MODIFIKASI ENKRIPSI ELGAMAL DALAM ALJABAR MAX-PLUS UNTUK PENGAMANAN DOKUMEN BAHASA ARAB

SKRIPSI

Diajukan untuk Memenuhi Sebagian Syarat
Guna Memperoleh Gelar Sarjana Matematika
dalam Ilmu Matematika

Oleh : **REGITA NURUL FITRIANI**
NIM : 1908046007

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI WALISONGO
SEMARANG
2023

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

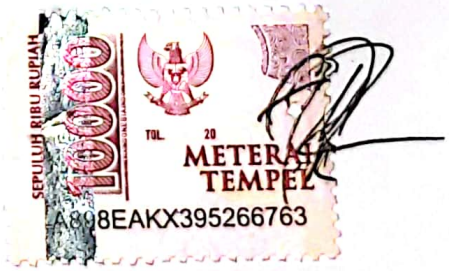
Nama	:	REGITA NURUL FITRIANI
NIM	:	1908046007
Program Studi	:	Matematika

menyatakan bahwa skripsi yang berjudul :

MODIFIKASI ENKRIPSI ELGAMAL DALAM ALJABAR MAX-PLUS UNTUK PENGAMANAN DOKUMEN BAHASA ARAB

secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali bagian tertentu yang dirujuk sumbernya.

Semarang, 25 Mei 2023
Pembuat pernyataan,



REGITA NURUL FITRIANI
NIM : 1908046007

KEMENTERIAN AGAMA R.I.
UNIVERSITAS ISLAM NEGERI WALISONGO
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Prof. Dr. Hamka (Kampus II) Ngaliyan Semarang
Telp. 024-7601295 Fax. 7615387

PENGESAHAN

Naskah skripsi berikut ini :

Judul : **MODIFIKASI ENKRIPSI ELGAMAL DALAM ALJABAR MAX-PLUS UNTUK PENGAMANAN DOKUMEN BAHASA ARAB**
Penulis : REGITA NURUL FITRIANI
NIM : 1908046007
Jurusan : Matematika

Telah diujikan dalam sidang *tugas akhir* oleh Dewan Penguji Fakultas Sains dan Teknologi UIN Walisongo dan dapat diterima sebagai salah satu syarat memperoleh gelar sarjana dalam Ilmu Matematika.

Semarang, 25 Mei 2023

DEWAN PENGUJI

Penguji I,
Prihadi Kurniawan, M.Sc.
NIP : 19901226 201903 1 012

Penguji II,
Any Muanalifah, M.Si., Ph.D.
NIP : 19820113 201101 2 009

Penguji III,
Ayus Riana Isnawati, M.Sc.
NIP : 19851019 201903 2 014

Penguji IV,
Dinni Rahma Oktaviani, M.Si.
NIP : 19941009 201903 2 017

Pembimbing I,
Any Muanalifah, M.Si., Ph.D.
NIP : 19820113 201101 2 009

Pembimbing II,
Agus Wayan Yulianto, M.Sc.
NIP : 19890716 201903 1 007

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI UIN WALISONGO SEMARANG REPUBLIK INDONESIA

NOTA DINAS

Semarang, 25 Mei 2023

Yth. Ketua Program Studi Matematika
Fakultas Sains dan Teknologi
UIN Walisongo Semarang

Assalamu'alaikum warahmatullahi wabarakatuh

Dengan ini diberitahukan bahwa saya telah melakukan bimbingan, arahan dan koreksi naskah skripsi dengan:

Judul	:	MODIFIKASI ENKRIPSI ELGAMAL DALAM ALJABAR MAX-PLUS UNTUK PENGAMANAN DOKUMEN BAHASA ARAB
Nama	:	REGITA NURUL FITRIANI
NIM	:	1908046007
Jurusan	:	Matematika

Saya memandang bahwa naskah skripsi tersebut sudah dapat diajukan kepada Fakultas Sains dan Teknologi UIN Walisongo untuk diujikan dalam Sidang Munaqasyah.

Wassalamu'alaikum warahmatullahi wabarakatuh

Pembimbing I,

Any Muanalifah, M.Si., Ph.D.
NIP : 19820113 201101 2 009

NOTA DINAS

Semarang, 25 Mei 2023

Yth. Ketua Program Studi Matematika
Fakultas Sains dan Teknologi
UIN Walisongo Semarang

Assalamu'alaikum warahmatullahi wabarakatuh

Dengan ini diberitahukan bahwa saya telah melakukan bimbingan, arahan dan koreksi naskah skripsi dengan:

Judul	:	MODIFIKASI ENKRIPSI ELGAMAL DALAM ALJABAR MAX-PLUS UNTUK PENGAMANAN DOKUMEN BAHASA ARAB
Nama	:	REGITA NURUL FITRIANI
NIM	:	1908046007
Jurusan	:	Matematika

Saya memandang bahwa naskah skripsi tersebut sudah dapat diajukan kepada Fakultas Sains dan Teknologi UIN Walisongo untuk diujikan dalam Sidang Munaqasyah.

Wassalamu'alaikum warahmatullahi wabarakatuh

Pembimbing II,

Agus Wayan Yulianto, M.Sc.
NIP : 19890716 201903 1 007

ABSTRAK

Penelitian ini membahas mengenai modifikasi enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab. Operasi yang digunakan dalam aljabar max-plus meliputi operasi penjumlahan $\oplus$ yang didefinisikan sebagai operasi maksimum dan operasi perkalian $\otimes$ yang didefinisikan sebagai operasi penjumlahan biasa. Algoritma enkripsi elgamal pada aljabar max-plus dimodifikasi menjadi dua algoritma yaitu dengan menggunakan bilangan bulat dan matriks.

Pada aljabar max-plus invers matriks hanya dimiliki oleh matriks permutasi dan matriks diagonal. Oleh karena itu, pada penelitian kali ini penulis menggunakan matriks diagonal untuk proses enkripsi dan dekripsinya.Di aljabar max-plus tidak ada proses diagonalisasi untuk menghasilkan matriks diagonal. Dengan demikian, untuk memperoleh matriks diagonal dilakukan dengan menghapus entri-entri non diagonal pada matriks dan menggantinya dengan $\varepsilon = -\infty$. Entri-entri diagonal utama tetap dipertahankan sehingga terbentuk matriks diagonal yang dapat dicari inversnya.

Kata kunci : Modifikasi, aljabar max-plus, elgamal, enkripsi, dekripsi,matriks diagonal

KATA PENGANTAR

Assalamu'alaikum warrahmatullahi wabarakatuh

Puji syukur penulis panjatkan atas kehadirat Allah SWT yang telah melimpahkan rahmat, taufik dan hidayah-Nya sehingga penulis bisa menyelesaikan skripsi yang berjudul *Modifikasi Enkripsi Elgamal dalam Aljabar Max-Plus untuk Pengamanan Dokumen Bahasa Arab*. Sholawat serta salam semoga tetap tercurah limpahkan kepada baginda Nabi Muhammad saw yang menjadi suri tauladan bagi seluruh umat manusia.

Penyusunan skripsi ini bertujuan guna memenuhi syarat dalam menyelesaikan studi Srata 1 (S1) program studi Matematika di Universitas Islam Negeri Walisongo Semarang.Proses penyusunan skripsi ini tidak lepas dari doa, bantuan, bimbingan, motivasi dan peran dari banyak pihak. Oleh sebab itu, penulis ingin mengucapkan terimakasih kepada :

1. Bapak Prof. Dr. Imam Taufiq, M.Ag., selaku Rektor Universitas Islam Negeri Walisongo Semarang.
2. Bapak Dr. H.Ismail, M.Ag selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Walisongo Semarang.
3. Ibu Hj. Emy Siswanah, M.Sc selaku Ketua Program Studi Matematika Universitas Islam Negeri Walisongo Semarang.
4. Ibu Any Muanalifah, M.Si., Ph.D dan Bapak Agus Wayan Yulianto,M.Sc selaku dosen pembimbing yang telah berkenan meluangkan waktu serta membimbing dan memberikan dorongan kepada penulis sehingga dapat menyelesaikan skripsi dengan baik.

5. Bapak Suyanto, S.Si dan Ibu Diah Kurnia selaku orang tua penulis yang selalu memberikan semangat, dukungan, nasehat dan do'a-do'anya yang tiada henti sehingga penulis termotivasi untuk mengerjakan skripsi ini dengan giat.

6. Muhammad Ulil Albab, Rizky Amalia dan Ayu Nurhayati selaku teman sebimbingan yang telah berjuang bersama dalam menyusun skripsi atas segala bantuan dan semangat yang telah diberikan.

7. Mahardika Karunia Dewi Purnamasari yang telah memberikan banyak bantuan dan dukungan kepada penulis sehingga dapat menyelesaikan skripsi dengan baik.

8. Ayu Faizah, Jihan Ramadhani Ar-Raafi 'Ulna, Dwi Zaratunisah, Mita Nurrohmah, Annisa Nur Latifah, Suaibatul Aslamiah, Fiki Syaban Nugroho dan Muhammad Niamul Maula yang selalu membantu, menemani dan memberi keceriaan selama masa perkuliahan.

9. Seluruh teman-teman mahasiswa program studi matematika 2019 yang sudah menemani studi selama empat tahun. Terkhusus untuk matematika kelas A yang sudah membersamai selama ini, memberikan semangat dan membangun persaudaraan yang semoga selalu kita jaga.

10. Rizky Eka Adiistya N, Nida Maulidia Z, Ginan Nur Izzi, Trisnia Nur Aissyah dan Inka Fatimah Rimadhani selaku sahabat di segala cuaca yang selalu memberikan motivasi dan semangat serta membersamai penulis pada masa-masa sulit.

11. Juga kepada seluruh pihak yang membantu yang tidak

bisa penulis sebutkan satu persatu, sehingga penulis bisa menyelesaikan skripsi ini tepat waktu dengan baik.

12. *Last but not least, for my self, Rere. I wanna thank me for believing in me, for doing all this hard work, for having no days off, for never quitting, for just being me at all time.*

Penulis menyadari masih banyak kekurangan dan kesalahan dalam penulisan skripsi ini. Oleh karena itu, diharapkan kritik dan saran yang membangun guna perbaikan penulisan di masa yang akan datang.Tetapi dengan adanya kekurangan tersebut, penulis berharap penyusunan skripsi ini bisa bermanfaat dan menambah wawasan bagi para pembaca.

Semarang, 25 Mei 2023

Penulis,

Regita Nurul Fitriani

NIM : 1908046007

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMPIRAN

Halaman

BAB I
PENDAHULUAN

Pada bagian ini akan dijelaskan mengenai latar belakang munculnya permasalahan. Selanjutnya permasalahan tersebut dituangkan ke dalam rumusan masalah dan dikaji mengenai tujuan, manfaat, batasan serta metode penelitian.

A. Latar Belakang

Berkembangnya ilmu pengetahuan yang pesat berpengaruh pada kemajuan perkembangan teknologi khususnya internet. Perkembangan internet memberikan kemudahan bagi setiap orang untuk berkomunikasi dan mencari informasi secara efisien. Hal itu dibuktikan dengan mudahnya mencari suatu informasi secara cepat tanpa memperhatikan batasan ruang dan waktu. Informasi yang ada bisa tersebar dalam hitungan menit bahkan detik melalui media sosial. Akan tetapi berkembangnya teknologi internet mendorong sebagian individu untuk mencuri data demi kebutuhan pribadi yang merugikan pihak tertentu.Pada era *society* 5.0 tuntutan akan keamanan atau kerahasiaan sebuah pesan dalam komunikasi menjadi hal yang sangat penting. Oleh karena itu, muncul lah istilah kriptografi yang dapat digunakan sebagai jaminan keamanan informasi rahasia (Reswan, dkk, 2018).
Kriptografi memberikan solusi agar pesan-pesan yang dikirim dapat diubah ke dalam kode dan bisa dibaca oleh pihak penerima pesan yang tertuju. Pesan yang dikirim tidak dapat terbaca oleh pihak ketiga atau dalam kata lain tetap terjaga kerahasiaannya. Sebagaimana firman Allah SWT dalam Q.S. An-Nisa ayat 83 yang berbunyi :

وَاِذَا جَاۤءَهُمْ اَمْرٌ مِّنَ الْاَمْنِ اَوِ الْخَوْفِ اَذَاعُوْا بِهٖ ۗوَلَوْ رَدُّوْهُ اِلَى الرَّسُوْلِ وَاِلٰٓى اُولِى الْاَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِيْنَ يَسْتَنْۢبِطُوْنَهٗ مِنْهُمْ ۗوَلَوْلَا فَضْلُ اللّٰهِ عَلَيْكُمْ وَرَحْمَتُهٗ لَاتَّبَعْتُمُ الشَّيْطٰنَ اِلَّا قَلِيْلًا ٨٣

Artinya : *"Apabila datang kepada mereka suatu berita tentang keamanan (kemenangan) atau ketakutan (kekalahan), mereka menyebarluaskannya. Padahal, seandainya mereka menyerahkannya kepada Rasul dan Ulil Amri (pemegang kekuasaan) di antara mereka, tentulah orang-orang yang ingin mengetahui kebenarannya (akan dapat) mengetahuinya (secara resmi) dari mereka (Rasul dan Ulul Amri). Sekiranya bukan karena karunia dan rahmat Allah kepadamu, tentulah engkau mengikuti setan, kecuali sebagian kecil saja (di antara kamu)."*

Selama ini, kriptografi dibangun atas aljabar klasik dan teori bilangan. Pada tahun 1970-an seorang matematikawan Brazil, Imre Simon memperkenalkan aljabar max-plus. Aljabar max-plus merupakan struktur aljabar $\mathbb{R}_{\max} = (\mathbb{R}_\varepsilon, \oplus, \otimes)$ dimana $\mathbb{R}_\varepsilon = \mathbb{R} \bigcup -\infty$. Operasi $\oplus$ sebagai maksimum dan $\otimes$ sebagai operasi penjumlahan biasa (Schutter, 1996). Aljabar max-plus dapat diterapkan dalam penjadwalan pekerjaan seperti yang dilakukan oleh (Rauf, dkk, 2021), transportasi oleh (Winarni, 2011) dan sistem jaringan (Kurniawan,2020).

Dalam kriptografi dikenal istilah enkripsi dan dekripsi. Alice dan Bob saling bertukar pesan melalui saluran yang tidak aman dan melakukan pertukaran kunci. Alice mengirim pesan kepada Bob, pesan yang dikirim oleh Alice terlebih dahulu diubah ke dalam kode-kode rahasia yang tidak dapat dipahami makna nya. Proses itu disebut dengan enkripsi. Pesan yang telah dienkripsi dikirim kepada Bob, kemudian pesan yang berupa kode-kode rahasia tersebut akan diubah menjadi kalimat yang dapat dipahami makna nya serta dibaca oleh Bob. Proses itu disebut dengan dekripsi (Mehmood,2019).

Salah satu komponen penting dalam kriptografi yaitu kunci. Kunci tersebut digunakan dalam proses enkripsi dan dekripsi. Pihak yang saling berkomunikasi dapat melakukan pembentukan kunci dengan bertemu secara langsung. Akan tetapi, jika tidak memungkinkan bertemu secara langsung diperlukan metode untuk melakukan perjanjian kunci. Metode tersebut dikenal dengan protokol perjanjian kunci. Metode ini dapat membantu

kedua pihak tanpa harus bertemu untuk melakukan perjanjian kunci rahasia yang sama secara aman. Kunci yang telah diperoleh digunakan untuk mengirimkan pesan yang sudah dienkripsi untuk dilanjutkan ke proses dekripsi (Menezes dkk, 1996).

Kunci publik yang pertama kali digunakan adalah Diffie-Hellman. Kunci publik Diffie-Hellman diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976 (Maurer dan Wolf, 2000). Protokol ini memungkinkan dua pihak Alice dan Bob, yang dihubungkan oleh saluran yang dipercaya aman tetapi sebaliknya yaitu menjadi tidak aman. Protokol ini bertujuan untuk menghasilkan kunci rahasia yang sulit untuk diretas oleh pihak ketiga yaitu Eve yang mendengar komunikasi antara Alice dan Bob (Mehmood, 2019).

Enkripsi elgamal ditemukan pada tahun 1985 oleh Taher Gamal. Ide algoritma ini didasarkan pada protokol pertukaran kunci publik yang paling populer, yaitu Diffie-Hellman. Enskripsi elgamal ini membuat sistem kunci publik Diffie-Hellman lebih baik dan menghasilkan algoritma yang dapat digunakan untuk enkripsi (Elgamal, 1985).

Kriptografi pada aljabar max-plus pertama kali diperkenalkan oleh Grigoriev dan Shpilrain.Beberapa penelitian yang mengkaji tentang kriptografi dalam aljabar max-plus diantaranya penelitian yang dilakukan Grigoriev dan Shpilrain (2013). Dalam penelitiannya, aljabar max-plus dapat digunakan untuk beberapa skema kriptografi. Hal itu dilakukan dengan mengadopsi konsep pada aljabar klasik yang sudah dikenal yaitu penjumlahan dan perkalian. Selanjutnya penelitian yang dilakukan oleh Muanalifah (2015) membahas tentang mengkontruksi kunci publik untuk mengenkripsi dokumen berbasis teks arab dengan memanfaatkan operasi matriks pada aljabar max-plus.

Musthofa dan Lestari (2013) melakukan penelitian mengenai metode perjanjian password berdasarkan operasi matriks pada aljabar min-plus untuk keamanan pengiriman informasi rahasia. Hasil dari penelitian tersebut menyimpulkan bahwa operasi matriks pada aljabar min-plus dapat diterapkan untuk menjaga

keamanan informasi rahasia. Penelitian oleh Kotov dan Ushakov (2018) mengenai penyerangan terhadap protokol pertukaran kunci Grigoriev dan Shpilrain yang menggunakan matriks atas aljabar max-plus.

Selanjutnya diikuti oleh beberapa penelitian yang mengkaji tentang kriptanalisis dalam aljabar max-plus diantaranya penelitian oleh Isaac dan Kahrobaei (2020). Dalam penelitiannya menganalisis tentang dua protokol pertukaran kunci yang didasarkan pada matriks dalam aljabar max-plus.Kedua protokol tersebut menggunakan konsep semidirect product dan semigrup. Penelitian lain oleh Chauvet dan Mahe (2017) membahas mengenai kriptografi pensil hessian tropis. Kriptografi ini menggunakan konsep semiring tropis dan mengeksplorasi tropis pensil hessian dari kurva kubik bidang sebagai kriptografi berbasis grup. Hasil dari penelitian ini berupa penjumlahan dan penggandaan rumus yang diinduksi dari metode Jacobian dan menyelesaikan *Discrete Logarithm Problem* ketika dibatasi pada titik integral Kemudian penelitian yang dilakukan oleh Muanalifah dan Isnawati (2022) mengenai versi baru pada kriptografi tropis yaitu enkripsi elgamal.Penelitian tersebut bertujuan untuk memodifikasi enkripsi elgamal pada aljabar klasik dengan menggunakan matriks pada aljabar tropis dan matriks diagonal.

Bahasa Arab merupakan bahasa terbesar dengan akar kebahasaan yang kuat. Dalam kitab *Al- Mufashal fi Tarikh Al-Arab Qabl Al-Islam* disebutkan bahwa jumlah kosa kata Bahasa Arab mencapai 12,3 juta kosa kata.Selain itu, fakta bahwa bahasa Arab merupakan bahasa terbesar ke dua di dunia setelah bahasa Inggris yang dijadikan sebagai bahasa internasional. Berdasarkan pemaparan diatas,peneliti tertarik mengangkat judul "**Modifikasi Enkripsi Elgamal dalam Aljabar Max-Plus Untuk Pengamanan Dokumen Bahasa Arab**".

B. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengontruksi algoritma enkripsi elgamal dalam aljabar max-plus?
2. Bagaimana implementasi algoritma enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab?

C. Tujuan Penelitian

1. Mengetahui cara mengontruksi algoritma enkripsi elgamal dalam aljabar max-plus.
2. Memahami implementasi algoritma enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab.

D. Manfaat Penelitian

Manfaat penelitian ini bagi peneliti adalah memperkaya sumber pengetahuan tentang kriptografi yaitu algoritma enkripsi elgamal yang bisa digunakan untuk menjaga keamanan data khususnya yang bersifat rahasia.

E. Batasan Masalah

Batasan permasalahan dalam penelitian kali ini adalah:

1. Penelitian ini terbatas hanya pada konsep matematis yang melandasi algoritma enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab.
2. Proses perhitungan dalam penelitian ini menggunakan software *Python*.
3. Matriks yang digunakan dalam penelitian ini merupakan matriks yang entri-entrinya berhingga.
4. Huruf hijaiyah yang digunakan dalam penelitian ini yaitu huruf arab pego.

5. Huruf latin yang digunakan hanya melibatkan huruf latin kapital.

F. Metode Penelitian

Metode yang digunakan dalam penyusunan skripsi ini adalah metode studi literatur. Penelitian ini dilakukan dengan cara membahas dan mengkaji lebih dalam mengenai teorema-teorema serta materi dari berbagai sumber. Berikut langkah-langkah yang digunakan dalam penelitian :

1. Melakukan studi literatur mengenai materi aljabar max-plus yang meliputi matriks dan operasi yang berlaku dalam aljabar max-plus. Selanjutnya membahas mengenai kriptografi yang meliputi definisi, sejarah, kunci publik dalam aljabar max-plus serta algoritma el-gamal dalam aljabar klasik maupun aljabar max-plus.

2. Melakukan pengadopsian konsep penjumlahan dan perkalian matriks pada aljabar klasik dan menerapkannya pada aljabar max-plus.

3. Mengkontruksi algoritma enkripsi elgamal pada aljabar max-plus.

4. Mengaplikasikan algoritma enkripsi elgamal dalam aljabar max-plus untuk proses enkripsi dan dekripsi dokumen bahasa Arab.

G. Sistematika Penulisan

Dalam penyusunan skripsi ini, penulis membaginya ke dalam lima bab yang disusun secara runtun dan sistematis. Adapun sistematika penulisannya yaitu sebagai berikut.

1. BAB I Pendahuluan
   Bab ini membahas mengenai latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian serta sistematika penulisan.

2. BAB II Landasan Teori
   Pada bagian ini dijelaskan mengenai materi dasar yang mendukung penelitian. Materi tersebut meliputi aljabar max-plus, matriks dan operasinya dalam aljabar max-plus, definisi dan sejarah kriptografi, kunci publik serta kriptografi dalam aljabar max-plus.

3. BAB III Algoritma Enkripsi Elgamal
   Bab ini menjelaskan mengenai materi algoritma enkripsi elgamal pada aljabar klasik serta aplikasinya pada dokumen bahasa latin dan bahasa Arab.

4. BAB IV Algoritma Enkripsi Elgamal dalam Aljabar Max-Plus
   Bab ini merupakan inti kajian dari penyusunan skripsi yang menjelaskan mengenai modifikasi algoritma enkripsi elgamal pada aljabar max-plus serta aplikasinya pada dokumen bahasa latin dan bahasa Arab.

5. BAB V Penutup
   Bab ini berisi mengenai kesimpulan yang merupakan jawaban secara umum dari rumusan masalah dan saran dari penulis mengenai penelitian yang dilakukan.

BAB II
LANDASAN TEORI

Dalam bab ini akan diberikan definisi dasar dan sifat-sifat aljabar max-plus, matriks dalam aljabar max-plus dan kriptografi dalam aljabar klasik maupun aljabar max-plus.

A. Aljabar Max-Plus

Aljabar max-plus pertama kali diperkenalkan oleh Imre Simon, seorang matematikawan Brazil pada tahun 1970. Selanjutnya diperkenalkan definisi dari aljabar max-plus yang merupakan bagian dari semiring tropis.

Definisi 2.1 *(Aljabar Max-Plus, e.g (Bacelli, 1992))*
Diketahui $\mathbb{R}$ *merupakan suatu himpunan bilangan real. Dinotasikan* $\mathbb{R}_\varepsilon = \mathbb{R} \cup \{-\infty\}$ *untuk setiap* $a, b \in \mathbb{R}_{\max}$ *yang diikuti oleh dua operasi biner yaitu* $\oplus$ *dan* $\otimes$ *yang didefinisikan:*

$$a \oplus b = \max(a, b) \text{ dan } a \otimes b = a + b$$

Struktur aljabar $\mathbb{R}_{\max} = (\mathbb{R}_\varepsilon, \oplus, \otimes)$ dikatakan aljabar max-plus jika $\forall\, a, b, c \in \mathbb{R}_{\max}$ dan $\varepsilon = -\infty$ memenuhi sifat-sifat semiring idempoten sebagai berikut:

1. $(\mathbb{R}_\varepsilon, \oplus)$ memiliki sifat :
   a Komutatif : $a \oplus b = b \oplus a$
   b Asosiatif : $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
   c Terdapat elemen identitas : $\varepsilon \oplus a = a \oplus \varepsilon = a$
   d Idempoten : $a \oplus a = a$
2. $(\mathbb{R}_\varepsilon, \otimes)$ memiliki sifat :
   a Komutatif : $a \otimes b = b \otimes a$
   b Asosiatif : $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

c Terdapat elemen identitas : $0 \otimes a = a \otimes 0 = a$

d Invers : $\forall a \notin \varepsilon$ terdapat $b \in \mathbb{R}_\varepsilon$ sehingga $a \otimes b = 0$

e Elemen netral bersifat penyerap : $a \otimes \varepsilon = \varepsilon \otimes a = \varepsilon$

3. $(\mathbb{R}_\varepsilon, \oplus, \otimes)$ memiliki sifat :

a Distributif kanan : $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

b Distributif kiri : $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Selanjutnya diberikan beberapa contoh operasi aritmetika sederhana dalam aljabar max-plus.

Contoh 2.1
Misalkan diambil $a = 8, b = 10$ *dengan* $a, b, \in \mathbb{R}_{\max}$ *maka :*

$$a \oplus b = 8 \oplus 10 = \max(8, 10) = 10$$
$$a \otimes b = 8 \otimes 10 = 8 + 10 = 18$$

Dalam aljabar max-plus operasi pangkat bilangan dilakukan dengan menerapkan sifat asosiatif. Berikut ini diberikan definisi mengenai pangkat bilangan.

Definisi 2.2 *(Pangkat Bilangan, e.g (Heidergott,2006))*
Misalkan $n \in \mathbb{N}_0$ *dan* $g \in \mathbb{R}_{\max}$ *maka operasi pangkat bilangan didefinisikan dengan*

$$g^{\otimes n} = \underbrace{g \otimes g \otimes g \ldots \otimes g}_{n}$$

Contoh 2.2
Misalkan dipunyai $g = 5$ *dan* $n = 4$ *maka*

$$\begin{aligned} 5^{\otimes 4} &= \underbrace{5 \otimes 5 \otimes \ldots \otimes 5}_{4} \\ &= \underbrace{5 + 5 + \ldots + 5}_{4} \\ &= 4 \times 5 \\ &= 20 \end{aligned}$$

B. Matriks dan Operasinya Dalam Aljabar Max-Plus

Dalam aljabar max-plus himpunan matriks $m \times n$ untuk $m, n \in \mathbb{N}$ pada $\mathbb{R}_{\max}$ dinotasikan dengan $\mathbb{R}_{\max}^{m \times n}$. Dalam matriks, m menunjukan jumlah baris dan n menunjukan jumlah kolom (Farlow K, 2009). Lebih lanjut, matriks $A \in \mathbb{R}_{\max}^{m \times n}$ ditulis sebagai berikut.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{qn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Berikut ini akan dijelaskan mengenai jenis-jenis matriks pada aljabar max-plus yang meliputi matriks identitas dan matriks diagonal.

Definisi 2.3 *(Matriks Identitas, e.g (Bacelli,dkk 1992))*
Matriks identitas $I \in \mathbb{R}_{\max}^{n \times n}$ merupakan matriks yang entri-entri pada diagonal utamanya bernilai 0 dan ε untuk entri-entri selain diagonal utamanya. Dengan kata lain matriks identitas didefinisikan sebagai $I = \begin{cases} 0 & ; i = j \\ \varepsilon & ; i \neq j \end{cases}$

Contoh 2.3

$$I = \begin{bmatrix} 0 & \varepsilon & \varepsilon \\ \varepsilon & 0 & \varepsilon \\ \varepsilon & \varepsilon & 0 \end{bmatrix}$$

Definisi 2.4 *(Invers Matriks, e.g (Bacelli, dkk 1992))*
Misalkan dipunyai $A \in \mathbb{R}_{\max}^{n \times n}$. Matriks A memiliki invers jika $\exists$ matriks B sehingga $A \otimes B = I$. Invers dari matriks A dinotasikan dengan A^{-1}.Dalam hal ini I merupakan matriks identitas.

Pada aljabar max-plus tidak semua matriks memiliki invers. Matriks yang mempunyai invers hanya matriks diagonal dan

matriks permutasi. Oleh karena itu, pada penelitian ini penulis menggunakan matriks diagonal untuk proses enkripsi dan dekripsinya.

Definisi 2.5 *(Matriks Diagonal, e.g (Bacelli,dkk 1992))*
Misalkan dipunyai matriks $D \in \mathbb{R}_{\max}^{n\times n}$ *matriks* D *disebut matriks diagonal jika*

$$D = \begin{cases} k & ; i = j \\ \varepsilon & ; i \neq j \end{cases}$$

Contoh 2.4

$$D = \begin{bmatrix} 5 & \varepsilon & \varepsilon \\ \varepsilon & -2 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{bmatrix}$$

Matriks diagonal $D(k)$ memiliki invers yaitu $D(-k)$ dengan $-k = k^{\otimes -1}$ sehingga $D(k) \otimes D(-k) = I$ (Farlow K,2009).

Contoh 2.5

Misalkan dipunyai matriks $D(k) = \begin{bmatrix} 4 & \varepsilon \\ \varepsilon & 7 \end{bmatrix}$

Maka $D(-k)$ *dengan* $-k = k^{\otimes -1} = \begin{bmatrix} -4 & \varepsilon \\ \varepsilon & -7 \end{bmatrix}$ *Dengan demikian diperoleh* $D^{\otimes -1} = \begin{bmatrix} -4 & \varepsilon \\ \varepsilon & -7 \end{bmatrix}$

Selain jenis-jenis matriks, terdapat operasi matriks yang berlaku dalam aljabar max-plus. Operasi $\otimes$ dan $\oplus$ dalam aljabar max-plus dapat diperluas untuk operasi matriks atas aljabar max-plus. Matriks dalam aljabar max-plus yang berukuran $m \times n$ dinotasikan dengan $\mathbb{R}_{\max}^{m\times n}$. Untuk $m, n \in \mathbb{N}$, didefinisikan $\bar{n} = \{1, 2, .., n\}, \bar{m} = \{1, 2, .., m\}$ dan $m, n \neq 0$. Elemen dari matriks $A \in \mathbb{R}_{\max}^{m\times n}$ dalam baris i dan kolom j dinotasikan dengan a_{ij}, untuk $i \in \bar{m}$ dan $j \in \bar{n}$, atau elemen a_{ij} dapat ditulis sebagai $[A]_{ij}$ dengan $i \in \bar{m}$ dan $j \in \bar{n}$ (Farlow K,2009).

Definisi 2.6 *(Penjumlahan Matriks,e.g (Heidergott,dkk 2006)) Misalkan dipunyai matriks* $A, B \in \mathbb{R}_{\max}^{m\times n} m, n \in \mathbb{N}$ *maka operasi* $\oplus$ *matriksnya adalah*

$$(A \oplus B)_{ij} = [a_{ij} \oplus b_{ij}] = [\max(a_{ij}, b_{ij})]$$

untuk $i \in \bar{m}$ *dan* $j \in \bar{n}$*.*

Contoh 2.6
Misalkan dipunyai matriks $A, B \in \mathbb{R}_{\max}^{m\times n} m, n \in \mathbb{N}$ *dengan* $A = \begin{bmatrix} 1 & 2 \\ 5 & -1 \end{bmatrix}$ *dan matriks* $B = \begin{bmatrix} 0 & 3 \\ 2 & 8 \end{bmatrix}$ *maka*

$$\begin{aligned} A \oplus B &= \begin{bmatrix} 1 & 2 \\ 5 & -1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 3 \\ 2 & 8 \end{bmatrix} \\ &= \begin{bmatrix} 1 \oplus 0 & 2 \oplus 3 \\ 5 \oplus 2 & -1 \oplus 8 \end{bmatrix} \\ &= \begin{bmatrix} \max(1,0) & \max(2,3) \\ \max(5,2) & \max(-1,8) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 3 \\ 5 & 8 \end{bmatrix}. \end{aligned}$$

dan

$$\begin{aligned} B \oplus A &= \begin{bmatrix} 0 & 3 \\ 2 & 8 \end{bmatrix} \oplus \begin{bmatrix} 1 & 2 \\ 5 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 0 \oplus 1 & 3 \oplus 2 \\ 2 \oplus 5 & 8 \oplus -1 \end{bmatrix} \\ &= \begin{bmatrix} \max(0,1) & \max(3,2) \\ \max(2,5) & \max(8,-1) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 3 \\ 5 & 8 \end{bmatrix}. \end{aligned}$$

Jadi diperoleh $A \oplus B = B \oplus A = \begin{bmatrix} 1 & 3 \\ 5 & 8 \end{bmatrix}$.

Definisi 2.7 *(Perkalian Matriks, e.g (Heidergott,dkk 2006))*
Misalkan dipunyai matriks $A \in \mathbb{R}_{\max}^{m\times l}$ *dan* $B \in \mathbb{R}_{\max}^{l\times n}$ *maka* $A \otimes B$ *didefinsikan*

$$\begin{aligned} A \otimes B &= [A \otimes B]_{i,j} \\ &= \bigoplus_{k=1}^{l} (a_{i,k} \otimes b_{k,j}) \\ &= \max_{k=1}^{l} (a_{i,k} + b_{k,j}) \end{aligned}$$

untuk $i \in \bar{m}$ *dan* $j \in \bar{n}$.

Contoh 2.7
Misalkan dipunyai matriks $A \in \mathbb{R}_{\max}^{m\times l}$ *dengan* $A = \begin{bmatrix} 9 & 1 \\ 2 & 0 \end{bmatrix}$ *dan matriks* $B \in \mathbb{R}_{\max}^{l\times n}$ *dengan* $B = \begin{bmatrix} 1 & -1 \\ 2 & 5 \end{bmatrix}$ *maka*

$$\begin{aligned} A \otimes B &= \begin{bmatrix} 9 & 1 \\ 2 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & -1 \\ 2 & 5 \end{bmatrix} \\ &= \begin{bmatrix} (9 \otimes 1) \oplus (1 \otimes 2) & (9 \otimes -1) \oplus (1 \otimes 5) \\ (2 \otimes 1) \oplus (0 \otimes 2) & (2 \otimes -1) \oplus (0 \otimes 5) \end{bmatrix} \\ &= \begin{bmatrix} (9+1) \oplus (1+2) & (9-1) \oplus (1+5) \\ (2+1) \oplus (0+2) & (2-1) \oplus (0+5) \end{bmatrix} \\ &= \begin{bmatrix} 10 \oplus 3 & 8 \oplus 6 \\ 3 \oplus 2 & 1 \oplus 5 \end{bmatrix} \\ &= \begin{bmatrix} \max(10,3) & \max(8,6) \\ \max(3,2) & \max(1,5) \end{bmatrix} \\ &= \begin{bmatrix} 10 & 8 \\ 3 & 5 \end{bmatrix}. \end{aligned}$$

dan

$$\begin{aligned} B \otimes A &= \begin{bmatrix} 1 & -1 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 9 & 1 \\ 2 & 0 \end{bmatrix} \\ &= \begin{bmatrix} (1 \otimes 9) \oplus (-1 \otimes 2) & (1 \otimes 1) \oplus (-1 \otimes 0) \\ (2 \otimes 9) \oplus (5 \otimes 2) & (2 \otimes 1) \oplus (5 \otimes 0) \end{bmatrix} \\ &= \begin{bmatrix} (1+9) \oplus (-1+2) & (1+1) \oplus (-1+0) \\ (2+9) \oplus (5+2) & (2+1) \oplus (5+0) \end{bmatrix} \\ &= \begin{bmatrix} 10 \oplus 1 & 2 \oplus -1 \\ 11 \oplus 7 & 3 \oplus 5 \end{bmatrix} \\ &= \begin{bmatrix} \max(10,1) & \max(2,-1) \\ \max(11,7) & \max(3,5) \end{bmatrix} \\ &= \begin{bmatrix} 10 & 2 \\ 11 & 5 \end{bmatrix}. \end{aligned}$$

Dengan demikian diperoleh bahwa $A \otimes B \neq B \otimes A$

Definisi 2.8 *(Perpangkatan Matriks, e.g (Heidergott,dkk,2006)) Misalkan dipunyai matriks* $A \in \mathbb{R}_{\max}^{n \times n}$*, operasi perpangkatan matriks dapat dihitung dengan*

$$A^{\otimes n} = \underbrace{A \otimes A \otimes A \ldots \otimes A}_{n}$$

Contoh 2.8

Diberikan matriks $A \in \mathbb{R}_{\max}^{m \times n} m, n \in \mathbb{N}$ *dengan* $A = \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix}$

maka

$$
\begin{aligned}
A^{\otimes 3} &= \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix}^{\otimes 2} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} (3 \otimes 3) \oplus (2 \otimes 5) & (3 \otimes 2) \oplus (2 \otimes 0) \\ (5 \otimes 3) \oplus (0 \otimes 5) & (5 \otimes 2) \oplus (0 \otimes 0) \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} (3+3) \oplus (2+5) & (3+2) \oplus (2+0) \\ (5+3) \oplus (0+5) & (5+2) \oplus (0+0) \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix}. \\
&= \begin{bmatrix} 6 \oplus 7 & 5 \oplus 2 \\ 8 \oplus 5 & 7 \oplus 0 \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} \max(6,7) & \max(5,0) \\ \max(8,5) & \max(7,0) \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 7 & 5 \\ 8 & 7 \end{bmatrix} \otimes \begin{bmatrix} 3 & 2 \\ 5 & 0 \end{bmatrix} \\
&= \begin{bmatrix} (7 \otimes 3) \oplus (5 \otimes 5) & (7 \otimes 2) \oplus (5 \otimes 0) \\ (8 \otimes 3) \oplus (7 \otimes 5) & (8 \otimes 2) \oplus (7 \otimes 0) \end{bmatrix} \\
&= \begin{bmatrix} (7+3) \oplus (5+5) & (7+2) \oplus (5+0) \\ (8+3) \oplus (7+5) & (8+2) \oplus (7+0) \end{bmatrix} \\
&= \begin{bmatrix} 10 \oplus 10 & 9 \oplus 5 \\ 11 \oplus 12 & 10 \oplus 7 \end{bmatrix} \\
&= \begin{bmatrix} \max(10,10) & \max(9,5) \\ \max(11,12) & \max(10,7) \end{bmatrix} \\
&= \begin{bmatrix} 10 & 9 \\ 12 & 10 \end{bmatrix}
\end{aligned}
$$

Definisi 2.9 *(Perkalian Matriks Terhadap Skalar, e.g (Heidergott,dkk,2006))*
Misalkan dipunyai matriks $A \in \mathbb{R}_{max}^{m \times n}$ $m, n \in \mathbb{N}$ *dan* $k \in \mathbb{R}_{\max}$ *maka*

perkalian terhadap skalarnya didefinisikan oleh

$$\begin{aligned} k \otimes A &= (k \otimes A)_{i,j} \\ &= [k \otimes a_{i,j}] \\ &= [k + a_{i,j}] \end{aligned}$$

Contoh 2.9

Misalkan dipunyai skalar k *= 6 dan matriks* $A = \begin{bmatrix} 3 & -8 \\ 2 & 7 \end{bmatrix}$ *maka*

$$\begin{aligned} k \otimes A &= 6 \otimes \begin{bmatrix} 3 & -8 \\ 2 & 7 \end{bmatrix} \\ &= \begin{bmatrix} 6 \otimes 3 & 6 \otimes 8 \\ 6 \otimes 2 & 6 \otimes 7 \end{bmatrix} \\ &= \begin{bmatrix} 6+3 & 6-8 \\ 6+2 & 6+7 \end{bmatrix} \\ &= \begin{bmatrix} 9 & -2 \\ 8 & 13 \end{bmatrix}. \end{aligned}$$

dan

$$\begin{aligned} A \otimes k &= \begin{bmatrix} 3 & -8 \\ 2 & 7 \end{bmatrix} \otimes 6 \\ &= \begin{bmatrix} 3 & 6 \otimes 8 \\ 6 \otimes 2 & 6 \otimes 7 \end{bmatrix} \otimes 6 \\ &= \begin{bmatrix} 3+6 & -8+6 \\ 2+6 & 7+6 \end{bmatrix} \\ &= \begin{bmatrix} 9 & -2 \\ 8 & 13 \end{bmatrix}. \end{aligned}$$

Dengan demikian diperoleh $k \otimes A = A \otimes k$.

C. Kriptografi

Pada sub bab ini akan dibahas mengenai definisi, sejarah, algoritma serta kunci publik dalam kriptografi.

1. Definisi Kriptografi

Kriptografi diartikan sebagai ilmu yang mendalami terkait metode untuk menjamin keamanan data yang dikirim dengan tidak ada hambatan dari pengguna lainnya. Kriptografi terdiri dari dua bagian penting yakni proses enkripsi dan deskripsi. Selain algoritma yang digunakan, kunci juga berperan penting dalam proses enkripsi dan dekripsi sehingga kerahasiannya sangatlah penting. Apabila kerahasiannya terbongkar, maka isi pesan tersebut dapat diketahui (Myasnikov, dkk, 2000).

2. Sejarah Kriptografi

Kriptografi memiliki segudang sejarah yang menakjubkan. Dalam buku yang berjudul *The Codebreakers* karya David Khan menyebutkan bahwa istilah kriptografi muncul pertama kali pada zaman Mesir Kuno yaitu sekitar 4000 tahun yang lalu. Kriptografi saat itu digunakan sebagai alat untuk melindungi rahasia dan strategi nasional.

Sebagian besar sejarah kriptografi merupakan kriptografi klasik. Terdapat dua algoritma kriptografi klasik yaitu, algoritma substitusi *(subtitution chiper)* dan algoritma transposisi *(transposition chiper)*. Pada tahun 400 SM algoritma transposisi digunakan oleh tentara Sparta di Yunani. Sedangkan *Caesar Chiper* merupakan algoritma substitusi yang pertama digunakan oleh Julius Caesar, seorang raja Yunani kuno.

Pada tahun 1976 Diffie dan Hellman mempublikasikan karya nya yang berjudul *" New Direction in Crypthography "*. Dalam karya nya, mereka memperkenalkan konsep kriptografi kunci publik serta memberikan metode baru untuk melakukan pertukaran kunci. Selanjutnya, pada tahun 1978 Rivest, Shamir dan

Adleman menemukan algoritma enkripsi yang kemudian dikenal dengan algoritma RSA. Rancangan algoritma ini mengacu pada faktorisasi bilangan yang sulit. Oleh karena itu, diperlukan usaha agar memperoleh metode yang lebih efisien untuk pemfaktoran. Algoritma enkripsi lain berhasil ditemukan oleh Taher Elgamal pada tahun 1984. Algoritma ini lebih dikenal dengan nama algoritma elgamal. *Digital Signature Standard* merupakan sebuah mekanisme yang berdasarkan pada algoritma elgamal (Menezes, dkk 1996).

3. Kunci Publik

Berdasarkan sifat kuncinya kriptografi dibagi menjadi dua yaitu kriptografi kunci simetris *(Symmetric Key Cryptography)* dan kriptografi kunci asimetris *(Asymmetric Key Cryptography)*. Kriptografi kunci simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsinya. Contoh kunci publik yang menggunakan jenis ini yaitu DES *(Data Encryption Standard)* dan AES *(Advanced Encryption Standard)*. Kriptografi kunci asimetris menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsinya. Contoh kunci publik yang menggunakan jenis ini yaitu, diffie-hellman (Mehmood,2019).
Diffie-Hellman merupakan protokol pertukaran kunci yang pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Protokol pertukaran kunci Diffie-Hellman bekerja pada grup $\mathbb{Z}_p$ dengan p bilangan prima. Pihak ketiga yaitu Eve yang ingin mengetahui pesan Alice dan Bob harus memecahkan masalah logaritma diskrit untuk mendapatkan kunci rahasia (Paar dan Pelzl, 1998).

Berikut diberikan skema protokol pertukaran kunci Diffie-Hellman (Wolf,S dan Ueli, M 2000).

Tabel 2.1. Skema Protokol Pertukaran Kunci-Diffie Hellman

Alice dan Bob sepakat terhadap grup $\mathbb{Z}_p$ dengan p bilangan prima dan kunci publik g. Informasi ini bersifat umum.	
Alice	Bob
1. Alice memilih bilangan bulat $k \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $u = g^k \mod p$	1. Bob memilih bilangan bulat $l \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $v = g^l \mod p$
2. Alice mengirimkan u kepada Bob	2. Bob mengirimkan v kepada Alice
3. Alice menerima v dari Bob	3. Bob menerima u dari Alice
4. Alice menghitung $k_A = v^k \mod p$	4. Bob menghitung $k_B = u^l \mod p$
Dengan demikian $k_A = k_B$	

Selanjutnya untuk memastikan kedua pihak yang saling bertukar pesan yaitu Alice dan Bob mendapatkan kunci privat yang sama diberikan teorema sebagai berikut.

Teorema 2.1 *(Teorema Kesamaan Kunci Privat)*
Diberikan $k_A = v^k \mod p$ *dan* $k_B = u^l \mod p$ *dengan* k, l *bilangan bulat rahasia dan* $u = g^k \mod p$, $v = g^l \mod p$ *dimana* $g \in \mathbb{Z}_p$ *maka* $k_A = k_B$

Bukti 1
Dipunyai $k_A = v^k \mod p$...(1).
Akan ditunjukkan bahwa $k_A = k_B$
Kita tahu bahwa $v = g^l \mod p$...(2)
maka dengan mensubstitusikan persamaan (2) ke persamaan (1) diperoleh

$$\begin{aligned} k_A &= v^k \mod p \\ &= (g^l)^k \mod p \end{aligned}$$

Dengan menerapkan sifat eksponen maka diperoleh

$$k_A = (g^k)^l \mod p$$

fakta bahwa $u = g^k \mod p$ *menyebabkan*

$$\begin{aligned} k_A &= (g^k)^l \mod p \\ &= u^l \mod p \\ &= k_B \end{aligned}$$

Jadi terbukti bahwa $k_A = k_B$

Berikut ini diberikan contoh pertukaran kunci Diffie-Hellman.

Contoh 2.10
Misalkan Alice dan Bob sepakat dengan kunci publik $g = 7$ *dan* $p = 13$ *,* p *bilangan prima dengan* $g \in \mathbb{Z}_{13}$*. Alice dan Bob melakukan pertukaran kunci sebagai berikut.*

1. *Alice memilih* $k = 9$ *secara acak dan rahasia lalu menghitung*

$$\begin{aligned} u &= g^k \mod p \\ &= 7^9 \mod 13 \\ &= 40353607 \mod 13 \\ &= 8 \end{aligned}$$

Bob memilih $l = 7$ *secara acak dan rahasia lalu menghitung*

$$\begin{aligned} v &= g^l \mod p \\ &= 7^7 \mod 13 \\ &= 823543 \mod 13 \\ &= 6 \end{aligned}$$

2. *Alice mengirim* $u = 8$ *kepada Bob dan Bob mengirim* $v = 6$ *kepada Alice.*

3. *Alice menerima* $v = 6$ *dari Bob dan Bob menerima* $u = 8$ *dari Alice.*

4. *Alice menghitung kunci privat*

$$\begin{aligned} k_A &= v^k \mod p \\ &= 6^9 \mod 13 \\ &= 10077696 \mod 13 \\ &= 5 \end{aligned}$$

dan Bob menghitung kunci privat

$$\begin{aligned} k_B &= u^l \mod p \\ &= 8^7 \mod 13 \\ &= 2097152 \mod 13 \\ &= 5 \end{aligned}$$

Dengan demikian diperoleh $k_A = k_B = 5$

Seiring dengan berjalannya waktu, peneliti di bidang kriptografi melakukan modifikasi protokol pertukaran kunci Diffie-Hellman dengan menggunakan grup matriks. Di bawah ini diberikan contoh pertukaran kunci Diffie-Hellman menggunakan grup matriks.

Contoh 2.11
Misalkan Alice dan Bob sepakat dengan grup matriks dan bilangan prima $p = 11$. *Misalkan* $G = \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix}$ *dengan* $G \in \mathbb{M}_{3\times 3}(\mathbb{Z}_{11})$.
Alice dan Bob melakukan pertukaran kunci sebagai berikut.

1. *Alice memilih $k = 4$ secara acak dan rahasia lalu menghitung*

$$
\begin{aligned}
U &= G^k \mod p \\
&= \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix}^4 \mod 11 \\
&= \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \mod 11 \\
&= \begin{bmatrix} 105 & 122 & 70 \\ 45 & 88 & 43 \\ 46 & 74 & 53 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \mod 11 \\
&= \begin{bmatrix} 1399 & 1922 & 1100 \\ 710 & 1142 & 663 \\ 721 & 1144 & 607 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \mod 11 \\
&= \begin{bmatrix} 19735 & 28726 & 16306 \\ 10663 & 16416 & 9213 \\ 10598 & 16046 & 9211 \end{bmatrix} \mod 11 \\
&= \begin{bmatrix} 1 & 5 & 4 \\ 4 & 4 & 6 \\ 5 & 8 & 4 \end{bmatrix}
\end{aligned}
$$

Bob memilih $l = 2$ secara acak dan rahasia lalu menghitung

$$
\begin{aligned}
V &= G^l \mod p \\
&= \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix}^2 \mod 11 \\
&= \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 6 & 4 \\ 2 & 6 & 5 \\ 3 & 8 & 1 \end{bmatrix} \mod 11
\end{aligned}
$$

$$= \begin{bmatrix} 105 & 122 & 70 \\ 45 & 88 & 43 \\ 46 & 74 & 53 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix}$$

2. *Alice mengirimkan* $U = \begin{bmatrix} 1 & 5 & 4 \\ 4 & 4 & 6 \\ 5 & 8 & 4 \end{bmatrix}$ *kepada Bob. Kemudian Bob mengirimkan* $V = \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix}$ *kepada Alice.*

3. *Alice menerima* V *dari Bob dan Bob menerima* U *dari Alice.*

4. *Alice menghitung*

$$K_A = V^k \mod p$$
$$= \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix}^4 \mod 11$$
$$= \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix}^3 \times \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 45 & 38 & 70 \\ 26 & 81 & 94 \\ 38 & 74 & 169 \end{bmatrix} \times \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix} \times \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 448 & 605 & 1190 \\ 425 & 778 & 1760 \\ 640 & 1390 & 2413 \end{bmatrix} \times \begin{bmatrix} 6 & 1 & 4 \\ 1 & 0 & 10 \\ 2 & 8 & 9 \end{bmatrix} \mod 11$$

$$= \begin{bmatrix} 5673 & 9968 & 18552 \\ 6848 & 14505 & 25320 \\ 10056 & 19944 & 38177 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 8 & 0 & 2 \\ 7 & 8 & 0 \\ 2 & 4 & 4 \end{bmatrix}.$$

Bob menghitung

$$K_B = U^l \mod p$$
$$= \begin{bmatrix} 1 & 5 & 4 \\ 4 & 4 & 6 \\ 5 & 8 & 4 \end{bmatrix}^2 \mod 11$$
$$= \begin{bmatrix} 1 & 5 & 4 \\ 4 & 4 & 6 \\ 5 & 8 & 4 \end{bmatrix} \times \begin{bmatrix} 1 & 5 & 4 \\ 4 & 4 & 6 \\ 5 & 8 & 4 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 41 & 57 & 50 \\ 50 & 84 & 64 \\ 57 & 89 & 84 \end{bmatrix} \mod 11$$
$$= \begin{bmatrix} 8 & 0 & 2 \\ 7 & 8 & 0 \\ 2 & 4 & 4 \end{bmatrix}.$$

Sehingga diperoleh kunci yang sama yaitu $K_A = K_B = \begin{bmatrix} 8 & 0 & 2 \\ 7 & 8 & 0 \\ 2 & 4 & 4 \end{bmatrix}$.

Protokol pertukaran kunci Diffie-Hellman dibuat dengan menggunakan struktur aljabar komutatif. Pihak ketiga yang ingin mencuri data harus memecahkan masalah logaritma diskrit untuk mendapatkan kunci rahasia. Protokol ini cukup kuat saat itu. Namun dengan adanya ancaman komputer kuantum di masa depan membuat protokol ini mudah untuk dipecahkan. Oleh karena itu, para peneliti mengembangkan protokol pertukaran kunci menggunakan struktur aljabar non-komutatif. Dengan

menggunakan struktur aljabar non-komutatif diharapkan tingkat keamanannya lebih tinggi dan pihak ketiga sulit untuk memecahkannya. Pada tahun 2005 Stickel memperkenalkan konsep pertukaran kunci dengan menggunakan struktur aljabar non-komutatif. Skema protokol pertukaran kunci ini didasarkan pada grup non-komutatif yang selanjutnya dapat diperumum menjadi semigrup non-komutatif. Berikut ini diberikan skema protokol pertukaran kunci Stickel(Menezes, Oorschot, dan Vanstone,1996).

Tabel 2.2. Skema Protokol Pertukaran Kunci Stickel

Alice dan Bob sepakat terhadap semigrup non-komutatif G dan mempublikasikan $a, b \in G$ dengan $ab \neq ba$. Informasi ini bersifat umum.	
Alice	Bob
1. Alice memilih bilangan bulat $m, n \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $u = a^n b^m$	1. Bob memilih bilangan bulat $r, s \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $v = a^r b^s$
2. Alice mengirimkan u kepada Bob	2. Bob mengirimkan v kepada Alice
3. Alice menerima v dari Bob	3. Bob menerima u dari Alice
4. Alice menghitung $k_A = a^n v b^m$	4. Bob menghitung $k_B = a^r u b^s$
Dengan demikian Alice dan Bob menyepakati kunci yang sama yaitu $k_A = k_B$	

Berdasarkan protokol pertukaran kunci Stickel tersebut, diperoleh sebuah teorema baru yang menjamin kedua pihak yang sedang bertukar pesan yaitu Alice dan Bob memperoleh kunci privat yang sama.

Berikut ini diberikan teorema kesamaan kunci privat

Teorema 2.2 *(Teorema Kesamaan Kunci Privat)*
Diberikan $k_A = a^n v b^m$ *dan* $k_B = a^r u b^s$ *dengan* m, n, r, s *bilangan bulat dan* $u = a^n b^m$, $v = a^r b^s$ *dimana* $a, b \in G$ *maka* $k_A = k_B$

Bukti 2
Dipunyai $k_A = a^n v b^m ...(1)$
dan $v = a^r b^s ...(2)$
Akan ditunjukkan $k_A = k_B$
Dengan melakukan substitusi persamaan (2) ke persamaan (1) maka diperoleh

$$\begin{aligned} k_A &= a^n v b^m \\ &= a^n a^r b^s b^m \end{aligned}$$

Menggunakan sifat eksponen diperoleh

$$\begin{aligned} k_A &= a^n a^r b^s b^m \\ &= a^{n+r} b^{s+m} \end{aligned}$$

Selanjutnya, pada eksponen berlaku sifat komutatif sehingga menyebabkan

$$\begin{aligned} k_A &= a^{r+n} b^{m+s} \\ &= a^r a^n b^m b^s \end{aligned}$$

Mengingat fakta bahwa $u = a^n b^m$ *maka*

$$\begin{aligned} k_A &= a^r a^n b^m b^s \\ &= a^r u b^s \\ &= k_B \end{aligned}$$

Jadi terbukti bahwa $k_A = k_B$

Berikut ini diberikan contoh protokol pertukaran kunci Stickel.

Contoh 2.12
Misalkan Alice dan Bob sepakat dengan grup matriks . Diketahui $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ *dan* $B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ *dengan* $A, B \in \mathbb{M}_{2\times 2}(\mathbb{Z})$.

1. *Alice memilih secara acak dan rahasia* $m = 1, n = 3$ *lalu menghitung*

$$\begin{aligned} U &= A^n B^m \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}^3 \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 43 & 21 \\ 42 & 22 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 43 & 149 \\ 42 & 150 \end{bmatrix}. \end{aligned}$$

Bob memilih secara acak dan rahasia $r = 2, s = 1$ *lalu menghitung*

$$\begin{aligned} V &= A^r B^s \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}^2 \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix}. \end{aligned}$$

2. *Alice mengirimkan* $U = \begin{bmatrix} 43 & 149 \\ 42 & 150 \end{bmatrix}$ *kepada Bob. Dan Bob mengirimkan* $V = \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix}$ *kepada Alice.*

3. *Alice menerima* V *dari Bob dan Bob menerima* U *dari Alice.*

4. *Alice menghitung*

$$\begin{aligned} K_A &= A^n V B^m \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}^3 \times \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 43 & 21 \\ 42 & 22 \end{bmatrix} \times \begin{bmatrix} 11 & 37 \\ 10 & 38 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 683 & 2389 \\ 682 & 2390 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 683 & 8533 \\ 682 & 8534 \end{bmatrix}. \end{aligned}$$

Bob menghitung

$$\begin{aligned} K_B &= A^r U B^s \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}^2 \times \begin{bmatrix} 43 & 149 \\ 42 & 150 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \times \begin{bmatrix} 43 & 149 \\ 42 & 150 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \end{aligned}$$

$$
\begin{aligned}
&= \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \times \begin{bmatrix} 43 & 149 \\ 42 & 150 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\
&= \begin{bmatrix} 683 & 2389 \\ 682 & 2390 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \\
&= \begin{bmatrix} 683 & 8533 \\ 682 & 8534 \end{bmatrix}.
\end{aligned}
$$

Dengan demikian diperoleh $K_A = K_B$ *yaitu* $\begin{bmatrix} 683 & 8533 \\ 682 & 8534 \end{bmatrix}$.

D. Kriptografi dalam Aljabar Max-Plus

Efektivitas dan keamanan dari setiap sistem kriptografi ditentukan oleh algoritma dan protokol yang digunakan. Kriptografi merupakan bidang kajian yang terus mengalami perkembangan dari waktu ke waktu. Dima Grigoriev dan Vladimir Sphilrain menemukan sebuah protokol baru dengan menggunakan platform semiring idempoten yang kemudian dikenal dengan kriptografi dalam aljabar max-plus. Seperti yang kita ketahui bahwa, pada aljabar max-plus operasi perkalian $\otimes$ didefinisikan sebagai operasi penjumlahan biasa. Hal itu menyebabkan perhitungan dalam aljabar max-plus lebih cepat dibandingkan dengan aljabar klasik. Pada aljabar max-plus protokol pertukaran kunci Diffie-Hellman menggunakan semigrup komutatif atas aljabar max-plus. Berikut ini diberikan skema protokol pertukaran kunci Diffie-Hellman.

Tabel 2.3. Skema Protokol Pertukaran Kunci Diffie- Hellman

Alice dan Bob sepakat terhadap semigrup $g \in \mathbb{R}_{\max}$	
Alice	Bob
1. Alice memilih bilangan bulat $k \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $u = g^{\otimes k}$	1. Bob memilih bilangan bulat $l \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $v = g^{\otimes l}$
2. Alice mengirimkan u kepada Bob	2. Bob mengirimkan v kepada Alice
3. Alice menerima v dari Bob	3. Bob menerima u dari Alice
4. Alice menghitung $k_A = v^{\otimes k}$	4. Bob menghitung $k_B = u^{\otimes l}$
Dengan demikian Alice dan Bob menyepakati kunci yang sama yaitu $k_A = k_B$	

Dengan adanya protokol pertukaran kunci Diffie-Hellman dalam aljabar max-plus diperoleh teorema yang menjamin kedua pihak yang saling berkomunikasi memperoleh kunci privat yang sama. Diberikan teorema sebagai berikut.

Teorema 2.3 *(Teorema Kesamaan Kunci Privat)*
Diberikan $k_A = v^{\otimes k}$ *dan* $k_B = u^{\otimes l}$ *dengan* k, l *bilangan bulat dan* $u = g^{\otimes k}, v = g^{\otimes l}$ *dimana* $g \in \mathbb{R}_{\max}$ *maka* $k_A = k_B$

Bukti 3 *Dipunyai* $k_A = v^{\otimes k} ...(1)$.
Akan ditunjukkan bahwa $k_A = k_B$.
Kita tahu bahwa $v = g^{\otimes l}$*...(2)*
maka dengan menerapkan sifat komutatif perpangkatan pada aljabar max-plus diperoleh

$$\begin{aligned} k_A &= v^{\otimes k} \\ &= (g^{\otimes l})^{\otimes k} \end{aligned}$$

Dengan menerapkan sifat komutatif perpangkatan pada aljabar

max-plus diperoleh

$$\begin{aligned} k_A &= (g^{\otimes l})^{\otimes k} \\ &= (g^{\otimes k})^{\otimes l} \end{aligned}$$

Fakta bahwa $u = g^{\otimes k}$
maka

$$\begin{aligned} &= (g^{\otimes k})^{\otimes l} \\ &= u^{\otimes l} \\ &= k_B \end{aligned}$$

Jadi terbukti $k_A = k_B$.

Berikut ini diberikan contoh protokol pertukaran kunci Diffie-Hellman dalam aljabar max-plus.

Contoh 2.13
Misalkan Alice dan Bob sepakat $g = 12$ *Alice dan Bob melakukan pertukaran kunci sebagai berikut.*

1. *Alice memilih* $k = 5$ *secara rahasia dan menghitung*

$$\begin{aligned} u &= g^{\otimes k} \\ &= 12^{\otimes 5} \\ &= \underbrace{12 \otimes 12 \otimes \ldots \otimes 12}_{5} \\ &= \underbrace{12 + 12 + \ldots + 12}_{5} \\ &= 5 \times 12 \\ &= 60 \end{aligned}$$

dan Bob memilih $l = 4$ *secara rahasia serta menghitung*

$$\begin{aligned} v &= g^{\otimes l} \\ &= 12^{\otimes 4} \\ &= \underbrace{12 \otimes 12 \otimes \ldots \otimes 12}_{4} \\ &= \underbrace{12 + 12 + \ldots + 12}_{4} \\ &= 4 \times 12 \\ &= 48 \end{aligned}$$

2. *Alice mengirimkan* $u = 60$ *kepada Bob dan Bob mengirimkan* $v = 48$ *kepada Alice.*

3. *Alice menerima* v *dari Bob dan Bob menerima* u *dari Alice.*

4. *Alice menghitung*

$$\begin{aligned} k_A &= v^{\otimes k} \\ &= 48^{\otimes 5} \\ &= \underbrace{48 \otimes 48 \otimes \ldots \otimes 48}_{5} \\ &= \underbrace{48 + 48 + \ldots + 48}_{5} \\ &= 5 \times 48 \\ &= 240 \end{aligned}$$

dan Bob menghitung

$$\begin{aligned} k_B &= u^{\otimes l} \\ &= 60^{\otimes 4} \end{aligned}$$

$$
\begin{aligned}
&= \underbrace{60 \otimes 60 \otimes \ldots \otimes 60}_{4} \\
&= \underbrace{60 + 60 + \ldots + 60}_{4} \\
&= 4 \times 60 \\
&= 240
\end{aligned}
$$

Jadi diperoleh $k_A = k_B = 240$

Protokol pertukaran kunci Stickel dalam aljabar max-plus merupakan pengembangan protokol pertukaran kunci Stickel pada aljabar klasik. Gagasan ini muncul sebagai upaya untuk meningkatkan efisiensi perhitungan yang lebih cepat.Protokol pertukaran kunci Stickel dalam aljabar max-plus menggunakan semigrup non-komutatif atas aljabar max-plus. Berikut ini diberikan protokol pertukaran kunci Stickel dalam aljabar max-plus.

Tabel 2.4. Skema Protokol Pertukaran Kunci Stickel dalam Aljabar Max-Plus

Alice dan Bob sepakat terhadap semigrup non-komutatif $\mathbb{G}_{n\times n}(\mathbb{Z}_{\max})$ dan kunci publik $a, b \in \mathbb{G}_{n\times n}(\mathbb{Z}_{\max})$ dengan $a \otimes b \neq b \otimes a$. Informasi ini bersifat umum.	
Alice	Bob
1. Alice memilih $m, n \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $u = a^{\otimes n} \otimes b^{\otimes m}$	1. Bob memilih $r, s \in \mathbb{N}$ secara acak dan rahasia lalu menghitung $v = a^{\otimes r} \otimes b^{\otimes s}$
2. Alice mengirimkan u kepada Bob	2. Bob mengirimkan v kepada Alice
3. Alice menerima v dari Bob	3. Bob menerima u dari Alice
4. Alice menghitung $k_A = a^{\otimes n} \otimes v \otimes b^{\otimes m}$	4. Bob menghitung $k_B = a^{\otimes r} \otimes u \otimes b^{\otimes s}$
Dengan demikian Alice dan Bob menyepakati kunci yang sama yaitu $k_A = k_B$	

Contoh 2.14

Misalkan Alice dan Bob sepakat dengan $A = \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix}$ *dan* $B = \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}$ $A, B \in \mathbb{G}_{2\times 2}(\mathbb{Z}_{\max})$ *dengan* $A \otimes B \neq B \otimes A$

1. *Alice memilih secara acak dan rahasia* $m = 2, n = 1$ *lalu menghitung*

$$\begin{aligned} U &= A^{\otimes n} \otimes B^{\otimes m} \\ &= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}^{\otimes 2} \end{aligned}$$

$$
\begin{aligned}
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 5 & 8 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix}.
\end{aligned}
$$

Bob memilih secara acak dan rahasia $r = 3, s = 2$ *lalu menghitung*

$$
\begin{aligned}
V &= A^{\otimes r} \otimes B^{\otimes s} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix}^{\otimes 3} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}^{\otimes 2} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 5 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 6 & 7 \\ 5 & 6 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 9 & 12 \\ 8 & 11 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 14 & 17 \\ 13 & 16 \end{bmatrix}.
\end{aligned}
$$

2. *Alice mengirimkan* $U = \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix}$ *kepada Bob, dan Bob mengirimkan* $V = \begin{bmatrix} 14 & 17 \\ 13 & 16 \end{bmatrix}$ *kepada Alice.*

3. *Alice menerima* $V = \begin{bmatrix} 14 & 17 \\ 13 & 16 \end{bmatrix}$ *dari Bob, dan Bob menerima* $U = \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix}$ *dari Alice.*

4. *Alice menghitung*

$$
\begin{aligned}
K_A &= A^{\otimes n} \otimes V \otimes B^{\otimes m} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 14 & 17 \\ 13 & 16 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}^{\otimes 2} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 14 & 17 \\ 13 & 16 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 16 & 19 \\ 15 & 18 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 21 & 24 \\ 20 & 23 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 26 & 29 \\ 25 & 28 \end{bmatrix}.
\end{aligned}
$$

Bob menghitung

$$
\begin{aligned}
K_B &= A^{\otimes r} \otimes U \otimes B^{\otimes s} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix}^{\otimes 3} \otimes \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}^{\otimes 2} \\
&= \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 4 & 5 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 6 & 7 \\ 5 & 6 \end{bmatrix} \otimes \begin{bmatrix} 10 & 13 \\ 7 & 10 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 16 & 19 \\ 15 & 18 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 21 & 24 \\ 20 & 23 \end{bmatrix} \otimes \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 26 & 29 \\ 25 & 28 \end{bmatrix}.
\end{aligned}
$$

Dengan demikian diperoleh $K_A = K_B$ *yaitu* $\begin{bmatrix} 26 & 29 \\ 25 & 28 \end{bmatrix}$.

BAB III
Algoritma Enkripsi Elgamal

Algoritma ini pertama kali diperkenalkan oleh ilmuwan berkebangsaan Mesir yaitu Taher Elgamal pada tahun 1985. Pada umumnya algoritma ini digunakan untuk tanda tangan digital, namun seiring dengan berkembangnya waktu mengalami modifikasi sehingga dapat digunakan untuk enkripsi dan deskripsi. Pada proses pembentukan salah satu kuncinya, algoritma ini menggunakan bilangan prima yang besar dan menitik beratkan kekuatan kuncinya pada masalah logaritma diskrit. Hal ini menyebabkan keamanan kunci pada algoritma elgamal lebih terjamin (Elgamal, T 1985).

Algoritma enkripsi elgamal diawali dengan pembentukan kunci yang dilakukan oleh penerima pesan. Pembentukan kunci melibatkan dua pasangan kunci yaitu kunci privat dan kunci publik. Kunci publik bersifat tidak rahasia sehingga bisa diketahui oleh pihak luar. Sedangkan kunci privat bersifat rahasia yang hanya diketahui oleh dirinya sendiri. Pesan rahasia yang akan dikirim, harus dikonversikan terlebih dahulu dalam bilangan bulat (Myasnikov, dkk,2011). Pada penelitian kali ini penulis menggunakan unicode sebagai standar pengkodean. Unicode adalah suatu standar teknis yang dirancang untuk mengizinkan teks dan simbol dari semua sistem tulisan di dunia untuk ditampilkan dan dimanipulasi secara konsisten oleh komputer. Tabel unicode dapat dilihat pada lampiran I.

Algoritma enkripsi elgamal menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsinya. Hal itu memberikan kemudahan kepada pihak pengirim dan penerima pesan dalam melakukan proses pertukaran kunci karena tidak mengharuskan dua pihak untuk bertemu secara langsung.Algoritma enkripsi elgamal memiliki tiga tahapan penting yaitu pembentukan kunci, enkripsi dan dekripsi. Berikut ini akan dijelaskan tahapan algoritma enkripsi elgamal klasik.

Algoritma 1 *Algoritma Enkripsi Elgamal*
Alice dan Bob sepakat terhadap grup siklik $G =< g >$ *modulo* p *dengan* p *adalah bilangan prima dan* $g \in \mathbb{Z}_p$. *Informasi ini disampaikan secara umum dan tidak rahasia.*

1. *Pembentukan Kunci*
   Pembentukan kunci dilakukan oleh penerima pesan yaitu Alice. Alice membangkitkan kunci privat dan kunci publik sebagai berikut.

   (a) *Alice memilih secara acak dan rahasia suatu bilangan bulat* k *yang memenuhi syarat* $1 < k < p - 1$.
   (b) *Alice menghitung kunci publik* $u = g^k \mod p$
   (c) *Alice mengirim kunci publik* u *dan tetap menyimpan kunci privat* k.

2. *Enkripsi*
   Proses enkripsi dilakukan oleh pengirim pesan yaitu Bob. Langkah-langkah yang dilakukan dalam proses enkripsi yaitu sebagai berikut.

   (a) *Bob memilih secara acak dan rahasia suatu bilangan bulat* l, *dengan syarat* $1 < l < p - 1$
   (b) *Bob menghitung kunci publik* $v = g^l \mod p$
   (c) *Bob menghitung* $k_B = u^l = g^{kl} \mod p$
   (d) *Bob mengirim pesan* m. *Kemudian pesan tersebut diterjemahkan ke dalam unicode yang ada pada lampiran 1.*
   (e) *Bob mengenkripsi pesan menggunakan fungsi enkripsi* $e(m) = m \times k_B \mod p$.
   Proses enkripsi ini menghasilkan $e(m) = c$ *yaitu chipertext atau pesan yang tidak dapat dipahami maknanya.*
   (f) *Bob mengirim* c, v *kepada Alice.*

3. *Dekripsi*
   Proses dekripsi dilakukan oleh penerima pesan yaitu Alice. Dalam mendekripsikan pesan m yang berupa (c, v) Alice melakukan hal-hal sebagai berikut.

   (a) *Alice menghitung* $k_A = v^k \mod p$

   (b) *Alice menghitung invers modulo* k_A

   (c) *Alice mendekripsikan pesan menggunakan fungsi dekripsi* $d(c)$ *dengan menghitung :*
   $d(c) = c \times k_A^{-1} \mod p$

   Sehingga diperoleh chipertext yang dideskripsi oleh Alice sama dengan pesan yang dikirim oleh Bob.

Contoh 3.1
Misalkan Alice dan Bob sepakat terhadap $p = 89$ *dengan* p *adalah bilangan prima dan* $g = 5$*. Alice dan Bob saling bertukar pesan dengan langkah-langkah sebagai berikut.*

1. *Pembangkitan Kunci*

   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 4$

   (b) *Alice menghitung kunci publik* u

$$\begin{aligned} u &= g^k \mod p \\ &= 5^4 \mod 89 \\ &= 625 \mod 89 \\ &= 2 \end{aligned}$$

   (c) *Alice mengirim kunci publik* $u = 2$ *kepada Bob dan tetap menyimpan kunci privat* $k = 4$*.*

2. *Proses Enkripsi*

   (a) *Bob memilih bilangan bulat secara acak dan rahasia* $l = 6$

(b) Bob menghitung kunci privat v

$$\begin{aligned} v &= g^l \mod p \\ &= 5^6 \mod 89 \\ &= 15.625 \mod 89 \\ &= 50 \end{aligned}$$

(c) Bob menghitung

$$\begin{aligned} k_B &= u^l \mod p \\ &= 2^6 \mod 89 \\ &= 64 \mod 89 \\ &= 64 \end{aligned}$$

(d) Bob mengirimkan pesan m *= "AWAS"*
Kata tersebut diterjemahkan terlebih dahulu ke dalam unicode sehingga menjadi $m_1 = 65, m_2 = 87, m_3 = 65$ *dan* $m_4 = 83$

(e) Bob mengenkripsi pesan menggunakan fungsi enkripsi

$$\begin{aligned} e(m_1) &= m_1 \times k_B \mod p \\ c_1 &= 65 \times 64 \mod 89 \\ &= 4160 \mod 89 \\ &= 66. \\ e(m_2) &= m_2 \times k_B \mod p \\ c_2 &= 87 \times 64 \mod 89 \\ &= 5568 \mod 89 \\ &= 50. \\ e(m_3) &= m_3 \times k_B \mod p \\ c_3 &= 65 \times 64 \mod 89 \\ &= 4160 \mod 89 \\ &= 66. \end{aligned}$$

$$\begin{aligned} e(m_4) &= m_4 \times k_B \mod p \\ c_4 &= 83 \times 64 \mod 89 \\ &= 5312 \mod 89 \\ &= 61. \end{aligned}$$

Dengan demikian dihasilkan $c_1 = 66, c_2 = 50, c_3 = 66, c_4 = 61$

(f) Bob mengirim c, v *kepada Alice.*

3. Proses Dekripsi

(a) Alice menghitung

$$\begin{aligned} k_A &= v^k \mod p \\ &= 50^4 \mod 89 \\ &= 6250000 \mod 89 \\ &= 64 \end{aligned}$$

(b) Alice menghitung invers 64 $\mod 89$ *yaitu 32. Maka* $k_A^{-1} = 32$

(c) Alice mendekripsi pesan

$$\begin{aligned} d(c_1) &= c_1 \times k_A^{-1} \mod p \\ &= 66 \times 32 \mod 89 \\ &= 2112 \mod 89 \\ &= 65 \\ d(c_2) &= c_2 \times k_A^{-1} \mod p \\ &= 50 \times 32 \mod 89 \\ &= 1600 \mod 89 \\ &= 87 \\ d(c_3) &= c_3 \times k_A^{-1} \mod p \\ &= 66 \times 32 \mod 89 \\ &= 2112 \mod 89 \\ &= 65 \end{aligned}$$

$$\begin{aligned} d(c_4) &= c_4 \times k_A^{-1} \mod p \\ &= 61 \times 32 \mod 89 \\ &= 1952 \mod 89 \\ &= 83 \end{aligned}$$

Diperoleh $m_1 = d(c_1) = 65, m_2 = d(c_2) = 87, m_3 = d(c_3) = 65, m_4 = d(c_4) = 83$ *atau jika terjemahkan ke dalam kode numerik menjadi kata 'AWAS' sama dengan pesan yang dikirim oleh Bob.*

Pada proses pengiriman pesan bahasa Arab huruf hijaiyah diterjemahkan ke dalam kode numerik sesuai dengan yang ada dalam tabel huruf hijaiyah pada lampiran II. Berikut diberikan contoh untuk pengiriman pesan bahasa Arab.

Contoh 3.2
Misalkan Alice dan Bob sepakat terhadap $p = 107$ *dengan* p *bilangan prima dan* $g = 7$*. Alice dan Bob saling bertukar pesan dengan langkah-langkah sebagai berikut.*

1. *Pembangkitan Kunci*
   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 4$
   (b) *Alice menghitung kunci publik* u

$$\begin{aligned} u &= g^k \mod p \\ &= 7^4 \mod 107 \\ &= 2401 \mod 107 \\ &= 47 \end{aligned}$$

   (c) *Alice mengirimkan kunci publik* u *kepada Bob dan tetap menyimpan* $k = 4$*.*
2. *Proses Enkripsi*
   (a) *Bob memilih bilangan bulat secara acak dan rahasia* $l = 5$

(b) Bob menghitung kunci publik v

$$\begin{aligned} v &= g^l \mod p \\ &= 7^5 \mod 107 \\ &= 16807 \mod 107 \\ &= 8. \end{aligned}$$

(c) Bob menghitung

$$\begin{aligned} k_B &= u^l \mod p \\ &= 47^5 \mod 107 \\ &= 229345007 \mod 107 \\ &= 30 \end{aligned}$$

(d) Bob mengirimkan pesan

مساء

Huruf hijaiyah diubah ke dalam kode numerik sehingga menjadi
$m_1 = 88, m_2 = 76, m_3 = 65, m_4 = 100.$

(e) Bob melakukan proses enkripsi dengan menggunakan rumus

$$\begin{aligned} e(m) &= m \times k_B \mod p \\ e(m_1) &= m_1 \times k_B \mod p \\ c_1 &= 88 \times 30 \mod 107 \\ &= 2640 \mod 107 \\ &= 72 \end{aligned}$$

$$
\begin{aligned}
e(m_2) &= m_2 \times k_B \mod p \\
c_2 &= 76 \times 30 \mod 107 \\
&= 2280 \mod 107 \\
&= 33 \\
e(m_3) &= m_3 \times k_B \mod p \\
c_3 &= 65 \times 30 \mod 107 \\
&= 1950 \mod 107 \\
&= 24
\end{aligned}
$$

$$
\begin{aligned}
e(m_4) &= m_4 \times k_B \mod p \\
c_4 &= 100 \times 30 \mod 107 \\
&= 3000 \mod 107 \\
&= 4
\end{aligned}
$$

Bob mengirimkan $c_1, c_2, c_3, c_4, c_5, v$ *kepada Alice.*

3. *Proses Dekripsi*

   (a) *Alice menghitung*

$$
\begin{aligned}
k_A &= v^k \mod p \\
&= 8^4 \mod 107 \\
&= 4096 \mod 107 \\
&= 30
\end{aligned}
$$

   (b) *Alice mencari invers 30* $\mod 107$ *yaitu* 25. *Diperoleh* $k_A^{-1} = 25$

(c) Alice mendeskripsi pesan dengan menggunakan rumus

$$
\begin{aligned}
d(c) &= c \times k_A^{-1} \mod p \\
d(c_1) &= c_1 \times k_A^{-1} \mod p \\
&= 72 \times 25 \mod 107 \\
&= 1800 \mod 107 \\
&= 88 \\
d(c_2) &= c_2 \times k_A^{-1} \mod p \\
&= 33 \times 25 \mod 107 \\
&= 825 \mod 107 \\
&= 76
\end{aligned}
$$

$$
\begin{aligned}
d(c_3)) &= c_3 \times k_A^{-1} \mod p \\
&= 24 \times 25 \mod 107 \\
&= 600 \mod 107 \\
&= 65 \\
d(c_4) &= c_4 \times k_A^{-1} \mod p \\
&= 4 \times 25 \mod 107 \\
&= 100
\end{aligned}
$$

Diperoleh $m = d(c)$ ***yaitu*** $m_1 = d(c_1) = 88, m_2 = d(c_2) = 76, m_3 = d(c_3) = 65, m_4 = d(c_4) = 100$ ***jika diterjemahkan ke dalam kode numerik menjadi kata***

مساء

sama dengan pesan yang dikirim oleh Bob.

BAB IV
Algoritma Enkripsi Elgamal dalam Aljabar Max-Plus

Algoritma enkripsi elgamal pada aljabar max-plus masih trivial dengan algoritma enkripsi elgamal pada aljabar klasik. Perbedaannya hanya pada operasi yang berlaku pada keduanya. Operasi penjumlahan dalam aljabar max-plus yaitu $\oplus$ yang didefinisikan sebagai operasi maksimum. Sementara operasi perkalian yaitu $\otimes$ didefinisikan sebagai operasi penjumlahan biasa. Algoritma enkripsi elgamal pada aljabar max-plus dimodifikasi menjadi dua algoritma yaitu menggunakan semigrup bilangan bulat dan matriks atas aljabar max-plus.
Berikut ini diberikan tahapan algoritma enkripsi elgamal dalam aljabar max-plus .

Algoritma 2 *(Algoritma Enkripsi Elgamal dalam Aljabar Max-Plus)*
Alice dan Bob sepakat terhadap semigrup $g \in \mathbb{G}_{n\times n}(\mathbb{Z}_{\max})$. *Informasi ini disampaikan secara umum dan tidak rahasia.*

1. *Pembentukan Kunci*
   Pembentukan kunci dilakukan oleh penerima pesan yaitu Alice. Alice membangkitkan kunci privat dan kunci publik sebagai berikut.

   (a) *Alice memilih secara acak dan rahasia suatu bilangan bulat* k *yang memenuhi* $k > 1$
   (b) *Alice menghitung kunci publik* $u = g^{\otimes k}$.
   (c) *Alice mengirim kunci publik* u *kepada Bob dan tetap menyimpan* k.

2. *Enkripsi*
   Proses enkripsi dilakukan oleh pengirim pesan yaitu Bob. Langkah-langkah yang dilakukan dalam proses enkripsi yaitu sebagai berikut.

(a) *Bob memilih secara acak dan rahasia suatu bilangan bulat l, dengan syarat $l > 1$*

(b) *Bob menghitung kunci publik $v = g^{\otimes l}$*

(c) *Bob menghitung $k_B = u^{\otimes l} = (g^{\otimes k})^{\otimes l}$*

(d) *Bob mengirim pesan m.Kemudian pesan tersebut diterjemahkan ke dalam unicode yang ada dalam tabel pada lampiran I.*

(e) *Bob mengenkripsi pesan menggunakan fungsi enkripsi $e(m) = m \otimes k_B$.*
Proses enkripsi ini menghasilkan $e(m) = c$ yaitu chipertext atau pesan yang tidak dapat dipahami maknanya.

(f) *Bob mengirim c, v kepada Alice.*

3. *Dekripsi*
Proses dekripsi dilakukan oleh penerima pesan yaitu Alice. Dalam mendekripsikan pesan m yang berupa (c, v) Alice melakukan hal-hal sebagai berikut.

(a) *Alice menghitung $k_A = v^{\otimes k}$*

(b) *Alice mendekripsikan pesan menggunakan fungsi dekripsi $d(c)$ dengan menghitung :*
$d(c) = c \otimes k_A^{-1}$

Sehingga diperoleh chipertext yang didekripsi oleh Alice sama dengan pesan yang dikirim oleh Bob.

Untuk memvalidasi kebenaran algoritma enkripsi elgamal pada aljabar max-plus maka diperoleh teorema sebagai berikut.

Teorema 4.1 *Teorema Kebenaran Algoritma Enkripsi Elgamal*
Jika fungsi enkripsi $e(m) = m \otimes k_B = c$ dimana m adalah pesan dan k_B adalah kunci privat Bob dan fungsi dekripsi $d(c) = c \otimes k_A^{-1}$ maka $m = e(m) \otimes k_A^{-1} = d(c)$

Bukti 4
Dipunyai $e(m) = m \otimes k_B = c...(1)$
dan $d(c) = c \otimes k_A^{-1}...(2)$
Dari Teorema 1 didapatkan $k_A = k_B$ *sehingga*
$d(c) = c \otimes k_B^{-1}...(3)$.
Substitusi persamaan (1) ke persamaan (3) maka

$$d(c) = m \otimes k_B \otimes k_B^{-1}$$

dengan $e = k_B \otimes k_B^{-1}$

$$\begin{aligned} &= m \otimes e \\ &= m \end{aligned}$$

Jadi terbukti $m = c \otimes k_A^{-1} = d(c)$

Selanjutnya diberikan contoh proses pertukaran pesan dengan menggunakan algoritma enkripsi elgamal pada aljabar max-plus.

Contoh 4.1
Misalkan Alice dan Bob sepakat dengan $g = 8$. *Alice dan Bob saling bertukar pesan dengan langkah-langkah sebagai berikut.*

1. *Pembangkitan Kunci*
   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 7$
   (b) *Alice menghitung kunci publik* u

$$\begin{aligned} u &= 8^{\otimes 7} \\ &= \underbrace{8 \otimes 8 \otimes \ldots \otimes 8}_{7} \\ &= \underbrace{8 + 8 + \ldots + 8}_{7} \\ &= 7 \times 8 \\ &= 56 \end{aligned}$$

(c) *Alice mengirimkan u kepada Bob dan tetap menyimpan k.*

2. *Proses Enkripsi*

(a) *Bob memilih bilangan bulat secara acak dan rahasia $l = 5$*

(b) *Bob menghitung kunci publik v*

$$\begin{aligned} v &= 8^{\otimes 5} \\ &= \underbrace{8 \otimes 8 \otimes \ldots \otimes 8}_{5} \\ &= \underbrace{8 + 8 + \ldots + 8}_{5} \\ &= 5 \times 8 \\ &= 40 \end{aligned}$$

(c) *Bob menghitung*

$$\begin{aligned} k_B &= 56^{\otimes 5} \\ &= \underbrace{56 \otimes 56 \otimes \ldots \otimes 56}_{5} \\ &= \underbrace{56 + 56 + \ldots + 56}_{5} \\ &= 5 \times 56 \\ &= 280 \end{aligned}$$

(d) *Bob mengirimkan pesan m = "MAKAN"*
Pesan tersebut diterjemahkan terlebih dahulu ke dalam unicode sehingga menjadi $m_1 = 77, m_2 = 65, m_3 = 75, m_4 = 65$ dan $m_5 = 78$.

(e) *Bob mengenkripsi pesan*

$$
\begin{aligned}
e(m_1) &= m_1 \otimes k_B \\
c_1 &= 77 \otimes 280 \\
&= 357 \\
e(m_2) &= m_2 \otimes k_B \\
c_2 &= 65 \otimes 280 \\
&= 345
\end{aligned}
$$

$$
\begin{aligned}
e(m_3) &= m_3 \otimes k_B \\
c_3 &= 75 \otimes 280 \\
&= 355 \\
e(m_4) &= m_4 \otimes k_B \\
c_4 &= 65 \otimes 280 \\
&= 345 \\
e(m_5) &= m_5 \otimes k_B \\
c_5 &= 78 \otimes 280 \\
&= 358
\end{aligned}
$$

(f) Bob mengirim c_1, c_2, c_3, c_4 dan v kepada Alice.

3. Proses Dekripsi

(a) Alice menghitung

$$
\begin{aligned}
k_A &= u^{\otimes k} \\
&= 40^{\otimes 7} \\
&= \underbrace{40 \otimes 40 \otimes \ldots \otimes 40}_{7} \\
&= \underbrace{40 + 40 + \ldots + 40}_{7} \\
&= 7 \times 40 \\
&= 280
\end{aligned}
$$

(b) Mencari invers dari k_A yaitu $k_A^{-1} = -280$

(c) Alice mendekripsi pesan

$$\begin{aligned} d(c_1) &= c_1 \otimes k_A^{-1} \\ &= 357 \otimes -280 \\ &= 77 \end{aligned}$$

$$\begin{aligned} d(c_2) &= c_2 \otimes k_A^{-1} \\ &= 345 \otimes -280 \\ &= 65 \end{aligned}$$

$$\begin{aligned} d(c_3) &= c_3 \otimes k_A^{-1} \\ &= 355 \otimes -280 \\ &= 75 \end{aligned}$$

$$\begin{aligned} d(c_4) &= c_4 \otimes k_A^{-1} \\ &= 345 \otimes -280 \\ &= 65 \end{aligned}$$

$$\begin{aligned} d(c_5) &= c_5 \otimes k_A^{-1} \\ &= 358 \otimes -280 \\ &= 78 \end{aligned}$$

Diperoleh $m_1 = d(c_1) = 77, m_2 = d(c_2) = 65, m_3 = d(c_3) = 75, m_4 = d(c_4) = 65, m_5 = d(c_5) = 78$ ***jika diterjemahkan ke dalam unicode menjadi kata 'MAKAN' sama dengan pesan yang dikirim oleh Bob.***

Pada aljabar max-plus tidak semua matriks memiliki invers. Terdapat dua jenis matriks yang memiliki invers dalam aljabar max-plus yaitu matriks diagonal dan matriks permutasi. Pada penelitian kali ini menggunakan matriks diagonal untuk proses enkripsi dan deskripsinya. Entri-entri non diagonal pada matriks A dihapuskan dan digantikan dengan ε. Dengan demikian, terbentuk

$$A = \begin{cases} a_{ij} & ; i = j \\ \varepsilon & ; i \neq j \end{cases}$$

Contoh 4.2
Misalkan Alice dan Bob sepakat terhadap semigrup $\mathbb{G}_{2\times 2}(\mathbb{Z}_{\max})$ *dan* $G = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in \mathbb{G}_{2\times 2}(\mathbb{Z}_{max})$*.Alice dan Bob saling bertukar pesan dengan langkah-langkah sebagai berikut.*

1. *Pembangkitan Kunci*
   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 3$
   (b) *Alice menghitung kunci publik* U

$$\begin{aligned} U &= G^{\otimes 3} \\ &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^{\otimes 3} \\ &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix} \end{aligned}$$

   (c) *Alice mengirimkan* U *kepada Bob dan tetap menyimpan* k*.*

2. *Proses Enkripsi*
   (a) *Bob memilih bilangan bulat secara acak dan rahasia* $l = 2$

(b) Bob menghitung kunci publik V

$$\begin{aligned} V &= G^{\otimes l} \\ &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^{\otimes 2} \\ &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \end{aligned}$$

(c) Bob menghitung

$$\begin{aligned} K_B &= U^{\otimes l} \\ &= \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix}^{\otimes 2} \\ &= \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix} \otimes \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix} \\ &= \begin{bmatrix} 21 & 22 \\ 23 & 34 \end{bmatrix} \end{aligned}$$

(d) Entri-entri non diagonal pada matriks K_B *dihapuskan dan menggantinya dengan* ε*. Dengan demikian diperoleh*
$K_B = \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix}$

(e) Bob mengirimkan pesan m *= "AKU SUKA MATEMATIKA." Kalimat tersebut dibagi menjadi beberapa matriks berordo* 2×2 *dengan* M_1, M_2, M_3, M_4 *dan* M_5 *sebagai berikut*
$M_1 = \begin{pmatrix} A & K \\ U & spasi \end{pmatrix}$
$M_2 = \begin{pmatrix} S & U \\ K & A \end{pmatrix}$
$M_3 = \begin{pmatrix} spasi & M \\ A & T \end{pmatrix}$

$$M_4 = \begin{pmatrix} E & M \\ A & T \end{pmatrix}$$
$$M_5 = \begin{pmatrix} I & K \\ A & . \end{pmatrix}$$

(f) Kemudian pesan tersebut diterjemahkan ke dalam unicode menghasilkan

$$M_1 = \begin{bmatrix} 65 & 75 \\ 85 & 32 \end{bmatrix}$$
$$M_2 = \begin{bmatrix} 83 & 85 \\ 75 & 65 \end{bmatrix}$$
$$M_3 = \begin{bmatrix} 32 & 77 \\ 65 & 84 \end{bmatrix}$$
$$M_4 = \begin{bmatrix} 69 & 77 \\ 65 & 84 \end{bmatrix}$$
$$M_5 = \begin{bmatrix} 73 & 75 \\ 65 & 46 \end{bmatrix}$$

(g) Bob melakukan proses enkripsi

$$\begin{aligned} e(M_1) &= M_1 \otimes K_B \\ &= \begin{bmatrix} 65 & 75 \\ 85 & 32 \end{bmatrix} \otimes \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix} = \begin{bmatrix} 86 & 99 \\ 106 & 56 \end{bmatrix} = C_1 \\ e(M_2) &= M_2 \times K_B \\ &= \begin{bmatrix} 83 & 85 \\ 75 & 65 \end{bmatrix} \otimes \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix} = \begin{bmatrix} 104 & 109 \\ 96 & 89 \end{bmatrix} = C_2 \\ e(M_3) &= M_3 \times K_B \\ &= \begin{bmatrix} 32 & 77 \\ 65 & 84 \end{bmatrix} \otimes \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix} = \begin{bmatrix} 53 & 101 \\ 86 & 108 \end{bmatrix} = C_3 \end{aligned}$$

$$
\begin{aligned}
e(M_4) &= M_4 \times K_B \\
&= \begin{bmatrix} 69 & 77 \\ 65 & 84 \end{bmatrix} \otimes \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix} = \begin{bmatrix} 90 & 101 \\ 86 & 108 \end{bmatrix} = C_4 \\
e(M_5) &= M_5 \otimes K_B \\
&= \begin{bmatrix} 73 & 75 \\ 65 & 46 \end{bmatrix} \otimes \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix} = \begin{bmatrix} 94 & 99 \\ 86 & 70 \end{bmatrix} = C_5
\end{aligned}
$$

Bob mengirim V, C_1, C_2, C_3, C_4 dan C_5 kepada Alice.

3. *Proses Dekripsi*

   (a) *Alice menghitung*

$$
\begin{aligned}
K_A &= V^{\otimes k} \\
&= \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}^{\otimes 3} \\
&= \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \\
&= \begin{bmatrix} 13 & 14 \\ 15 & 16 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \\
&= \begin{bmatrix} 21 & 22 \\ 23 & 24 \end{bmatrix}
\end{aligned}
$$

   (b) *Entri-entri non diagonal matriks K_A dihapuskan dan menggantinya dengan ε. Dengan demikian diperoleh* $K_A = \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix}$

   (c) *Mencari invers dari matriks diagonal*
   $K_A = \begin{bmatrix} 21 & \varepsilon \\ \varepsilon & 24 \end{bmatrix}$ *maka* $K_A^{-1} = \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix}$

(d) Alice mendekripsi pesan

$$
\begin{aligned}
d(C_1) &= C_1 \otimes K_A^{-1} \\
&= \begin{bmatrix} 86 & 99 \\ 106 & 56 \end{bmatrix} \otimes \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix} = \begin{bmatrix} 65 & 75 \\ 85 & 32 \end{bmatrix} \\
d(C_2) &= C_2 \otimes K_A^{-1} \\
&= \begin{bmatrix} 104 & 109 \\ 96 & 89 \end{bmatrix} \otimes \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix} = \begin{bmatrix} 83 & 85 \\ 75 & 65 \end{bmatrix} \\
d(C_3) &= C_3 \otimes K_A^{-1} \\
&= \begin{bmatrix} 53 & 101 \\ 86 & 108 \end{bmatrix} \otimes \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix} = \begin{bmatrix} 32 & 77 \\ 65 & 84 \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
d(C_4) &= C_4 \otimes K_A^{-1} \\
&= \begin{bmatrix} 90 & 101 \\ 86 & 108 \end{bmatrix} \otimes \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix} = \begin{bmatrix} 69 & 77 \\ 65 & 84 \end{bmatrix} \\
d(C_5) &= C_5 \otimes K_A^{-1} \\
&= \begin{bmatrix} 94 & 99 \\ 86 & 70 \end{bmatrix} \otimes \begin{bmatrix} -21 & \varepsilon \\ \varepsilon & -24 \end{bmatrix} = \begin{bmatrix} 73 & 75 \\ 65 & 46 \end{bmatrix}
\end{aligned}
$$

Diperoleh chipertext yang didekripsi adalah

$$
\begin{aligned}
d(C_1) = M_1 &= \begin{bmatrix} 65 & 75 \\ 85 & 32 \end{bmatrix} \\
d(C_2) = M_2 &= \begin{bmatrix} 83 & 85 \\ 75 & 65 \end{bmatrix} \\
d(C_3) = M_3 &= \begin{bmatrix} 32 & 77 \\ 65 & 84 \end{bmatrix} \\
d(C_4) = M_4 &= \begin{bmatrix} 69 & 77 \\ 65 & 84 \end{bmatrix} \\
d(C_5) = M_5 &= \begin{bmatrix} 73 & 75 \\ 65 & 46 \end{bmatrix}
\end{aligned}
$$

Jika diterjemahkan ke dalam unicode menjadi kalimat "AKU SUKA MATEMATIKA."sama dengan pesan yang dikirim oleh Bob.

Modifikasi enkripsi elgamal dalam aljabar max-plus bisa

digunakan untuk pengamanan dokumen bahasa Arab. Hal itu dilakukan dengan cara huruf hijaiyah diterjemahkan ke dalam kode numerik sesuai dengan yang ada dalam tabel huruf hijaiyah pada lampiran II. Berikut ini diberikan contoh untuk pengiriman pesan bahasa Arab menggunakan enkripsi elgamal dalam aljabar max-plus.

Contoh 4.3
Alice dan Bob sepakat terhadap semigrup bilangan bulat $g = 6$. Alice dan Bob bertukar pesan dengan langkah-langkah sebagai berikut.

1. *Pembangkitan Kunci*

   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 4$

   (b) *Alice menghitung kunci publik* u

$$\begin{aligned} u &= 6^{\otimes 4} \\ &= \underbrace{6 \otimes 6 \otimes \ldots \otimes 6}_{4} \\ &= \underbrace{6 + 6 + \ldots + 6}_{4} \\ &= 4 \times 6 \\ &= 24 \end{aligned}$$

   (c) *Alice mengirimkan* u *kepada Bob dan tetap menyimpan* k.

2. *Proses Enkripsi*

   (a) *Bob memilih bilangan bulat secara acak dan rahasia* $l = 8$

(b) Bob menghitung kunci publik v

$$\begin{aligned} v &= 6^{\otimes 8} \\ &= \underbrace{6 \otimes 6 \otimes \ldots \otimes 6}_{8} \\ &= \underbrace{6 + 6 + \ldots + 6}_{8} \\ &= 8 \times 6 \\ &= 48 \end{aligned}$$

(c) Bob menghitung

$$\begin{aligned} k_B &= 24^{\otimes 8} \\ &= \underbrace{24 \otimes 24 \otimes \ldots \otimes 24}_{8} \\ &= \underbrace{24 + 24 + \ldots + 24}_{8} \\ &= 8 \times 24 \\ &= 192 \end{aligned}$$

(d) Bob mengirimkan pesan m *=*

صباح الخير

Pesan tersebut diterjemahkan terlebih dahulu ke dalam kode numerik yang ada pada lampiran II sehingga menjadi $m_1 = 78, m_2 = 66, m_3 = 65, m_4 = 70, m_5 = 65, m_6 = 87, m_7 = 71, m_8 = 101$ *dan* $m_9 = 74$.

(e) Bob mengenkripsi pesan

$$\begin{aligned} e(m_1) &= m_1 \otimes k_B \\ c_1 &= 78 \otimes 192 \\ &= 270 \end{aligned}$$

$$
\begin{aligned}
e(m_2) &= m_2 \otimes k_B \\
c_2 &= 66 \otimes 192 \\
&= 258 \\
e(m_3) &= m_3 \otimes k_B \\
c_3 &= 65 \otimes 192 \\
&= 257
\end{aligned}
$$

$$
\begin{aligned}
e(m_4) &= m_4 \otimes k_B \\
c_4 &= 70 \otimes 192 \\
&= 262 \\
e(m_5) &= m_5 \otimes k_B \\
c_5 &= 65 \otimes 192 \\
&= 257 \\
e(m_6) &= m_6 \otimes k_B \\
c_6 &= 87 \otimes 192 \\
&= 279 \\
e(m_7) &= m_7 \otimes k_B \\
c_7 &= 71 \otimes 192 \\
&= 263 \\
e(m_8) &= m_8 \otimes k_B \\
c_8 &= 101 \otimes 192 \\
&= 293 \\
e(m_9) &= m_9 \otimes k_B \\
c_9 &= 74 \otimes 192 \\
&= 266
\end{aligned}
$$

(f) Bob mengirim $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9$ *dan* v *kepada Alice.*

3. Proses Dekripsi

(a) Alice menghitung

$$\begin{aligned} k_A &= v^{\otimes k} \\ &= 48^{\otimes 4} \\ &= \underbrace{48 \otimes 48 \otimes \ldots \otimes 48}_{4} \\ &= \underbrace{48 + 48 + \ldots + 48}_{4} \\ &= 4 \times 48 \\ &= 192 \end{aligned}$$

(b) Mencari invers dari k_A yaitu $k_A^{-1} = -192$

(c) Alice mendekripsi pesan

$$\begin{aligned} d(c_1) &= c_1 \otimes k_A^{-1} \\ &= 270 \otimes -192 \\ &= 78 \\ d(c_2) &= c_2 \otimes k_A^{-1} \\ &= 258 \otimes -192 \\ &= 66 \\ d(c_3) &= c_3 \otimes k_A^{-1} \\ &= 257 \otimes -192 \\ &= 65 \\ d(c_4) &= c_4 \otimes k_A^{-1} \\ &= 262 \otimes -192 \\ &= 70 \\ d(c_5) &= c_5 \otimes k_A^{-1} \\ &= 257 \otimes -192 \\ &= 65 \end{aligned}$$

$$
\begin{aligned}
d(c_6) &= c_6 \otimes k_A^{-1} \\
&= 279 \otimes -192 \\
&87 \\
d(c_7) &= c_7 \otimes k_A^{-1} \\
&= 263 \otimes -192 \\
&= 71 \\
d(c_8) &= c_8 \otimes k_A^{-1} \\
&= 293 \otimes -192 \\
&= 101 \\
d(c_9) &= c_9 \otimes k_A^{-1} \\
&= 266 \otimes -192 \\
&= 74
\end{aligned}
$$

Diperoleh $m_1 = d(c_1) = 78, m_2 = d(c_2) = 66, m_3 = d(c_3) = 65, m_4 = d(c_4) = 70, m_5 = d(c_5) = 65, m_6 = d(c_6) = 87, m_7 = d(c_7) = 71, m_8 = d(c_8) = 101, m_9 = d(c_9) = 74$ *jika diterjemahkan ke dalam kode yang ada pada lampiran II menjadi* صباح الخير *sama dengan pesan yang dikirim oleh Bob.*

Contoh 4.4

Misalkan Alice dan Bob menyepakati semigrup $\mathbb{G}_{2\times 2}(\mathbb{Z}_{\max})$ *dan* $G = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \in \mathbb{G}_{2\times 2}(\mathbb{Z}_{\max})$ *. Alice dan Bob saling bertukar pesan dengan langkah-langkah sebagai berikut.*

1. *Pembangkitan Kunci*

   (a) *Alice memilih bilangan bulat secara acak dan rahasia* $k = 2$

(b) *Alice menghitung kunci publik* U

$$\begin{aligned} U &= G^{\otimes 2} \\ &= \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}^{\otimes 2} \\ &= \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \otimes \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 6 & 4 \\ 8 & 6 \end{bmatrix} \end{aligned}$$

(c) *Alice mengirimkan* U *kepada Bob dan tetap menyimpan* k.

2. *Proses Enkripsi*

(a) *Bob memilih bilangan bulat secara acak dan rahasia* $l = 3$

(b) *Bob menghitung kunci publik* V

$$\begin{aligned} V &= G^{\otimes l} \\ &= \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}^{\otimes 3} \\ &= \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \otimes \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \otimes \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 6 & 4 \\ 8 & 6 \end{bmatrix} \otimes \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 9 & 7 \\ 11 & 9 \end{bmatrix}. \end{aligned}$$

(c) *Entri-entri non diagonal pada matriks* K_B *dihapuskan dan menggantinya dengan* ε. *Dengan demikian diperoleh* $K_B = \begin{bmatrix} 18 & \varepsilon \\ \varepsilon & 18 \end{bmatrix}$

(d) *Bob mengirim pesan*

بارك الله فيكم

Pesan tersebut diterjemahkan ke dalam kode numerik dan dibagi menjadi beberapa matriks berordo 2×2 *sehingga diperoleh*

$$M_1 = \begin{bmatrix} 66 & 65 \\ 74 & 86 \end{bmatrix}$$
$$M_2 = \begin{bmatrix} 65 & 87 \\ 87 & 99 \end{bmatrix}$$
$$M_3 = \begin{bmatrix} 85 & 101 \\ 86 & 88 \end{bmatrix}$$

(e) *Bob melakukan proses enkripsi*

$$\begin{aligned} e(M_1) &= M_1 \otimes K_B \\ &= \begin{bmatrix} 66 & 65 \\ 74 & 86 \end{bmatrix} \otimes \begin{bmatrix} 18 & \varepsilon \\ \varepsilon & 18 \end{bmatrix} = \begin{bmatrix} 84 & 83 \\ 92 & 104 \end{bmatrix} = C_1 \\ e(M_2) &= M_2 \otimes K_B \\ &= \begin{bmatrix} 66 & 65 \\ 74 & 86 \end{bmatrix} \otimes \begin{bmatrix} 18 & \varepsilon \\ \varepsilon & 18 \end{bmatrix} = \begin{bmatrix} 83 & 105 \\ 105 & 117 \end{bmatrix} = C_2 \end{aligned}$$

$$\begin{aligned} e(M_3) &= M_3 \otimes K_B \\ &= \begin{bmatrix} 85 & 101 \\ 86 & 88 \end{bmatrix} \otimes \begin{bmatrix} 18 & \varepsilon \\ \varepsilon & 18 \end{bmatrix} = \begin{bmatrix} 103 & 119 \\ 104 & 106 \end{bmatrix} = C_3 \end{aligned}$$

Bob mengirim V, C_1, C_2, C_3 *dan* V *kepada Alice.*

3. *Proses Dekripsi*

(a) Alice menghitung

$$\begin{aligned} K_A &= V^{\otimes k} \\ &= \begin{bmatrix} 9 & 7 \\ 11 & 9 \end{bmatrix}^{\otimes 2} \\ &= \begin{bmatrix} 9 & 7 \\ 11 & 9 \end{bmatrix} \otimes \begin{bmatrix} 9 & 7 \\ 11 & 9 \end{bmatrix} \\ &= \begin{bmatrix} 18 & 16 \\ 20 & 18 \end{bmatrix}. \end{aligned}$$

(b) Entri-entri non diagonal pada matriks K_A dihapuskan dan menggantinya dengan ε. Dengan demikian diperoleh

$K_A = \begin{bmatrix} 18 & \varepsilon \\ \varepsilon & 18 \end{bmatrix}$

(c) Mencari invers dari matriks diagonal

$K_A = \begin{bmatrix} 18 & 16 \\ 20 & 18 \end{bmatrix}$ *maka* $K_A^{-1} = \begin{bmatrix} -18 & \varepsilon \\ \varepsilon & -18 \end{bmatrix}$

(d) Alice mendekripsi pesan

$$\begin{aligned} d(C_1) &= C_1 \otimes K_A^{-1} \\ &= \begin{bmatrix} 84 & 83 \\ 92 & 104 \end{bmatrix} \otimes \begin{bmatrix} -18 & \varepsilon \\ \varepsilon & -18 \end{bmatrix} = \begin{bmatrix} 66 & 65 \\ 74 & 86 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} d(C_2) &= C_2 \otimes K_A^{-1} \\ &= \begin{bmatrix} 83 & 105 \\ 105 & 117 \end{bmatrix} \otimes \begin{bmatrix} -18 & \varepsilon \\ \varepsilon & -18 \end{bmatrix} = \begin{bmatrix} 65 & 87 \\ 87 & 99 \end{bmatrix} \\ d(C_3) &= C_3 \otimes K_A^{-1} \\ &= \begin{bmatrix} 103 & 119 \\ 104 & 106 \end{bmatrix} \otimes \begin{bmatrix} -18 & \varepsilon \\ \varepsilon & -18 \end{bmatrix} = \begin{bmatrix} 85 & 101 \\ 86 & 88 \end{bmatrix} \end{aligned}$$

Diperoleh chipertext yang didekripsi adalah

$d(C_1) = M_1 = \begin{bmatrix} 66 & 65 \\ 74 & 86 \end{bmatrix}$

$$d(C_2) = M_2 = \begin{bmatrix} 65 & 87 \\ 87 & 99 \end{bmatrix}$$

$$d(C_3)M_3 = \begin{bmatrix} 85 & 101 \\ 86 & 88 \end{bmatrix}$$

Jika diterjemahkan ke dalam kode huruf hijaiyah yang ada dalam lampiran II menjadi

بارك الله فيكم

sama dengan pesan yang dikirim oleh Bob.

BAB V
PENUTUP

Berdasarkan pembahasan mengenai algoritma enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab, dapat diambil beberapa kesimpulan dan saran sebagai berikut.

A. Kesimpulan

Algoritma enkripsi elgamal dalam aljabar max-plus untuk pengamanan dokumen bahasa Arab dimodifikasi menjadi dua algoritma yaitu dengan menggunakan semigrup bilangan bulat dan matriks atas aljabar max-plus.Huruf hijaiyah di kodekan sesuai dengan yang ada dalam tabel huruf hijaiyah pada lampiran II. Pesan yang dikirim Bob akan dienkripsi terlebih dahulu menghasilkan chipertext yang tidak dapat dipahami maknanya. Setelah dienkripsi chipertext akan dikirimkan oleh Bob kepada Alice. Selanjutnya, chipertext akan didekripsi oleh penerima pesan yaitu Alice dan menghasilkan sebuah pesan yang sama dengan pesan yang dikirim oleh Bob. Dengan demikian, algoritma enkripsi elgamal bisa digunakan untuk pengamanan dokumen bahasa Arab.

B. Saran

Setelah membahas dan mengkontruksi algoritma enkripsi elgamal pada aljabar max-plus untuk pengamanan dokumen bahasa Arab, penulis ingin menyampaikan beberapa saran sebagai berikut.

1. Modifikasi enkripsi elgamal pada aljabar max-plus ini dilakukan dengan alternatif mengubah matriks ke dalam matriks diagonal. Diharapkan penelitian selanjutnya bisa memanfaatkan matriks permutasi untuk memperoleh invers yang akan digunakan dalam proses enkripsi dan dekripsi.
2. Dokumen bahasa Arab yang digunakan harus diubah

dulu ke dalam kode numerik untuk diinputkan ke dalam software phyton. Diharapkan penelitian selanjutnya, dapat menyempurnakan program ini sehingga bisa menginputkan dokumen bahasa Arab tanpa diubah terlebih dahulu ke dalam kode numerik.

3. Pada penelitian kali ini menerapkan algoritma enkripsi elgamal untuk pengamanan dokumen bahasa Arab. Diharapkan penelitian selanjutnya bisa memodifikasi menggunakan bahasa lainnya.

DAFTAR PUSTAKA

A. Myasnikov, V. Shpilrain And A. Ushakov. 2011.*Non-Commutative Cryptography and Complexity of Group-Theoretic Problems, Math* Surveys Monogr. 177, American Mathematical Society, Providence.

Bacelli, F., Cohen, Olsder, & Quadrat. 1992.*Synchronization and Linearity An Algebra For Discrete Event Systems* Paris : INRIA

Chauvet, Marie J dan Eric Mahe . 2016. *Cryptography From The Tropical Hessian Pencil*

Dody A.Rauf, dkk. 2021. *Model Penjadwalan Proyek Pembangunan Perumahan Menggunakan Petri Net dan Aljabar Max-Plus* Jurnal Edukasi dan Sains Matematika vol.7 no.1

ElGamal, T., 1985.*A Public Key Cryptosystem and a Signature Scheme based on discrete logarithms* IEEE transactions on information theory. 31(4)

Farlow, G.Kasie. 2009.*Max-Plus Algebra* Tesis. Virginia : Universitas Negeri dan Institut Politeknik Virginia.

Grigoriev, D and Vladimir Shpilrain. 2013. *Tropical Cryptography*

Grigoriev, D and Vladimir Shpilrain. 2018. *Tropical Cryptography II: Extensions by Homomorphisms*

Heidergott, B., Olsder, G.J & Van Der Woude J.W. 2006. *Max Plus at Work* Amsterdam: Princeton University Press

Isaac, S. and Kahrobei, D., (2020).*A closer look at the tropical cryptography. Communication* in Algebra, pages 137-142

Kotov, M. and Ushakov, A., 2018. *Analysis of a key exchange protocol based on tropical matrix algebra*Journal of Mathematical Cryptology, 12(3), pp.137-141.

Kurniawan, Andro . 2020 . *Sistem Persamaan Linear Max-Plus dan Terapannya pada Sistem Jaringan Kereta Api*. Universitas Gadjah Mada.

Lestari, Dwi dan Musthofa. 2014 .*Metode Perjanjian Password berdasarkan Operasi Matriks atas Aljabar Min-Plus untuk keamanan pengiriman informasi rahasia* Jurnal Sains Dasar Vol.3(1)

Maurer, Ueli dan Stefan Wolf . 2000. *The Diffie-Hellman Protocol* Computer Science Department Swiss Federal Institute of Technology Zurich Switzerland

Mehmood, Sania . 2019 . *Key Exchange Protocol Based on Matrices Using Tropical Algebra*Thesis Master of Philosophy Faculty of Computing Department of Mathematics.

Menezes, A.J., et al. 1996. *Handbook of Applied Cryptography.* Florida: CRC Press

Muanalifah, Any . 2015 .*Constructions Of Key Exchange Protocol over Max-Plus algebra to Encrypt and Decrypt Arabic Documents* Jounal of Natural Sciences and Mathematics Research, vol.1 No.2

Muanalifah, A dan Isnawati A,R., .2022. *The Tropical Version Of Elgamal Encryption* Department of Mathematics UIN Walisongo Semarang

Munir, R. 2019 . Kriptografi . Edisi Kedua. Penerbit : Informatika Bandung

Paar, Christof dan Jal Pelzl .1998. *Understanding Cryptography A Textbook for students and Practitioners* Department of Electrical Engineering and Information Sciences

Reswan, Y., dan Prabowo, D.A. 2018.*Perancangan Aplikasi Pengamanan Data Text Menggunakan Kombinasi*

Algoritma Hill Cipher dan Algoritma RSA Jurnal Sistem Informasi.Vol(10).2

Shpilrain, Vladimir. 2000. *Group Based on Cryptography* Department of Mathematics The City College of New York

Shpilrain, Vladimir. 2008 .*Cryptanalysis Of Stickel's key exchange scheme* Department of Mathematics The City College of New York

Winarni. 2011. *Penjadwalan Jalur Bus Dalam Kota dengan Model Petrinet dan Aljabar Max-Plus (Studi Kasus Busway Transjakarta)* Jurnal Chaucy. Vol(1).4

Lampiran 1. Tabel Unicode

Unicode	NAMA	SYMBOL
0	Null	
32	Space	
33	Tanda seru	!
48	Angka 0	0
49	Angka 1	1
50	Angka 2	2
51	Angka 3	3
52	Angka 4	4
53	Angka 5	5
54	Angka 6	6
55	Angka 7	7
56	Angka 8	8
57	Angka 9	9
63	tanda tanya	?
65	Huruf latin kapital A	A
66	Huruf latin kapital B	B
67	Huruf latin kapital C	C
68	Huruf latin kapital D	D
69	Huruf latin kapital E	E
70	Huruf latin kapital F	F
71	Huruf latin kapital G	G
72	Huruf latin kapital H	H

KODE ASCII	NAMA	SYMBOL
73	Huruf latin kapital I	I
74	Huruf latin kapital J	J
75	Huruf latin kapital K	K
76	Huruf latin kapital L	L
77	Huruf latin kapital M	M
78	Huruf latin kapital N	N
79	Huruf latin kapital O	O
80	Huruf latin kapital P	P
81	Huruf latin kapital Q	Q
82	Huruf latin kapital R	R
83	Huruf latin kapital S	S
84	Huruf latin kapital T	T
85	Huruf latin kapital U	U
86	Huruf latin kapital V	V
87	Huruf latin kapital W	W
88	Huruf latin kapital X	X
89	Huruf latin kapital Y	Y
90	Huruf latin kapital Z	Z
46	Tanda titik	.

Lampiran 2. Tabel Huruf Hijaiyah

Huruf Hijaiyah	Kode
ا	65
ب	66
ت	67
ث	68
ج	69
ح	70

Huruf Hijaiyah	Kode ASCII
خ	71
د	72
ذ	73
ر	74
ز	75
س	76

Huruf Hijaiyah	Kode ASCII
ش	77
ص	78
ض	79
ط	80
ظ	81
ع	82

Huruf Hijaiyah	Kode ASCII
غ	83
ف	84
ق	85
ك	86
ل	87
م	88

Huruf Hijaiyah	Kode ASCII
ن	97
و	98
ه	99
ء	100
ي	101

Lampiran 3. Program Python ElGamal untuk Matriks

```
from numpy import linalg as LA
from time import process_time
import numpy as np
import secrets
from time import process_time
import random
from math import pow


#=====================================
#======Aljabar Max-Plus ===============
#=====================================

#generate random matrix

def generate_random_matrix(m,n, min, max):
    H = [[secrets.randbelow((max - min) + 1)
    + min for i in range(m)] for j in range(n)]
    return H

#generate random exponent
def generate_exponent(order):
  secretsGenerator = secrets.SystemRandom()
  m = secretsGenerator.randint(3,2**order)
  return m

#Tropical Identity (Addition)/have checked(correct)
def maxpluszeros(n):
  return np.zeros((n,n))+-np.inf

#Tropical Identity (Multipication)
def maxeins(n):
```

```
  #id=np.zeros((n,n))
  id=generate_random_matrix(n,n,0,0)
  for i in range(0,n):
    for j in range(0,n):
      if i==j:
        id[i][j]=id[i][j]
      else:
        id[i][j]=-np.inf
  return id
#Tropical addition
#def oplus(A,B):
  #T=np.maximum(A,B)
 # return T
# Tropical Matrix Addition
def oplus(x, y):
    return [[a if a > b else b for a, b in
    zip(x_rows, y_rows)]
    for x_rows, y_rows in zip(x, y)]

def sub(x, y):
    return [[1 if (abs(a-b) <=0.0000001)
    else 0 for a, b in zip(x_rows, y_rows)]
    for x_rows, y_rows
    in zip(x, y)]

def minus(p,q):
  return[[a-b for a,b  in zip(p_rows, q_rows)]
  for p_rows, q_rows in zip(p, q)]

def plus(p,q):
  return[[a+b for a,b  in zip(p_rows, q_rows)]
  for p_rows, q_rows in zip(p, q)]

def multi(p,q):
  return[[a*b for a,b  in zip(p_rows, q_rows)]
```

```
  for p_rows, q_rows in zip(p, q)]

# Tropical Matrix Multiplication
def otimes(x, y):
    return [[max(a + b for a, b in zip(row, col))
    for col in zip(*y)] for row in x]

# Tropical Adjoint Multiplication
def adj_multiply(x, y):
    return oplus(oplus(x, y), otimes(x, y))


# Tropical Adjoint Multiplication
def adj_multiply(x, y):
    return oplus(oplus(x, y), otimes(x, y))

#faster max plus multiplication
def fastpower(A,t):
  exp = bin(t)
  C = A
  for i in range(3, len(exp)):
    C = otimes(C,C)
    if (exp[i:i+1]=='1'):
      C = otimes(C,A)
  return C

#maxpower (slow version)
def maxpower(A,t):
  n=len(A)
  C=maxeins(n)
  for i in range(t):
    C=otimes(A,C)
  return C

def generate_integer(below,upper):
```

```
    secretsGenerator = secrets.SystemRandom()
    m = secretsGenerator.randint(below,upper)
    return m

def diagonalmax(n):
    A=maxeins(n)
    n=len(A)
    for i in range(n):
        for j in range(n):
            A[i][i]=(-1)*generate_integer(1,100)
            +generate_integer(1,100)
    return A



#program merubah matriks diagonal
def diagonalkey(A):
    n=len(A)
    for i in range(n):
        for j in range(n):
            if i==j:
                A[i][i]=(-1)*generate_integer(1,100)
                +generate_integer(1,100)


    return A

    #program invers matriks A

def inversmaxplus(A):
    n=len(A)
    for i in range(n):
        for j in range(n):
            A[i][i]=(-1)*A[i][i]
    return A
```

```
#-----------------------------------
#Experiment
#Enkripsi ElGamal
#input:  matriks A
#-----------------------------------
# Random Matriks
A=generate_random_matrix(4,4, -10, 10)
print("A=",A)

#=========================
#Generate Kunci (Alice)
#=========================
#random bilangan bulat k
k=random.randint(2,2**10)
print('k=',k)
# Alice menghitung U=A^k
U=maxpower(A,k)

#======================
#Enkripsi
#======================
#Bob menerima U dari Alice
#Bob memilih secara acak bilangan bulat l
l=random.randint(2,2**10)
print('l=',l)
#Bob menghitung V
V=fastpower(A,l)
#Bob menghitung K_bob
Kb=fastpower(U,l)
print('Kb',Kb)
#Bob merubah B menjadi matrik diagonal
Kbdiagonal=diagonalkey(Kb)
#Masukkan message
```

```
M=generate_random_matrix(4,4, -10, 10)
#Menginkripsi pesan
C=otimes(M,Kbdiagonal)
print('C=',C)

#================
#Deskripsi
#================
#Alice menghitung kunci
Ka=fastpower(V,k)
print('Ka=',Ka)
#Alice merubah Ka ke diagonal
Kadiagonal=diagonalkey(Ka)
print('Kadiagonal=',Kadiagonal)
D=otimes(M,inversmaxplus(Kadiagonal))
print('D=',D)
```

Lampiran 4. Program Python ElGamal untuk Bilangan Bulat

```
from numpy import linalg as LA
from time import process_time
import numpy as np
import secrets
from time import process_time
import random
from math import pow


#=====================================
#======Aljabar Max-Plus ===============
#=====================================

#generate random integer
g=random.randint(3,2**10)

def generate_random_matrix(m,n, min, max):
    H = [[secrets.randbelow((max - min) + 1)
    + min for i in range(m)] for j in range(n)]
    return H

#generate random exponent
def generate_exponent(order):
  secretsGenerator = secrets.SystemRandom()
  m = secretsGenerator.randint(3,2**order)
  return m

#Tropical Identity (Addition)/have checked(correct)
def maxpluszeros(n):
  return np.zeros((n,n))+-np.inf

#Tropical Identity (Multipication)
```

```
def maxeins(n):
  #id=np.zeros((n,n))
  id=generate_random_matrix(n,n,0,0)
  for i in range(0,n):
    for j in range(0,n):
      if i==j:
        id[i][j]=id[i][j]
      else:
        id[i][j]=-np.inf
  return id
#Tropical addition
#def oplus(A,B):
  #T=np.maximum(A,B)
 # return T
# Tropical Matrix Addition
def oplus(x, y):
    return [[a if a > b else b for a, b in
    zip(x_rows, y_rows)]
    for x_rows, y_rows in zip(x, y)]

def sub(x, y):
    return [[1 if (abs(a-b) <=0.0000001)
    else 0 for a, b in zip(x_rows, y_rows)]
    for x_rows, y_rows
    in zip(x, y)]

def minus(p,q):
  return[[a-b for a,b  in zip(p_rows, q_rows)]
  for p_rows, q_rows in zip(p, q)]

def plus(p,q):
  return[[a+b for a,b  in zip(p_rows, q_rows)]
  for p_rows, q_rows in zip(p, q)]

def multi(p,q):
```

```
  return[[a*b for a,b  in zip(p_rows, q_rows)]
  for p_rows, q_rows in zip(p, q)]

# Tropical Matrix Multiplication
def otimes(x, y):
    return [[max(a + b for a, b in zip(row, col))
    for col in zip(*y)] for row in x]

# Tropical Adjoint Multiplication
def adj_multiply(x, y):
    return oplus(oplus(x, y), otimes(x, y))
```

```
#-----------------------------------
#Experiment
#Enkripsi ElGamal
#input:  integer g
#-----------------------------------
# Random Integer
g=random.randint(3,2**10)
print("A=",g)

#=========================
#Generate Kunci (Alice)
#=========================
#random bilangan bulat k
k=random.randint(2,2**10)
print('k=',k)
# Alice menghitung u=g^k
u=k*g
```

```
#=====================
#Enkripsi
#=====================
#Bob menerima u dari Alice
#Bob memilih secara acak bilangan bulat l
l=random.randint(2,2**10)
print('l=',l)
#Bob menghitung v
v=l*g
#Bob menghitung K_bob
kb=u*l
print('kb',kb)

#Mengenkripsi pesan
m=random.randint(2,2**10)
print('m=',m)
c=m+kb
print('c=',c)

#================
#Deskripsi
#================
#Alice menghitung kunci
ka=v*k
print('ka=',ka)
D=c-ka
print('D=',D)
```

DAFTAR RIWAYAT HIDUP

A. Identitas Diri

1. Nama Lengkap	:	Regita Nurul Fitriani
2. Tempat & Tgl.Lahir	:	Majalengka, 4 Mei 2001
3. Alamat Rumah	:	Dukuh Warung Timur RT 001/ RW 004 Desa Pagandon Kecamatan Kadipaten Kabupaten Majalengka, Jawa Barat
4. HP	:	0887 0761 6696
5. E-mail	:	fitrianiregita21@gmail.com

B. Riwayat Pendidikan

1. SD Negeri Gandu II I (2007-2011)
2. SD Negeri Kadipaten I (2011-2013)
3. SMP Negeri I Majalengka (2013-2016)
4. SMA Negeri I Majalengka (2016-2019)

Semarang, 25 Mei 2023