dari polinomial pertama. Penelitian ini akan menggunakan sistem polinomial pertama untuk menunjukkan proses konstruksi kriptografi kunci publik multivariat lebih lanjut.

Berikut akan diberikan tahap pembangkitan kunci dan contoh perhitungan menggunakan polinomial pertama. Tahap pertama pembangkitan kunci adalah menentukan lapangan, persamaan polinomial, dan transformasi invertibel yang

digunakan. Selanjutnya, didefinisikan empat polinomial dari sistem persamaan pertama yang akan digunakan, yaitu $F(x_1, x_2, x_3, x_4) = \{f_1, f_2, f_3, f_4\}$ dengan

$$\begin{aligned} f_1 &= x_1x_2 + x_3, \\ f_2 &= x_2x_3 + x_4, \\ f_3 &= x_1 + x_3x_4, \\ f_4 &= x_2 + x_1x_4. \end{aligned} \tag{4.1}$$

Polinomial $F(x_1, x_2, x_3, x_4)$ serta transformasi S dan T ini merupakan kunci privat yang hanya diketahui oleh penerima pesan. Selanjutnya akan ditentukan kunci publik yang akan dikirim kepada pihak pengirim pesan dengan komposisi polinomial dengan transformasi S dan T.

$$S(x_1, x_2, x_3, x_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \tag{4.2}$$

$$T(x_1, x_2, x_3, x_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{4.3}$$

Perhitungan Kunci publik dilakukan menggunakan Persamaan (2.1) pada Bab 2. Misalkan $x = x_1, x_2, x_3, x_4,$ merupakan variabel yang akan menjadi pertama, sehingga transformasi T pada Persamaan (4.3) akan mengubah variabel $x_1, x_2, x_3,$ dan x_4.

$$\begin{aligned} y &= T(x_1, x_2, x_3, x_4) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \end{aligned}$$

Sehingga diperoleh hasil:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} x_1 + 1 \\ x_2 \\ x_3 + 1 \\ x_4 \end{pmatrix}. \tag{4.4}$$

Tahap selanjutnya adalah subtitusi Persamaan (4.4) pada Persamaan (4.1).

Perhitungan masing-masing polinomial akan dijelaskan sebagai berikut:

1. Perhitungan $f_1(y)$:

   $f_1 = x_1x_2 + x_3$

   $f_1(y) = y_1y_2 + y_3$

   $= (x_1 + 1)(x_2) + (x_3 + 1)$

   $= x_1x_2 + x_2 + x_3 + 1$

2. Perhitungan $f_2(y)$:

   $f_2 = x_2x_3 + x_4,$

   $f_2(y) = y_2y_3 + y_4$

   $= (x_2 + x_3)(x_3 + 1) + (x_4)$

   $= (x_2x_3 + x_2 + {x_3}^2 + x_3) + (x_4)$

   $= x_2x_3 + x_2 + x_4$

3. Perhitungan $f_3(y)$:

   $f_3 = x_1 + x_3x_4,$

   $f_3(y) = y_1 + y_3y_4,$

   $= (x_1 + 1) + (x_3 + 1)(x_4)$

   $= (x_1 + 1) + (x_3x_4 + x_4)$

   $= x_1 + x_3x_4 + x_4 + 1$

4. Perhitungan $f_4(y)$:

   $f_4 = x_2 + x_1x_4$

$$f_4(y) = y_2 + y_1 y_4$$
$$= (x_2) + (x_1 + 1)(x_4)$$
$$= (x_2) + (x_1 x_4 + x_4)$$
$$= x_2 + x_1 x_4 + x_4$$

Sehingga hasil $z = F(y)$ dalam bentuk matriks adalah:

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} x_1 x_2 + x_2 + x_3 + 1 \\ x_2 x_3 + x_2 + x_4 \\ x_1 + x_3 x_4 + x_4 + 1 \\ x_2 + x_1 x_4 + x_4 \end{pmatrix} \quad (4.5)$$

Langkah berikutnya adalah transformasi S Persamaan (4.2) pada Persamaan (4.5).

$$P(x) = S(z)$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} z_1 \\ z_2 + 1 \\ z_3 \\ z_4 + 1 \end{pmatrix}$$
$$= \begin{pmatrix} x_1 x_2 + x_2 + x_3 + 1 \\ x_2 x_3 + x_2 + x_4 + 1 \\ x_1 + x_3 x_4 + x_4 + 1 \\ x_2 + x_1 x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kunci publik yang akan digunakan adalah

$$P(x_1, x_2, x_3, x_4) = \begin{pmatrix} x_1 x_2 + x_2 + x_3 + 1 \\ x_2 x_3 + x_2 + x_4 + 1 \\ x_1 + x_3 x_4 + x_4 + 1 \\ x_2 + x_1 x_4 + x_4 + 1 \end{pmatrix} \quad (4.6)$$

4.2 Enkripsi Plainteks Kriptografi Kunci Publik Multivariat

Proses enkripsi plainteks kriptografi kunci publik multivariat dilakukan oleh pengirim pesan menggunakan kunci publik (Riyanto, 2010). Langkah enkripsi

dimulai dengan memilih pesan yang akan dienkripsi. Pesan yang akan dienkripsi harus diubah menjadi bentuk biner terlebih dahulu.

Misalkan kata yang dipilih adalah kata "BISA" maka setiap huruf akan direpresentasikan menjadi biner ASCII berikut

$$01000010\ 01001001\ 01010011\ 01000001.$$

Setiap huruf menjadi biner 8-bit dan akan dibagi menjadi 2 bagian sehingga menjadi 4-bit. Setiap 4-bit akan disebut sebagai blok yang akan dienkripsi. Jadi, enkripsi kata "BISA" akan dilakukan dalam perhitungan 8 blok biner 4-bit.

$$0100\ 0010\ 0100\ 1001\ 0101\ 0011\ 0100\ 0001.$$

Setiap blok yang telah dibagi akan mewakili variabel x_1, x_2, x_3, x_4 yang akan disubtitusikan pada kunci publik. Tahap-tahap enkripsi untuk setiap blok akan dihitung dengan melakukan subtitusi pada Persamaan (4.5). berikut merupakan hasil subtitusi pada setiap blok.

1. Blok Pertama

$$(x_1, x_2, x_3, x_4) = (0,1,0,0)$$

$$P(0,1,0,0) = \begin{pmatrix} 0+1+0+1 \\ 0+1+0+1 \\ 0+0+0+1 \\ 1+0+0+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

2. Blok Kedua

$$(x_1, x_2, x_3, x_4) = (0,0,1,0)$$

$$P(0,0,1,0) = \begin{pmatrix} 0+0+1+1 \\ 0+0+0+1 \\ 0+0+0+1 \\ 0+0+0+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

3. Blok Ketiga

$$(x_1, x_2, x_3, x_4) = (0,1,0,0)$$

$$P(0,1,0,0) = \begin{pmatrix} 0+1+0+1 \\ 0+1+0+1 \\ 0+0+0+1 \\ 1+0+0+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

4. Blok Keempat

$$(x_1, x_2, x_3, x_4) = (1,0,0,1)$$

$$P(1,0,0,1) = \begin{pmatrix} 0+0+0+1 \\ 0+0+1+1 \\ 1+0+1+1 \\ 0+1+1+1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

5. Blok Kelima

$$(x_1, x_2, x_3, x_4) = (0,1,0,1)$$

$$P(0,1,0,1) = \begin{pmatrix} 0+1+0+1 \\ 0+1+1+1 \\ 0+0+1+1 \\ 1+0+1+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

6. Blok Keenam

$$(x_1, x_2, x_3, x_4) = (0,0,1,1)$$

$$P(0,0,1,1) = \begin{pmatrix} 0+0+1+1 \\ 0+0+1+1 \\ 0+1+1+1 \\ 0+0+1+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

7. Blok Ketujuh

$$(x_1, x_2, x_3, x_4) = (0,1,0,0)$$

$$P(0,1,0,0) = \begin{pmatrix} 0+1+0+1 \\ 0+1+0+1 \\ 0+0+0+1 \\ 1+0+0+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

8. Blok Kedelapan

$$(x_1, x_2, x_3, x_4) = (0,0,0,1)$$

$$P(0,0,0,1) = \begin{pmatrix} 0+0+0+1 \\ 0+0+1+1 \\ 0+0+1+1 \\ 0+0+1+1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Jadi, cipherteks hasil enkripsi semua blok plainteks adalah

$$c = 0010\ 0111\ 0010\ 1011\ 0101\ 0010\ 0010\ 0010\ 1000.$$

4.3 Dekripsi Cipherteks Kriptografi Kunci Publik Multivariat

Dekripsi cipherteks kriptografi kunci publik multivariat dilakukan menggunakan kunci rahasia yang telah dibentuk dan hanya diketahui oleh penerima pesan. Proses ini merupakan transformasi balik dari tranformasi yang dilakukan pada pembangkitan kunci (Riyanto, 2010).

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) \tag{4.7}$$

Sebelum melakukan transformasi balik diperlukan invers dari transformasi affine S dan T. Transformasi S telah didefinisikan pada Persamaan (4.9) dan dapat dicari inversnya sebagai berikut:

Misalkan $S(x) = y$, maka $y = Ax + b$.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

sehingga $x = S^{-1}(y) = A^{-1}(y - b)$. A adalah matriks identitas sehingga inversnya adalah matriks itu sendiri. Oleh karena itu inversnya dapat dicari dengan menghitung $S^{-1}(y) = A(y - b)$. Proses yang sama juga digunakan pada trasformasi T yang membedakan adalah vektor translasi yang digunakan. Jadi, invers trasformasi T dapat didefinisikan sebagai $T^{-1}(y) = A(y - b)$ dengan

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Berikut merupakan dekripsi cipherteks hasil enkripsi kriptografi kunci publik multivariat:

1. Dekripsi blok pertama (0010).

   Tahap pertama dekripsi sesuai dengan Persamaan (4.7) yaitu tranformasi cipherteks menggunakan transformasi S.

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

   Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

   Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{gathered} x_1x_2 + x_3 = 0 \\ x_2x_3 + x_4 + 1 = 0 \\ x_1 + x_3x_4 + 1 = 0 \\ x_2 + x_1x_4 + 1 = 0 \end{gathered}$$

   Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Misalkan $x_1 = 1$, maka terdapat beberapa kemungkinan yang sesuai dengan hasil berikut:

   a. Nilai asumsi $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1$

$$\begin{gathered} 0 + 0 = 0 \\ 0 + 1 = 1 \\ 1 + 0 = 1 \\ 0 + 1 = 1 \end{gathered}$$

b. Nilai asumsi $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0$

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 0 = 1$$

Pada tahap ini dapat digunakan basis Gröbner sehingga mempermudah pencarian solusi yang mungkin dari persamaan polinomial. Berikut hasil perhitungan basis Gröbner menggunakan algoritma Buchberger pada Python.

```
: from sympy import symbols, groebner, GF, solve

  # Mendefinisikan variabel
  x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

  # Mendefinisikan polinomial
  f1 = x1*x2 + x3
  f2 = x2*x3 + x4 + 1
  f3 = x1 + x3*x4 + 1
  f4 = x2 + x1*x4 + 1

  # Membuat basis Gröbner di lapangan GF(2)
  G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

  # Menampilkan basis Gröbner
  print("Basis Gröbner di GF(2):")
  for g in G:
      print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3*x4 + 1
x2 + x3 + x4**2 + x4
x3**2 + x3*x4 + x3 + x4**2 + x4
x3*x4**2 + x3 + x4**2 + 1
x4**4 + x4**2
```

Gambar 4.3 Perhitungan Basis Gröbner pada Dekripsi Blok Pertama

Basis Gröbner yang dihasilkan yaitu $\{x_1 + x_3x_4 + 1, x_2 + x_3 + x_4^2 + x_4,$ $x_3^2 + x_3x_4 + x_3 + x_4^2 + x_4,\ x_3x_4^2 + x_3 + x_4^2 + 1,$ dan $x_4^4 + x_4^2\}$.

Solusi yang sesuai dapat dihitung sebagai berikut

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(-1, 1, -1, 0)
```

Gambar 4.4 Perhitungan Solusi Basis Gröbner Dekripsi Blok Pertama

Solusi yang didapatkan sesuai dengan nilai asumsi kedua yaitu (1,1,1,0). Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Hasil dekripsi cipherteks blok pertama sesuai dengan blok pertama plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks apada blok pertama.

2. Dekripsi blok kedua

Blok kedua juga didekripsi dengan cara yang sama seperti blok pertama. Oleh karena itu tahap pertama adalah tranformasi cipherteks menggunakan transformasi S.

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{gathered} x_1x_2 + x_3 = 0 \\ x_2x_3 + x_4 = 0 \\ x_1 + x_3x_4 + 1 = 0 \\ x_2 + x_1x_4 = 0 \end{gathered}$$

Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Pada persamaan ini nilai asumsi yang sesuai yaitu $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0$

Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Hasil dekripsi cipherteks blok pertama sesuai dengan blok pertama plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks apada blok kedua.

3. Dekripsi blok ketiga

   Blok ketiga memiliki nilai biner yang sama dengan blok pertama sehingga dapat dienkripsi dengan cara yang sama dan memiliki hasil dekripsi yang sama.

4. Dekripsi blok keempat.

   Transformasi S pada blok empat menghasilkan:

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{aligned} x_1x_2 + x_3 + 1 &= 0 \\ x_2x_3 + x_4 + 1 &= 0 \\ x_1 + x_3x_4 + 1 &= 0 \\ x_2 + x_1x_4 &= 0 \end{aligned}$$

Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Pada persamaan ini nilai asumsi yang sesuai yaitu $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1$

Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Hasil dekripsi cipherteks blok keempat sesuai dengan blok keempat plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks pada blok keempat.

5. Blok Kelima

Transformasi S pada blok empat menghasilkan:

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{aligned} x_1x_2 + x_3 &= 0 \\ x_2x_3 + x_4 &= 0 \\ x_1 + x_3x_4 &= 0 \\ x_2 + x_1x_4 &= 0 \end{aligned}$$

Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Pada persamaan ini nilai asumsi yang sesuai yaitu $x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1$.

Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Hasil dekripsi cipherteks blok keempat sesuai dengan blok kelima plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks pada blok kelima.

6. Blok Keenam

Transformasi S pada blok empat menghasilkan:

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{aligned} x_1x_2 + x_3 &= 0 \\ x_2x_3 + x_4 + 1 &= 0 \\ x_1 + x_3x_4 + 1 &= 0 \\ x_2 + x_1x_4 + 1 &= 0 \end{aligned}$$

Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Pada persamaan ini nilai asumsi yang sesuai yaitu $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1$

Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Hasil dekripsi cipherteks blok keenam sesuai dengan blok keenam plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks pada blok keenam.

7. Blok Ketujuh

   Blok ketujuh juga memiliki nilai biner yang sama dengan blok pertama untuk blok plainteks dan cipherteks sehingga dapat dienkripsi dengan cara yang sama dan memiliki hasil dekripsi yang sama.

8. Blok kedelapan

   Transformasi S pada blok empat menghasilkan:

$$S^{-1}(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

   Selanjutnya, pemetaan $F(x_1, x_2, x_3, x_4)$ direpresentasikan menjadi vektor kolom 4×1, sehingga dapat dioperasikan dengan hasil transformasi.

$$F\left(S^{-1}(c)\right) = \begin{pmatrix} x_1x_2 + x_3 \\ x_2x_3 + x_4 \\ x_1 + x_3x_4 \\ x_2 + x_1x_4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

   Solusi dari sistem persamaan dengan mengevaluasi semua kemungkinan nilai yang sesuai. Sistem persamaan akan diselesaikan dengan menyatakan persamaan tersebut sama dengan nol.

$$\begin{aligned} x_1x_2 + x_3 + 1 &= 0 \\ x_2x_3 + x_4 + 1 &= 0 \\ x_1 + x_3x_4 &= 0 \\ x_2 + x_1x_4 + 1 &= 0 \end{aligned}$$

   Penyelesaian sistem persamaan polinomial dapat dilakukan dengan mencoba memberikan masukan yang cocok. Pada persamaan ini nilai asumsi yang sesuai yaitu $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1$

   Selanjutnya tranformasi terakhir dapat dilakukan untuk melihat apakah dekripsi berhasil.

$$T^{-1}\left(F\left(S^{-1}(c)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Hasil dekripsi cipherteks blok kedelapan sesuai dengan blok kedelapan plainteks. Jadi, dapat disimpulkan bahwa proses dekripsi berhasil mengembalikan plainteks pada blok kedelapan.

Tahap dekripsi kriptografi kunci publik multivariat telah berhasil mengembalikan semua blok plainteks yang digunakan, yaitu

$$0100\ 0010\ 0100\ 1001\ 0101\ 0011\ 0100\ 0001.$$

4.4 Kriptanalisis Basis Gröbner pada Hasil Enkripsi Kriptografi

Kriptanalisis pada kriptografi kunci publik multivariat adalah proses dekripsi pesan tanpa menggunakan kunci privat yang digunakan. Kriptanalisis basis Gröbner digunakan dengan memanfaatkan perhitungan basis Gröbner sehingga mempermudah pencarian solusi sistem persamaan polinomial (Das & Reza, 2018).

Kriptanalisis dapat dilakukan oleh seseorang yang mengetahui kunci publik dan cipherteks yang dikirimkan melalui jalur yang tidak aman. Kriptanalisis juga dapat dilakukan untuk mencari kelemahan dari skema kriptografi yang dilakukan. Hal ini dilakukan untuk meningkatkan keamanan kriptografi (Riyanto, 2010). Misalkan seorang penyerang ingin melakukan kriptanalisis dengan menggunakan basis Gröbner. Penyerang hanya mengetahui kunci publik dan cipherteks yang didistribusikan melalui jalur yang tidak aman. Berikut kunci publik $P(x)$ dan cipherteks c yang diketahui penyerang:

$$c = 0010\ 0111\ 0010\ 1011\ 0101\ 0010\ 0010\ 0010\ 1000.$$

Perhitungan untuk meperoleh basis Gröbner pada kunci publik dan cipherteks ubtuk mengembalikan plainteks setiap blok dilakukan sebagai berikut:

1. Perhitungan blok pertama

$$P(x) + c = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 + 1 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$\begin{aligned} x_1x_2 + x_2 + x_3 &= 1 \\ x_2x_3 + x_2 + x_4 &= 1 \\ x_1 + x_3x_4 + x_4 &= 0 \\ x_2 + x_1x_4 + x_4 &= 1 \end{aligned}$$

```python
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 1
f2 = x2*x3 + x2 + x4 + 1
f3 = x1 + x3*x4 + x4
f4 = x2 + x1*x4 + x4 + 1

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3*x4 + x4
x2 + x3 + x4**2 + x4 + 1
x3**2 + x3*x4 + x3 + x4**2
x3*x4**2 + x3
x4**4 + x4**2
```

Gambar 4.5 Perhitungan Basis Gröbner pada Kriptanalisis Blok Pertama

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_3x_4 + x_4, x_2 + x_3 + x_4^2 + x_4 + 1, x_3^2 + x_3x_4 + x_3 + x_4^2, x_3x_4^2 + x_3, x_4^4 + x_4^2\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner menggunakan Python**.**

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(0, -1, 0, 0)
```

Gambar 4.6 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Pertama

Solusi yang dihasilkan sesuai plainteks blok pertama yaitu (0,1,0,0), sehingga dapat disimpulkan bahwa kriptanalisis basis Gröbner pada blok pertama berhasil.

Pencarian solusi basis Gröbner juga dapat dicari menggunakan teori eliminasi. Langkah pertama dalam pencarian solusi yang sesuai adalah memilih salah satu persamaan yang memiliki variabel paling sedikit, sehingga dapat diasumsikan nilai variabel pada persamaan. Pada persamaan $x_4^4 + x_4^2 = 0$ terdapat kemungkinan solusi yaitu $x_4 = 0$ dan $x_4 = 1$. Nilai-nilai yang sesuai dapat dicari dengan kedua asumsi tersebut.

a. $x_4 = 0$,

   Jika $x_4 = 0$ maka berdasarkan persamaan $x_3 x_4^2 + x_3 = 0$ terdapat dua kemungkinan solusi, yaitu $x_3 = 0$ dan $x_3 = 1$.

   Selanjutnya jika nilai $x_3 = 0$, maka solusi untuk $x_2 = 1$ dan $x_1 = 0$. Solusi lain didapatkan jika $x_3 = 1$, yaitu $x_2 = 0$ dan $x_1 = 0$.

b. $x_4 = 1$.

   Jika $x_4 = 1$ maka berdasarkan persamaan $x_3 x_4^2 + x_3 = 0$ solusi yang sesuai adalah $x_3 = 0, x_2 = 1$, dan $x_1 = 1$.

Berdasarkan perhitungan di atas, beberapa solusi yang dihasilkan dari basis Gröbner blok pertama adalah (0,1,0,0), (0,0,1,0), dan (1,1,0,1). Solusi yang sesuai dengan plainteks yang dicari adalah (0,1,0,0). Jadi, dapat disimpulkan bahwa kriptanalisis basis Gröbner pada blok pertama berhasil.

2. Perhitungan blok kedua

$$P(x) + c = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 + 1 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$\begin{aligned} x_1x_2 + x_2 + x_3 &= 1 \\ x_2x_3 + x_2 + x_4 &= 0 \\ x_1 + x_3x_4 + x_4 &= 0 \\ x_2 + x_1x_4 + x_4 &= 0 \end{aligned}$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 1
f2 = x2*x3 + x2 + x4 + 0
f3 = x1 + x3*x4 + x4 + 0
f4 = x2 + x1*x4 + x4 + 0

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3 + x4**4 + x4**2 + 1
x2 + x3 + x4**2 + 1
x3**2 + x3 + x4**2
x3*x4 + x3 + x4**4 + x4**2 + x4 + 1
x4**5 + x4**4 + x4**3 + x4
```

Gambar 4.7 Perhitungan Basis Gröbner pada Kriptanalisis Blok Kedua

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_3 + {x_4}^4 + {x_4}^2 + 1, x_2 + x_3 + x_4^2 + 1,\ x_3^2 + x_3 + x_4^2,\ x_3x_4 + x_3 + {x_4}^4 + {x_4}^2 + x_4 + 1,\ {x_4}^5 + x_4^4 + x_4^3 + x_4\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(0, 0, -1, 0)
```

Gambar 4.8 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Kedua

Solusi yang dihasilkan sesuai plainteks blok kedua yaitu (0,0,1,0), sehingga dapat disimpulkan bahwa kriptanalisis basis Gröbner pada blok kedua berhasil.

Selanjutnya, dapat dicari solusi dari basis Gröbner tersebut dengan beberapa asumsi nilai yang sesuai:

a. $x_4 = 0$.

   Menggunakan asumsi $x_4 = 0$, maka nilai x lain yang sesuai adalah $x_3 = 0$, $x_2 = 1$, dan $x_1 = 0$.

b. $x_4 = 1$

   Asumsi $x_4 = 1$, akan menghasilkan solusi lain yaitu $x_3 = 0$, $x_2 = 0$, dan $x_1 = 1$.

Terdapat solusi yang sesuai plainteks blok kedua yaitu (0,0,1,0), sehingga dapat disimpulkan bahwa kriptanalisis basis Gröbner pada blok kedua berhasil.

3. Perhitungan blok ketiga

$$P(x)+c=\begin{pmatrix}x_1x_2+x_2+x_3+1\\ x_2x_3+x_2+x_4+1\\ x_1+x_3x_4+x_4+1\\ x_2+x_1x_4+x_4+1\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}x_1x_2+x_2+x_3+1\\ x_2x_3+x_2+x_4+1\\ x_1+x_3x_4+x_4\\ x_2+x_1x_4+x_4+1\end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$\begin{aligned}x_1x_2+x_2+x_3&=1\\ x_2x_3+x_2+x_4&=1\\ x_1+x_3x_4+x_4&=0\\ x_2+x_1x_4+x_4&=1\end{aligned}$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 1
f2 = x2*x3 + x2 + x4 + 1
f3 = x1 + x3*x4 + x4 + 0
f4 = x2 + x1*x4 + x4 + 1

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3*x4 + x4
x2 + x3 + x4**2 + x4 + 1
x3**2 + x3*x4 + x3 + x4**2
x3*x4**2 + x3
x4**4 + x4**2
```

Gambar 4.9 Perhitungan Basis Gröbner pada Kriptanalisis Blok Ketiga

Basis Gröbner yang dihasilkan adalah $\{x_1+x_3x_4+x_4,\ x_2+x_3+x_4^2+x_4+1,\ x_3^2+x_3x_4+x_3+x_4^2,\ x_3x_4^2+x_3,\ x_4^4+x_4^2\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(0, -1, 0, 0)
```

Gambar 4.10 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Ketiga

Blok ketiga memiliki biner yang sama dengan blok pertama sehingga langkah yang dilakukan untuk mencari solusi akan sesuai dengan blok pertama. Solusi yang dihasilkan sesuai plainteks blok ketiga yaitu (0,1,0,0).

4. Perhitungan blok keempat

$$P(x)+c=\begin{pmatrix}x_1x_2+x_2+x_3+1\\x_2x_3+x_2+x_4+1\\x_1+x_3x_4+x_4+1\\x_2+x_1x_4+x_4+1\end{pmatrix}+\begin{pmatrix}1\\0\\1\\1\end{pmatrix}=\begin{pmatrix}x_1x_2+x_2+x_3\\x_2x_3+x_2+x_4+1\\x_1+x_3x_4+x_4\\x_2+x_1x_4+x_4\end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$\begin{aligned}x_1x_2+x_2+x_3&=0\\x_2x_3+x_2+x_4&=1\\x_1+x_3x_4+x_4&=0\\x_2+x_1x_4+x_4&=0\end{aligned}$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 0
f2 = x2*x3 + x2 + x4 + 1
f3 = x1 + x3*x4 + x4 + 0
f4 = x2 + x1*x4 + x4 + 0

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex',domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3*x4 + x4
x2 + x3 + x4**2 + x4
x3**2 + x3*x4 + x4**2 + 1
x3*x4**2 + x3
x4**4 + 1
```

Gambar 4.11 Perhitungan Basis Gröbner pada Kriptanalisis Blok Keempat

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_3x_4 + x_4, x_2 + x_3 + x_4^2 + x_4, x_3^2 + x_3x_4 + x_4^2 + 1, x_3x_4^2 + x_3, x_4^4 + 1\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(0, 1, -1, -1)
```

Gambar 4.12 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Keempat

Solusi yang dihasilkan tidak berhasil mengembalikan plainteks sehingga perlu dicari solusi yang lain. Namun plainteks blok pertama yaitu (1,0,0,1) juga memenuhi persamaan dengan pembuktian sebagai berikut:

$$1 + 0 + 1 = 0$$
$$0 + 0 + 1 + 1 = 0,$$
$$0 + 0 + 1 + 1 = 0,$$
$$0 + 0 = 0,$$
$$1 + 1 = 0.$$

Jadi, dapat disimpulkan bahwa kriptanalisis basis Gröbner tidak langsung menghasilkan solusi yang sesuai tetapi plainteks blok keempat juga merupakan solusi dari basis Gröbner.

5. Perhitungan blok kelima

$$P(x) + c = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 + 1 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$x_1x_2 + x_2 + x_3 = 1$$
$$x_2x_3 + x_2 + x_4 = 0$$
$$x_1 + x_3x_4 + x_4 = 1$$
$$x_2 + x_1x_4 + x_4 = 0$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 1
f2 = x2*x3 + x2 + x4 + 0
f3 = x1 + x3*x4 + x4 + 1
f4 = x2 + x1*x4 + x4 + 0

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x4**3 + 1
x2 + x4**4
x3 + x4**2 + 1
x4**6 + x4
```

Gambar 4.13 Perhitungan Basis Gröbner pada Kriptanalisis Blok Kelima

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_3x_4 + 1, x_2 + x_4^4, x_3 + x_4^2 + 1, x_3 + x_4^2 + 1, x_4^6 + x_4\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(-1, 0, -1, 0)
(0, -1, -2, -1)
```

Gambar 4.14 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Kelima

Solusi yang dihasilkan sesuai plainteks blok kelima yaitu (0,1,0,1), sehingga dapat disimpulkan bahwa kriptanalisis menggunakan basis Gröbner pada blok kelima berhasil.

Selanjutnya, dapat dicari solusi dari basis Gröbner menggunakan teori eliminasi. Berdasarkan persamaan $x_4^6 + x_4 = 0$, maka terdapat dua kemungkinan nilai x_4 yaitu

a. $x_4 = 0$

   Jika nilai $x_4 = 0$, maka nilai yang sesuai adalah $x_3 = 1$, $x_2 = 0$, dan $x_1 = 1$. Nilai solusi sistem persamaan berdasarkan kemungkinan ini yaitu (1,0,1,0).

b. $x_4 = 1$

   Kemungkinan kedua ini akan menghasilkan nilai $x_3 = 0$, $x_2 = 1$, dan $x_1 = 0$. Sehingga solusi sistem persamaan yang sesuai adalah (0,1,0,1).

Solusi yang dihasilkan sesuai plainteks blok kelima yaitu (0,1,0,1), sehingga dapat disimpulkan bahwa kriptanalisis basis Gröbner pada blok kelima berhasil.

6. Perhitungan blok keenam

$$P(x)+c=\begin{pmatrix}x_1x_2+x_2+x_3+1\\ x_2x_3+x_2+x_4+1\\ x_1+x_3x_4+x_4+1\\ x_2+x_1x_4+x_4+1\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}x_1x_2+x_2+x_3+1\\ x_2x_3+x_2+x_4+1\\ x_1+x_3x_4+x_4\\ x_2+x_1x_4+x_4+1\end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$\begin{aligned}x_1x_2+x_2+x_3&=1\\ x_2x_3+x_2+x_4&=1\\ x_1+x_3x_4+x_4&=0\\ x_2+x_1x_4+x_4&=1\end{aligned}$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 1
f2 = x2*x3 + x2 + x4 + 1
f3 = x1 + x3*x4 + x4 + 0
f4 = x2 + x1*x4 + x4 + 1

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x3*x4 + x4
x2 + x3 + x4**2 + x4 + 1
x3**2 + x3*x4 + x3 + x4**2
x3*x4**2 + x3
x4**4 + x4**2
```

Gambar 4.15 Perhitungan Basis Gröbner pada Kriptanalisis Blok Keenam

Basis Gröbner yang dihasilkan adalah $\{x_1+x_3x_4+x_4,\ x_2+x_3+x_4^2+x_4+1, x_3^2+x_3x_4+x_3+x_4^2, x_3x_4^2+x_3, x_4^4+x_4^2\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(0, -1, 0, 0)
```

Gambar 4.16 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Keenam

Solusi yang dihasilkan yaitu (0,1,0,0), yang masih belum sesuai dengan plainteks asli. Selanjutnya dapat dibuktikan bahwa plainteks asli sebenarnya juga solusi basis Gröbner:

$$0 + 1 + 1 = 0,$$
$$0 + 1 + 1 + 1 + 1 = 0,$$
$$1 + 1 + 1 + 1 = 0,$$
$$1 + 1 = 0,$$
$$1 + 1 = 0.$$

Sehingga terbukti bahwa (0,0,1,1) juga termasuk solusi basis Gröbner blok keenam. Sehingga terdapat kemungkinan penyerang salah dalam melakukan kriptanalisis blok keenam.

Selanjutnya, dapat dicari solusi dari basis Gröbner. Terdapat dua solusi untuk x_4 yaitu 0 dan 1. Berikut hasil perhitungan kemungkinan solusi:

a. $x_4 = 0$

   Jika nilai $x_4 = 0$, maka nilai yang sesuai adalah $x_3 = 1$, $x_2 = 0$, dan $x_1 = 1$. Nilai solusi sistem persamaan berdasarkan kemungkinan ini yaitu (1,0,1,0).

b. $x_4 = 1$

   Kemungkinan kedua ini akan menghasilkan nilai $x_3 = 1$, $x_2 = 0$, dan $x_1 = 0$. Sehingga solusi sistem persamaan yang sesuai adalah (0,0,1,1).

Selanjutnya dapat dibuktikan (1,1,0,0) adalah solusi basis Gröbner:

$$0 + 1 + 1 = 0,$$
$$0 + 1 + 1 + 1 + 1 = 0,$$
$$1 + 1 + 1 + 1 = 0,$$
$$1 + 1 = 0,$$
$$1 + 1 = 0.$$

Sehingga terbukti bahwa (0,0,1,1) juga termasuk solusi basis Gröbner blok keenam. Jadi, kriptanalisis basis Gröbner pada blok keenam berhasil.

7. Perhitungan blok ketujuh

$$P(x) + c = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 + 1 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$x_1x_2 + x_2 + x_3 = 1$$
$$x_2x_3 + x_2 + x_4 = 1$$
$$x_1 + x_3x_4 + x_4 = 0$$
$$x_2 + x_1x_4 + x_4 = 1$$

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_3x_4 + x_4, x_2 + x_3 + x_4^2 + x_4 + 1, x_3^2 + x_3x_4 + x_3 + x_4^2, x_3x_4^2 + x_3, x_4^4 + x_4^2\}$. Blok ketujuh memiliki cipherteks dan plainteks yang sama dengan blok pertama dan ketiga sehingga perhitungannya pasti akan sama sehingga kriptanalisis berhasil.

8. Perhitungan blok kedelapan

$$P(x) + c = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 + 1 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_2 + x_3 + 1 \\ x_2x_3 + x_2 + x_4 + 1 \\ x_1 + x_3x_4 + x_4 \\ x_2 + x_1x_4 + x_4 + 1 \end{pmatrix}$$

Jadi, kriptanalisis dapat dilakukan dengan cara menghitung basis Gröbner dari sistem persamaan linear.

$$x_1x_2 + x_2 + x_3 = 0$$
$$x_2x_3 + x_2 + x_4 = 1$$
$$x_1 + x_3x_4 + x_4 = 1$$
$$x_2 + x_1x_4 + x_4 = 1$$

```
from sympy import symbols, groebner, GF, solve

# Mendefinisikan variabel
x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

# Mendefinisikan polinomial
f1 = x1*x2 + x2 + x3 + 0
f2 = x2*x3 + x2 + x4 + 1
f3 = x1 + x3*x4 + x4 + 1
f4 = x2 + x1*x4 + x4 + 1

# Membuat basis Gröbner di lapangan GF(2)
G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex', domain=GF(2))

# Menampilkan basis Gröbner
print("Basis Gröbner di GF(2):")
for g in G:
    print(g)
```

```
Basis Gröbner di GF(2):
x1 + x4**3 + x4**2 + x4 + 1
x2 + x4**4 + x4**3 + x4**2 + 1
x3 + x4**2 + x4
x4**6 + x4**4
```

Gambar 4.17 Perhitungan Basis Gröbner pada Kriptanalisis Blok Kedelapan

Basis Gröbner yang dihasilkan adalah $\{x_1 + x_4^3 + x_4^2 + x_4 + 1, x_2 + x_4^4 + x_4^3 + x_4^2 + 1,\ x_3 + x_4^2 + x_4,\ x_4^6 + x_4^4\}$. Selanjutnya, dapat dicari solusi dari basis Gröbner.

```
# Mencari solusi dari basis Gröbner
solusi = solve(list(G), x1, x2, x3, x4, domain=GF(2))

# Menampilkan solusi yang mungkin
print("\nSolusi:")
for s in solusi:
    print(s)
```

```
Solusi:
(-1, -1, 0, 0)
```

Gambar 4.18 Perhitungan Solusi Basis Gröbner Kriptanalisis Blok Kedelapan

Solusi yang dihasilkan blok kedelapan yaitu (1,1,0,0). Solusi ini masih belum tepat sehingga perlu diperiksa apakah plainteks merupakan solusi basis Gröbner untuk membuktikan bahwa kriptanalisis berhasil.

$$0 + 1 + 1 + 1 + 1 = 0,$$
$$0 + 1 + 1 + 1 + 1 = 0,$$
$$0 + 1 + 1 = 0,$$
$$1 + 1 = 0.$$

Kriptanalisis blok kedelapan belum tentu berhasil dipulihkan karena tidak langsung memberikan hasil yang sesuai dengan plainteks.

Selanjutnya, dapat dicari solusi dari basis Gröbner. Pada blok terakhir ini solusi basis Gröbner juga memiliki dua kemungkinan nilai x_4 yang berbeda. Hal ini dikarenakan lapangan yang digunakan adalah $GF(2)$ dan persamaan yang dihitung adalah $x_4^6 + x_4^4 . = 0$. Jadi, terdapat dua kemungkinan solusi yaitu:

a. $x_4 = 0$

   Jika nilai $x_4 = 0$, maka nilai yang sesuai adalah $x_3 = 0, x_2 = 1$, dan $x_1 = 1$. Nilai solusi sistem persamaan berdasarkan kemungkinan ini yaitu $(0,0,1,1)$.

b. $x_4 = 1$

   Kemungkinan kedua ini akan menghasilkan nilai $x_3 = 0$, $x_2 = 0$, dan $x_1 = 0$. Sehingga solusi sistem persamaan yang sesuai adalah (0,0,0,1).

Solusi basis Gröbner yang sesuai plainteks adalah (0,0,0,1). Untuk membuktikan bahwa kriptanalisis berhasil maka perhitungan dilakukan di bawah ini:

$$0 + 1 + 1 + 1 + 1 = 0,$$
$$0 + 1 + 1 + 1 + 1 = 0,$$
$$0 + 1 + 1 = 0,$$
$$1 + 1 = 0.$$

Kriptanalisis blok kedelapan berhasil dilakukan menggunakan basis Gröbner karena blok plainteks telah berhasil dipulihkan.

Kriptanalisis cipherteks semua blok telah berhasil mengembalikan semua blok plainteks,

$$0100\ 0010\ 0100\ 1001\ 0101\ 0011\ 0100\ 0001.$$

Jadi, dapat disimpulkan bahwa kriptanalisis kriptografi kunci publik multivariat menggunakan basis Gröbner telah berhasil dilakukan. Blok plainteks yang berhasil didapatkan dapat diubah menjadi bentuk biner 8 bit sehingga didapatkan kembali plainteks yang dienkripsi.

$$01000010 \quad 01001001 \quad 01010011 \quad 01000001$$
$$\text{B} \qquad \text{I} \qquad \text{S} \qquad \text{A}$$

Hasil kriptanalisis sesuai dengan plainteks yang digunakan. Namun beberapa blok tidak langsung mengembalikan plainteks asli seperti pada blok 4, 6, dan 8 meskipun telah dibuktikan bahwa plainteks asli juga merupakan solusi. Karena itu terdapat hasil lain yang mungkin ditemukan yaitu

$$01000010 \quad 01000111 \quad 01010100 \quad 01001100.$$
$$\text{B} \qquad \text{G} \qquad \text{T} \qquad \text{L}$$

Solusi ini merupakan solusi yang mungkin didapatkan jika penyerang hanya menggunakan alat bantu pada Python. Beberapa solusi lain juga akan didapatkan saat penyerang hanya menggunakan teori eliminasi karena harus melakukan banyak asumsi untuk mencari nilai solusi yang sesuai.

Jadi, dapat disimpulkan bahwa sistem polinomial yang digunakan bisa digunakan untuk mengamankan pesan meskipun belum terlalu kuat karena masih bisa dipecahkan Untuk meningkatkan keamanan beberapa hal dapat dilakukan seperti mengganti lapangan serta polinomial menjadi yang lebih kompleks dengan variabel atau derajat yang lebih besar.

4.5 Kriptografi dalam Perspektif Keislaman

Kriptografi memiliki prinsip dan nilai yang sesuai dengan Al-Qur'an dan Hadits. Nilai tersebut di antaranya keamanan, kerahasiaan, dan keadilan. Konsep nilai dan prinsip ini merupakan beberapa hal yang penting dalam kriptografi. Berikut ini beberapa konsep nilai yang penting dalam kriptografi dan dapat dijumpai pada ayat Al-Qur'an dan hadits.

1. Konsep rahasia dan amanah

   Kriptografi kunci publik multivariat merupakan kriptografi yang sangat efektif untuk menjaga kerahasiaan informasi dan data. Hal ini dikarenakan terdapat kunci privat yang hanya diketahui oleh pembuat kunci. Oleh karena itu, akses terhadap informasi akan terbatas kepada orang tertentu yang diberi amanah. Konsep rahasia dan amanah juga terdapat dalam Al-Qur'an dan Hadits. Salah satunya terdapat pada surat Al-Anfal ayat 27 berikut:

   يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ (٢٧)

   Artinya:
   "*Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedang kamu mengetahui*". (QS Al-Anfal:27)

   Ayat ini menekankan pada pentingnya menjaga kepercayaan atau amanah yang diberikan. Amanah yang diberikan salah satu contohnya berupa

informasi pribadi yang hanya diketahui oleh orang tertentu atau yang diberi amanah. Hal ini sejalan dengan konsep kriptografi dalam penjagaan data yang bisa berupa pesan rahasia yang merupakan perwujudan dari sikap amanah. Menjaga rahasia juga disebutkan pada hadits shahih Bukhori berikut (AL-Albani, 2008):

عَنْ أَنَسَ بْنَ مَالِكٍ قَالَ: أَسَرَّ إِلَيَّ النَّبِيُّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ سِرًّا فَمَا أَخْبَرْتُ بِهِ أَحَدًا بَعْدَهُ وَلَقَدْ سَأَلَتْنِي أُمُّ سُلَيْمٍ فَمَا أَخْبَرْتُهَا بِهِ (رواه البخاري)

Artinya:
"Anas bin Malik berkata:"Nabi SAW. membicarakan pembicaraan rahasia kepadaku. Aku sama sekali tidak memberitahukan pembicaraan rahasia tersebut kepada seorang pun setelah kematian beliau. Ummu Sulaim pernah bertanya kepadaku tentang hal itu, namun aku sama sekali tidak mau memberitahukannya kepadanya.". (HR Bukhari)

Hadits yang diriwayatkan oleh imam Bukhori di atas menunjukkan bahwa suatu pembicaraan rahasia tidak boleh dibicarakan kepada orang lain. Suatu rahasia hanya boleh diketahui oleh orang tertentu. Hal ini sejalan dengan tujuan kriptografi yaitu mengamankan pesan sehingga tidak diketahui oleh orang yang tidak berhak.

2. Keamanan informasi

Menjaga keamanan informasi serta melindungi data termasuk kewajiban setiap individu. Memastikan bahwa informasi tidak dapat diakses, dibocorkan, atau dimanipulasi merupakan upaya dalam keamanan informasi. hal ini sejalan dengan konsep sebelumnya yaitu amanah dan kepercayaan yang juga menjadi prinsip kriptografi. Keduanya merupakan prinsip nilai Islam yang harus selalu dipegang teguh dalam kehidupan. Ayat tentang keamanan informasi salah satunya terdapat pada surat An-Nur ayat 27 berikut:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ (٢٧)

Artinya:
"Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat". (QS An-Nur:27)

Pada surat An-Nur ayat 23 disebutkan bahwa seseorang tidak boleh memasuki rumah orang lain tanpa izin dari pemilik rumah. Hal ini sama dengan privasi seseorang yang dijaga dan tidak ada orang yang berhak memasukinya tanpa seizin pemilik. Seseorang memiliki hak untuk menjaga privasinya ataupun informasi pribadi agar tidak diketahui oleh orang-orang yang tidak diinginkan.

3. Keadilan dalam penggunaan teknologi kriptografi

Keadilan adalah prinsip yang harus dijunjung tinggi dalam semua aspek kehidupan termasuk pada teknologi. Keadilan ini bertujuan agar penggunaan teknologi tidak merugikan serta tidak diskriminatif. Penggunaan teknologi kriptografi secara adil berarti tidak membedakan atau mengeksploitasi beberapa pihak tertentu dalam upaya perlindungan data. Nilai keadilan juga menjadi salah satu nilai yang ditekankan dalam islam sehingga disebutkan dalam Al-Qur'an dan hadits. Sikap adil disebutkan dalam QS Al-Maidah ayat 8:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا كُوْنُوْا قَوَّامِيْنَ لِلّٰهِ شُهَدَاۤءَ بِالْقِسْطِۖ وَلَا يَجْرِمَنَّكُمْ شَنَاٰنُ قَوْمٍ عَلٰٓى اَلَّا تَعْدِلُوْا ۗاِعْدِلُوْاۗ هُوَ اَقْرَبُ لِلتَّقْوٰىۖ وَاتَّقُوا اللّٰهَ ۗاِنَّ اللّٰهَ خَبِيْرٌۢ بِمَا تَعْمَلُوْنَ (٨)

Artinya:
"*Wahai orang-orang yang beriman! Jadilah kamu sebagai penegak keadilan karena Allah, (ketika) menjadi saksi dengan adil. Dan janganlah kebencianmu terhadap suatu kaum mendorong kamu untuk berlaku tidak adil. Berlaku adillah. Karena (adil) itu lebih dekat kepada takwa. Dan*

bertakwalah kepada Allah, sungguh, Allah Maha teliti terhadap apa yang kamu kerjakan". (QS Al-Maidah:8)

Nilai keadilan sangat penting dalam penggunaan teknologi dan kriptografi. Nilai keadilan di sini berarti menempatkan sesuatu pada tempatnya. Hal ini dikarenakan teknologi termasuk kriptografi dapat digunakan tidak seharusnya. Contohnya, kriptanalisis dapat digunakan untuk mendekripsi pesan tanpa kunci privat. Hal ini memungkinkan pihak lain dapat membaca pesan yang dikirimkan sehingga merugikan beberapa pihak. Namun, kriptanalisis juga berguna untuk menganalisis keamanan suatu kriptografi dan membuatnya agar lebih baik.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan, diperoleh dua hasil kesimpulan berikut:

1. Konstruksi sistem kriptografi kunci publik multivariat memanfaatkan sifat polinomial pada lapangan berhingga. Proses dalam kriptografi melibatkan pembentukan kunci privat menggunakan trasformasi affine dan sistem persamaan polinomial. Tingkat keamanan kriptografi bergantung pada kompleksitas polinomial serta transformasi yang dipilih.
2. Penerapan basis Gröbner pada kriptanalisis dapat dilakukan dengan menyelesaikan sistem persamaan polinomial kunci publik dan hasil enkripsi. Basis Gröbner mampu menyederhanakan polinomial sehingga memungkinkan pencarian solusi polinomial. Kriptanalisis menggunakan basis Gröbner dapat mengevaluasi tingkat kerentanan kriptografi, meskipun tingkat keberhasilannya dipengaruhi oleh kompleksitas polinomial yang digunakan.

5.2 Saran untuk Penelitian Lanjutan

Penelitan ini telah menganalisis bagaimana tahapan kriptografi kunci publik multivariat dan bagaimana basis Gröbner dapat diterapkan. Namun penelitian hanya terbatas pada lapangan berhingga $GF(2)$ dan polinomial yang digunakan pada 4 variabel. Penelitian selanjutnya dapat menganalisis lapangan dan variabel yang lebih besar. Selain itu, algoritma basis Gröbner lain dapat digunakan untuk penelitian yang lebih lanjut.

DAFTAR PUSTAKA

Adams, W. W., & Loustaunau, P. (1994). *An Introduction to Grobner Bases*. American Mathematical Society.

AL-Albani, M. N. (2008). *Ringkasan Shahih Muslim*. Gema Insani.

Al-Bayan. (2008). *Shahih Bukhari Muslim: Hadis-Hadis Yang Diriwayatkan Oleh 2 Ahli Hadis Imam Bukhori & Imam Muslim*. Jabal.

Al-Mundziri, A.-H. (2020). *Mukhtashar Shahih Muslim*. Hikam Pustaka.

Amiruddin. (2021). Amanah dalam Perspektif Al-Quran (Studi Komparatif Tafsir Al-Misbah dan Al-Azhar). *Jurnal MUDARRISUNA: Media Kajian Pendidikan Agama Islam*, *11*(4), 833–850.

Angriani, P. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *DIKTUM: Jurnal Syariah Dan Hukum*, *19*(2), 149–165.

Benvenuto, C. J. (2012). Galois Field in Cryptography. *Math Washington*.

Cox, D., Little, J., & O'Shea, D. (2015). Ideals, Varieties, and Algorithms. In *Undergraduate texts in mathematics: Ideals, varieties, and algorithms* (4th ed.). Springer.

Das, H. K., & Reza, N. (2018). On Gröbner Bases and Their Uses in Solving System of Polynomial Equations and Graph Coloring. *Journal of Mathematics and Statistics*, *14*(1), 175–182.

Ding, J., Petzoldt, A., & Schmidt, D. (2016). *Multivariate Public Key Cryptosystems* (2nd ed.). Springer. http://www.springer.com/series/5576

Gallian, J. A. (2017). *Contemporary Abstract Algebra* (9th ed.). Cengage Learning.

Gilbert, L., & Gilbert, J. (2013). Element of Modern Algebra. In *Cengage Learning* (8th ed.). Cengage Learning.

Guevara, C. (2016). *Applications of Gröbner Bases in Commutative Algebra and Algebraic Geometry*. long Island University.

Kara, G., & Yayla, O. (2022). Gröbner Basis Attack on STARK-Friendly Symmetric-Key Primitives: JARVIS, MiMC and GMiMCerf. *15th International Conference on Information Security and Cryptography, ISCTURKEY 2022 - Proceedings*, *2*, 1–7. https://doi.org/10.1109/ISCTURKEY56345.2022.9931846

Kementrian Agama RI. (2019). *Qur'an Kemenag*. Lajnah Pentashihan Mushaf Al-Qur'an.

Mencinger, M. (2013). On Groebner Bases and Their Use in Solving Some Practical Problems. *Universal Journal of Computational Mathematics*, *1*(1), 5–14.

Mukhtar, H. (2018). *Kriptografi untuk Keamanan Data*. Deepublish.

Noviani, E., Sulandra, I. M., & Susanto, H. (2013). Implementasi Basis Groebner Dalam Menentukan Keanggotaan Ideal Di "Cas Singular." *Jurusan Matematika-Fakultas MIPA UM*, *3*, 1–9.

Rasiman, Rubowo, M. R., & Pramasdyahsari, A. S. (2018). Teori Ring. In *Univ. PGRI Semarang Press*. http://eprints.upgris.ac.id/637/1/Buku Teori Ring.pdf

Riyanto, M. Z. (2010). Sistem Kriptografi Kunci Publik Multivariat. *Seminar Nasional Matematika Dan Pendidikan Matematika*, 52–58.

Soediro. (2018). Prinsip Keamanan, Privasi, Dan Etika Dalam Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif Hukum Islam. *Kosmik Hukum*, *18*(2).

Wahyuni, S., Wijayanti, I. E., Yuwaningsih, D. A., & Hartanto, A. D. (2016). *Teori Ring dan Modul*. Gadjah Mada University Press.

Zhao, K., Cui, J., & Xie, Z. (2017). Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2017/9828967

LAMPIRAN

Lampiran 1. Program Python Perhitungan Basis Gröbner

```
from sympy import symbols, groebner

# Mendefinisikan variabel dan polinomial

x1, x2, x3, x4 = symbols('x1 x2 x3 x4')

f1 = x1*x2 + x3

f2 = x2*x3 + x4

f3 = x1 + x3*x4

f4 = x2 + x1*x4

# Membuat basis Gröbner

G = groebner([f1, f2, f3, f4], x1, x2, x3, x4, order='lex')

# Menampilkan basis Gröbner

print("Basis Gröbner:")

for g in G:

   print(g)
```

Lampiran 2. Program Python Perhitungan Solusi dari Basis Gröbner

```
from sympy import symbols, groebner, solve

# Mencari solusi dari basis Gröbner

solusi = solve(list(G), x1, x2, x3, x4)

# Menampilkan solusi yang mungkin

print("\nSolusi:")

for s in solusi:

   print(s)
```

Lampiran 3. Program Singular CAS Perhitungan Basis Gröbner

```
// Mendefinisikan polinomial atas lapangan tak hingga (GF(2)) dengan variabel x1, x2, x3, x4, x5

ring r = 2, (x1, x2, x3, x4, x5), lp;

//Mendefinisikan polinomial-polinomial dari cipherteks

poly f1 = x1^3 + 1 + 1101;

poly f2 = x2^3 + 1 + 1011;

poly f3 = x3^3 + 1 + 1001;

poly f4 = x4^3 + 1 + 0101;

poly f5 = x5^3 + 1 + 0110;

// Mendefinisikan ideal yang dibangun oleh polinomial-polinomial tersebut

ideal I = f1, f2, f3, f4, f5;

// Menghitung basis Grobner dari ideal I

ideal G = groebner(I);

// Output the Gröbner basis

G;
```

Lampiran 4. Hasil Lanjutan Perhitungan Basis Gröbner Sistem Polinomial Kedua

```
x3+x4^479+x4^478+x4^476+x4^475+x4^474+x4^472+x4^467+x4^466+x4^464+x4^455+x4^454+
x4^452+x4^451+x4^450+x4^448+x4^447+x4^446+x4^439+x4^438+x4^436+x4^428+x4^427+x4^
426+x4^424+x4^423+x4^422+x4^419+x4^418+x4^412+x4^411+x4^410+x4^408+x4^400+x4^399
+x4^398+x4^396+x4^395+x4^394+x4^391+x4^390+x4^388+x4^384+x4^383+x4^382+x4^380+x4
^371+x4^370+x4^368+x4^367+x4^366+x4^364+x4^363+x4^362+x4^360+x4^355+x4^354+x4^35
2+x4^343+x4^342+x4^340+x4^335+x4^334+x4^332+x4^327+x4^326+x4^324+x4^323+x4^322+x
4^320+x4^311+x4^310+x4^308+x4^307+x4^306+x4^303+x4^301+x4^300+x4^299+x4^298+x4^2
97+x4^295+x4^293+x4^291+x4^290+x4^289+x4^286+x4^285+x4^284+x4^281+x4^280+x4^278+
x4^277+x4^275+x4^274+x4^273+x4^272+x4^271+x4^270+x4^264+x4^260+x4^259+x4^258+x4^
256+x4^254+x4^253+x4^252+x4^251+x4^250+x4^249+x4^248+x4^247+x4^245+x4^244+x4^241
+x4^239+x4^237+x4^236+x4^233+x4^230+x4^229+x4^228+x4^227+x4^226+x4^225+x4^224+x4
^222+x4^221+x4^219+x4^218+x4^217+x4^214+x4^213+x4^212+x4^209+x4^208+x4^200+x4^19
9+x4^198+x4^195+x4^194+x4^191+x4^189+x4^187+x4^186+x4^185+x4^184+x4^183+x4^181+x
4^180+x4^179+x4^178+x4^177+x4^175+x4^174+x4^172+x4^168+x4^167+x4^166+x4^164+x4^1
63+x4^162+x4^159+x4^158+x4^148+x4^147+x4^146+x4^143+x4^142+x4^139+x4^138+x4^136+
x4^128+x4^119+x4^118+x4^116+x4^112+x4^110+x4^109+x4^107+x4^106+x4^105+x4^102+x4^
101+x4^100+x4^99+x4^98+x4^97+x4^95+x4^93+x4^91+x4^90+x4^89+x4^86+x4^85+x4^83+x4^
82+x4^81+x4^80+x4^76+x4^75+x4^74+x4^68+x4^62+x4^61+x4^60+x4^59+x4^58+x4^57+x4^56
+x4^54+x4^53+x4^49+x4^48+x4^47+x4^46+x4^44+x4^40+x4^35+x4^34+x4^31+x4^30+x4^27+x
4^26+x4^24+x4^20+x4^19+x4^18+x4^12+1,
x2*x4^3+x2*x4^2+x2+x3^30*x4^5+x3^30*x4^4+x3^30*x4^3+x3^30+x3^29*x4^12+x3^25*x4^5
+x3^25*x4^4+x3^25*x4^3+x3^25+x3^24*x4^12+x3^24*x4^8+x3^24*x4^4+x3^24*x4^2+x3^24+
x3^23*x4^15+x3^23*x4^14+x3^23*x4^12+x3^10*x4^5+x3^10*x4^4+x3^10*x4^3+x3^10+x3^9*
x4^12+x3^6*x4^11+x3^6*x4^10+x3^6*x4^8+x3^6*x4^7+x3^6*x4^6+x3^6*x4^5+x3^6*x4^3+x3
^6+x3^5*x4^12+x3^5*x4^5+x3^5*x4^4+x3^5*x4^3+x3^5+x3^4*x4^12+x3^4*x4^8+x3^4*x4^4+
x3^4*x4^2+x3^4+x3^3*x4^15+x3^3*x4^14+x3^3*x4^12+x3^2*x4^19+x3^2*x4^17+x3^2*x4^13
+x4^18+x4^16+x4^14+x4^10+x4^4,
x2^20+x2^16+x2^12*x3^10+x2^10*x3*x4^6+x2^10*x4^9+x2^8*x3^15+x2^8*x3^9*x4^3+x2^8*
x3^9*x4^2+x2^8*x3^9+x2^8*x3^5+x2^8*x3^3*x4^6+x2^8*x3^3*x4^4+x2^8*x3^3+x2^6*x4^9+
x2^6*x4^8+x2^6*x4^6+x2^4*x3^10+x2^4+x3^25+x3^20+x3^19*x4^3+x3^19*x4^2+x3^19+x3^1
3*x4^6+x3^13*x4^4+x3^13+x3^9*x4^3+x3^9*x4^2+x3^9+x3^5+x3^3*x4^6+x3^3*x4^4+x3^3+1
,
x1+x2^19*x3+x2^16*x4^4+x2^15*x3+x2^12*x3*x4+x2^12*x4^4+x2^11*x3^11+x2^10*x3^2*x4
^3+x2^9*x3^2*x4^5+x2^9*x3^2*x4^3+x2^9*x3*x4^8+x2^9*x3*x4^6+x2^9*x3*x4+x2^8*x3^10
*x4^4+x2^8*x3*x4^8+x2^8*x3*x4^7+x2^8*x3*x4^6+x2^8*x3*x4^4+x2^8*x3*x4+x2^8*x4^4+x
2^8*x4^3+x2^8*x4+x2^7*x3^11+x2^7*x3+x2^6*x3*x4^9+x2^6*x3*x4^7+x2^6*x4^12+x2^6*x4
^10+x2^5*x3*x4^8+x2^5*x3*x4^7+x2^5*x3*x4^6+x2^5*x3*x4^3+x2^4*x3^11*x4+x2^4*x3^10
*x4^4+x2^4*x3*x4+x2^4*x4^4+x2^3*x3^11+x2^3*x3+x2^2*x3^12*x4^3+x2^2*x3^2*x4^3+x2^
2*x4^12+x2^2*x4^11+x2^2*x4^10+x2^2*x4^7+x2*x3^11*x4+x2*x3*x4+x3^11*x4^8+x3^11*x4
^7+x3^11*x4^6+x3^11*x4^4+x3^11*x4+x3^10*x4^3+x3^10*x4+x3*x4^8+x3*x4^7+x3*x4^6+x3
*x4^4+x3*x4+x4^3+x4
```

RIWAYAT HIDUP

Firdaus Masitha, lahir di Malang pada tanggal 26 Maret 2000. Memiliki nama panggilan Firda. Bertempat tinggal di Desa Kuwolu, RT 08/RW 03, Kecamatan Bululawang, Kabupaten Malang, Jawa Timur. Merupakan anak pertama dari tiga bersaudara dari pasangan Bapak Solichan dan Ibu Suliati.

Pendidikan yang ditempuh yaitu MI Al-Hikmah Bululawang, lulus pada tahun 2011. Kemudian dilanjutkan dengan menempuh pendidikan yang lebih lanjut di MTS Al-Hikmah Bululawang dan lulus pada tahun 2014. Pada tahun yang sama melanjutkan pendidikan di SMA Islam Al-Hikmah Bululawang dan lulus pada tahun 2017. Pada tahun 2019 melanjutkan studi di Universitas Islam Negeri Maulana Malik Ibrahim Malang pada Program Studi Matematika.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Firdaus Masitha
NIM : 196100333
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Aplikasi Basis Gröbner Pada Kriptografi Kunci Publik Multivariat
Pembimbing I : Intan Nisfulaila, M.Si
Pembimbing II : Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	17 Januari 2023	Konsultasi Bab I	1.
2.	31 Maret 2023	Konsultasi Bab II dan III	2.
3.	14 April 2023	Konsultasi Revisi Bab I, II, dan III	3.
4.	24 Mei 2023	Konsultasi Revisi Bab I, II, dan III	4.
5.	20 Maret 2024	ACC Bab I, II, dan III	5.
6.	27 Maret 2024	Konsultasi Kajian Agama Bab I dan II	6.
7.	3 April 2024	Konsultasi Revisi Kajian Agama Bab I dan II	7.
8.	4 April 2024	ACC Kajian Agama Bab I dan II	8.
9.	11 September 2024	ACC Seminar Proposal	9.
10.	2 November 2024	Konsultasi Revisi Seminar Proposal	10.
11.	5 November 2024	Konsultasi Bab IV dan V	11.
12.	6 November 2024	Konsultasi Kajian Agama Bab IV	12.
13.	7 November 2024	ACC Kajian Agama Bab IV	13.
14.	11 November 2024	ACC Seminar Hasil	14.
15.	9 Desember 2024	Konsultasi Revisi Seminar Hasil	15.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

16.	10 Desember 2024	ACC Sidang Skripsi	16.
17.	19 Desember 2024	ACC Keseluruhan	17.

Malang, 24 Desember 2024
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005