ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *ELGAMAL* UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

OLEH
SITI NUR FADLILAH
NIM. 17610003

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *ELGAMAL* UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

OLEH
SITI NUR FADLILAH
NIM. 17610003

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *ELGAMAL* UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

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

Oleh
Siti Nur Fadlilah
NIM. 17610003

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *ELGAMAL* UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Siti Nur Fadlilah
NIM. 17610003

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 25 September 2021

Pembimbing I,	Pembimbing II,
Prof. Dr. H. Turmudi, M.Si., Ph.D	Muhammad Khudzaifah, M.Si
NIP. 19571005 198203 1 006	NIDT. 19900511 20160801 1 057

Mengetahui,
Ketua Program Studi Matematika

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

ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA *HILL CIPHER* DAN *ELGAMAL* UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Siti Nur Fadilah
NIM. 17610003

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 25 Desember 2021

Penguji Utama	: Juhari, S.Pd., M.Si	.....
Ketua Penguji	: Hisyam Fahmi, M.Kom	.....
Sekretaris Penguji	: Prof. Dr. H. Turmudi, M.Si., Ph.D	.....
Anggota Penguji	: Muhammad Khudzaifah, M.Si	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Siti Nur Fadlilah
NIM	: 17610003
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Enkripsi dan Dekripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal* untuk Mengamankan Pesan Teks

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

Malang, 06 Desember 2021
Yang membuat pernyataan,

Siti Nur Fadlilah
NIM. 17610003

MOTO

“Tidak ada yang mudah tetapi bisa diusahakan”

فَاِنَّ مَعَ الْعُسْرِيُسْرًا﴿٥﴾اِنَّ مَعَ الْعُسْرِيُسْرًا﴿٦﴾

“Maka sesungguhnya bersama kesulitan ada kemudahan.
Sesungguhnya bersama kesulitan ada kemudahan” (Q.S al-Insyirah/30:5-6)

PERSEMBAHAN

Skripsi ini penulis persembahkah untuk:

Ayahanda Nurhuda, ibunda Rusiati, adik tersayang Ibnu Syabbil yang selalu mendukung di setiap langkah dan menjadi alasan terbesar penulis untuk lebih baik dan lebih baik lagi. Serta diri sendiri, selamat atas pencapaiannya.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt. atas rahmat, taufik serta hidayah-Nya, sehingga penulis mampu menyelesaikan penyusunan skripsi yang berjudul "Enkripsi dan Dekripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal* untuk Mengamankan Pesan Teks" sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat serta salam selalu terlimpahkan kepada Nabi Muhammad Saw. yang telah menuntun manusia ke jalan kebenaran yakni agama Islam.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama kepada:

1. Prof. Dr. H. M. Zainuddin,MA, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang
4. Prof. Dr. H. Turmudi, M.Si., Ph.D, selaku dosen pembimbing I serta wali dosen yang telah banyak memberikan arahan, nasihat, motivasi, dan berbagi pengalaman yang berharga kepada penulis.
5. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing II yang telah banyak memberikan arahan dan berbagi ilmunya kepada penulis.
6. Juhari, S.Pd., M,Si, selaku penguji utama yang telah memberikan saran dan masukan-masukan yang sangat berharga untuk penulisan skripsi ini.
7. Hisyam Fahmi, M.Kom, selaku ketua penguji yang telah memberikan saran dan masukan-masukan yang sangat berharga untuk penulisan skripsi ini.

8. Segenap sivitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terima kasih atas segala ilmu dan bimbingannya.
9. Ayahanda Nurhuda, Ibunda Rusiati dan adik penulis yang selalu memberikan doa, semangat, serta motivasi kepada penulis sampai saat ini.
10. Seluruh teman-teman di Keluarga Besar Mahasiswa Bidikmisi (KBMB), terutama Zahratuttakiyah, S.Si, Dika Frantiko, S.Hum, Vivy Endang Try Santi, S.Pd, Fery Setiowati, Lailatul Badriyah dan Sisi Susilowati Rahma. Teman-teman di Program Studi Matematika angkatan 2017, terutama Uswatun Hasanah dan Widya Nur Faizah, S.Mat terima kasih atas segala pengalaman yang berharga dan kenangan terindah saat menuntut ilmu bersama.
11. Semua pihak yang tidak dapat disebutkan satu-persatu yang telah membantu dalam menyelesaikan skripsi ini baik moril maupun materil.

Semoga Allah Swt. melimpahkan rahmat dan karunia-Nya kepada kita semua. Selain itu, penulis berharap semoga skripsi ini bermanfaat bagi penulis danbagi pembaca. *Aamiin*

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 06 Desember 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

Simbol-simbol yang digunakan pada skripsi ini mempunyai makna yaitu sebagai berikut:

C : *Ciphertext*

K : Matriks kunci pada algoritma *Hill Cipher* untuk melakukan proses enkripsi

P : *Plaintext*

N : Banyaknya kode ASCII 256

$\overline{K}$: Matriks 3×3 kunci pada algoritma *Hill Cipher* untuk melakukan proses dekripsi

p : Bilangan prima yang merupakan kunci publik pada algorima *ElGamal*

α : Akar primitif yang memenuhi $\alpha < p$ sebagai kunci publik pada algorima *ElGamal*

β : Kunci publik pada algoritma *ElGamal* yang dihasilkan dari perhitungan $\beta = \alpha^d mod\ p$

d : Kunci privat pada algoritma *ElGamal* yang memenuhi $1 \leq d \leq p - 2$

(a, b) : *Ciphertext* yang diperoleh dari hasil enkripsi menggunakan algoritma *ElGamal*

r : Matriks dengan elemen pembangunnya bilangan acak dengan $r \in \{0,1, \cdots, p - 2\}$

ABSTRAK

Fadlilah, Siti Nur. 2021. **Enkripsi dan Dekripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal* untuk Mengamankan Pesan Teks**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Prof. Dr. H. Turmudi, M.Si., Ph.D (II) Muhammad Khudzaifah, M.Si

Kata Kunci: Enkripsi, Dekripsi, *Hill Cipher*, *ElGamal*.

Penelitian ini bertitik tolak dari kerangka berfikir bahwa seiring perkembangan teknologi dan banyaknya pengguna media komunikasi jarak jauh, maka pengamanan pesan teks harus ditingkatkan. Melakukan penyandian pada pesan teks menjadi cara yang digunakan untuk meningkatkan keamanan pada proses enkripsi dan dekripsi pesan. Pada penelitian ini penyandian pesan menggunakan dua algoritma yaitu *Hill Cipher* dan *ElGamal*. Algoritma *Hill Cipher* menggunakan kunci simetris dan *ElGamal* menggunakan kunci publik dan privat. Kedua algoritma memiliki kekurangan dan kelebihan masing-masing sehingga jika digabungkan akan meningkatkan keamanan dan kecepatan proses enkripsi dan dekripsi. Tujuan dari penelitian ini adalah untuk mengetahui proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* dan *ElGamal*. Penelitian yang dilakukan menggunakan pendekatan kualitatif dengan metode *library research*. Tahap penelitian yang dilakukan yaitu dengan menentukan *plaintext* dan mengkonversikan pada tabel ASCII 256. Kemudian membentuk kunci simetris algoritma *Hill Cipher* serta kunci publik dan privat dari algoritma *ElGamal*. Pada proses enkripsi menggunakan algoritma *Hill Cipher* diperoleh *ciphertext* pesan. Enkripsi kedua dilakukan dengan mengubah kunci simetris menjadi kunci rahasia menggunakan kunci publik algoritma *ElGamal*. Kemudian proses dekripsi dimulai dengan menggunakan kunci privat dari algoritma *ElGamal*. Sehingga diperoleh kunci simetris algoritma *Hill Cipher* yang akan digunakan untuk mendekripsikan *ciphertext*. Kemudian dari proses dekripsi menggunakan algoritma *Hill Cipher* diperoleh *plaintext* asli. Proses enkripsi dan dekripsi pada penelitian ini menggunakan perhitungan matematika manual. Kesimpulan dari penelitian ini adalah proses enkripsi dan dekripsi pada pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal* dengan perhitungan matematika secara manual dapat meningkatkan keamanan pesan secara efektif, sehingga dapat mengurangi serangan kriptanalis.

ABSTRACT

Fadlilah, Siti Nur. 2021. On The **Encryption and Decryption Using *Hill Cipher* and *ElGamal* Algorithms to Secure Text Messages**. Thesis. Mathematics Study Program, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang. Supervisor: (I) Prof. Dr. H. Turmudi, M.Si., Ph.D (II) Muhammad Khudzaifah., M.Si

Keywords: Encryption, Decryption, Hill Chipher, ElGamal

This research depends on the framework of thinking that the security of text messages must be improved along with the development of technology and the number of users of remote communication media. Encoding text messages becomes a way to improve security in the process of encrypting and decrypting messages. In this study, message encoding used two algorithms, namely Hill Cipher and ElGamal. The Hill Cipher algorithm uses symmetrical keys and ElGamal uses public and private keys. Both algorithms have their own advantages and disadvantages which will improve the security and speed of the encryption and decryption process if it combined. The purpose of the study was to find out the encryption and decryption process using the Hill Cipher and ElGamal algorithms. The Research is conducted using qualitative approaches with library research methods. The research phase is to determine the plaintext and convert it using the ASCII table 256. Then, it forms the symmetrical key of the Hill Cipher algorithm as well as the public and private keys of the ElGamal algorithm. Ciphertext message obtained in the encryption process used the Hill Cipher algorithm. The second encryption is done by converting the symmetrical key into a secret key using the ElGamal algorithm public key. Then the decryption process begins by using the private key of the ElGamal algorithm. The result obtained a symmetrical key hill cipher algorithm that will be used to decrypt the ciphertext. Then from the decryption process using the Hill Cipher algorithm obtained the original plaintext. The encryption and decryption process in this study used manual mathematical calculations. The conclusion of this study is that the process of encryption and decryption on text messages using hill cipher and ElGamal algorithms with manual mathematical calculations can improve the security of messages effectively, thus reducing cryptanalysis attacks.

ملخص

فضليلة، سيتي نور. ٢٠٢١. **التشفير وفك التشفير باستخدام خوارزميات هيل سيفهير (*Hill Cipher*) و إلغامال (*ElGamal*) لتأمين الرسالة النصية**. بحث العلم. قسم الدراسة الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. مشرفان: (١) أستاذ الدكتور الحج تورمودي، الماجستير، (٢) محمد خذيفة، الماجستير.

الكلمات المفتاحية: التشفير، فك التشفير، هيل سيفهير، إلغامال

يبدأ هذا البحث من إطار التفكير أنه إلى جانب تطور التكنولوجيا وعدد مستخدمين وسائط الاتصال البعيدة، يجب تحسين أمان الرسالة النصية. تشفير الرسالة النصية هي طريقة تستخدم لزيادة الأمان في عملية تشفير وفك تشفير الرسالة. هذا البحث يستخدم ترميز الرسالة خوارزميتين هما هيل سيفهير و إلغامال. خوارزمية هيل سيفهير يستخدم مفاتيح متماثلة ويستخدم إلغامال مفاتيح العامة والخاصة. كل من الخوارزميتين لهما مزايا وعيوب بحيث يؤدي الجمع بينهما إلى زيادة أمان وسرعة عملية التشفير وفك التشفير. الهدف من هذا البحث هو لمعرفة عملية التشفير وفك التشفير باستخدام خوارزميتين هما هيل سيفهير و إلغامال. إجراء البحث باستخدام منهج نوعي بطريقة البحث المكتبية. مرحلة البحث مستخدم هي تحديد النص العادي وتحويله إلى جدول ASCII 256. ثم تشكيل المفتاح المتماثل لخوارزمية هيل سيفهير ومفاتيح العامة والخاصة لخوارزمية إلغامال. في عملية التشفير باستخدام خوارزمية هيل سيفهير يتم الحصول على النص المشفر. يتم التشفير الثاني بطريق تحويل المفتاح المتماثل إلى مفتاح سري باستخدام المفتاح العام لخوارزمية إلغامال. ثم تبدأ عملية فك التشفير باستخدام المفتاح الخاص من خوارزمية إلغامال. بحيث يتم الحصول على مفتاح خوارزمية هيل سيفهير المتماثل والذي سيتم استخدامه لفك تشفير النص المشفر. ثم من عملية فك التشفير باستخدام خوارزمية هيل سيفهير يتم الحصول على النص العادي الأصلي. تستخدم عملية التشفير وفك التشفير في هذا البحث بحسابات رياضية يدوية. استنتاج هذا البحث هو أن عملية التشفير وفك التشفير على الرسالة النصية باستخدام خوارزميتين هيل سيفهير و إلغامال مع الحسابات الرياضية اليدوية يمكن أن تحسن أمان الرسالة بشكل جيّد، وذلك لتقليل هجمات تحليل التشفير.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi memiliki pengaruh yang sangat besar terhadap aspek kehidupan manusia. Internet merupakan salah satu bentuk kemajuan teknologi yang dapat digunakan manusia dengan sangat mudah. Dengan menggunakan internet manusia dapat melakukan komunikasi jarak jauh dengan mudah dan cepat. Namun jika menggunakan internet dengan tingkat keamanan relatif rendah maka informasi yang dikirim melalui jaringan mudah diketahui oleh pihak-pihak yang tidak berkepentingan. Bagi pihak pemerintahan, militer, perbankkan, pendidikan dan lain-lain menggunakan internet sebagai alat untuk mengirimkan pesan rahasia, maka tingkat keamanan informasi menjadi faktor utama yang harus terpenuhi (Ramadani, 2020). Perintah untuk menjaga kerahasiaan pesan sesuai dengan firman Allah Swt. Q.S al-Anfal ayat 27, yaitu:

يٰٓاَيُّهَاالَّذِيْنَ اٰمَنُوْالاَتَخُوْنُوْاالله وَالرَّسُوْلَ وَتَخُوْنُوْٓاَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ﴿٢٧﴾

"*Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui"* (*Q.S al-Anfal/9:27*).

Ayat tersebut mengajarkan pada manusia pentingnya menjaga kerahasiaan pesan yang telah diamanatkan kepada sesama manusia. Sebagai seorang pengirim tentunya memiliki keinginan agar pesan yang dikirim tersampaikan pada penerima yang dituju dan isi pesan sesuai dengan pesan yang telah terkirim. Pada

proses pengiriman pesan yang dilakukan dengan menggunakan teknologi informasi tentunya melalui perantara yang rawan terjadi pencurian informasi oleh pihak yang tidak berkepentingan. Hal ini berarti seseorang telah melakukan pengkhianatan karena tidak dapat menjaga kerahasiaan informasi. Berbagai cara dilakukan agar kerahasiaan pesan tetap terjaga. Salah satunya dengan mengubah informasi yang dikirim menjadi kode-kode yang tidak dimengerti menggunakan metode penyandian, sehingga akan menyulitkan pihak yang tidak berkepentingan apabila mencoba untuk mengetahui informasi yang sebenarnya (Hamidah, 2009).

Pesan yang dikirim melalui metode penyandian akan mengalami perubahan menjadi kode yang tidak dapat dimengerti oleh pihak lain. Sehingga metode penyandian dikembangkan seiring dengan perkembangan teknologi informasi dan tingkat efisien ketika digunakan masyarakat untuk membantu kegiatan sehari-hari. Pada awal pembentukannya metode penyandian difokuskan pada kerahasiaan algoritma. Sehingga mengakibatkan kurangnya tingkat kenyamanan bagi pengguna ketika digunakan oleh banyak orang karena harus membentuk algoritma baru setiap akan melakukan pertukaran informasi. Kemudian dikembangkan metode penyandian baru yang difokuskan pada kerahasiaan kunci yang dikenal dengan kriptografi. Sehingga tidak perlu membentuk algoritma baru setiap melakukan pertukaran informasi. Namun tidak menutup kemungkinan bahwa kerahasiaan pesan dapat terjaga dengan baik karena pihak yang tidak berkepentingan juga memiliki banyak cara dalam melakukan pencurian informasi (Hamidah, 2009). Pada kriptografi terdapat dua algoritma yaitu simetris seperti *Hill Cipher* dan asimetris seperti *ElGamal*.

Laster S. Hill dalam artikel yang berjudul *Cryptography In An Algebraic Alphabet* pada tahun 1929 melakukan proses penyandian menggunakan matriks dengan pendekatan aljabar. Penerapannya dilakukan pada abjad dengan jumlah 26 dan menggunakan operasi penjumlahan dan perkalian pada matriks. Matriks digunakan sebagai kunci dengan syarat matriks invertibel. Untuk menentukan invers matriks maka harus mengetahui determinan matriks dengan nilai determinan tidak sama dengan nol. Pada proses dekripsi diperlukan untuk mengetahui invers modulo dari matriks kunci. Karena alfabet yang digunakan terdapat 26 huruf maka digunakan juga operasi aritmatika modulo. Sehingga ketika melakukan enkripsi maupun dekripsi setiap huruf dapat dikembalikan sesuai dengan pesan semulanya. Dengan menggunakan matriks ukuran $n \times n$ berhasil dilakukan proses enkripsi dan dekripsi (Hill, 1929).

Menurut penelitian Shahram dan Siavash dengan judul *Ciphertext-Only Attack on* $d \times d$ *Hill in* $O(d13^d)$ pada tahun 2016. Algoritma *Hill Cipher* mampu dalam menghadapi serangan *Ciphertext-Only Attack* (COA) namun COA telah mampu dipecahkan dengan *Chinese Remainder Theorem*. Sehingga keamanan pada algoritma *Hill Cipher* harus ditingkatkan dan tetap mempertimbangkan kecepatan pada proses penyandian pesan (Ahmadi, 2016). Oleh sebab itu algoritma *Hill Cipher* dikombinasikan dengan algoritma *ElGamal* yang memiliki tingkat keamanan lebih baik.

Kemudian Suci Ramadani pada tahun 2020 melakukan penelitian dengan melakukan kombinasi algoritma *Hill Cipher* dan *ElGamal* diterapkan pada citra yang berjudul *Hybird Cryptosystem Algoritma Hill Cipher dan Algoritma ElGamal pada Keamanan Citra*. Pada penelitian ini menunjukkan bahwa

pengamanan citra dengan menggunakan algoritma *Hill Cipher* dan *ElGamal* untuk merahasiakan citra berjalan dengan baik. Diperoleh kesimpulan bahwa citra berhasil dienkripsi dan didekripsikan, percobaan yang dilakukan pada algoritma *Hill Cipher* dan *ElGamal* dan waktu proses yang digunakan mendekripsikan *ciphertext* lebih cepat dibandingkan hasil enkripsi *plaintext* (Ramadani, 2020).

Berdasarkan penelitian yang telah dilakukan pada algoritma *Hill Cipher* dan *ElGamal* menunjukkan bahwa kedua algoritma tersebut memiliki kekurangan dan kelebihan masing-masing. Oleh karena itu penulis tertarik untuk melakukan kombinasi pada kedua algoritma dengan menerapkannya pada pesan teks. Penelitian ini memiliki tujuan untuk meningkatkan keamanan pesan teks ketika melakukan proses enkripsi dan dekripsi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, diperoleh rumusan masalah penelitian ini sebagai berikut:

1. Bagaimana proses enkripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal* ?
2. Bagaimana proses dekripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal* ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, diperoleh tujuan penelitian sebagai berikut:

1. Untuk mengetahui proses enkripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal*.
2. Untuk mengetahui proses dekripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal*.

1.4 Manfaat Penelitian

Penelitian ini dapat memberikan manfaat yang positif pada pembaca di ranah pendidikan sebagai berikut:

1. Bagi Peneliti

   Menambah wawasan tentang enkripsi dan dekripsi kriptografi algoritma *Hill Cipher* dan *ElGamal* menggunakan pendekatan matematika.

2. Bagi Lembaga

   Sebagai tambahan referensi pembelajaran mata kuliah yang berhubungan dengan algoritma kriptografi terutama algoritma *Hill Cipher* dan *ElGamal*.

3. Bagi Mahasiswa

   Menambah wawasan keilmuan mengenai proses enkripsi dan dekripsi untuk pengamanan pesan rahasia menggunakan ilmu kriptografi pada algoritma *Hill Cipher* dan *ElGamal*.

1.5 Batasan Masalah

Permasalahan pada penelitian ini difokuskan agar tidak meluas sehingga diberikan batasan masalah pada penelitian ini sebagai berikut:

1. Mengonversikan *plaintext* pada tabel ASCII 256.
2. Menggunakan matriks 3×3 sebagai kunci algoritma *Hill Cipher*.

1.6 Metode Penelitian

Penelitian ini menggunakan metode kepustakaan *library research* (penelitian kepustakaan) atau studi pustaka. Kutipan informasi diperoleh dari buku, artikel atau skripsi-skripsi terdahulu dan dikumpulkan sesuai dengan judul penelitian sehingga jenis penelitian ini adalah penelitian kualitatif. Untuk mencapai tujuan yang diinginkan maka langkah-langkah yang digunakan adalah sebagai berikut:

1. Pembentukan kunci algoritma *Hill Cipher*. Pada algoritma *Hill Cipher* menggunakan satu kunci yang terbentuk dalam matriks persegi 3×3 dengan syarat harus menggunakan matriks yang memiliki invers modulo N. Menentukan invers matriks menggunakan $\bar{\Delta}$ dan adjoin matriks.
2. Pembentukan kunci algoritma *ElGamal*. Kunci publik terdiri dari bilangan prima p, pilih akar primitif α yang memenuhi $\alpha < p$ dan β hasil dari perhitungan menggunakan rumus algoritma *ElGamal* $\beta = \alpha^d \, mod \, p$. Kemudian kunci privat hanya diketahui oleh penerima pesan yang terdiri dari sembarang bilangan bulat d yang memenuhi $1 \leq d \leq p - 2$ yang akan digunakan untuk melakukan dekripsi.

3. Melakukan enkripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal*.
   a. Menentukan *plaintext*.
   b. Mengubah *plaintext* sesuai dengan kode ASCII 256.
   c. Melakukan proses enkripsi menggunakan algoritma *Hill Cipher* dengan membagi *plaintext* menjadi blok-blok sesuai dengan *ordo* 3×3 dari matriks kunci. Menggunakan rumus enkripsi dari algoritma *Hill Cipher* $C = K \cdot P \ mod \ N$ sehigga diperoleh *ciphertext*.
   d. Melakukan proses enkripsi kunci K menggunakan kunci publik dari algoritma *ElGamal*. Berdasarkan hasil pembentukan kunci algoritma *ElGamal* diperoleh kunci publik $(p, \alpha, \beta) = (241, 11, 63)$ yang digunakan pengirim untuk melakukan proses enkripsi. Proses enkripsi kunci K menggunakan rumus $a = \alpha^r \ mod \ p$ dan $b = P \times \beta^r \ mod \ p$, sehingga diperoleh *ciphertext* a, b.
4. Melakukan proses dekripsi menggunakan algoritma *ElGamal* dan *Hill Cipher*.
   a. Melakukan dekripsi pada kunci K menggunakan kunci privat d dari algoritma *ElGamal* yang dimiliki oleh penerima dengan menentukan $(a^x)^{-1} = a^{p-1-d} mod \ p$ dan $P = b \times (a^x)^{-1} mod \ p$ untuk mengetahui *plaintext* kunci simetris K.
   b. Menentukan invers modulo matriks K sebagai matriks kunci pada proses dekripsi. Untuk memenuhi rumus invers matriks diperlukan untuk menentukan determinan matriks K dan adjoin matriks K.

c. Melakukan dekripsi pesan menggunakan kunci K dengan menggunakan rumus $P = K^{-1} \cdot C \ mod \ N$.

d. *Plaintext* yang diperoleh harus dikonversikan pada tabel ASCII 256. Sehingga mendapatkan *plaintext* semula yang merupakan pesan asli dari pengirim.

1.7 Sistematika Penulisan

Sistematika penulisan pada proposal penelitian ini terdiri dari empat bab dan masing-masing bab memiliki subbab dengan rumusan sebagai berikut:

1. BAB I Pendahuluan, dalam bab pendahuluan ini terdiri dari beberapa subbab yang berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dalam penelitian, metode penelitian dan sistematika penulisan.
2. BAB II Kajian Pustaka, pada bab ini terdiri dari teori-teori yang digunakan pada penelitian ini seperti, kriptografi, algoritma *Hill Cipher*, algoritma *ElGamal*, penggunakan matematika pada algoritma *Hill Cipher* dan *ElGamal*, kode ASCII 256 dan implementasi kriptografi pada ayat al-Qur'an dan Hadits.
3. BAB III Pembahasan, berisi tentang proses pembentukan kunci algoritma *Hill Cipher* dan *ElGamal*. Kemudian proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* dan *ElGamal* dengan melakukan percobaan sebanyak dua kali.
4. BAB IV Penutup, berisi kesimpulan dari hasil penelitian dan saran dari penulis yang ditujukan pada pihak pembaca.

BAB II

KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan melakukan penyandian menjadi pesan yang tidak memiliki makna (Munir, 2010). Pengertian modern kriptografi merupakan ilmu yang bersandarkan pada tenik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas (Sadikin, 2012). Seorang pengirim melakukan pengiriman pesan melalui media komunikasi dan penerima pesan akan menerima pesan dari media komunikasi. Ketika pesan sampai pada media komunikasi menjadi peluang bagi kriptanalis untuk mengetahui isi pesan yang dikirimkan. Untuk menghindari serangan kriptanalis pesan akan diubah menjadi kode-kode yang tidak bisa dimengerti oleh pihak lain supaya kerahasiaan pesan tetap terjaga.

2.1.1 Terminologi dalam Kriptografi

Istilah atau terminologi penting yang sering ditemukan dalam kriptografi. Berikut istilah atau terminologi yang perlu diketahui:

a. Pesan, *Plaintext* dan *Ciphertext*

   Pesan merupakan sesuatu yang disampaikan oleh pengirim kepada penerima. Pesan bisa berbentuk data atau informasi yang dapat

dimengerti. Supaya pesan dapat dimengerti oleh media komunikasi manusia menciptakan lambang komunikasi berupa suara, mimik, gerak-gerik, bahasa lisan dan bahasa tulisan. Dalam ilmu kriptografi pesan yang dapat dimengerti disebut *plaintext*. Agar *plaintext* tidak dimengerti oleh pihak lain, maka pesan diubah dalam bentuk kode atau lambang dengan melakukan penyandian. Setelah dilakukan penyandian maka akan terbentuk pesan baru yang tidak bisa dimengerti disebut *ciphertext*.

b. Penerima dan pengirim

Ketika melakukan proses komunikasi pertukaran pesan melibatkan dua entitas. Pengirim (*sender*) merupakan entitas yang melakukan proses pengiriman pesan. Kemudian penerima (*receiver*) merupakan entitas yang menerima pesan dari pengirim. Entitas dapat berupa mesin komputer, orang atau kartu kredit.

c. Enkripsi dan dekripsi

Enkripsi (*encyption*) merupakan proses penyandian yang merupakan perubahan sebuah pesan yang bisa dimengerti atau *plaintext* menjadi sebuah pesan yang tidak bisa dimengerti atau *ciphertext* sedangkan proses pengembalian *ciphertext* menjadi *plaintext* semula disebut sebagai proses dekripsi (*decryption*).

d. Cipher dan kunci

Algoritma yang digunakan untuk menampilkan proses enkripsi dan dekripsi disebut dengan cipher. Sedangkan kunci merupakan parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Memiliki berbagai

macam jenis bergantung pada kunci yang digunakan untuk mengubah susunan operasi algoritma kriptografi. Cipher tidak bisa digunakan untuk dekripsi dan enkripsi apabila tidak menggunakan kunci.

e. Sistem Kriptografi

Terbentuknya sebuah sistem dalam sebuah kriptografi sebagai fasilitas untuk mengubah *plaintext* menjadi *ciphertext* atau sebaliknya disebut sistem kriptografi (*cryptosystem*). Sistem kriptografi terdiri dari algoritma kriptografi, *plaintext*, *ciphertext* dan kunci.

f. Penyadap atau kriptanalis (*cryptanalis*)

Penyadap merupakan pihak yang tidak berhak mengetahui informasi namun melakukan pencurian informasi. Kegiatan penyadapan sangat merugikan pengirim karena tujuan dari penyadap adalah untuk memperoleh informasi tentang sistem kriptografi yang digunakan untuk komunikasi kemudian akan mengetahui pesan asli yang telah dikirimkan (Sadikin, 2012).

2.1.2 Analisis Sandi

Analisis sandi merupakan ilmu atau seni yang digunakan untuk memecahkan *ciphertext* sehingga akan diketahui *plaintext* dan kunci rahasianya. Berikut beberapa analisis sandi yang sering terjadi pada algoritma kriptografi,

a. *Ciphertext-only attack*

Ciphertext-only attack mengasumsikan pemecah kode hanya dapat mengakses jalur komunikasi publik sehingga hanya dapat mengumpulkan

ciphertext yang melintas dari jalur komunikasi tersebut. Pemecah kode berusaha untuk memecahkan teks sandi dengan cara menganalisis himpunan teks sandi yang dikumpulkan.

b. *Known-plaintext attack*

Known-plaintext attack mengasumsukan pemecah kode mempunyai sehimpunan pasangan teks asli dan sandi yang diperoleh melalui kebocoran, mata-mata atau kecelakaan.

c. *Chosen-plaintext attack*

Chosen-plaintext attack mengasumsikan pemecah sandi dapat mengakses algoritma enkripsi melalui penyandian, sehingga pemecah sandi dapat memilih beberapa teks asli pilihannya untuk melakukan penyandian sehingga diperoleh pasangan teks sandinya.

d. *Chosen-ciphertext attack*

Chosen-ciphertext attack diasumsikan pemecah sandi dapat mengakses algoritma dekripsi melalui penyulih sandi sehingga pemecah sandi dapat memilih beberapa teks sandi untuk mengetahui pasangan teks aslinya. Sistem kriptografi yang mampu bertahan dari serangan *Chosen-ciphertext attack* dapat dijalankan pada jaringan publik (Sadikin, 2012).

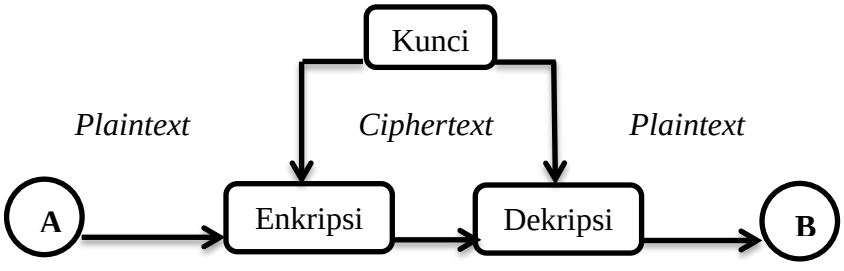
2.1.3 Algoritma Kriptografi

Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi

(Munir, 2010) Berdasarkan kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi algoritma kriptografi dibagi menjadi dua bagian yaitu:

a. Algoritma Simetris

Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Sebelum melakukan komunikasi diharuskan seorang pengirim dan penerima untuk menyetujui suatu kunci. Tingkat keamanan algoritma simetris bergantung pada kunci oleh karena itu, kunci harus dijaga kerahasiaannya. Algoritma simetris sering disebut dengan algoritma kunci tunggal. Algoritma simetris memiliki kelebihan bahwa tingkat kecepatan ketika melakukan proses enkripsi dan dekripsi lebih cepat dibandingkan dengan algoritma asimetris sehingga dapat digunakan pada sistem *real-time*. Kelemahan dari algoritma simetris terletak pada kunci yang digunakan. Ketika melakukan pertukaran informasi dengan pengguna lain harus membuat kunci yang berbeda sehingga agak terjadi kesulitan memanajemen kunci tersebut. Contoh algoritma kriptografi simetris adalah cipher permutasi, cipher substitusi, *Hill Cipher*, OTP, RC6, Twofish (Ariyus, 2008).



Gambar 2.1 Proses Enkripsi dan Dekripsi Algoritma Kunci Simetris

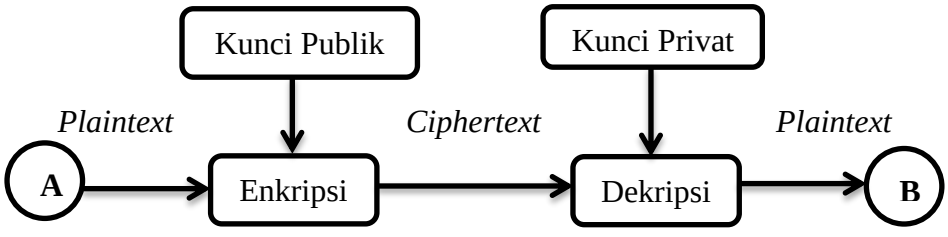
Keterangan: A = Pengirim Pesan

B = Penerima Pesan

→ = Proses Perjalanan Pesan

b. Algoritma Asimetris

Algoritma asimetris dikenal dengan algoritma kunci publik dengan menggunakan dua jenis kunci yaitu kunci publik (*publik key*) dan kunci privat (*private key*) ketika melakukan proses pengiriman pesan. Kunci publik bersifat umum sehingga kunci tidak dirahasiakan dan dapat diketahui oleh semua orang. Sedangkan kunci rahasia merupakan kunci yang dirahasiakan sehingga hanya orang tertentu saja yang dapat mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan bagi pelaku pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya. Namun, kecepatan dalam proses melakukan enkripsi dan dekripsi lebih rendah dibandingkan dengan algoritma simetris. Kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi antara pengirim dan penerima lebih panjang. Contoh dari algoritma asimetris adalah RSA, *ElGamal*, McEliece, LUC dan DSA (*Digital Signature Algorithm*) (Ariyus, 2008).



Gambar 2.2 Proses Enkripsi dan Dekripsi Algoritma Asimetris

Keterangan: A = Pengirim Pesan

B = Penerima Pesan

→ = Proses Perjalanan Pesan

2.2 Algoritma *Hill Cipher*

Hill Cipher merupakan salah satu algoritma kriptografi dengan kunci simetris. Algoritma *Hill Cipher* merupakan sandi *polyalphabet* dengan menggunakan metode substitusi dengan perhitungan perkalian matriks sebagai pembentukan kunci yang digunakan pada proses enkripsi dan dekripsi. Kunci pada algoritma *Hill Cipher* merupakan sebuah matriks K berukuran $n \times n$ yang harus memiliki invers dan nilai determinan matriks K memiliki invers perkalian pada jumlah alfabet yang digunakan (Sadikin, 2012). Dasar teori matriks pada algoritma *Hill Cipher* adalah penjumlahan matriks dan perkalian matriks. Agar dapat menciptakan cipher yang sulit dipecahkan dengan menggunakan teknik analisis frekuensi maka Lester S. Hill menciptakan kriptografi pada tahun 1929 yang dikenal dengan nama kriptografi *Hill Cipher*. *Hill Cipher* dapat dipecahkan oleh kriptanalis menggunanakan tenik *known-plaintext attack* (Jamaludin, 2018). Kelemahan utama algoritma *Hill Cipher* adalah menggunakan persamaan linier dengan matriks sebagai operasi substitusi. Apabila penyerang mampu mengumpulkan pasangan teks asli dan teks sandi yang menggunakan kunci yang sama, penyerang dapat menemukan kunci *Hill Cipher* dengan menyelesaikan sistem persamaan linier (Sadikin, 2012).

2.2.1 Pembentukan Kunci Algoritma *Hill Cipher*

Algoritma *Hill Cipher* menggunakan satu kunci yang disepakati dan diketahui oleh pengirim serta penerima pesan. Kunci pada algoritma *Hill Cipher* berbentuk matriks dengan ukuran baris dan kolom sama bisa menggunakan ordo $2 \times 2, 3 \times 3$ dan seterusnya. Matriks yang digunakan merupakan matriks yang memiliki invers. Kemudian *plaintext* akan dienkripsi menggunakan kunci simetris yang telah ditentukan dan *ciphertext* akan dikirimkan. Kemudian penerima pesan mendekripsikan *ciphertext* menggunakan kunci yang sama sehingga akan mengetahui *plaintext* sebenarnya (Jamaludin, 2018).

2.2.2 Enkripsi dan Dekripsi Algoritma *Hill Cipher*

Proses enkripsi pada *Hill Cipher* dilakukan pada setiap blok *plaintext*. Ukuran blok yang digunakan sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi blok-blok tertentu, *plaintext* terlebih dahulu diubah menjadi angka sesuai tabel ASCII 256 (Sadikin, 2012). Secara matematis, proses enkripsi pada *Hill Cipher* adalah,

$$C = K \cdot P \bmod N$$

Kemudian proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Sebelumnya harus mencari invers dari matriks kunci terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* adalah

$$P = \overline{K} \cdot C \bmod N$$

(Sadikin, 2012)

Contoh perhitungan algoritma *Hill Cipher*

a. Pembentukan Kunci Algoritma *Hill Cipher*

$K = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$

$det\ K = ad - bc = 5 \cdot 3 - 8 \cdot 17 = 15 - 136 = -121 \neq 0$

Menggunakan *Plaintext* $P = KODE$

Konversikan pada tabel alfabet 26 diperoleh $P = (K = 10)\ (O = 14)(D = 3)\ (E = 4)$

Tabel 2.1 Nomor Index Huruf Alfabet 26

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Kemudian dibagi menjadi blok-blok sesuai dengan ordo matriks diperoleh,

$p_1 = \begin{bmatrix} 10 \\ 14 \end{bmatrix}, p_2 = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$

b. Proses Enkripsi

Menggunakan rumus algoritma *Hill Cipher* $C = K \cdot P\ mod\ 26$ maka,

$c_1 = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \begin{bmatrix} 10 \\ 14 \end{bmatrix} mod\ 26$

$= \begin{bmatrix} 5 \cdot 10 + 8 \cdot 14 \\ 17 \cdot 10 + 3 \cdot 14 \end{bmatrix} mod\ 26$

$= \begin{bmatrix} 50 + 112 \\ 170 + 42 \end{bmatrix} mod\ 26$

$c_2 = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix} mod\ 26$

$= \begin{bmatrix} 5 \cdot 3 + 8 \cdot 4 \\ 17 \cdot 3 + 3 \cdot 4 \end{bmatrix} mod\ 26$

$= \begin{bmatrix} 15 + 32 \\ 51 + 12 \end{bmatrix} mod\ 26$

$= \begin{bmatrix}162\\212\end{bmatrix} mod\ 26$ $= \begin{bmatrix}47\\63\end{bmatrix} mod\ 26$

$= \begin{bmatrix}6\\4\end{bmatrix} = \begin{matrix}G\\E\end{matrix}$ $= \begin{bmatrix}21\\11\end{bmatrix} = \begin{matrix}V\\L\end{matrix}$

Diperoleh *Ciphertext* $C = GEVL$

c. Proses Dekripsi

Menentukan invers matriks $K\ mod\ 26$ dengan diketahui $\det K = -121$.

Kemudian menentukan $\bar{\Delta}$ yang merupakan invers dari $-121\ mod\ 26$

$-121\ mod\ 26 = -121 \cdot x \equiv 1\ mod\ 26$

$-121 \cdot x = \ 26y + 1$

$x = \frac{26y+1}{121}$

$x = \frac{26 \cdot 1+1}{121}$

$x = \frac{27}{121}$

$27 - 26 \equiv 1\ mod\ 26$

Sehingga diperoleh invers dari $det\ K = 3\ mod\ 26$

Karena invers dari $9\ mod\ 26$ maka diperoleh

$\overline{K} = \bar{\Delta}\ \cdot adj\ K = 3 \cdot \begin{bmatrix}3 & -8\\-17 & 5\end{bmatrix} = \begin{bmatrix}9 & -24\\-51 & 15\end{bmatrix} = \begin{bmatrix}9 & 2\\1 & 15\end{bmatrix}\ mod\ 26$

Gunakan $\overline{K} = \begin{bmatrix}9 & 2\\1 & 15\end{bmatrix}$ sebagai matriks kunci dalam melakukan dekripsi.

Proses dekripsi dilakukan dengan menggunakan rumus algoritma *Hill Cipher* $P = \overline{K} \cdot C\ mod\ 26$ sehingga diperoleh *plaintext* yang merupakan pesan asli dari pengirim. Jika *ciphertext* sudah sesuai dengan pesan *plaintext* maka dapat diartikan bahwa pesan terhindar dari pencurian kriptanalis.

$$p_1 = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \end{bmatrix} mod\ 26 \qquad p_2 = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \begin{bmatrix} 21 \\ 11 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 9 \cdot 6 + 2 \cdot 4 \\ 1 \cdot 6 + 15 \cdot 4 \end{bmatrix} mod\ 26 \qquad = \begin{bmatrix} 9 \cdot 21 + 2 \cdot 11 \\ 1 \cdot 21 + 15 \cdot 11 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 54 + 8 \\ 6 + 60 \end{bmatrix} mod\ 26 \qquad = \begin{bmatrix} 189 + 22 \\ 21 + 165 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 62 \\ 66 \end{bmatrix} mod\ 26 \qquad = \begin{bmatrix} 211 \\ 186 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 10 \\ 14 \end{bmatrix} = \begin{matrix} K \\ O \end{matrix} \qquad = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{matrix} D \\ E \end{matrix}$$

Dari hasil dekripsi diperoleh *plaintext* semula $P = KODE$

2.3 Penggunaan Konsep Matematika pada Algoritma *Hill Cipher*

Pembentukan algoritma *Hill Cipher* menggunakan ilmu matematika khususnya aljabar yang diterapkan pada alfabet. Seperti matriks digunakan sebagai kunci dan aritmatika modulo yang digunakan sebagai enkripsi dan dekripsi. Selain itu terdapat perkalian dan penjumlahan matriks untuk mengubah *plaintext* menjadi *ciphertext* ataupun sebaliknya.

2.3.1 Aritmetika *Integer*

Operasi aritmatika terdiri dari penjumlahan, perkalian, pengurangan dan pembagian. Pada aritmatika *integer* terdiri dari himpunan bilangan *integer* dan operasi aritmatika. Himpunan bilangan *integer* $\mathbb{Z}$ merupakan bilangan bulat dari $-\infty$ sampai ∞ seperti,

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, 4, \cdots\}$$

Pada bilangan *integer* memiliki 3 operasi *biner*: penjumlahan $(a + b)$, pengurangan $(a - b)$, dan perkalian $(a \times b)$. Operasi pembagian $\frac{a}{n}$ pada

bilangan *integer* diinterpretasikan memiliki hasil bagi (q) dan sisa bagi (r) (Sadikin, 2012).

Contoh:

Jika $a = 33, n = 16$ dapat ditemukan $q = 2$ (*integer* terbesar yang $n \times q \leq a$) dan sisa bagi $r = 1$ atau memenuhi $a = q \times n + r$ yaitu $33 = 2 \times 16 + 1$.

Suatu bilangan a dikatakan dibagi habis oleh n jika tidak memiliki sisa bagi $(r = 0)$ atau $a = n \times q$ dinyatakan dengan $a|n$. Sedangkan $a \nmid n$ menyatakan bahwa a tidak habis dibagi n. Himpunan bilangan *integer* yang membagi habis sebuah bilangan *integer* disebut dengan *divisor*. Misalkan 42 memiliki *divisor* $\{1,2,3,6,7,14,21,42\}$. Perhatikan bahwa bilangan 1 yang memiliki satu *divisor* sedangkan bilangan *integer* lainnya memiliki paling sedikit dua *divisor* yaitu bilangan itu sendiri dan 1. Bilangan *integer* p memiliki *divisor* $\{1, p\}$ disebut bilangan prima selain itu merupakan bilangan komposit.

a. Faktor Persekutuan Terbesar (FPB)

   FPB merupakan elemen terbesar dari himunan *divisor* dua bilangan *integer*. Suatu bilangan *integer* bisa saja memiliki beberapa elemen *divisor* yang sama namun hanya satu yang terbesar. Misalkan 42 memiliki *divisor* $\{1,2,3,6,7,14,21,42\}$ dan 12 memiliki *divisor* $\{1,2,3,4,6,12\}$ maka himpunan *divisor* persamaannya $\{1,2,3,6\}$ dan memiliki *divisor* terbesar adalah 6. Terdapat algoritma yang dapat menemukan FPB dua bilangan *integer* a dan b dengan cara rekursif dengan menggunakan kasus dasar, yaitu ketika $b = 0$

   $$gcd(a, 0) = a$$

Karena semua bilangan *integer* habis membagi 0 dan a habis membagi dirinya sendiri sehingga $gcd(a,0) = a$. Sedangkan pada kasus umum, yaitu $b \neq 0$

$$gcd(a,b) = gcd\ (b, a\ mod\ b)$$

Untuk menentukan $gcd(a,b)$ dapat direduksi menjadi $gcd\ (b, a\ mod\ b)$ yang dilakukan berkali-kali hingga bertemu dengan kasus dasar untuk menentukan $gcd(a,b)$ (Sadikin, 2012).

Contoh:

Tentukan $gcd(68,19)$ dengan menggunakan kasus umum diperoleh,

$gcd(68,19) = gcd(19{,}68\ mod\ 19) = gcd(19{,}11)$

$gcd(19{,}11) = gcd(11{,}19\ mod\ 11) = gcd(11{,}8)$

$gcd(3{,}2) = gcd(2{,}3\ mod\ 2) = gcd(2{,}1)$

$gcd(2{,}1) = gcd(1{,}2\ mod\ 1) = gcd(1{,}0)$

Aplikasikan pada kasus dasar

$gcd(1{,}0) = 1$

Karena itu $gcd(68,19) = 1$

b. Keterbagian

Keterbagian merupakan salah satu pokok bahasan dari teori bilangan yang berkaitan dengan sifat pembagian dalam matematika. Penjelasan mengenai definisi dan teorema yang berkaitan dengan keterbagian telah diberikan oleh banyak buku dengan berbagai bahasa yang berbeda. Berikut definisi dan teorema yang menjelaskan tentang keterbagian.

Definisi keterbagian:

Untuk setiap $a, b \in \mathbb{Z}$ dengan $a \neq 0$. a dikatakan habis membagi b jika ada $k \in \mathbb{Z}$ yang memenuhi $a = k \cdot b$ dan dinotasikan $a|b$ (Irawan, 2014).

Contoh:

$2|10$ karena terdapat bilangan bulat 5 sehingga $10 = 2 \cdot 5$

Algoritma keterbagian:

Jika $a, b \in \mathbb{Z}$, $a > 0$ maka ada bilangan $q, r \in \mathbb{Z}$ yang tunggal sehingga $b = qa + r$, untuk $0 \leq r < a$. Bilangan bulat q disebut hasil bagi dan r disebut sisa pembagan a oleh b (Irawan, 2014).

Bukti Bagian 1:

Akan dibuktikan bahwa $S \neq \emptyset$. $S = \{b - aq | q \in \mathbb{Z}, b - aq \geq 0\}$ karena bilangan bulat $a \geq 1$, maka $|b|a \geq |a|$. Akibatnya $b - (-|b|)a = b + |b|a \geq b + |b| \geq 0$. Dengan memilih $x = -|b|$, berakibat $(b - xa) \in S$. Hal ini berarti $S \neq \emptyset$ Sehingga S memiliki anggota terkecil misalnya r. Berdasarkan definisi himpunan S, maka terdapat bilangan bulat q yang memenuhi $r = b - aq \geq 0$. Jadi $b = qa + r, r \geq 0$.

Bagian 2:

Akan dibuktikan $0 \leq r < a$, andaikan $r \geq a$ berlaku

$r - a \geq 0$

$(b - qa) - a \geq 0$

$b - (q + 1)a \geq 0$

Maka $b - (r + 1)a \in S$ sehingga $r - a \in S$

Karena $a > 0$ maka $r - a < r$, kontradiksi dengan pengandaian $r \geq a$, maka terbukti bahwa $r < a$.

Bagian 3:

Kemudian akan dibuktikan bahwa q dan r tunggal. Andaikan tidak tunggal maka,

$q_1, r_1 \in \mathbb{Z}$ sehingga $a = bq_1 + r_1 \cdots$

$q_2, r_2 \in \mathbb{Z}$ sehingga $a = bq_2 + r_2 \cdots$

Ingat $q_2 \neq q_1, r_1 \neq r_2$ misal $r_1 > r_2$

Maka $bq_1 + r_1 = bq_2 + r_2$

$r_1 - r_2 = bq_2 - bq_1$

$r_1 - r_2 = (q_2 - q_1)b$

Menggunakan definisi keterbagian diperoleh $p|r_1 - r_2$.

$0 \leq r_1 < a, 0 \leq r_2 < a$ terdapat dua kemungkinan bahwa $r_1 - r_2 < a$ dan $r_1 - r_2 > -p$ artinya $-a < r_1 - r_2 < a$.

1. $-a < r_1 - r_2 < 0$ maka $r_1 - r_2 > 0$ dan $r_1 - r_2 < p$ sehingga $a \nmid |r_1 - r_2$. Kontradiksi dengan pengandaian $r \geq a$.
2. $0 < r_1 - r_2 < a$ maka $r_1 - r_2 > 0$ dan $r_1 - r_2 < p$ sehingga $p \nmid |r_1 - r_2$. Kontradiksi dengan pengandaian $r \geq a$.
3. $r_1 - r_2 = 0$ maka,

   $r_1 - r_2 = (q_2 - q_1)a$

   $0 = (q_2 - q_1)$

   $q_2 = q_1$ kontradiksi dengan pengandaian $r \geq a$, karena $q_2 = q_1$

Sehingga terbukti bahwa q dan r tunggal.

Contoh:

1. $a = 15, b = 8$

   $15 = (0)8 + 15$

   $15 = (1)8 + 7$

   $15 = (2)8 + (-1)$

   $15 = (-1)8 + 23$

   Karena $r < a$ maka yang memenuhi adalah $15 = (1)8 + 7$

2. $a = -3, -2{,}65$ dibagi oleh $b = -6$

   $-3 = (1) - 6 + 3$

   $-2 = (1) - 6 + 4$

   $65 = (-10)(-6) + 5$

2.3.2 Aritmatika Modulo

Aritmatika modulo digunakan agar operasi aritmatika selalu menghasilkan *integer* pada lingkup yang sama sehingga proses transformasi penyandian memiliki pasangan *symbol* yang digunakan. Misalkan pada kriptografi yang menggunakan alphabet latin "A" sampai "Z", petakan terlebih dahulu $\{A, \cdots, Z\}$ menjadi $\{0, \cdots, 25\}$. Operator yang digunakan pada aritmatika modulo adalah mod. Operasi modular mengembalikan r yang merupakan sisa bagi atas operasi a dibagi n dinotasikan dengan

$$a \bmod n = r$$

Misalkan a dan m adalah bilangan bulat dengan $m > 0$. Operasi $a \bmod m$ memberikan sisa jika a dibagi dengan m. Dengan kata lain $a \bmod m = r$ sedemikian sehingga $a = mq + r$ dengan $0 \leq r < m$ (Munir, 2010).

Contoh:

1. $23\ mod\ 5$

   23 dibagi 5 adalah 4 sisa 3, $23 = (5 \times 4) + 3$. Jadi $23\ mod\ 5 = 3$

2. $-22\ mod\ 8$

   -22 dibagi 8 adalah -2 dengan sisa 6, $-22 = (8 \times -2) - 6$. Jadi $-22\ mod\ 8 = -6$, supaya bernilai positif -6 ditambah dengan nilai modulo 8 menghasilkan 2. Jadi $-22\ mod\ 8 = 2$

   a. Kongruensi

      Bilangan *integer* a dan b disebut kongruensi pada modulo n apabila memiliki sisa bagi yang sama. Misalkan a dan b adalah *integer* dan n merupakan *integer* positif. $a \equiv b(mod\ n)$ jika n membagi habis $a - b$. Jika $a - b$ tidak membagi n maka dikatakan bahwa a tidak kongruen dengan $b(mod\ n)$ atau dapat ditulis $a \not\equiv b(mod\ n)$ (Sadikin, 2012). Jika $n > 0$ dan $n|(a - b)$ maka terdapat suatu bilangan bulat t sehingga $a - b = nt$. Sehingga $a \equiv b(mod\ n)$ dapat dinyatakan sebagai $a - b = nt$, sama artinya dengan $a \equiv b(mod\ n)$ atau beda antara a dan b merupakan kelipatan n. Jadi $a \equiv b(mod\ n)$ dapat juga dinyatakan dengan $a = nt + b$, yaitu $a = b$ ditambah kelipatan n (Irawan, 2014).

   b. Contoh Kongruensi

      $18 \equiv 6(mod\ 4)$, karena $18 - 6 = 12$ yang merupakan kelipatan dari 4 sehingga 4 habis membagi 12

2.3.3 Definisi Matriks

Matriks terbentuk dari susunan skalar elemen-elemen dalam bentuk baris dan kolom. Elemen-elemen penyusun matriks terdiri dari bilangan-bilangan bulat. *Ordo* merupakan ukuran matriks berdasarkan banyaknya jumlah baris dan kolom. Kemudian nama matriks ditulis dengan huruf kapital seperti A. Misalkan matriks A dengan *ordo* $m \times n$ di mana m baris dan n kolom adalah:

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Entri a_{ij} merupakan elemen matriks dari baris ke-i dengan $i = 1,2,3, \dots, m$ dan kolom ke-j dengan $j = 1,2,3, \dots, n$. $A = [a_{ij}]$ disebut sebagai notasi matriks secara ringkas. Jika $m = n$ maka disebut sebagai matriks bujursangkar (*square matrix*) (Munir, 2010).

Contoh:

$$A = \begin{bmatrix} 3 & 1 \\ 4 & 5 \\ 2 & 1 \end{bmatrix}$$

Disebut dengan matriks A ordo 3×2 dengan 3 susunan baris elemen, yaitu $(3,1), (4,5), (2,1)$.

a. Jenis-Jenis Matriks

   Terdapat beberapa jenis matriks khusus berdasarkan elemen-elemen yang membangun sebuah matriks. Seperti matriks diagonal, matriks identitas, matriks segitiga bawah dan matriks segitiga atas. Namun pada algoritma *Hill Cipher* matriks khusus yang digunakan terdiri dari,

matriks bujursangkar, matriks identitas, matriks *adjoin* dan matriks *transpose*.

i. Matriks Persegi (*Square Matrix*)

Matriks bujur sangkar (persegi) merupakan matriks yang memiliki jumlah baris dan kolom nya sama $(n \times n)$ atau banyaknya baris sama dengan banyaknya kolom yang terdapat pada matriks tersebut. Matriks persegi disebut juga dengan matriks berordo n (Munir, 2010).

Contoh:

$$B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}$$

ii. Matriks *Transpose*

Matriks *transpose* merupakan matriks yang diperoleh dengan menukarkan baris-baris dan kolom-kolom. Misalkan $A = [a_{ij}]$ berukuran $m \times n$, maka *transpose* dari matriks A adalah matriks berukuran $n \times m$ yang dituliskan dengan A^T (Munir, 2010).

Jika,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & A_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Maka,

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & A_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

Contoh:

Misalkan diberikan matriks A

$$A = \begin{bmatrix} 3 & 5 \\ 2 & 1 \\ 2 & 0 \end{bmatrix}$$

Maka diperoleh A^T

$$A^T = \begin{bmatrix} 3 & 2 & 2 \\ 5 & 1 & 0 \end{bmatrix}$$

iii. Matriks Identitas

Matriks identitas merupakan matriks persegi yang diagonal utamanya terdiri dari bilangan 1 dan yang lainnya nol (Munir, 2010).

Contoh :

$$P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

b. Operasi Matriks

Operasi pada matriks yang digunakan pada algoritma *Hill Cipher* adalah operasi penjumlahan dan perkalian dua buah matriks, serta perkalian matriks dengan skalar.

1. Penjumlahan dua buah matriks

Penjumlahan dua buah matriks dapat dilakukan jika ukurannya sama. Misalkan $A = [a_{ij}]$ dan $B = [b_{ij}]$ masing-masing dengan ukuran $m \times n$, sehingga penjumlahan $A + B$ menghasilkan matriks $C = [c_{ij}]$ merupakan matriks berukuran $m \times n$ dan elemen-elemennya memenuhi

$$c_{ij} = a_{ij} + b_{ij}$$

dengan $i = 1,2,3, \dots, m$ dan $j = 1,2,3, \dots, n$ (Munir, 2010)

Contoh:

$$\begin{bmatrix} 0 & 1 & 4 \\ -1 & 2 & 0 \\ 3 & 2 & 1 \end{bmatrix} + \begin{bmatrix} 4 & 2 & 3 \\ 2 & -1 & 6 \\ -2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 0+4 & 1+2 & 4+3 \\ -1+2 & 2-1 & 0+6 \\ 3-2 & 2+4 & 1+3 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 3 & 7 \\ 1 & 1 & 6 \\ 1 & 6 & 4 \end{bmatrix}$$

2. Perkalian dua buah matriks

Dua buah matriks dapat dikalikan jika jumlah kolom matriks pertama sama dengan jumlah baris matriks kedua. Misalkan $A = [a_{ij}]$ adalah matriks $m \times n$ dan $B = [b_{ij}]$ merupakan matriks $n \times p$. Maka, perkalian A dan B dilambangkan dengan AB, menghasilkan matriks $C = [c_{ij}]$ dengan ukuran $m \times p$ yang elemen - elemennya adalah (Munir, 2010),

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

Contoh:

Misalkan A adalah matriks ordo 2×2 dan B matriks ordo 2×1 dengan

$$A = \begin{bmatrix} 10 & 15 \\ 9 & 7 \end{bmatrix}, \; B = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

3. Perkalian matriks dengan skalar

Misalkan jika A merupakan matriks ordo $m \times n$ dengan $i = 1,2,3, \dots, n$ dan $j = 1,2,3, \dots, m$ dan k adalah sebuah skalar. Maka perkalian matriks A dengan skalar k adalah dengan mengalikan setiap

matriks dengan k (Munir, 2010),

$$kA = k[a_{ij}] = [ka] = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \vdots & \vdots & & \vdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}$$

Contoh:

Misalkan matriks A berordo 2×2 dan k skalar dengan

$$A = \begin{bmatrix} 10 & 15 \\ 9 & 7 \end{bmatrix}, k = 4$$

Maka,

$$kA = 4\begin{bmatrix} 10 & 15 \\ 9 & 7 \end{bmatrix} = \begin{bmatrix} 10 \times 4 & 15 \times 4 \\ 9 \times 4 & 7 \times 4 \end{bmatrix} = \begin{bmatrix} 40 & 60 \\ 36 & 28 \end{bmatrix}$$

c. Determinan Matriks

Misalkan A matriks persegi. Fungsi determinan A biasanya disingkat dengan determinan A dinyatakan dengan $det(A)$ sebagai jumlah semua hasil kali elemen bertanda dari A.

Misalkan matriks A dengan ukuran 2×2, tentukan $det(A)$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$det(A) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Hitung determinan dari matriks persegi A berukuran 3×3, misalkan

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$det(A) = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$

Contoh 1:

Misalkan matriks A dengan ukuran 2×2

$A = \begin{bmatrix} 1 & -1 \\ 2 & 3 \end{bmatrix}$

$det(A) = (1 \cdot 3 - (-1) \cdot 2) = (3 + 2) = 5$

Contoh 2:

Misalkan matriks $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}$

$det(A) = 1\begin{vmatrix} 2 & 3 \\ 4 & 9 \end{vmatrix} - 1\begin{vmatrix} 1 & 3 \\ 1 & 9 \end{vmatrix} + 1\begin{vmatrix} 1 & 2 \\ 1 & 4 \end{vmatrix}$

$= 1(6) - 1(6) + 1(2)$

$det(A) = 2$

Determinan matriks pada algoritma *Hill Cipher* digunakan untuk menentukan invers matriks yang digunakan sebagai kunci ketika melakukan proses dekripsi (Anton, 1987).

2.3.4 Kongruensi Matriks

Misalkan A dan B adalah matriks $n \times k$ dengan unsur-unsurnya bilangan bulat, unsur ke (i, j) berturut-turut adalah a_{ij} dan b_{ij}. A dikatakan kongruensi dengan B modulo m, jika $a_{ij} \equiv b_{ij}(mod\ m)$ untuk setiap pasangan (i, j) dengan $1 \leq i \leq n$ dan $i \leq j \leq k$ dan dinotasikan dengan $A \equiv B(mod\ m)$ (Irawan, 2014).

Contoh:

1. $\begin{bmatrix}34 & 46\\23 & 29\end{bmatrix} \equiv \begin{bmatrix}8 & 7\\10 & 3\end{bmatrix} (mod\ 13)$

2. $\begin{bmatrix}-20 & 5 & 39\\15 & 7 & 58\\-62 & 12 & 41\end{bmatrix} \equiv \begin{bmatrix}1 & 5 & 4\\1 & 0 & 2\\1 & 5 & 6\end{bmatrix} (mod\ 7)$

a. Invers Modulo Matriks

Menentukan invers dari matriks A yaitu $\bar{A}$ sedemikian sehingga $\bar{A}$A $\equiv$ $I(mod\ m)$ dimana I adalah matriks identitas.

Definisi: jika Ā dan A adalah matriks $n \times n$ dari bilangan-bilangan bulat, dan ĀA $\equiv$ AA $\equiv$ $I(mod\ m)$ dimana:

$$\begin{bmatrix}1 & 0 & \cdots & 0\\0 & 0 & \cdots & 0\\\vdots & \vdots & \vdots & \vdots\\0 & 0 & \cdots & 1\end{bmatrix}$$

Merupakan matriks identitas berorde n, maka $\bar{A}$ dikatakan invers dari A modulo m.

Jika $\bar{A}$ invers dari A dan $B \equiv \bar{A}(mod\ m)$, maka B juga invers dari A karena $BA \equiv \bar{A}A \equiv I(mod\ m)$. Sebaliknya, jika B_1 dan B_2 keduanya invers dari A maka $B_1 \equiv B_2(mod\ m)$. Sehingga $B_1A \equiv B_2A \equiv I(mod\ m)$, diperoleh $B_1AB_1 \equiv B_2AB_2(mod\ m)$. Karena $AB_1 \equiv I(mod\ m)$, dapat disimpulkan bahwa $B_1 \equiv B_2(mod\ m)$ (Irawan, 2014).

Contoh:

Misalkan matriks $A\begin{bmatrix}3 & 4\\1 & 2\end{bmatrix}$, maka $\bar{A} = \begin{bmatrix}1 & 3\\2 & 4\end{bmatrix}$ adalah invers dari $A(mod\ 5)$ sebab,

$A\bar{A} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 11 & 25 \\ 5 & 11 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\ 5)$

Teorema

Misalkan $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ merupakan matriks bilangan bulat sedemikian sehingga $\Delta = \det A = ad - bc$ dengan relatif prima terhadap bilangan bulat positif m, maka $A = \bar{\Delta}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dimana $\bar{\Delta}$ adalah invers dari Δ modulo m, dan $\bar{A}$ adalah invers dari A modulo m.

Bukti:

Untuk menunjukkan bahwa matriks $\bar{A}$ merupakan invers dari A modulo m, cukup menunjukkan bahwa $A\bar{A} \equiv \bar{A}A \equiv I(mod\ m)$.

$A\bar{A} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}\bar{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv \bar{\Delta}\begin{bmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{bmatrix}$

$\equiv \bar{\Delta}\begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I(mod\ m)$ dan

$\bar{A}A \equiv \bar{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \bar{\Delta}\begin{bmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{bmatrix}$

$\equiv \bar{\Delta}\begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I(mod\ m)$

dimana $\bar{\Delta}$ adalah invers dari $\Delta(mod\ m)$, yang terjadi karena $(\Delta, m) = 1$ (Irawan, 2014).

Contoh:

Misalkan $\begin{bmatrix} 5 & 3 \\ 7 & 8 \end{bmatrix}$ dengan demikian $\Delta = 5 \cdot 8 - 7 \cdot 3 = 19$, invers dari $\Delta = 19\ mod\ 11$ adalah $\bar{\Delta} = 7$ karena $\Delta\bar{\Delta} = 19 \cdot 7 = 133 \equiv 1(mod\ 11)$. Jadi, invers A adalah,

$\bar{A} = 7\begin{bmatrix} 8 & -3 \\ -7 & 5 \end{bmatrix} = \begin{bmatrix} 56 & -21 \\ -49 & 35 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 6 & 2 \end{bmatrix} (mod\ 11)$

Untuk menentukan rumus invers dari matriks $n \times n$ dimana n adalah bilangan bulat positif memerlukan adjoin dari suatu matriks.

b. Adjoin Matriks $n \times n$

Adjoin matriks $A_{n\times n}$ adalah matriks $n \times n$ dimana unsur (i, j) adalah C_{ji}, dengan C_{ji} adalah -1^{i+j} kali determinan dari matriks yang diperoleh dengan menghapus baris ke-i dan kolom ke-j dari A. Adjoin A dinotasikan $adj(A)$. Misalnya matriks $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & A_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ dengan unsur-unsurnya a_{ij} dan $adj(A) = \begin{bmatrix} C_{11} & C_{21} & \cdots & C_{n1} \\ C_{12} & C_{22} & \cdots & C_{n2} \\ \vdots & \vdots & & \vdots \\ C_{1n} & C_{2n} & \cdots & C_{nn} \end{bmatrix}$. Dengan unsur-unsurnya C_{ji}. Dimana $C_{ji} = (-1)^{i+j} \left| M_{ij} \right|$ yang diperoleh dengan menghapus baris ke-i dan kolom ke-j dari matriks A (Irawan, 2014).

Contoh:

Misalkan matriks A dengan ordo 3×3

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}$$

Menentukan minor kofaktor,

$$M_{11} \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{vmatrix} = \begin{vmatrix} 2 & 3 \\ 4 & 9 \end{vmatrix} = (2 \cdot 9 - 3 \cdot 4) = (18 - 12) = 6,$$

$$C_{11}(-1)^{1+1} M_{12} = 6$$

$$M_{12}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 3\\ 1 & 9\end{vmatrix} = (1\cdot 9 - 3\cdot 1) = (9-3) = 6,$$

$$C_{12} = (-1)^{1+2}M_{12} = -6$$

$$M_{13}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 2\\ 1 & 4\end{vmatrix} = (1\cdot 4 - 2\cdot 1) = (4-2) = 2,$$

$$C_{13} = (-1)^{1+3}M_{13} = 2$$

$$M_{21}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 4 & 9\end{vmatrix} = (1\cdot 9 - 1\cdot 4) = (9-4) = 5,$$

$$C_{21} = (-1)^{2+1}M_{21} = -5$$

$$M_{22}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 1 & 9\end{vmatrix} = (1\cdot 9 - 1\cdot 1) = (9-1) = 8,$$

$$C_{22} = (-1)^{2+2}M_{22} = 8$$

$$M_{23}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 1 & 4\end{vmatrix} = (1\cdot 4 - 1\cdot 1) = (4-1) = 3,$$

$$C_{23} = (-1)^{2+3}M_{23} = -3$$

$$M_{31}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 2 & 3\end{vmatrix} = (1\cdot 3 - 1\cdot 2) = (3-2) = 1,$$

$$C_{31} = (-1)^{3+1}M_{31} = 1$$

$$M_{32}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 1 & 3\end{vmatrix} = (1\cdot 3 - 1\cdot 1) = (3-1) = 2,$$

$$C_{32} = (-1)^{3+2}M_{32} = -2$$

$$M_{33}\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{vmatrix} = \begin{vmatrix}1 & 1\\ 1 & 2\end{vmatrix} = (1\cdot 2 - 1\cdot 1) = (2-1) = 1,$$

$$C_{33} = (-1)^{3+3}M_{33} = 1$$

Diperoleh kofaktor A,

$$\begin{bmatrix} 6 & -6 & 2 \\ -5 & 8 & -3 \\ 1 & -2 & 1 \end{bmatrix}$$

Sehingga adjoin A,

$$adj(A) = \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix} = \begin{bmatrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{bmatrix}$$

Teorema:

Jika A adala matriks $n \times n$ dengan $\det A \neq 0$, maka $A\ (adj\ A) = (\det A)I$.

Bukti:

Misalkan $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ dimana $\det A \neq 0$

$$A\ (adj\ A) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i1} & & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} C_{11} & C_{21} & \cdots C_{j1} & \cdots & C_{n1} \\ C_{12} & C_{22} & \cdots C_{j2} & \cdots & C_{n2} \\ \vdots & & \vdots & & \vdots \\ C_{1n} & C_{2n} & \cdots C_{jn} & \cdots & C_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} |A| & 0 & \cdots & 0 \\ 0 & |A| & \cdots & 0 \\ 0 & 0 & \cdots & |A| \end{bmatrix}$$

$$= |A| \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{bmatrix} = |A| \cdot I = (\det A)I$$

Sehingga terbukti (Irawan, 2014).

Teorema:

Jika A adala matriks $n \times n$ dengan unsur-unsurnya bilangan bulat dan m adalah bilangan bulat positif, sedemikian sehingga $(det\, A, m) = 1$, maka matriks $\bar{A} = \bar{\Delta}\,(adj\, A)$ adalah invers dari A modulo m, dimana $\bar{\Delta}$ adalah invers dari $\Delta = \det A$ modulo m.

Bukti:

Jika $(det\, A, m) = 1$, maka $\det A \neq 0$ diperoleh $A\,(adj\, A) = (det\, A\,)I = \Delta I$. Karena $(det\, A, m) = 1$, maka terdapat $\bar{\Delta}$ adalah invers dari $\Delta = det\, A$ modulo m. Sehingga,

$$A\,(\Delta\, adj\, A) \equiv A(\text{adj } A)\,\bar{\Delta} \equiv \Delta\,\bar{\Delta}\, I \equiv I(mod\, m)$$

dan

$$\bar{\Delta}\,(adj\, A)A \equiv \bar{\Delta}(\text{adj } A \cdot A) \equiv \bar{\Delta}\,\Delta\, I \equiv I(mod\, m)$$

Ini menunjukkan bahwa $A = \Delta\,(adj\, A)$ adalah invers dari A modulo m (Munir, 2010).

Contoh:

Diketahui

$A = \begin{bmatrix} 2 & 2 & -2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$, sehingga $\Delta = 4$ dan $\bar{\Delta} \equiv 3(mod\ 11)$

$$\bar{A} = \bar{\Delta}\,(adj\, A) = 3\begin{bmatrix} -1 & -14 & 10 \\ 2 & 12 & -8 \\ -1 & -2 & 2 \end{bmatrix} = \begin{bmatrix} -3 & -42 & 30 \\ 6 & 36 & -24 \\ -3 & -6 & 6 \end{bmatrix} \equiv$$

$$\begin{bmatrix} 8 & 2 & 8 \\ 6 & 3 & 9 \\ 8 & 5 & 6 \end{bmatrix} (mod\ 11)$$

2.4 Algoritma *ElGamal*

Algoritma *ElGamal* merupakan algoritma kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Algoritma ini didasarkan atas masalah logaritma diskrit. Algoritma *ElGamal* terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok *plaintext* dan menghasilkan blok-blok *ciphertext* yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti (Sadikin, 2012).

Pada proses enkripsi dan dekripsi menggunakan algoritma *ElGamal* terdapat besaran perlu dipenuhi. Berdasarkan sifatnya besaran tersebut dibagi menjadi dua, yaitu besaran yang bersifat tidak rahasia dan rahasia. Besaran yang bersifat tidak rahasia berarti dapat diketahui oleh pengirim dan penerima sebagai berikut,

1. Bilangan prima p
2. Akar Primitif α dengan $\alpha < p$
3. β yang diperoleh dari perhitungan $\beta = \alpha^d mod\ p$
4. Kunci publik yang terdiri dari (p, α, β)
5. *Ciphertext* a dan b

Kemudian besaran yang bersifat rahasia hanya diketahui oleh penerima saja atau pengirim saja seperti,

1. *Plaintext P*
2. Sembarang bilangan bulat d dengan $1 \leq d \leq p-2$
3. Pilih acak elemen matriks r dengan $r \in \{0,1,2,\cdots,p-2\}$

4. Kunci privat d

2.4.1 Pembentukan Kunci Algoritma *ElGamal*

Langkah pertama yang dilakukan pembangkit kunci adalah dengan memilih sebuah bilangan prima p untuk membentuk grup perkalian $(\mathbb{Z}_p^*,\times)$. Kemudian pilih akar primitif α pada $(\mathbb{Z}_p^*,\times)$. α merupakan akar prmitif $(\mathbb{Z}_p^*,\times)$ jika *order* α dinotasikan sebagai $\langle\alpha\rangle = p-1$. Selanjutnya memilih sebuah bilangan bulat d yang memenuhi $1 \leq d \leq p-2$ dan menghitung $\beta = \alpha^d mod\ p$. Pada langkah terakhir pembentukan kunci algoritma *ElGamal* mendapatkan kunci publik (p, α, β) dan kunci privat d (Sadikin, 2012).

Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi, keuntungan menggunakan algoritma kriptografi kunci publik adalah tidak ada serta tidak ada kepastian keamanan jalur pengiriman pesan yang digunakan (Sadikin, 2012).

2.4.2 Enkripsi dan Dekripsi Algoritma *ElGamal*

Pada proses enkripsi pesan menggunakan kunci publik (p, α, β) dan sebarang bilangan acak rahasia $d \in \{0,1,\ldots,p-2\}$. Misalkan P adalah pesan yang akan dikirim maka P diubah ke dalam blok-blok karakter dan setiap karakter diubah ke dalam kode ASCII 256, sehingga diperoleh *plaintext* $p_1, p_2, \ldots, p_n$.

dengan $p_1 \in \{1,2,\ldots,p-2\}$, dengan $i = 1,2,\ldots,n$. Proses enkripsi pada algoritma *ElGamal* dilakukan dengan menghitung,

$a = \alpha^r \ mod \ p$ dan $b = P \times \beta^r \ mod \ p$

dengan $r \in \{0,1,\ldots,p-2\}$ acak. Diperoleh *ciphertext* (a,b) (Sadikin, 2012).

Bilangan acak r ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya, tetapi nilai r hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan. Setelah menerima *ciphertext* (a,b), proses selanjutnya adalah mendekripsi *ciphertext* menggunakan kunci publik p dan kunci rahasia d. Sehingga *plaintext P* dapat diperoleh dari *ciphertext* menggunakan kunci rahasia d.

Contoh Perhitungan Algoritma *ElGamal*

1. Pembentukan kunci *ElGamal*

   a. Memilih bilangan prima $p = 83$ untuk membentuk grup perkalian $(\mathbb{Z}_{83}^*,\times)$.

   b. Kemudian pilih akar primitif pada $(\mathbb{Z}_{83}^*,\times)$ maka $\phi(83) = 82$, karena 83 merupakan bilangan prima. Sehingga terdapat 82 kandidat akar primitif pada $(\mathbb{Z}_{83}^*,\times)$. Misal dipilih $\alpha = 19$.

   c. Memilih sembarang bilangan bulat $d = 63$ yang memenuhi $1 \leq d \leq p-2$. Pada algoritma *ElGamal* memiliki kunci publik yang terdiri dari (p,α,β) sehingga untuk melengkapi kunci publik perlu menentukan β menggunakan persamaan $\beta = \alpha^d \ mod \ p$ sebagai berikut,

$\beta = \alpha^d \ mod \ p$

$= 19^{63} \ mod \ 83$

$= (19^3)^{21} mod \ 83$

$= 53^{21} mod \ 83$

$= (53^3)^7 mod \ 83$

$= 58^7 mod \ 83$

$= 58 \times (58^2)^3 mod \ 83$

$= 58 \times 44^3 mod \ 83$

$= 58 \times 26 \ mod \ 83$

$= 14$

Sehingga diperoleh kunci publik $(p, \alpha, \beta) = (83,19,14)$ dan kunci privat $d = 63$

2. Melakukan Enkripsi dan Dekripsi

$a = \alpha^r mod \ p = 19^2 mod \ 83 = 29$

$b = P \times \beta^r \ mod \ p = 5 \times 14^2 mod \ 83 = 980 \ mod \ 83 = 67$

$c_1 = (a, b) = (29,67)$

$(a^x)^{-1} = a^{p-1-d} \ mod \ 83$

$= 29^{83-1-63} \ mod \ 83$

$= 29^{19} \ mod \ 83$

$= 29 \times (29^3)^6 mod \ 83$

$= 29 \times 70^6 \ mod \ 83$

$= 29 \times (70^2)^3 mod \ 83$

$= 29 \times 3^3 \ mod \ 83$

$P = b \times (a^x)^{-1} \ mod \ p$

$= 67 \times 36 \ mod \ 83$

$= 2412 \ mod \ 83$

$= 5$

$$= 29 \times 27 \; mod \; 83$$

$$= 783 \; mod \; 83$$

$$= 36$$

$$a = \alpha^r mod \; p = 19^4 mod \; 83 = 11$$

$$b = P \times \beta^r \; mod \; p = 8 \times 14^4 mod \; 83 = 307328 \; mod \; 83 = 62$$

$$c_2 = (a, b) = (11{,}62)$$

$$(a^x)^{-1} = a^{p-1-d} \; mod \; 83$$

$$= 11^{83-1-63} \; mod \; 83$$

$$= 11^{19} \; mod \; 83$$

$$= 11 \times (11^3)^6 mod \; 83$$

$$= 11 \times 3^6 mod \; 83$$

$$= 11 \times (3^2)^3 mod \; 83$$

$$= 11 \times 9^3 mod \; 83$$

$$= 11 \times 65 \; mod \; 83$$

$$= 715 \; mod \; 83$$

$$= 51$$

$$P = b \times (a^x)^{-1} \; mod \; p$$

$$= 62 \times 51 \; mod \; 83$$

$$= 3162 \; mod \; 83$$

$$= 8$$

$$a = \alpha^r mod \; p$$

$$= 19^{12} mod \; 83$$

$$= (19^2)^6 \; mod \; 83$$

$$= 29^6 mod \; 83$$

$$= (29^2)^3 \; mod \; 83$$

$$= 11^3 mod \; 83$$

$$b = P \times \beta^r \; mod \; p$$

$$= 17 \times 14^{12} mod \; 83$$

$$= 17 \times (14^2)^6 mod \; 83$$

$$= 17 \times 30^6 mod \; 83$$

$$= 17 \times (30^2)^3 mod \; 83$$

$$= 17 \times 70^3 mod \; 83$$

$= 11 \times 11^2 mod\ 83$

$= 11 \times 38\ mod\ 83$

$= 418\ mod\ 83$

$= 3$

$= 17 \times 70 \times 70^2\ mod\ 83$

$= 17 \times 70 \times 3\ mod\ 83$

$= 17 \times 210\ mod\ 83$

$= 17 \times 44\ mod\ 83$

$= 748\ mod\ 83$

$= 1$

$c_3 = (a, b) = (3,1)$

$(a^x)^{-1} = a^{p-1-d}\ mod\ 83$

$= 3^{83-1-63}\ mod\ 83$

$= 3^{19}\ mod\ 83$

$= 3 \times (3^3)^6 mod\ 83$

$= 3 \times 27^6\ mod\ 83$

$= 3 \times (27^2)^3 mod\ 83$

$= 3 \times 65^3 mod\ 83$

$= 3 \times 65 \times 65^2 mod\ 83$

$= 3 \times 65 \times 75\ mod\ 83$

$= 14625\ mod\ 83$

$= 17$

$P = b \times (a^x)^{-1}\ mod\ p$

$= 1 \times 17\ mod\ 83$

$= 17\ mod\ 83$

$= 17$

$a = \alpha^r mod\ p = 19^1 mod\ 83 = 19$

$b = P \times \beta^r\ mod\ p = 3 \times 14^1 mod\ 83 = 42\ mod\ 83 = 42$

$c_4 = (a, b) = (19{,}42)$

$(a^x)^{-1} = a^{p-1-d}\ mod\ 83$

$= 19^{83-1-63}\ mod\ 83$

$= 19^{19}\ mod\ 83$

$= 19 \times (19^3)^6 mod\ 83$

$= 19 \times 53^6 mod\ 83$

$= 19 \times (53^2)^3 mod\ 83$

$= 19 \times 70^3 mod\ 83$

$= 19 \times 70 \times 70^2 mod\ 83$

$= 19 \times 70 \times 3\ mod\ 83$

$= 3990\ mod\ 83$

$= 6$

$P = b \times (a^x)^{-1}\ mod\ p$

$= 42 \times 6\ mod\ 83$

$= 252\ mod\ 83$

$= 3$

2.5 Penggunaan Konsep Matematika pada Algoritma *ElGamal*

Algoritma *ElGamal* merupakan kriptografi dengan algoritma kunci publik yang menggunakan himpunan bilangan bulat, Sehingga dapat meningkatkan kesulitan pemecahan kunci. Berikut konsep matematika yang digunakan pada algoritma *ElGamal*.

2.5.1 Bilangan Prima

Bilangan prima merupakan bilangan bulat positif yang mempunyai peran penting dalam ilmu komputer dan matematika diskrit. Bilangan prima adalah bilangan bulat positif yang lebih dari satu yang hanya habis dibagi oleh satu,

dirinya sendiri. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin jauh dan mendalam. Banyak definisi yang berkembang berdasarkan bilangan prima. Pada kriptografi kunci publik menggunakan bilangan prima sebagai dasar pembentukan algoritma seperti pada algoritma *ElGamal.*

Sebuah bilangan bulat $p > 1$ disebut bilangan prima jika bilangan tersebut hanya memiliki pembagi 1 dan p. Bilangan bulat $p > 1$ yang bukan bilangan prima disebut bilangan komposit. Sehingga dapat disimpulkan bahwa sebuah bilangan bulat p disebut prima jika dari semua bilangan $2, 3, 4, \cdots, p-1$ tidak ada satupun yang membagi p. Karena bilangan yang mungkin membagi p hanya bilangan yang lebih kecil atau sama dengan p (Munir, 2010).

Contoh:

23 merupakan bilangan prima karena hanya habis dibagi satu dan 23. Karena bilangan prima harus lebih besar dari satu, maka baris bilangan prima dimulai dari 2, yaitu $2,3,5,7, \cdots$ seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.

Jumlah bilangan prima adalah tak hingga, namun semakin besar bilangan *integer* semakin jarang bilangan prima. Bukti secara informal sebagai berikut:

Asumsikan bahwa jumlah bilangan prima berhingga, sehingga terdapat bilangan prima besar p. Bentuk bilangan komposit P hasil perkalian semua bilangan prima sampai p yaitu $P = 2 \times 3 \times \cdots p$. Sekarang ambil sebuah bilangan prima $q \leq p$, q jelas habis membagi P. Misalnya q juga membagi $(P+1)$ maka q juga habis membagi $(P+1) - = P$. Ini melanggar fakta

bahwa yang habis membagi 1 hanya 1 jadi asumsi awal adalah salah, sehingga jumlah bilangan prima adalah tak berhingga (Sadikin, 2012).

a. Bilangan Relatif Prima

   Bilangan bulat a dan b dikatakan relatif prima jika dan hanya jika $gcd(a, b) = 1$. Bilangan-bilangan bulat $a_1, a_2, \cdots, a_n$ adalah pasangan relatif prima jika dan hanya jika $gcd(a_i, a_j) = 1$ untuk setiap i dan j dengan $i \neq j$ (Munir, 2010).

   Contoh:

   1. Bilangan 20 dan 3 adalah relatif prima karena

      $gcd(20,3) = 1$

      Atau dapat ditulis $2 \cdot 20 + (-13) \cdot 3 = 1$

      Dengan $m = 2$ dan $n = 13$

   2. Bilangan 20 dan 5 tidak relatif prima karena

      $gcd(20,5) = 5 \neq 1$

      Sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \cdot 20 + n \cdot 5 = 1$

b. Algoritma Euclidean

   Algoritma ini digunakan untuk mencari nilai pembagi persekutuan terbesar (gcd) dari dua bilangan bulat yang relatif prima. Algoritma ini didasarkan pada pernyataan bahwa ada dua buah bilangan bulat tak negatif yakni m dan n di mana nilai $m \geq n$ (Munir, 2010).

Contoh:

1. Tentukan $gcd\ (108, 360)$

   $360\ mod\ 108\ =\ 36\ 108\ mod\ 36\ =\ 0$

   Jadi $gcd\ (108, 360)\ =\ 36$

2. Tentukan $gcd\ (45, 13)$

   $45\ mod\ 13\ =\ 6$

   $13\ mod\ 6\ =\ 1$

   $6\ mod\ 1\ =\ 0$

   Jadi $gcd\ (45, 13)\ =\ 1$. Apabila gcd dari m dan $n\ =\ 1$, maka m dan n disebut Relatif prima.

c. Fungsi ϕ-Euler

   Fungsi ϕ-Euler atau ditulis dengan $\phi(n)$ merupakan fungsi yang mengembalikan jumlah bilangan integer a yang $0 < a < n$ dan a prima relatif dengan n (a disebut prima relatif dengan n bila $gcd(a, n) = 1$ (Sadikin, 2012).

   Contoh:

   1. $\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$

   2. $\phi(1000) = 10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3$

      $= \phi(2^3 \cdot 5^3) = \phi(2^3) \cdot \phi(5^3) = 2^3(2 - 1) \cdot 5^2(5 - 1)$

      $= 100 \cdot 1 \cdot 4 = 400$

d. Teorema Euler

   Jika $(a, p) = 1$ maka $a^{\phi(p)} \equiv 1(mod\ p)$ (Irawan, 2014).

Bukti:

Andaikan $r_1, r_2, \cdots, r_{\phi(p)}$ merupakan suatu sistem residu reduksi modulo p. Sehingga $ar_1, ar_2, \cdots, ar_{\phi(p)}$ juga merupakan sistem residu reduksi modulo p. Oleh sebab itu, untuk setiap r_i tentu ada ar_j sedemikian sehingga $r_i \equiv ar_j (mod\ p)$. Akibatnya bilangan – bilangan $ar_1, ar_2, \cdots, ar_{\phi(p)}$ tidak lain dari pada residu- residu modulo p dari $r_1, r_2, \cdots, r_{\phi(p)}$ walaupun urutannya mungkin saja tidak sama. Maka diperoleh $ar_1, ar_2, \cdots, ar_{\phi(p)} = r_1, r_2, \cdots, r_{\phi(p)} (mod\ p)$. Akibatnya $a^{\phi(p)}(r_1, r_2, \cdots, r_{\phi(p)}) \equiv r_1, r_2, \cdots, r_{\phi(p)} (mod\ p)$. Karena $(r_i, p) = 1$ maka $a^{\phi(p)}(r_1, r_2, \cdots, r_{\phi(p)}) \equiv 1 (mod\ p)$.

Contoh:

Tentukan dua digit terahir lambang bilangan desimal dari 23^{500}

Dapat dinyatakan dengan mancari x jika $23^{500} \equiv x(mod\ 100)$. Kemudian bentuk $23^{500} \equiv x(mod\ 100)$dapat dipecah menjadi $23^{500} \equiv x(mod\ 4)$ dan $23^{500} \equiv x(mod\ 25)$.

Menentukan x dari $23^{500} \equiv x(mod\ 4)$.

$23 \equiv 3(mod\ 4)$, maka $23^2 \equiv 9(mod\ 4)$, sehingga $23^{500} = (23^2)^{250}$

Dengan demikian $23^{500} = (23^2)^{250} \equiv 1^{250}(mod\ 4)$ atau $x \equiv 1(mod\ 4) - 4(mod\ 25)$, $23^{64}16(mod\ 25)$, $23^{128} \equiv 6(mod\ 25)$ dan $23^{256} \equiv 11(mod\ 25)$

Dengan demikian $23^{500} = 23^{256} \cdot 23^{128} \cdot 23^{64} \cdot 23^{32} \cdot 23^{16} \cdot 23^4$

$\equiv 11 \cdot 6 \cdot 16 \cdot (-4) \cdot 11 \cdot 16 (mod\ 25)$

$\equiv (-4) \cdot 6 \cdot (-4) \cdot 6 (mod\ 25)$

$\equiv 576 (mod\ 25) \equiv 1 (mod\ 25)$

$x \equiv 1 (mod\ 25)$

Dari hasil perhitungan a dan b, yaitu $x \equiv 1 (mod\ 4)$ dan $x \equiv 1 (mod\ 25)$, maka $x \equiv 1\big(mod(4 \cdot 25)\big) = x \equiv 1 (mod\ 100)$. Jadi $23^{500} \equiv 1 (mod\ 100)$, berarti dua digit terakhir lambang bilangan desimal dari 23^{500} adalah 0 1.

e. Teorema Fermat

Jika p adalah suatu bilangan prima dan $p|a$, maka

$$a^{p-1} \equiv 1 (mod\ p)$$

dimana p adalah bilangan bulat dan a adalah urutan bilangan yang lebih kecil dari *p.* Dapat diartikan bahwa misal terdapat bilangan bulat a, b dan c, maka $a \equiv b\ (mod\ c)$ berarti $c \mid (a - b)$. Maka teorema fermat di atas dapat ditulis $p|(a^{p-1} - 1)$ (Irawan, 2014).

Bukti:

Jika p bilangan prima dan $p|a$, maka $(p, a) = 1$. Maka jika$(p, a) \neq 1$, yaitu p dan a tidak relatif prima, maka p dan a memiliki faktor selain 1 dan p, sehingga bertentangan dengan yang diketahui bahwa p bilangan prima. Kemudian, karena $(p, a) = 1$ maka menurut teorema Euler didapat $a^{p-1} \equiv 1 (mod\ p)$. p bilangan prima berarti terdiri dari bilangan-bilangan bulat $0,1,2,3, \cdots, p-1$ yang tidak relatif prima dengan p hanyalah 0 sehingga $\{0,1,2,3, \cdots, p-1\}$ merupakan sistem residu.

Contoh:

Tentukan x jika $2^{250} \equiv x(mod\ 7)$ dan $0 \leq x < 7$. Karena 7 adalah bilangan prima, $(2,7) = 1$, dan $\phi(7) = 7 - 1 = 6$ maka,

$2^{\phi(7)} \equiv 1(mod\ 7)$

$2^6 \equiv 1(mod\ 7)$

$2^{250} = (2^6)^{41} \cdot 2^4 \equiv 1 \cdot 2^4(mod\ 7) \equiv 16(mod\ 7) \equiv 2(mod\ 7)$

Jadi, $x = 2$

2.5.2 Eksponensial

Banyak sistem kriptografi berbasis pada persoalan logaritma diskrit di antaranya adalah sistem kriptografi *ElGamal*. Dalam sebuah medan terbatas mencari eksponensial $g^a = h$ adalah mudah akan tetapi mecari logaritma $log_g(h) = a$ adalah sulit karena itu logaritma diskrit menjadi dasar pengembangan sistem kriptografi (Sadikin, 2012).

a. Eksponensial Modulo

Dalam sistem kriptografi operasi modulo yang sering dijumpai adalah eksponensial. Sistem kriptografi *ElGamal* dalam prosedur enkripsi dan dekripsinya menggunakan operasi eksponensial modulo. Eksponensial modulo adalah operasi dalam persamaan berikut

$$y = a^x mod\ n$$

Implementasi perhitungan eksponensial modulo secara cepat dan efisien dapat menggunakan algoritma *Square and Multiply* yang mengasumsikan eksponen x dalam bentuk biner sehingga

$$x = \sum_{i=0}^{l-1} x_i 2^i$$

Dengan l adalah panjang x dalam biner. Dengan x_i bernilai 0 atau 1, $0 \leq i \leq l-1$ (Sadikin, 2012).

b. Contoh Eksponensial Modulo

$2^{1234}\ mod\ 789$

$2^2 \equiv 4\ mod\ 789$

$2^4 = 4^2 \equiv 16\ mod\ 789$

$2^8 = 16^2 \equiv 256\ mod\ 789$

$2^{16} = 256^2 \equiv 49\ mod\ 789$

$2^{32} \equiv 34\ mod\ 789$

$2^{64} \equiv 367\ mod\ 789$

$2^{128} \equiv 559\ mod\ 789$

$2^{256} \equiv 37\ mod\ 789$

$2^{512} \equiv 580\ mod\ 789$

$2^{1024} \equiv 286\ mod\ 789$

Karena $1234 = 1024 + 128 + 64 + 16 + 2$ maka akan didapatkan

$2^{1234} = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481\ mod\ 789$

2.5.3 Persoalan Logaritma Diskrit

Tidak seperti eksponensial, invers eksponensial (atau disebut logaritma) pada sebuah grup perkalian merupakan permasalahan yang sulit diselesaikan. Beberapa sistem kriptografi bersandar pada kesulitan penyelesaian logaritma diskrit seperti sistem kriptografi *ElGamal*.

Fungsi logaritma diskrit sama dengan logaritma biasa, yaitu logaritma sebuah bilangan y untuk sebuah basis g adalah nilai eksponensial x terhadap basis g agar menghasilkan bilangan tersebut. Fungsi logaritma dapat dipresentasikan sebagai fungsi berikut,

$$log_g(y) = x \rightarrow g^x = y$$

(Sadikin, 2012).

a. Persoalan Logaritma Diskrit pada Grup Perkalian Terbatas

Grup perkalian terbatas dapat berupa medan terbatas yang dibentuk oleh bilangan prima $\mathbb{G} = (\mathbb{Z}_p^*, \times)$ jumlah elemen grup (*order* grup) adalah $|\mathbb{G}| = \phi(p) = p - 1$. Elemen pada grup dapat membangkitkan elemen lain dengan cara dipangkatkan sehingga membentuk grup siklik. Jumlah elemen yang dapat dibangkitkan oleh sebuah elemen disebut *order* dinotasikan dengan $\langle a \rangle$. Misalnya $a \in \mathbb{Z}_p^*$ maka $(\langle a \rangle)$ adalah integer positif i terkecil sehingga $a^i \equiv 1 \, mod \, p$. Jika $\langle a \rangle = p - 1$ maka a disebut akar primitif untuk $\mathbb{G} = (\mathbb{Z}_p^*, \times)$. Jumlah akar primitif pada sebuah grup $(\mathbb{Z}_p^*, \times)$ adalah $\phi(\phi(p)) = \phi(p - 1)$. Persoalan logaritma diskrit dapat di formulasikan sebagai berikut:

Tabel 2.2 Persoalan Logaritma Diskrit

Persoalan	**Logaritma diskrit**
Diberikan	grup $(\mathbb{Z}_p^*, \times)$, akar primitif $\alpha, y \in \mathbb{Z}_p^*$
Ditemukan	x sehingga $\alpha^x = y \, mod \, p$

Untuk menyelesaikan persoalan logaritma diskrit akar primitif α dapat dipangkatkan dengan nilai eksponensial dari 1 sampai $p-1$. x adalah nilai eksponensial yang memenuhi $\alpha^x = y \; mod \; p$ (Sadikin, 2012).

b. Contoh Persoalan Logaritma Diskrit

Tentukan x yang memenuhi $2^i \equiv 10 \; mod \; 13$. 2 merupakan akar primitif pada grup perkalian $(\mathbb{Z}_{13}^*,\times)$. Diketahui $g = 2$ dan digunakan grup perkalian $(\mathbb{Z}_{13}^*,\times)$. Nilai x dapat dicari dengan menghitung 2^i untuk $i = \{0, \cdots, 12\}$ berhenti ketika $2^i \equiv 10 \; mod \; 13$, nilai i yang memenuhi persamaan adalah nilai x yang dicari.

Tabel 2.3 Contoh Persoalan Logaritma Diskrit

i	1	2	3	4	5	6	7	8	9
$2^i mod \; 13$	2	4	8	3	6	12	11	9	5

Karena ketika $i = 10$ nilai $2^i \equiv 10 \; mod \; 13$ maka $\log_2(10) = 10$ pada $\mathbb{Z}_{13}^*$. Penyelesaian persoalan logaritma diskrit menjadi sulit ketika *order* grup perkalian besar. Bila *order* grup besar percobaan nilai eksponensial dari 1 sampai $p-1$ tidak efisien. Salah satu grup perkalian dengan nilai *order* sangat besar adalah grup perkalian $(\mathbb{Z}_p^*,\times)$ dengan p adalah bilangan prima besar (Sadikin, 2012).

2.6 Pengertian Kode ASCII

ASCII memiliki kepanjangan *American Standard Code for Information Interchange* merupakan format umum file teks pada komputer dan internet yang dikembangkan oleh *American National Standards Institute* (ANSI). ASCII terdiri

dari kode huruf dan simbol dalam suatu standar internasional seperti Hex dan Unicode, tetapi ASCII lebih bersifat universal. Kode ASCII digunakan pada komputer untuk mewakili karakter-karakter angka maupun huruf. Terdapat 95 karakter yang dapat dicetak melalui kode ASCII yaitu sebanyak 26 huruf alfabet kapital (A-Z), huruf alfabet kecil (a-z) sebanyak 26, karakter angka (0-9) sebanyak 10 dan 33 karakter khusus yang termasuk simbol matematika, tanda baca dan karakter spasi (Yusman, 2015).

Seiring dengan perkembangan teknologi kode ASCII semakin banyak karakter yang digunakan menjadi delapan bit sehingga ASCII dikenal dengan US ASCII-8. Terdiri dari bilangan biner dimulai dari 00000000 hingga 11111111 maka akan menghasilkan 256 karakter yang dimulai dari kode 0 hingga 255 dalam sistem bilangan desimal. Kode ASCII dari 0 sampai 127 digunakan untuk memanipulasi teks, sedangkan kode ASCII dari 128 sampai 225 untuk memanipulasi grafik. ASCII memiliki karakter kontrol yang dibagi menjadi lima kelompok sesuai dengan fungsinya yaitu, *Logical Communication*, *Device Control*, *Information Separator*, *Code Extention*, dan *Physical Communication* (Yusman, 2015). Sampai sekarang ASCII digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Berikut pengelompokan kode ASCII menjadi beberapa bagian:

1. Kode ASCII yang tidak terlihat simbolnya seperti kode 10 (Line Feed), 13 (Carriage return), 8 (Tab), 32 (Space).
2. Kode ASCII yang terlihat simbolnya seperti kode abjad $(A, \cdots, Z)$, numerik $(0, \cdots, 9)$, karakter khusus (~!@#$%^&*()_+?:”{}).

3. Kode ASCII yang tidak tercantum pada keyboard tetapi dapat ditampilkan biasanya digunakan untuk kode grafik.

2.6.1 Jenis-Jenis Kode ASCII

Berdasarkan penggunaannya pada media komunikasi kode ASCII dibagi menjadi dua jenis sebagai berikut,

a. Kode ASCII Standard

   Kode ASCII standard digunakan untuk mempresentasikan karakter angka, huruf serta tombol-tombol standar seperti Enter, Escape, Backspace space. Kemudian karakter-karakter yang tidak terdapat pada keyboard yang dapat diaktifkan dengan menggunakan tombol kombinasi Alt dan angka. Karakter dasar yang digunakan untuk melakukan komunikasi menggunakan internet seperti ACK (Acknowledge) dan ENQ (Enquiry). Ketika melakukan komunikasi dengan komputer yang terjadi adalah komputer mengirimkan ACK (Acknowledge) pada komputer lain. Kemudian komputer lain merespon sehingga akan membalas dengan mengirim ENQ (Enquiry).

b. Kode ASCII Extended

   Kode ASCII extended lebih banyak digunakan untuk mempresentsikan kode-kode tombol khusus, seperti kode pada tombol F1 sampai dengan F12 yang ada pada keyboard komputer. Oleh karena itu, kode ASCII extended terdiri dari kode ASCII yang diperluas sehingga dapat menampung kode ASCII yang tidak terdapat pada kode ASCII standar.

2.7 Kajian Agama

Merahasiakan pesan teks yang dikirimkan bertujuan agar pesan dapat tersampaikan kepada pihak yang tepat. Untuk menghindari serangan dari kriptanalis yang tidak bertanggung jawab maka pesan teks dirahasiakan dengan menggunakan ilmu pengetahuan yang dikenal dengan kriptografi. Sebagai makhluk yang hidup berdampingan sebagai sesama manusia sebaiknya dapat saling menjaga privasi. Segala sesuatu yang dapat melanggar privasi dapat dinilai dengan pengambilan, pengubahan, atau pengaksesan terhadap data pribadi tanpa izin terlebih dahuli pada pemiliknya. Islam mengatur pentingnya menjaga privasi sesama manusia. Dalam al-Qur'an surat an-Nur ayat 27, yaitu:

يَٰٓأَيُّهَاٱلَّذِيْنَءَامَنُوْالَاتَدْخُلُوْابُيُوتًاغَيْرَبُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوْاوَتُسَلِّمُوْاعَلَىٰٓ أَهْلِهَاۖ ذَٰلِكُمْ خَيْرٌلَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ﴿٢٧﴾

"*Wahai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat" (QS. an-Nur/18:27).*

Rasulullah Saw bersabda, "*Sampaikanlah amanat kepada orang yang memberi amanat kepadamu. Dan janganlah kamu berkhianat kepada orang yang mengkhianatimu*" (H.R. Tirmidzi).

Amanat merupakan pesan untuk disampaikan oleh orang yang diamanahi. Berdasarkan hadits di atas, terdapat pesan agung yang ingin disampaikan oleh baginda Nabi Muhammad Saw. yaitu menyampaikan amanat walaupun kepada orang yang telah berkhianat. Memang, menyampaikan amanat kepada orang yang telah mengkhianati sangatlah berat dilakukan. Sebagai seorang pengirim pesan tentunya memiliki rasa percaya kepada seorang pembawa pesan

miliknya. Oleh karena itu sebagai sesama muslim tidak seharusnya membuat orang lain merasakan kekecewaan. Begitu juga dalam hal pengiriman pesan melalui media komunikasi yang membutuhkan tingkat keamanan yang tinggi. Ilmu kriptografi sangat berperan dalam pengamanan pesan dengan menggunakan algoritma dengan tingkat kerumitan yang tinggi. Sesuai dengan hadits Nabi Muhammad Saw. tentang menjaga amanat yang telah disampaikan maka ilmu kriptografi merupakan bentuk perkembangan media komunikasi sesuai dengan hadits.

BAB III

PEMBAHASAN

Algoritma *Hill Cipher* dan *ElGamal* memiliki ilmu matematika pada setiap prosesnya. Pada penelitian ini percobaan dilakukan dua kali dengan menggunakan algoritma yang sama yaitu *Hill Cipher* dan *Elgamal*. Sehingga pada pembentukan kunci simetris, kunci publik dan privat juga sama. Perbedaannya terletak pada jumlah *plaintext* yang digunakan pada percobaan pertama sesuai dengan *ordo* 3×3 matriks kunci K, sedangakan pada percobaan ke dua jumlah *plaintext* tidak sesuai degan *ordo* 3×3 matriks kunci K yang digunakan. Sehingga perlu menambahkan karakter yang tidak tercetak pada blok yang kosong sesuai dengan kode ASCII 256 (Hondro, 2017). Pada BAB III pembahasan yang dilakukan mengenai proses pembentukan kunci, enkripsi dan dekripsi menggunakan dua algoritma.

3.1 Enkripsi Algoritma *Hill Cipher* dan *ElGamal* pada Pesan Teks

Proses enkripsi dilakukan oleh pengirim dengan menggunakan algoritma *Hill Cipher*. Kunci yang digunakan yaitu kunci simetris dari algoritma *Hill Cipher* yang dibentuk oleh pengirim, kunci publik dan kunci privat dari algoritma *ElGamal* yang dibentuk oleh penerima. Berikut tahap yang harus dilakukan ketika melakukan proses pembentukan kunci simetris algoritma *Hill Cipher*.

3.1.1 Pembentukan Kunci Simetris Algoritma *Hill Cipher*

Pada algoritma *Hill Cipher* menggunakan satu kunci untuk melakukan enkripsi dan dekripsi yaitu kunci simetris. Pembentukan kunci algoritma *Hill*

Cipher dilakukan pengirim menggunakan matriks persegi 3×3. Misalkan kunci yang digunakan adalah

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$$

Melakukan pengecekan pada matriks kunci K bahwa matriks tersebut memiliki invers modulo 256 dengan menentukan $det\, K \neq 0$ sebagai berikut,

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$$

$$M_{11} = \begin{vmatrix} 8 & 7 \\ 5 & 6 \end{vmatrix} = 8 \cdot 6 - 7 \cdot 6 = 48 - 35 = 13$$

$$M_{21} = \begin{vmatrix} 2 & 7 \\ 1 & 6 \end{vmatrix} = 2 \cdot 6 - 7 \cdot 1 = 12 - 7 = 5$$

$$M_{31} = \begin{vmatrix} 2 & 8 \\ 1 & 5 \end{vmatrix} = 2 \cdot 5 - 8 \cdot 1 = 10 - 8 = 2$$

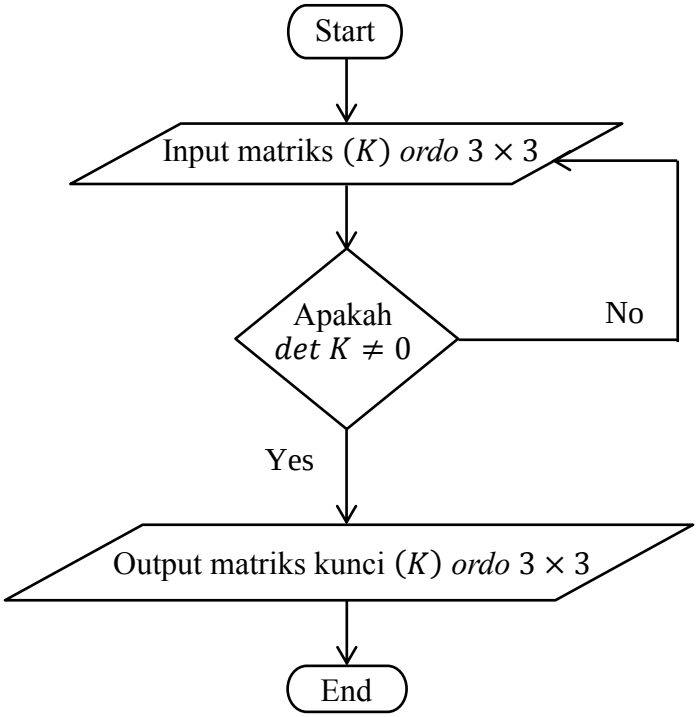
$$\det K = \ 1 \cdot 13 - 2 \cdot 5 + 3 \cdot 2 = 13 - 10 + 6 = 9$$

Diperoleh $det\, K = 9$ sehingga $det\, K \neq 0$. *Flowchart* pembentukan kunci simetris pada algoritma *Hill Cipher* dapat dilihat pada gambar 3.1.

3.1.2 Pembentukan Kunci Publik dan Privat Algoritma *ElGamal*

Pembentukan kunci algoritma *ElGamal*. Kunci terdiri dari kunci privat bersifat rahasia yang hanya akan diketahui oleh penerima untuk melakukan proses

dekripsi dan kunci publik dibuat oleh penerima dan diberikan pada pengirim untuk melakukan enkripsi.



Gambar 3.1 *Flowchart* Pembentukan Kunci (K) Algoritma *Hill Cipher*

Berikut proses pembentukan kunci algoritma *ElGamal*,

a. Memilih sebuah bilangan prima $p = 241$ untuk membentuk grup $(\mathbb{Z}_{241}^{*},\times)$

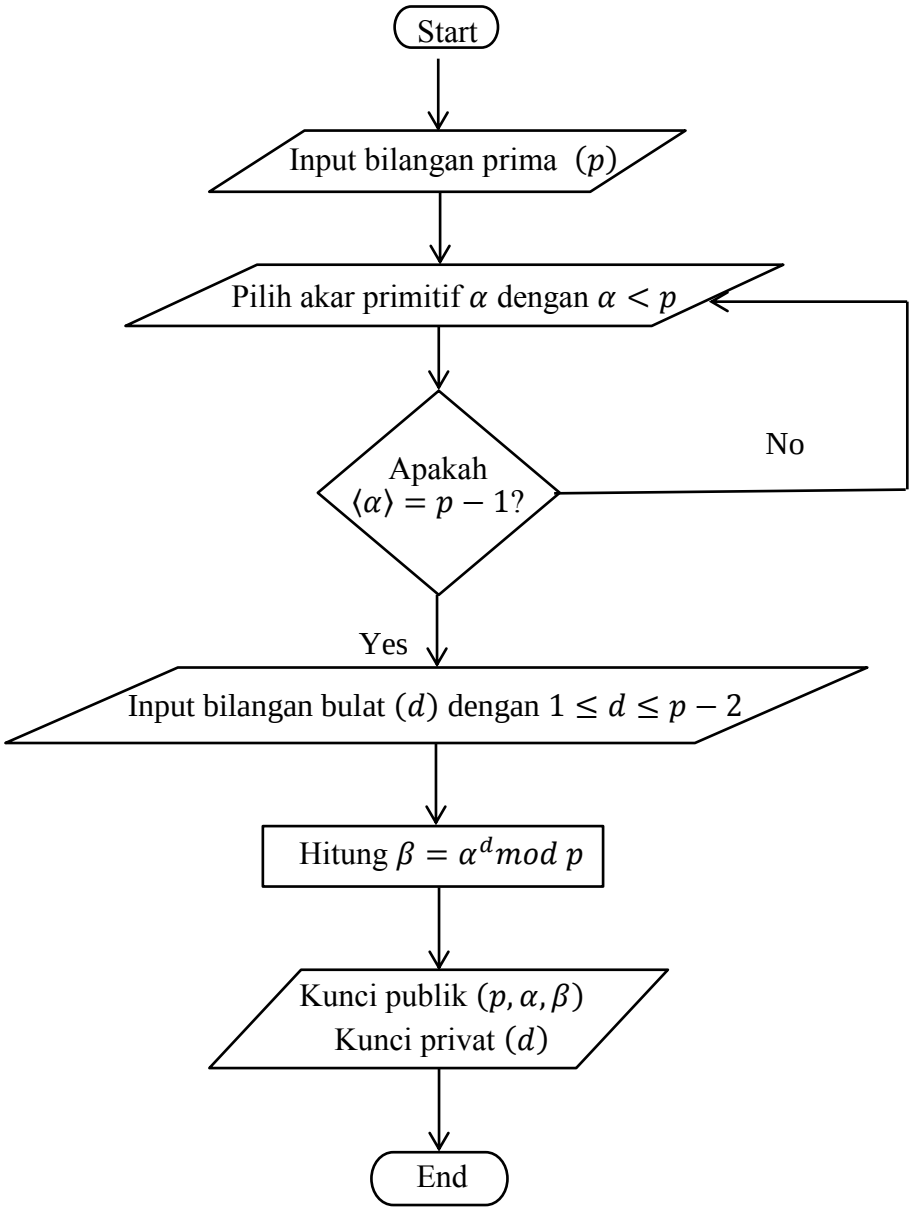
b. Kemudian pilih akar primitif pada $(\mathbb{Z}_{241}^{*},\times)$ maka $\phi(241) = 240$, karena 241 merupakan bilangan prima. Sehingga terdapat 240 kandidat akar primitif pada $(\mathbb{Z}_{241}^{*},\times)$. Misal dipilih $\alpha = 11$

c. Memilih sembarang bilangan bulat $d = 197$ yang memenuhi $1 \leq d \leq p - 2$. Pada algoritma *ElGamal* memiliki kunci publik yang terdiri dari (p, α, β) sehingga untuk melengkapi kunci publik perlu menentukan β menggunakan persamaan $\beta = \alpha^{d}\ mod\ p$ sebagai berikut,

$\beta = \alpha^d mod\ p = 11^{197}\ mod\ 256 = 63$

d. Sehingga diperoleh kunci publik $(p, \alpha, \beta) = (241, 11, 63)$ dan kunci privat $d = 197$. penerima menyimpan kunci privat untuk dirinya sendiri dan memberikan kunci publik pada pengirim.

Alur pembentukan kunci algoritma *ElGamal* dapat dilihat pada *flowchart* berikut,



Gambar 3.2 *Flowchart* Pembentukan Kunci Algoritma *ElGamal*

Berdasarkan proses pembentukan kunci menggunakan algoritma *ElGamal* diperoleh kunci publik dan privat yang akan digunakan untuk melakukan enkripsi dan dekripsi pada kunci simetris. Menggunakan kunci publik yang dimiliki oleh *ElGamal* akan mengubah kunci menjadi *ciphertext*. Kunci publik dapat diketahui oleh pihak pengirim dan penerima. Kunci publik dibentuk dengan mengambil sebarang bilangan prima. Selain kunci publik penerima memiliki kunci privat yang tidak diketahui oleh pengirim. Dalam proses dekripsi menggunakan algoritma *ElGamal* kunci privat yang digunakan. Kemudian proses yang dilakukan yaitu pengiriman pesan teks dan kunci simetris serta kunci publik. Pesan akan dikirim dan mengalami proses enkripsi yang pertama menggunakan algoritma *Hill Cipher*.

3.1.3 Proses Enkripsi Menggunakan Algoritma *Hill Cipher*

Berikut proses enkripsi menggunakan algoritma *Hill Cipher* yang dilakukan oleh pengirim pesan:

a. Menentukan *plaintext*. Sebelum melakukan proses pengiriman pesan pengirim menentukan pesan yang akan dikirimkan. Misalkan pesan yang dikirim berisi kalimat **Saya Mahasiswa Matematika 2017** sebagai *plaintext*.

b. Kemudian mengonversikan *plaintext* menjadi kode ASCII 256.

Tabel 3.1 Konversi *plaintext* pada Kode ASCII 256

S	a	y	a	spasi	M	a	H	a	s
83	97	121	97	32	77	97	104	97	115

i	s	w	a	spasi	M	a	T	e	m
105	115	119	97	32	77	97	116	101	109

a	t	i	k	a	spasi	2	0	1	7
97	116	105	107	97	32	50	48	49	55

c. Proses enkripsi algoritma *Hill Cipher*. *Plaintext* akan dibagi menjadi blok-blok sesuai dengan ukuran matriks kunci.

1. Matriks kunci (K) merupakan matriks persegi 3×3 maka *plaintext* akan dibagi menjadi blok-blok sebagai berikut,

$$p_1 = \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} \; p_2 = \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} \; p_3 = \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} \; p_4 = \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix} \; p_5 = \begin{bmatrix} 119 \\ 97 \\ 32 \end{bmatrix}$$

$$p_6 = \begin{bmatrix} 77 \\ 97 \\ 116 \end{bmatrix} \; p_7 = \begin{bmatrix} 101 \\ 109 \\ 97 \end{bmatrix} \; p_8 = \begin{bmatrix} 115 \\ 105 \\ 107 \end{bmatrix} \; p_9 = \begin{bmatrix} 97 \\ 32 \\ 50 \end{bmatrix} \; p_{10} = \begin{bmatrix} 48 \\ 49 \\ 55 \end{bmatrix}$$

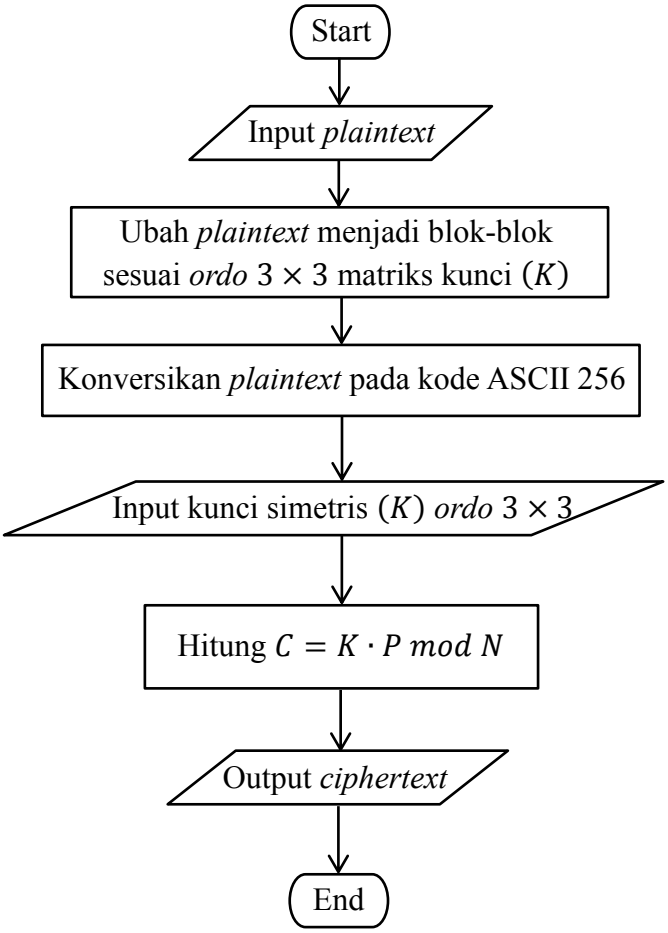
2. Akan dibuktikan bahwa *ciphertext* pada algoritma *Hill Cipher* akan memenuhi fungsi enkripsinya sebagai berikut,

$C \equiv (K \cdot P) \; mod \; 256$	Rumus enkripsi
$256 \mid C - (K \cdot P)$	Definisi kongruensi
$C - (K \cdot P) = 256 \cdot a$	Definisi keterbagian
$C - K \cdot P = 256 \cdot a$	Sifat distributif
$(C - K \cdot P = 256 \cdot a) \times K^{-1}$	Kedua ruas di kali K^{-1}
$K^{-1}C - K^{-1}K \cdot P = 256 \cdot (aK^{-1})$	Sifat distributif
$\left(K^{-1}C - K^{-1}K \cdot P = 256 \cdot (aK^{-1})\right) \times -1$	Kedua ruas dikali -1

$K^{-1}C - P = 256 \cdot (aK^{-1})$	Sifat identitas
$P - K^{-1}C = 256 \cdot (aK^{-1})$	Sifat distributif
$256 \mid P - K^{-1}C$	Definisi keterbagian
$P \equiv K^{-1}C \ mod\ 256$	Rumus dekripsi

Jadi terbukti bahwa *ciphertext* pada algoritma *Hill Cipher* memenuhi fungsi enkripsi dekripsinya.

d. Berikut ini *flowchart* untuk proses enkripsi menggunakan algoritma *Hill Cipher*



Gambar 3.3 *Flowchart* Enkripsi Menggunakan Algoritma *Hill Cipher*

e. Berikut proses enkripsi *Hill Cipher* dengan rumus $C = K \cdot P \ mod \ N$

$$c_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 83 + 194 + 363 \\ 166 + 776 + 847 \\ 83 + 485 + 726 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 640 \\ 1789 \\ 1294 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix} = \begin{bmatrix} Ç \\ ² \\ SO \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 64 + 231 \\ 194 + 256 + 539 \\ 97 + 160 + 462 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 392 \\ 989 \\ 719 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix} = \begin{bmatrix} ê \\ ¦ \\ ¤ \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 208 + 291 \\ 194 + 832 + 679 \\ 97 + 520 + 582 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 596 \\ 1705 \\ 1199 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 84 \\ 169 \\ 175 \end{bmatrix} = \begin{bmatrix} T \\ ® \\ » \end{bmatrix}$$

$$c_4 = \begin{bmatrix}1 & 2 & 3\\ 2 & 8 & 7\\ 1 & 5 & 6\end{bmatrix}\begin{bmatrix}115\\ 105\\ 115\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}115+210+345\\ 230+840+805\\ 115+525+690\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}670\\ 1875\\ 1330\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}158\\ 83\\ 50\end{bmatrix} = \begin{bmatrix}\times\\ S\\ 2\end{bmatrix}$$

$$c_5 = \begin{bmatrix}1 & 2 & 3\\ 2 & 8 & 7\\ 1 & 5 & 6\end{bmatrix}\begin{bmatrix}119\\ 97\\ 32\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}119+194+96\\ 238+776+224\\ 119+485+192\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}409\\ 1238\\ 796\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}153\\ 214\\ 28\end{bmatrix} = \begin{bmatrix}Ö\\ Í\\ FS\end{bmatrix}$$

$$c_6 = \begin{bmatrix}1 & 2 & 3\\ 2 & 8 & 7\\ 1 & 5 & 6\end{bmatrix}\begin{bmatrix}77\\ 97\\ 116\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}77+194+348\\ 154+776+812\\ 77+486+696\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}619\\ 1742\\ 1258\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}107\\ 206\\ 234\end{bmatrix} = \begin{bmatrix}K\\ ╬\\ Û\end{bmatrix}$$

$$c_7 = \begin{bmatrix}1 & 2 & 3\\ 2 & 8 & 7\\ 1 & 5 & 6\end{bmatrix}\begin{bmatrix}101\\ 109\\ 97\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix}101+218+291\\ 202+872+679\\ 101+545+582\end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 610 \\ 1753 \\ 1228 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 98 \\ 217 \\ 204 \end{bmatrix} = \begin{bmatrix} \text{B} \\ \text{┘} \\ \text{╠} \end{bmatrix}$$

$$c_8 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 115 \\ 105 \\ 107 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 115 + 210 + 321 \\ 230 + 840 + 749 \\ 115 + 525 + 642 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 646 \\ 1819 \\ 1282 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 134 \\ 27 \\ 2 \end{bmatrix} = \begin{bmatrix} \text{å} \\ \text{ESC} \\ \text{STX} \end{bmatrix}$$

$$c_9 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 32 \\ 50 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 64 + 150 \\ 194 + 256 + 350 \\ 97 + 160 + 300 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 311 \\ 800 \\ 557 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 55 \\ 32 \\ 45 \end{bmatrix} = \begin{bmatrix} 7 \\ Space \\ - \end{bmatrix}$$

$$c_{10} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 48 \\ 49 \\ 55 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 48 + 98 + 165 \\ 96 + 392 + 385 \\ 48 + 245 + 330 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 311 \\ 873 \\ 623 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 55 \\ 105 \\ 111 \end{bmatrix} = \begin{bmatrix} 7 \\ \text{I} \\ 0 \end{bmatrix}$$

Setelah melalui proses enkripsi pesan tidak dapat dimengerti yang disebut sebagai *ciphertext*. Mengonversikan *plaintext* berdasarkan tabel ASCII 256 yang tidak dapat dimengerti. Enkripsi pada algoritma *Hill Cipher* dengan menggunakan kunci simetris *K* dikalikan dengan *plaintext* pada modulo 256. Dengan demikian diperoleh *ciphertext* dari pesan yang telah dienkripsi sebagai berikut,

$$C_1 = \begin{bmatrix} \text{Ç} \\ ² \\ \text{SO} \end{bmatrix} C_2 = \begin{bmatrix} \hat{\text{e}} \\ ¦ \\ ¤ \end{bmatrix} C_3 = \begin{bmatrix} \text{T} \\ ® \\ » \end{bmatrix} C_4 = \begin{bmatrix} × \\ \text{S} \\ 2 \end{bmatrix} C_5 = \begin{bmatrix} \text{Ö} \\ \text{Í} \\ \text{FS} \end{bmatrix}$$

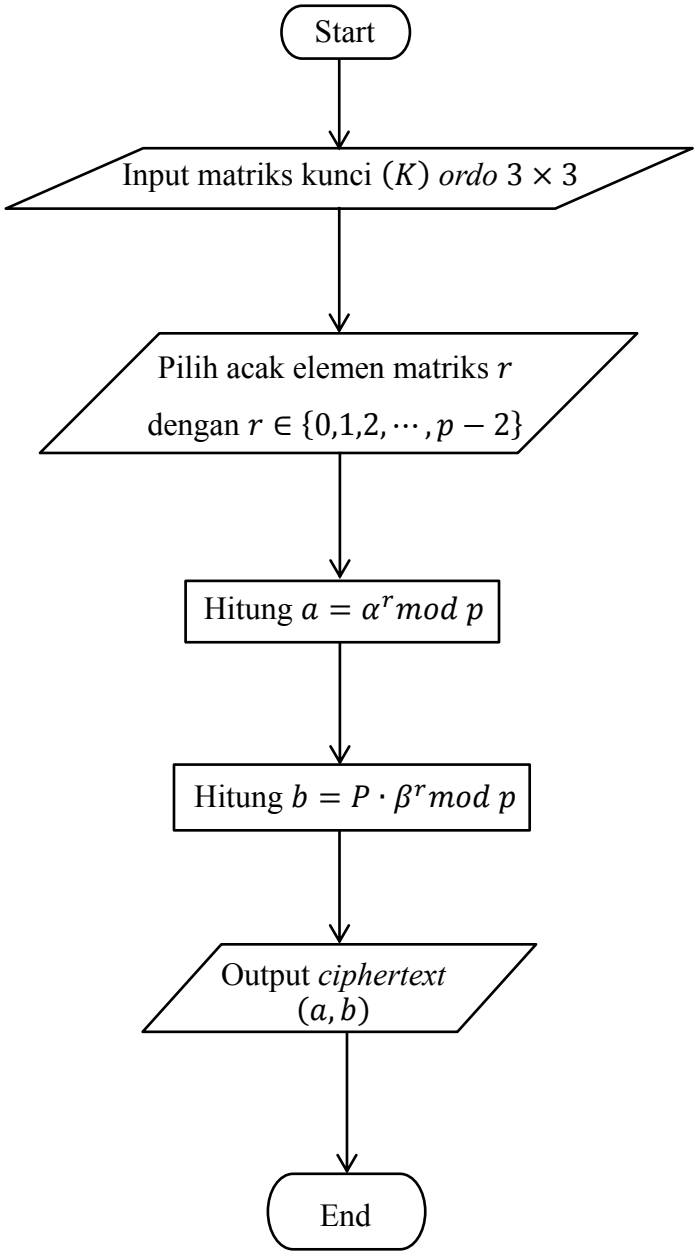
$$C_6 = \begin{bmatrix} \text{K} \\ ╬ \\ \hat{\text{U}} \end{bmatrix} C_7 = \begin{bmatrix} \text{B} \\ ┘ \\ ╠ \end{bmatrix} C_8 = \begin{bmatrix} \text{å} \\ \text{ESC} \\ \text{STX} \end{bmatrix} C_9 = \begin{bmatrix} 7 \\ \text{Space} \\ — \end{bmatrix} C_{10} = \begin{bmatrix} 7 \\ \text{I} \\ 0 \end{bmatrix}$$

Proses enkripsi kedua dilakukan menggunakan algoritma *ElGamal* dengan kunci publik yang dimilikinya. Pada enkripsi yang kedua kunci simetris *K* sebagai *plaintext* yang akan diubah menjadi *ciphertext*.

3.1.4 Proses Enkripsi Menggunakan Algoritma *ElGamal*

Proses enkripsi kunci *K* menggunakan kunci publik dari algoritma *ElGamal*. Berdasarkan hasil pembentukan kunci algoritma *ElGamal* diperoleh kunci publik $(p, \alpha, \beta) = (241, 11, 63)$. Proses enkripsi kunci *K* menggunakan persamaan $a = \alpha^r mod\ p$ dan $b = P \times \beta^r mod\ p$.

Pengirim menggunakan $r = \begin{bmatrix} 236 & 174 & 234 \\ 182 & 222 & 155 \\ 224 & 97 & 132 \end{bmatrix}$ yang merupakan elemen matriks yang dipilih acak dengan $r \in \{0,1,2,\cdots,p-2\}$ untuk melakukan enkripsi. Proses enkripsi menggunakan algoritma *ElGamal* dapat dilihat pada *flowchart* berikut,



Gambar 3.4 *Flowchart* Enkripsi Menggunakan Algoritma *ElGamal*

Kemudian proses enkripsi kunci K menggunakan rumus algoritma *ElGamal* dengan perhitungan matematika secara manual,

$a = \alpha^r mod\ p$

$= 11^{236} mod\ 241$

$= (11^2)^{118}\ mod\ 241$

$= 121^{118}\ mod\ 241$

$= (121^2)^{59}\ mod\ 241$

$= 181^{59}\ mod\ 241$

$= 181 \times (181^2)^{29}\ mod\ 241$

$= 181 \times 226^{29}\ mod\ 241$

$= 181 \times 226 \times (226^2)^{14}\ mod\ 241$

$= 181 \times 226 \times 225^{14}\ mod\ 241$

$= 181 \times 226 \times (225^2)^{7}\ mod\ 241$

$= 181 \times 226 \times 15^{7}\ mod\ 241$

$= 181 \times 226 \times 15 \times (15^2)^{3}\ mod\ 241$

$= 181 \times 226 \times 15 \times 225^{3}\ mod\ 241$

$= 181 \times 226 \times 15 \times 1\ mod\ 241$

$= 613590\ mod\ 241$

$= 4$

$b = P \times \beta^r mod\ p$

$= 1 \times 63^{236} mod\ 241$

$= 1 \times (62^2)^{118}\ mod\ 241$

$= 1 \times 113^{118}\ mod\ 241$

$= 1 \times (113^2)^{59} \ mod\ 241$

$= 1 \times 237^{59} \ mod\ 241$

$= 1 \times 237 \times (237^2)^{29} \ mod\ 241$

$= 1 \times 237 \times 16^{29} \ mod\ 241$

$= 1 \times 237 \times 16 \times (16^2)^{14} \ mod\ 241$

$= 1 \times 237 \times 16 \times 15^{14} \ mod\ 241$

$= 1 \times 237 \times 16 \times (15^2)^{7} \ mod\ 241$

$= 1 \times 237 \times 16 \times 225^{7} \ mod\ 241$

$= 1 \times 237 \times 16 \times 225 \times (225^2)^{3} \ mod\ 241$

$= 1 \times 237 \times 16 \times 225 \times 15^3 mod\ 241$

$= 1 \times 237 \times 16 \times 225 \times 1 \ mod\ 241$

$= 1 \times 853200 \ mod\ 241$

$= 60$

$a \ = \alpha^r mod\ p$

$= 11^{174} mod\ 241$

$= (11^2)^{87} \ mod\ 241$

$= 121^{87} \ mod\ 241$

$= 121 \times (121^2)^{43} \ mod\ 241$

$= 121 \times 181^{43} \ mod\ 241$

$= 121 \times 181 \times (181^2)^{21} \ mod\ 241$

$= 121 \times 181 \times (226^3)^{7} \ mod\ 241$

$= 121 \times 181 \times 240^{7} \ mod\ 241$

$= 121 \times 181 \times 240 \times (240^2)^{3} \ mod\ 241$

$= 121 \times 181 \times 240 \times 1^3 \ mod\ 241$

$= 121 \times 181 \times 240 \ mod\ 241$

$= 5256240 \ mod\ 241$

$= 30$

$b \ = p \times \beta^r mod\ p$

$= 2 \times (63^6)^{29} mod\ 241$

$= 2 \times 30^{29} mod\ 241$

$= 2 \times 30 \times (30^4)^7 mod\ 241$

$= 2 \times 30 \times 240^7 mod\ 241$

$= 2 \times 30 \times 240 \times (240^2)^3 mod\ 241$

$= 2 \times 30 \times 240 \times 1^3 \ mod\ 241$

$= 2 \times 211 \ mod\ 241$

$= 422 \ mod\ 241$

$= 181$

$a \ = \alpha^r mod\ p$

$= 11^{234} mod\ 241$

$= (11^2)^{117} \ mod\ 241$

$= 121^{117} \ mod\ 241$

$= (121^3)^{39} \ mod\ 241$

$= 211^{39} \ mod\ 241$

$= (211^3)^{13} \ mod\ 241$

$= 233^{13} \ mod\ 241$

$= 233 \times (233^3)^4 \ mod\ 241$

$= 233 \times 211^4 \ mod\ 241$

$= 233 \times (211^2)^2 \ mod\ 241$

$= 233 \times 177^2 \ mod\ 241$

$= 233 \times 240 \ mod\ 241$

$= 55920 \ mod\ 241$

$= 8$

$b \ = P \times \beta^r mod\ p$

$= 3 \times 63^{234} mod\ 241$

$= 3 \times (63^9)^{26} mod\ 241$

$= 3 \times 44^{26} mod\ 241$

$= 3 \times (44^2)^{13} mod\ 241$

$= 3 \times 8^{13} mod\ 241$

$= 3 \times 8 \times (8^3)^4 mod\ 241$

$= 3 \times 8 \times 30^4 mod\ 241$

$= 3 \times 8 \times (30^2)^2 mod\ 241$

$= 3 \times 8 \times 177^2 mod\ 241$

$= 3 \times 8 \times 240 \ mod\ 241$

$= 3 \times 1920 \ mod\ 241$

$= 3 \times 233 \ mod\ 241$

$= 699 \ mod\ 241$

$= 217$

$a \ = \alpha^r mod\ p$

$= 11^{182} mod\ 241$

$= (11^2)^{91}\ mod\ 241$

$= 121^{91}\ mod\ 241$

$= 121 \times (121^2)^{45}\ mod\ 241$

$= 121 \times 181^{45}\ mod\ 241$

$= 121 \times 181 \times (181^2)^{22}\ mod\ 241$

$= 121 \times 181 \times 226^{22}\ mod\ 241$

$= 121 \times 181 \times (226^2)^{11}\ mod\ 241$

$= 121 \times 181 \times 225^{11}\ mod\ 241$

$= 121 \times 181 \times 225 \times (225^2)^5\ mod\ 241$

$= 121 \times 181 \times 225 \times 15^5\ mod\ 241$

$= 121 \times 181 \times 225 \times 15 \times (15^2)^2\ mod\ 241$

$= 121 \times 181 \times 225 \times 15 \times 225^2\ mod\ 241$

$= 121 \times 181 \times 225 \times 15 \times 15\ mod\ 241$

$= 1108738125\ mod\ 241$

$= 32$

$b\ = P \times \beta^r mod\ p$

$= 2 \times (63^7)^{26} mod\ 241$

$= 2 \times 203^{26} mod\ 241$

$= 2 \times (203^2)^{13} mod\ 241$

$= 2 \times 239^{13} mod\ 241$

$= 2 \times 239 \times (239^3)^4 mod\ 241$

$= 2 \times 239 \times 233^4 mod\ 241$

$= 2 \times 239 \times (233^2)^2 mod\ 241$

$= 2 \times 239 \times 64^2 mod\ 241$

$= 2 \times 239 \times 240\ mod\ 241$

$= 2 \times 57360\ mod\ 241$

$= 2 \times 2 mod\ 241$

$= 4\ mod\ 241$

$= 4$

$a\ = \alpha^r mod\ p$

$= 11^{222} mod\ 241$

$= (11^3)^{74}\ mod\ 241$

$= 126^{74}\ mod\ 241$

$= (126^2)^{37}\ mod\ 241$

$= 211^{37}\ mod\ 241$

$= 211 \times (211^2)^{18}\ mod\ 241$

$= 211 \times (177^3)^6\ mod\ 241$

$= 211 \times 64^6\ mod\ 241$

$= 211 \times (64^2)^3\ mod\ 241$

$= 211 \times 240^3\ mod\ 241$

$= 211 \times 240\ mod\ 241$

$= 50640\ mod\ 241$

$= 30$

$b\ = P \times \beta^r mod\ p$

$= 8 \times (63^6)^{37} mod\ 241$

$= 8 \times 30^{37} mod\ 241$

$= 8 \times 30 \times (30^3)^{12} mod\ 241$

$= 8 \times 30 \times 8^{12} mod\ 241$

$= 8 \times 30 \times (8^3)^4 mod\ 241$

$= 8 \times 30 \times 30^4 mod\ 241$

$= 8 \times 30 \times 177^2 mod\ 241$

$= 8 \times 30 \times 240\ mod\ 241$

$= 8 \times 7200\ \ mod\ 241$

$= 8 \times 211\ mod\ 241$

$= 1688\ mod\ 241$

$= 1$

$a\ = \alpha^r mod\ p$

$= 11^{155} mod\ 241$

$= 11 \times (11^2)^{77}\ mod\ 241$

$= 11 \times 121^{77}\ mod\ 241$

$= 11 \times 121 \times (121^2)^{38}\ mod\ 241$

$= 11 \times 121 \times 181^{38}\ mod\ 241$

$= 11 \times 121 \times (181^2)^{19}\ mod\ 241$

$= 11 \times 121 \times 226^{19}\ mod\ 241$

$= 11 \times 121 \times 226 \times (226^2)^9\ mod\ 241$

$= 11 \times 121 \times 226 \times 225^9\ mod\ 241$

$= 11 \times 121 \times 226 \times (225^3)^3\ mod\ 241$

$= 11 \times 121 \times 226 \times 1^3\ mod\ 241$

$= 300806\ mod\ 241$

$= 38$

$b = P \times \beta^r mod\ p$

$= 7 \times 63 \times (63^2)^{77} mod\ 241$

$= 7 \times 63 \times 113^{77} mod\ 241$

$= 7 \times 63 \times 113 \times (113^4)^{19} mod\ 241$

$= 7 \times 63 \times 113 \times 16^{19} mod\ 241$

$= 7 \times 63 \times 113 \times 16 \times (16^2)^9 mod\ 241$

$= 7 \times 63 \times 113 \times 16 \times 15^9 mod\ 241$

$= 7 \times 63 \times 113 \times 16 \times (15^3)^3 mod\ 241$

$= 7 \times 63 \times 113 \times 16 \times 1^3 mod\ 241$

$= 7 \times 113904\ mod\ 241$

$= 7 \times 152\ mod\ 241$

$= 1064\ mod\ 241$

$= 100$

$a = \alpha^r mod\ p$

$= 11^{224} mod\ 241$

$= (11^2)^{112}\ mod\ 241$

$= 121^{112}\ mod\ 241$

$= (121^2)^{56}\ mod\ 241$

$= 181^{56}\ mod\ 241$

$= (181^2)^{28}\ mod\ 241$

$= 226^{28}\ mod\ 241$

$= (226^2)^{14}\ mod\ 241$

$= 225^{14}\ mod\ 241$

$= (225^2)^7 \ mod\ 241$

$= 15^7 \ mod\ 241$

$= 15 \times (15^2)^3 \ mod\ 241$

$= 15 \times 225^3 \ mod\ 241$

$= 15 \times 1 \ mod\ 241$

$= 15$

$b \ = P \times \beta^r mod\ p$

$= 1 \times (63^4)^{56} mod\ 241$

$= 1 \times 237^{56} mod\ 241$

$= 1 \times (237^2)^{28} mod\ 241$

$= 1 \times 16^{28} mod\ 241$

$= 1 \times (16^2)^{14} mod\ 241$

$= 1 \times 15^{14} mod\ 241$

$= 1 \times (15^2)^7 mod\ 241$

$= 1 \times 225^7 mod\ 241$

$= 1 \times 225 \times (225^2)^3 mod\ 241$

$= 1 \times 225 \times 15^3 mod\ 241$

$= 1 \times 225 \times 1 \ mod\ 241$

$= 1 \times 225 \ mod\ 241$

$= 225 \ mod\ 241$

$= 225$

$a \ = \alpha^r mod\ p$

$= 11^{97} mod\ 241$

$= 11 \times (11^2)^{48}\ mod\ 241$

$= 11 \times 121^{48}\ mod\ 241$

$= 11 \times (121^2)^{24}\ mod\ 241$

$= 11 \times 181^{24}\ mod\ 241$

$= 11 \times (181^2)^{12}\ mod\ 241$

$= 11 \times 226^{12}\ mod\ 241$

$= 11 \times (226^2)^{6}\ mod\ 241$

$= 11 \times 225^{6}\ mod\ 241$

$= 11 \times (225^2)^{3}\ mod\ 241$

$= 11 \times 15^{3}\ mod\ 241$

$= 11 \times 1\ mod\ 241$

$= 11$

$b\ = P \times \beta^r mod\ p$

$= 5 \times 63 \times (63^2)^{48} mod\ 241$

$= 5 \times 63 \times 113^{48} mod\ 241$

$= 5 \times 63 \times (113^4)^{12} mod\ 241$

$= 5 \times 63 \times 16^{12} mod\ 241$

$= 5 \times 63 \times (16^3)^{4} mod\ 241$

$= 5 \times 63 \times 240^{4} mod\ 241$

$= 5 \times 63 \times (240^2)^{2} mod\ 241$

$= 5 \times 63 \times 1^{2} mod\ 241$

$= 5 \times 63\ mod\ 241$

$= 315\ mod\ 241$

$= 74$

$a = \alpha^r mod\ p$

$= 11^{132} mod\ 241$

$= (11^2)^{66}\ mod\ 241$

$= 121^{66}\ mod\ 241$

$= (121^2)^{33}\ mod\ 241$

$= 181^{33}\ mod\ 241$

$= (181^3)^{11}\ mod\ 241$

$= 177^{11}\ mod\ 241$

$= 177 \times (177^2)^5\ mod\ 241$

$= 177 \times 240^5\ mod\ 241$

$= 177 \times 240 \times (240^2)^2\ mod\ 241$

$= 177 \times 240 \times 1^2\ mod\ 241$

$= 42480\ mod\ 241$

$= 64$

$b = P \times \beta^r mod\ p$

$= 6 \times (63^3)^{44} mod\ 241$

$= 6 \times 130^{44} mod\ 241$

$= 6 \times (130^4)^{11} mod\ 241$

$= 6 \times 177^{11} mod\ 241$

$= 6 \times 177 \times (177^2)^5 mod\ 241$

$= 6 \times 177 \times 240^5 mod\ 241$

$= 6 \times 177 \times 240 \times (240^2)^2 mod\ 241$

$= 6 \times 177 \times 240 \times 1^2 mod\ 241$

$= 6 \times 42480\ mod\ 241$

$= 6 \times 64\ mod\ 241$

$= 384\ mod\ 241$

$= 143$

Hasil enkripsi kunci K dapat di lihat pada tabel berikut,

Tabel 3.2 Hasil Enkripsi Kunci

Key	***a***	***b***
[1,1]	4	60
[1,2]	30	181
[1,3]	8	217
[2,1]	32	4
[2,2]	30	1
[2,3]	38	100
[3,1]	15	225
[3,2]	11	74
[3,3]	64	143

Berdasarkan tabel 3.2 dapat dilihat bahwa proses enkripsi pada algoritma *ElGamal* memiliki *ciphertext* yang lebih panjang dari *plaintext*nya. Sehingga membutuhkan waktu yang lebih lama ketika melakukan proses enkripsi. Setelah melakukan enkripsi pesan dan kunci kemudian dikirimkan pada penerima pesan. Penerima pesan akan melakukan dekripsi pada kunci menggunakan algoritma *ElGamal* terlebih dahulu kemudian diperoleh *plaintext* kunci $K_{3\times3}$ yang akan digunakan untuk melakukan proses dekripsi pesan.

3.2 Proses Dekripsi Menggunakan Algoritma *ElGamal* dan *Hill Cipher*

Pada proses dekripsi yang dilakukan oleh penerima pesan yaitu dengan mendekripsikan kunci menggunakan algoritma *ElGamal*. Sehingga akan diperoleh matriks kunci yang akan digunakan untuk melakukan proses dekripsi *ciphertext* pesan.

3.2.1 Proses Dekripsi Menggunakan Algoritma *ElGamal*

Setelah menerima *ciphertext* (a, b) proses selanjutnya adalah mendekripsikan *ciphertext* menggunakan kunci rahasia d. Dapat ditunjukkan bahwa *plaintext* P dapat diperoleh dari *ciphertext* menggunakan kunci rahasia d.

Teorema:

Diberikan (p, α, β) sebagai kunci publik dan d sebagai kunci rahasia pada algoritma *ElGamal*. Jika diberikan *ciphertext* (a, b), maka

$$P = b \cdot (a^d)^{-1} \, mod \, p$$

Dengan P adalah *plaintext*

Bukti:

Diketahui kunci publik (p, α, β) dan kunci rahasia d pada algoritma *ElGamal*. Diberikan *ciphertext* (a, b) dan persamaan $\beta = \alpha^d mod \, p$, $a = \alpha^r mod \, p$ dan $b = P \times \beta^r \, mod \, p$ diperoleh bahwa,

$$P \equiv b \cdot a^{-d} \, mod \, p$$

$$\equiv \beta^r \cdot P \cdot (\alpha^r)^{-d} \, mod \, p$$

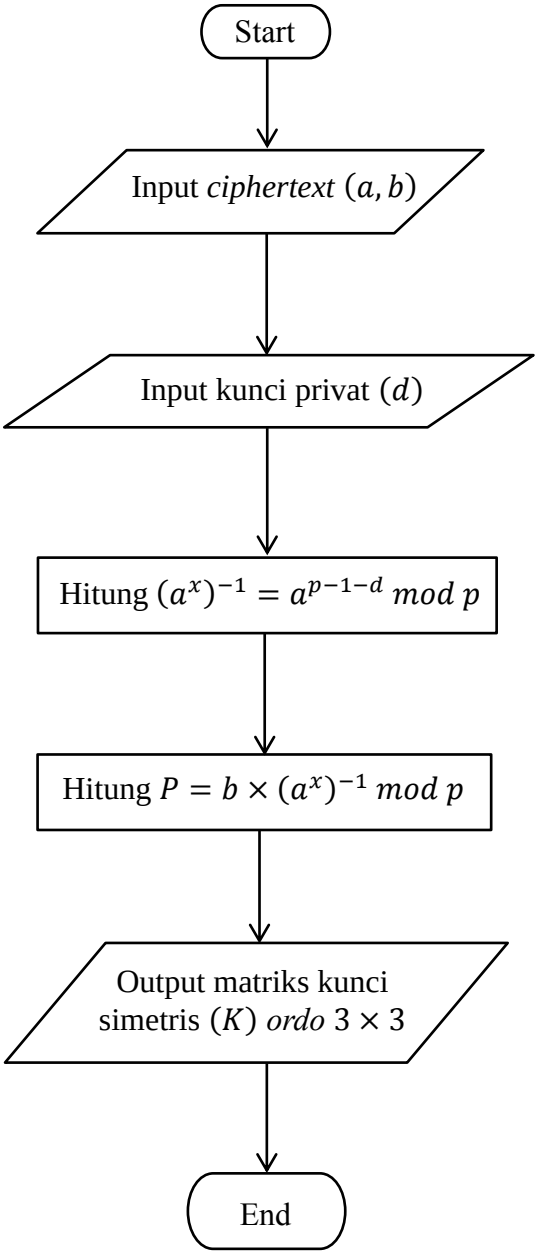
$$\equiv (\alpha^d)^r \cdot P \cdot (\alpha^r)^{-d} \, mod \, p$$

$$\equiv P \cdot (\alpha^{dr} \cdot \alpha^{-dr}) \, mod \, p$$

$\equiv P \ mod \ p$

Dengan demikian terbukti bahwa $P = b \cdot (a^d)^{-1} \ mod \ p$.

Tahap-tahap proses enkripsi kunci K menggunakan algoritma *ElGamal* dapat dilihat pada *flowchart* berikut,



Gambar 3.5 *Flowchart* Dekripsi Menggunakan Algoritma *ElGamal*

Berikut proses enkripsi kunci *K* menggunakan algoritma *ElGamal* dengan perhitungan matematika secara manual,

$c_{[1,1]} = (a, b) = (4,60)$

$(a^x)^{-1} = a^{p-1-d} \; mod \; p$

$= 4^{241-1-197} mod \; 241$

$= 4^{43} mod \; 241$

$= 4 \times (4^2)^{21} mod \; 241$

$= 4 \times 16^{21} mod \; 241$

$= 4 \times (16^3)^7 mod \; 241$

$= 4 \times 240^7 mod \; 241$

$= 4 \times 240 \times (240^2)^3 mod \; 241$

$= 4 \times 240 \times 1^3 mod \; 241$

$= 4 \times 240 \; mod \; 241$

$= 960 \; mod \; 241$

$= 237$

$P_{[1,1]} = b \times (a^x)^{-1} \; mod \; p$

$= 60 \times 237 \; mod \; 241$

$= 14220 \; mod \; 241$

$= 1$

$c_{[1,2]} = (a, b) = (30,181)$

$(a^x)^{-1} = a^{p-1-d} \; mod \; p$

$= 30^{241-1-197} mod \; 241$

$= 30^{43} \; mod \; 241$

$= 30 \times (30^2)^{21} mod\ 241$

$= 30 \times 900^{21} mod\ 241$

$= 30 \times (900^3)^7 mod\ 241$

$= 30 \times 64^7 mod\ 241$

$= 30 \times 64 \times (64^2)^3 mod\ 241$

$= 30 \times 64 \times 240^3 mod\ 241$

$= 30 \times 64 \times 240\ mod\ 241$

$= 460800\ mod\ 241$

$= 8$

$P_{[1,2]} = b \times (a^x)^{-1}\ mod\ p$

$= 181 \times 8\ mod\ 241$

$= 1448\ mod\ 241$

$= 2$

$c_{[1,3]} = (a, b) = (8,217)$

$(a^x)^{-1} = a^{p-1-d}\ mod\ p$

$= 8^{241-1-197} mod\ 241$

$= 8^{43}\ mod\ 241$

$= 8 \times (8^2)^{21} mod\ 241$

$= 8 \times (8^2)^{21} mod\ 241$

$= 8 \times 64^{21} mod\ 241$

$= 8 \times (64^3)^7 mod\ 241$

$= 8 \times 177^7 mod\ 241$

$= 8 \times 177 \times (177^2)^3 mod\ 241$

$= 8 \times 177 \times 240^3 mod\ 241$

$= 8 \times 177 \times 240\ mod\ 241$

$=\ 30$

$P_{[1,3]} = b \times (a^x)^{-1}\ mod\ p$

$= 217 \times 30\ mod\ 241$

$= 6510\ mod\ 241$

$= 3$

$c_{[2,1]} = (a, b) = (32,4)$

$(a^x)^{-1} = a^{p-1-d}\ mod\ p$

$= 32^{241-1-197} mod\ 241$

$= 32^{43}\ mod\ 241$

$= 32 \times (32^2)^{21} mod\ 241$

$= 32 \times 60^{21} mod\ 241$

$= 32 \times (60^3)^7 mod\ 241$

$= 32 \times 64^7 mod\ 241$

$= 32 \times 64 \times (64^2)^3 mod\ 241$

$= 32 \times 64 \times 240^3 mod\ 241$

$= 32 \times 64 \times 240\ mod\ 241$

$= 491520\ mod\ 241$

$= 121$

$P_{[2,1]} = b \times (a^x)^{-1}\ mod\ p$

$= 4 \times 121\ mod\ 241$

$= 484\ mod\ 241$

$= 2$

$c_{[2,2]} = (a, b) = (30,1)$

$(a^x)^{-1} = a^{p-1-d} \ mod \ p$

$= 30^{241-1-197} mod \ 241$

$= 30^{43} \ mod \ 241$

$= 30 \times (30^2)^{21} mod \ 241$

$= 30 \times 900^{21} mod \ 241$

$= 30 \times (900^3)^7 mod \ 241$

$= 30 \times 64^7 mod \ 241$

$= 30 \times 64 \times (64^2)^3 mod \ 241$

$= 30 \times 64 \times 240^3 mod \ 241$

$= 30 \times 64 \times 240 \ mod \ 241$

$= 460800 \ mod \ 241$

$=8$

$P_{[2,2]} = b \times (a^x)^{-1} \ mod \ p$

$= 1 \times 8 \ mod \ 241$

$= 8$

$c_{[2,3]} = (a, b) = (38,100)$

$(a^x)^{-1} = a^{p-1-d} \ mod \ p$

$= 38^{241-1-197} mod \ 241$

$= 38^{43} \ mod \ 241$

$= 38 \times (38^2)^{21} mod \ 241$

$= 38 \times 239^{21} mod \ 241$

$= 38 \times (239^3)^7 mod\ 241$

$= 38 \times 239 \times 233^7 mod\ 241$

$= 38 \times 239 \times (233^2)^3 mod\ 241$

$= 38 \times 239 \times 64^3 mod\ 241$

$= 38 \times 239 \times 177\ mod\ 241$

$= 1567158\ mod\ 241$

$= 176$

$P_{[2,3]} = b \times (a^x)^{-1}\ mod\ p$

$= 100 \times 176\ mod\ 241$

$= 17600\ mod\ 241$

$= 7$

$c_{[3,1]} = (a, b) = (15{,}225)$

$(a^x)^{-1} = a^{p-1-d}\ mod\ p$

$= 15^{241-1-197} mod\ 241$

$= 15^{43}\ mod\ 241$

$= 15 \times (15^2)^{21} mod\ 241$

$= 15 \times 225^{21} mod\ 241$

$= 15 \times (225^3)^7 mod\ 241$

$= 15 \times 1^7 mod\ 241$

$= 15\ mod\ 241$

$= 15$

$P_{[3,1]} = b \times (a^x)^{-1}\ mod\ p$

$= 225 \times 15\ mod\ 241$

$= 375 \; mod \; 241$

$= 1$

$c_{[3,2]} = (a, b) = (11{,}74)$

$(a^x)^{-1} = a^{p-1-d} \; mod \; p$

$= 11^{241-1-197} mod \; 241$

$= 11^{43} \; mod \; 241$

$= 11 \times (11^2)^{21} mod \; 241$

$= 11 \times 121^{21} mod \; 241$

$= 11 \times (121^3)^7 mod \; 241$

$= 11 \times 211^7 mod \; 241$

$= 11 \times 121 \times (211^2)^3 mod \; 241$

$= 11 \times 121 \times 177^3 mod \; 241$

$= 11 \times 121 \times 64 \; mod \; 241$

$= 148544 \; mod \; 241$

$= 88$

$P_{[3,2]} = b \times (a^x)^{-1} \; mod \; p$

$= 74 \times 88 \; mod \; 241$

$= 6512 \; mod \; 241$

$= 5$

$c_{[3,3]} = (a, b) = (64{,}143)$

$(a^x)^{-1} = a^{p-1-d} \; mod \; p$

$= 64^{241-1-197} mod \; 241$

$= 64^{43} \; mod \; 241$

$= 64 \times (64^2)^{21} mod\ 241$

$= 64 \times 240^{21} mod\ 241$

$= 64 \times (240^3)^7 mod\ 241$

$= 64 \times 240^7 mod\ 241$

$= 64 \times 240 \times (240^2)^3 mod\ 241$

$= 64 \times 240 \times 1^3 mod\ 241$

$= 15360\ mod\ 241$

$= 177$

$P_{[3,3]} = b \times (a^x)^{-1}\ mod\ p$

$= 143 \times 177\ mod\ 241$

$= 25311\ mod\ 241$

$= 6$

Hasil dari proses dekripsi kunci dapat dilihat pada tabel berikut,

Tabel 3.3 Hasil Dekripsi Kunci

Key	***Plaintext***
[1,1]	1
[1,2]	2
[1,3]	3
[2,1]	2
[2,2]	8
[2,3]	7
[3,1]	1
[3,2]	5
[3,3]	6

Pada proses dekripsi yang pertama dilakukan oleh penerima yaitu mengubah *ciphertext* menggunakan algoritma *ElGamal*. Penerima memiliki kunci privat yang hanya diketahui oleh dirinya sendiri untuk melakukan dekripsi. Hasil dekripsi menggunakan kunci privat $d = 197$ oleh penerima maka diperoleh *plaintext* yaitu kunci simetris

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$$

Algoritma *ElGamal* melakukan dekripsi sebanyak dua kali pada *ciphertext* sesuai dengan persamaan yang telah diberikan. Sehingga panjang *plaintext* dua kali lebih panjang dari *ciphertext*nya. Penerima terlebih dahulu mendapatkan kunci simetris $K_{3\times3}$. Kemudian digunakan untuk melakukan proses dekripsi kedua mengunakan algoritma *Hill Cipher*.

3.2.2 Proses Dekripsi Menggunakan Algoritma *Hill Cipher*

Pada proses dekripsi yang diperlukan adalah *ciphertext* dari pesan teks yang telah di enkripsi. Kemudian mendekripsikan *ciphertext* menggunakan kunci simetris K *ordo* 3×3 dengan rumus algoritma *Hill Cipher* $P = K^{-1} \cdot C \ mod \ N$.

a. Akan dibuktikan bahwa *plaintext* pada algoritma *Hill Cipher* akan memenuhi fungsi dekripsinya sebagai berikut,

$P \equiv K^{-1}C \ mod \ 256$	Rumus dekripsi
$256 \mid P - (K^{-1}C)$	Definisi kongruensi
$P - (K^{-1}C) = 256 \cdot a$	Definisi keterbagian

$P - K^{-1}C = 256 \cdot a$	Sifat distributif
$(P - K^{-1}C = 256 \cdot a\ ) \times K$	Kedua ruas di kali K
$KP - KK^{-1}C = 256 \cdot (aK)$	Sifat distributif
$KP - C = 256 \cdot (aK)$	Sifat identitas
$(KP - C = 256 \cdot (aK)\ ) \times -1$	Kedua ruas di kali -1
$-KP + C = 256 \cdot (aK)$	Sifat distributif
$C - Kp = 256 \cdot (aK)$	Sifat komutatif
$256 \mid C - KP$	Definisi keterbagian
$C \equiv (K \cdot P)\ mod\ 256$	Rumus enkripsi
$P \equiv k^{-1}C\ mod\ 256$	Rumus dekripsi

b. Menentukan Invers Modulo 256

Invers matriks modulo 256 dari kunci K dapat diperoleh menggunakan rumus $\overline{K} = \bar{\Delta} \cdot adj(K)$. Dengan demikian perlu menentukan $\bar{\Delta}$ dan $adj(K)$ sebagai berikut,

Diketahui $det\ K = 9$ sehingga untuk menentukan $\bar{\Delta}$ merupakan invers dari $9\ mod\ 256$ yaitu,

$$9\ mod\ 256 = 9 \cdot x \equiv 1\ mod\ 256$$

$$9 \cdot x\ \equiv\ 256y + 1$$

$$9 \cdot x - 256y \equiv 1\ mod\ 256$$

$$9 \cdot 57 - 256 \cdot 1 \equiv 1\ mod\ 256$$

$513 - 256 \equiv 1\ mod\ 256$

$257 \equiv 1\ mod\ 256$

Sehingga diperoleh invers dari $9\ mod\ 256$ adalah $57\ mod\ 256$.

c. Kemudian menentukan $adj(K)$ dengan menentukan minor dan kofaktornya sebagai berikut,

Diketahui $K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$

$M_{11} = \begin{vmatrix} 8 & 7 \\ 5 & 6 \end{vmatrix} = 8 \cdot 6 - 7 \cdot 6 = 48 - 35 = 13$

$M_{21} = \begin{vmatrix} 2 & 7 \\ 1 & 6 \end{vmatrix} = 2 \cdot 6 - 7 \cdot 1 = 12 - 7 = 5$

$M_{31} = \begin{vmatrix} 2 & 8 \\ 1 & 5 \end{vmatrix} = 2 \cdot 5 - 8 \cdot 1 = 10 - 8 = 2$

$M_{12} = \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = 2 \cdot 6 - 3 \cdot 5 = 12 - 15 = -3$

$M_{22} = \begin{vmatrix} 1 & 3 \\ 1 & 6 \end{vmatrix} = 1 \cdot 6 - 1 \cdot 3 = 6 - 3 = 3$

$M_{32} = \begin{vmatrix} 1 & 2 \\ 1 & 5 \end{vmatrix} = 1 \cdot 5 - 2 \cdot 1 = 5 - 2 = 3$

$M_{13} = \begin{vmatrix} 2 & 3 \\ 8 & 7 \end{vmatrix} = 2 \cdot 7 - 3 \cdot 8 = 14 - 24 = -10$

$M_{23} = \begin{vmatrix} 1 & 3 \\ 2 & 7 \end{vmatrix} 1 \cdot 7 - 3 \cdot 2 = 7 - 6 = 1$

$M_{33} = \begin{vmatrix} 1 & 2 \\ 2 & 8 \end{vmatrix} = 1 \cdot 8 - 2 \cdot 2 = 8 - 4 = 4$

Diperoleh $minor\ K = \begin{bmatrix} 13 & 5 & 2 \\ -3 & 3 & 3 \\ -10 & 1 & 4 \end{bmatrix}$ sehingga $kof\ K = \begin{bmatrix} 13 & -5 & 2 \\ 3 & 3 & -3 \\ -10 & -1 & 4 \end{bmatrix}$ kemudian transpose dari $kof\ K$ adalah $K^T = \begin{bmatrix} 13 & 3 & -10 \\ -5 & 3 & -1 \\ 2 & -3 & 4 \end{bmatrix}$ dengan demikian diperoleh $adj\ K = \begin{bmatrix} 13 & 3 & -10 \\ -5 & 3 & -1 \\ 2 & -3 & 4 \end{bmatrix}$ maka untuk menentukan $\overline{K}$ modulo 256 adalah,

$$\bar{K} = \bar{\Delta} \cdot (adj\ K)\ mod\ 256$$

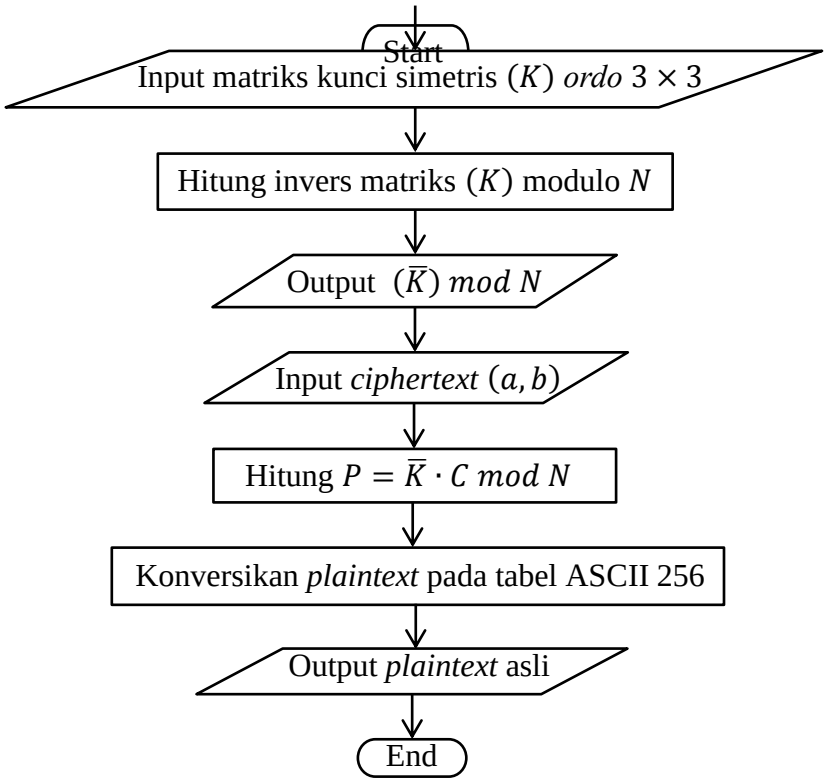
$$= 57 \cdot \begin{bmatrix} 13 & 3 & -10 \\ -5 & 3 & -1 \\ 2 & -3 & 4 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 741 & 171 & -570 \\ -285 & 171 & -57 \\ 114 & -171 & 228 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix}$$

Diperoleh $\bar{K} = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix}$ sebagai kunci yang digunakan untuk melakukan proses dekripsi

d. Proses dekripsi algoritma *Hill Cipher* dapat dilihat pada *flowchart* berikut,



Gambar 3.6 *Flowchart* Dekripsi Menggunakan Algoritma *Hill Cipher*

e. Proses dekripsi yang dilakukan penerima pesan menggunakan rumus dekripsi algoritma *Hill Cipher* $P = \overline{K} \cdot C \ mod \ N$ sebagai berikut,

$$p_1 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix} \qquad p_2 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix}$$

$$= \begin{bmatrix} 29312 + 43263 + 2772 \\ 29056 + 43263 + 2786 \\ 14592 + 21505 + 3192 \end{bmatrix} \qquad = \begin{bmatrix} 31144 + 37791 + 40986 \\ 30872 + 37791 + 41193 \\ 15504 + 18785 + 47196 \end{bmatrix}$$

$$= \begin{bmatrix} 75347 \\ 75105 \\ 39289 \end{bmatrix} mod \ 256 \qquad = \begin{bmatrix} 109921 \\ 109856 \\ 81485 \end{bmatrix} mod \ 256$$

$$= \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} = \begin{bmatrix} S \\ a \\ y \end{bmatrix} \qquad = \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix}$$

$$p_3 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 84 \\ 169 \\ 175 \end{bmatrix} \qquad p_4 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 158 \\ 83 \\ 50 \end{bmatrix}$$

$$= \begin{bmatrix} 19236 + 28899 + 34650 \\ 19068 + 28899 + 34825 \\ 9576 + 14365 + 39900 \end{bmatrix} \qquad = \begin{bmatrix} 36182 + 14193 + 9900 \\ 35866 + 14193 + 9950 \\ 18012 + 7055 + 11400 \end{bmatrix}$$

$$= \begin{bmatrix} 82785 \\ 82792 \\ 63841 \end{bmatrix} mod \ 256 \qquad = \begin{bmatrix} 60275 \\ 60009 \\ 36467 \end{bmatrix} mod \ 256$$

$$= \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} = \begin{bmatrix} a \\ h \\ a \end{bmatrix} \qquad = \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix} = \begin{bmatrix} s \\ i \\ s \end{bmatrix}$$

$$p_5 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 153 \\ 214 \\ 28 \end{bmatrix} \qquad p_6 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 107 \\ 206 \\ 234 \end{bmatrix}$$

$$= \begin{bmatrix} 35037 + 36594 + 5544 \\ 34731 + 36594 + 5572 \\ 17442 + 18190 + 6384 \end{bmatrix} \qquad = \begin{bmatrix} 24503 + 35226 + 46332 \\ 24289 + 35226 + 46566 \\ 12198 + 17510 + 53352 \end{bmatrix}$$

$$= \begin{bmatrix} 77175 \\ 76897 \\ 42016 \end{bmatrix} mod \ 256 \qquad = \begin{bmatrix} 106061 \\ 106081 \\ 83060 \end{bmatrix} mod \ 256$$

$$= \begin{bmatrix} 199 \\ 97 \\ 32 \end{bmatrix} = \begin{bmatrix} w \\ a \\ (spasi) \end{bmatrix} \qquad = \begin{bmatrix} 77 \\ 97 \\ 116 \end{bmatrix} = \begin{bmatrix} M \\ a \\ t \end{bmatrix}$$

$$p_7 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 101 \\ 109 \\ 97 \end{bmatrix} \qquad p_8 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 115 \\ 105 \\ 107 \end{bmatrix}$$

$$= \begin{bmatrix} 22442 + 37107 + 40392 \\ 22246 + 37107 + 40596 \\ 11172 + 18445 + 46512 \end{bmatrix} \qquad = \begin{bmatrix} 30686 + 4617 + 396 \\ 30418 + 4617 + 398 \\ 15276 + 2295 + 456 \end{bmatrix}$$

$$= \begin{bmatrix} 99941 \\ 99949 \\ 76129 \end{bmatrix} mod\ 256 \qquad = \begin{bmatrix} 35699 \\ 35433 \\ 18027 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 101 \\ 109 \\ 97 \end{bmatrix} = \begin{bmatrix} e \\ m \\ a \end{bmatrix} \qquad = \begin{bmatrix} 115 \\ 105 \\ 107 \end{bmatrix} = \begin{bmatrix} t \\ i \\ k \end{bmatrix}$$

$$p_9 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 97 \\ 32 \\ 50 \end{bmatrix} \qquad p_{10} = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 48 \\ 49 \\ 55 \end{bmatrix}$$

$$= \begin{bmatrix} 12595 + 5472 + 8910 \\ 12485 + 5472 + 8955 \\ 6270 + 2720 + 10260 \end{bmatrix} \qquad = \begin{bmatrix} 12595 + 17955 + 21978 \\ 12485 + 17955 + 22089 \\ 6270 + 8925 + 25308 \end{bmatrix}$$

$$= \begin{bmatrix} 26977 \\ 26912 \\ 19250 \end{bmatrix} mod\ 256 \qquad = \begin{bmatrix} 52528 \\ 52529 \\ 40503 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 \\ 32 \\ 50 \end{bmatrix} = \begin{bmatrix} a \\ spasi \\ 2 \end{bmatrix} \qquad = \begin{bmatrix} 48 \\ 49 \\ 55 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 7 \end{bmatrix}$$

Diperoleh *plaintext* semula sebagai berikut,

$$p_1 = \begin{bmatrix} S \\ a \\ y \end{bmatrix} p_2 = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix} p_3 = \begin{bmatrix} a \\ h \\ a \end{bmatrix} p_4 = \begin{bmatrix} s \\ i \\ s \end{bmatrix} p_5 = \begin{bmatrix} w \\ a \\ spasi \end{bmatrix}$$

$$p_6 = \begin{bmatrix} M \\ a \\ t \end{bmatrix} p_7 = \begin{bmatrix} e \\ m \\ a \end{bmatrix} p_8 = \begin{bmatrix} t \\ i \\ k \end{bmatrix} p_9 = \begin{bmatrix} a \\ spasi \\ 2 \end{bmatrix} p_{10} = \begin{bmatrix} 0 \\ 1 \\ 7 \end{bmatrix}$$

Berdasarkan hasil dekripsi yang kedua menggunakan algoritma *Hill Cipher* diperoleh *plaintext* semula yaitu **Saya Mahasiswa Matematika 2017**. *Ciphertext* yang diperoleh dari pengirim dibagi menjadi blok-blok sesuai dengan *ordo* kunci simetrisnya. Proses dekripsi menggunakan algoritma *Hill Cipher* dilakukan dengan mengalikan *ciphertext* dengan invers dari kunci simetris $\overline{K}$. *Plaintext* yang digunakkkan sesuai dengan jumlah *ordo* matriks kunci $K_{3\times3}$ sehingga dapat dibentuk blok-blok dengan mudah. Namun jika jumlah blok *plaintext* tidak sesuai dengan ordo matriks maka perlu ditambahkan karakter yang tidak tercetak pada ode ASCII 256. Dengan menggunakan algoritma *Hill Cipher* dan *ElGamal* maka proses enkripsi dan dekripsi adalah sebagai berikut,

3.3 Enkripsi Dekripsi pada *Plaintext* Berbeda dengan Matriks Kunci $K_{3\times3}$

Pada proses enkripsi dan dekripsi algoritma yang digunakan sama dengan subbab 3.1 dan 3.2 sehingga yang membedakan adalah jumlah blok-blok *plaintext* yang berbeda dengan *ordo* 3×3 matriks kunci K. Proses pembentukan kunci simetris K, kunci publik dan privat sama dengan proses pembentukan kunci menggunakan algoritma *Hill Cipher* dan *ElGamal* pada subbab 3.1.1 dan 3.1.2. Sehingga diperoleh kunci $K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$, kunci publik $(p, \alpha, \beta) = (241, 11, 63)$ dan kunci privat $d = 197$. Kemudian melakukan proses enkripsi menggunakan algoritma *Hill Cipher* dan *ElGamal* sebagai berikut.

3.3.1 Proses Enkripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal*

Berikut proses enkripsi menggunakan algoritma *Hill Cipher* dan *ElGamal* yang dilakukan oleh pengirim pesan.

a. Menentukan *plaintext*. Misalkan pesan yang dikirim berisi kalimat **Saya Mahasiswa** sebagai *plaintext*.

b. Kemudian mengkonversikan *plaintext* menjadi kode ASCII 256.

Tabel 3.4 Hasil Konversi *Plaintext* dengan Karakter Berbeda dengan *Ordo* 3×3 Matriks Kunci (K)

S	a	y	a	spasi	M	a	h	a
83	97	121	97	32	77	97	104	97

Jumlah *plaintext* yang digunakan berjumlah 14, sedangkan *ordo* matriks kunci yang digunakan 3×3. Maka perlu menambahkan karakter yang tidak tercetak seperti, NULL sehingga jumlah blok-blok *plaintext* sesuai dengan *ordo* matriks 3×3 seperti berikut,

Tabel 3.5 Hasil Konversi *Plaintext* dengan Karakter Sesuai *Ordo* (K)

s	i	s	w	a	NULL
115	105	115	119	97	0

c. Proses enkripsi algoritma *Hill Cipher*. *Plaintext* akan dibagi menjadi blok-blok sesuai dengan ukuran matriks kunci.

d. Matriks kunci (K) merupakan matriks persegi 3×3 maka *plaintext* akan dibagi menjadi blok-blok sebagai berikut,

$$p_1 = \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} \; p_2 = \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} \; p_3 = \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} \; p_4 = \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix} \; p_5 = \begin{bmatrix} 119 \\ 97 \\ 0 \end{bmatrix}$$

e. Berikut proses enkripsi *Hill Cipher* dengan rumus $C = K \cdot P \ mod \ N$

$$c_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 83 + 194 + 363 \\ 166 + 776 + 847 \\ 83 + 485 + 726 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 640 \\ 1789 \\ 1294 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix} = \begin{bmatrix} Ç \\ ² \\ SO \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 64 + 231 \\ 194 + 256 + 539 \\ 97 + 160 + 462 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 392 \\ 989 \\ 719 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix} = \begin{bmatrix} ê \\ ¦ \\ ¤ \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 + 208 + 291 \\ 194 + 832 + 679 \\ 97 + 520 + 582 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 596 \\ 1705 \\ 1199 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 84 \\ 169 \\ 175 \end{bmatrix} = \begin{bmatrix} T \\ ® \\ » \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 115 + 210 + 345 \\ 230 + 840 + 805 \\ 115 + 525 + 690 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 670 \\ 1875 \\ 1330 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 158 \\ 83 \\ 50 \end{bmatrix} = \begin{bmatrix} \times \\ S \\ 2 \end{bmatrix}$$

$$c_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix} \begin{bmatrix} 119 \\ 97 \\ 0 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 119 + 194 + 0 \\ 238 + 776 + 0 \\ 119 + 485 + 0 \end{bmatrix} mod\ 256 = \begin{bmatrix} 313 \\ 1014 \\ 604 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 57 \\ 246 \\ 92 \end{bmatrix} = \begin{bmatrix} 9 \\ \div \\ \backslash \end{bmatrix}$$

Diperoleh *ciphertext* dari pesan yang telah dienkripsi sebagai berikut,

$$C_1 = \begin{bmatrix} Ç \\ ² \\ SO \end{bmatrix} C_2 = \begin{bmatrix} ê \\ ¦ \\ ¤ \end{bmatrix} C_3 = \begin{bmatrix} T \\ ® \\ » \end{bmatrix} C_4 = \begin{bmatrix} \times \\ S \\ 2 \end{bmatrix} C_5 = \begin{bmatrix} 9 \\ \div \\ \backslash \end{bmatrix}$$

Dapat dilihat bahwa blok-blok *ciphertext* yang dihasilkan sama dengan blok-blok *plaintext*. Dengan menggunakan rumus algoritma *Hill Cipher* $C = K \cdot P\ mod\ N$ dan kunci K proses enkripsi yang pertama dapat dilakukan. Kemudian algoritma *ElGamal* digunakan untuk melakukan enkripsi pada kunci K. Karena kunci K sama dengan kunci simetris algoritma *Hill Cipher* pada subbab 3.1.1 dan kunci publik dari algoritma *ElGamal* juga sama dengan kunci publik pada subbab 3.1.2 maka hasil dari proses enkripsi dapat dilihat pada tabel berikut,

Tabel 3.6 Hasil Enkripsi Kunci *K*

Key	***a***	***b***
[1,1]	4	60
[1,2]	30	181
[1,3]	8	217
[2,1]	32	4
[2,2]	30	1
[2,3]	38	100
[3,1]	15	225
[3,2]	11	74
[3,3]	64	143

Berdasarkan hasil enkripsi menggunakan algoritma *ElGamal* dapat dilihat bahwa *ciphertext* dua kali lebih panjang dari *plaintext*nya. Kemudian *ciphertext* akan dikirimkan kepada penerima pesan. Sehingga penerima perlu mengetahui kunci simetris K supaya dapat melakukan dekripsi menggunakan algoritma *Hill Cipher*. Berikut proses dekripsi menggunakan algoritma *ElGamal* dan *Hill Cipher*.

3.3.2 Proses Dekripsi Menggunakan Algoritma *ElGamal* dan *Hill Cipher*

Menggunakan kunci privat $d = 197$ dari algoritma *ElGamal ciphertext* didekripsi dengan menentukan $(a^x)^{-1} = a^{p-1-d} \, mod \, p$ dan $P_{[n,n]} = b \times (a^x)^{-1} \, mod \, p$ sesuai dengan perhitungan pada subbab 3.2.1 sehingga diperoleh *plaintext* sebagai berikut,

Tabel 3.7 Hasil Dekripsi Kunci K

Key	***Plaintext***
[1,1]	1
[1,2]	2
[1,3]	3
[2,1]	2
[2,2]	8
[2,3]	7
[3,1]	1
[3,2]	5
[3,3]	6

Hasil dekripsi oleh penerima menggunakan kunci privat $d = 197$ maka diperoleh *plaintext* berupa kunci simetris sebagai berikut,

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 8 & 7 \\ 1 & 5 & 6 \end{bmatrix}$$

Setelah mendapatkan kunci K maka untuk melakukan dekripsi menggunakan algoritma *Hill Cipher* perlu menentukan invers matriks K modulo 256. Dapat dilihat pada subbab 3.2.2 yang mendapatkan nilai $\overline{K} = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix}$ sebagai kunci yang digunakan untuk melakukan proses dekripsi pada *ciphertext*. Proses dekripsi yang dilakukan penerima pesan menggunakan rumus dekripsi algoritma *Hill Cipher* $P = \overline{K} \cdot C \ mod \ N$ sebagai berikut,

$$p_1 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 128 \\ 253 \\ 14 \end{bmatrix}$$

$$= \begin{bmatrix} 29312 + 43263 + 2772 \\ 29056 + 43263 + 2786 \\ 14592 + 21505 + 3192 \end{bmatrix}$$

$$= \begin{bmatrix} 75347 \\ 75105 \\ 39289 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 83 \\ 97 \\ 121 \end{bmatrix} = \begin{bmatrix} S \\ a \\ y \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 136 \\ 221 \\ 207 \end{bmatrix}$$

$$= \begin{bmatrix} 31144 + 37791 + 40986 \\ 30872 + 37791 + 41193 \\ 15504 + 18785 + 47196 \end{bmatrix}$$

$$= \begin{bmatrix} 109921 \\ 109856 \\ 81485 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 \\ 32 \\ 77 \end{bmatrix} = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix}$$

$$p_3 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 84 \\ 169 \\ 175 \end{bmatrix}$$

$$= \begin{bmatrix} 19236 + 28899 + 34650 \\ 19068 + 28899 + 34825 \\ 9576 + 14365 + 39900 \end{bmatrix}$$

$$= \begin{bmatrix} 82785 \\ 82792 \\ 63841 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 97 \\ 104 \\ 97 \end{bmatrix} = \begin{bmatrix} a \\ h \\ a \end{bmatrix}$$

$$p_4 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 158 \\ 83 \\ 50 \end{bmatrix}$$

$$= \begin{bmatrix} 36182 + 14193 + 9900 \\ 35866 + 14193 + 9950 \\ 18012 + 7055 + 11400 \end{bmatrix}$$

$$= \begin{bmatrix} 60275 \\ 60009 \\ 36467 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 115 \\ 105 \\ 115 \end{bmatrix} = \begin{bmatrix} s \\ i \\ s \end{bmatrix}$$

$$p_5 = \begin{bmatrix} 229 & 171 & 198 \\ 227 & 171 & 199 \\ 114 & 85 & 228 \end{bmatrix} \begin{bmatrix} 57 \\ 246 \\ 92 \end{bmatrix}$$

$$= \begin{bmatrix} 13053 + 42066 + 18216 \\ 12939 + 42066 + 18308 \\ 6498 + 20910 + 20976 \end{bmatrix}$$

$$= \begin{bmatrix} 73335 \\ 73313 \\ 48384 \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} 119 \\ 97 \\ 97 \end{bmatrix} = \begin{bmatrix} w \\ a \\ \text{NULL} \end{bmatrix}$$

Diperoleh *plaintext* semula sebagai berikut,

$$p_1 = \begin{bmatrix} S \\ a \\ y \end{bmatrix} p_2 = \begin{bmatrix} a \\ spasi \\ M \end{bmatrix} p_3 = \begin{bmatrix} a \\ h \\ a \end{bmatrix} p_4 = \begin{bmatrix} s \\ i \\ s \end{bmatrix} p_5 = \begin{bmatrix} w \\ a \\ \text{NULL} \end{bmatrix}$$

Berdasarkan hasil dekripsi yang kedua menggunakan algoritma *Hill Cipher* diperoleh *plaintext* semula yaitu **Saya Mahasiswa** karena NULL termasuk karakter ASCII 256 yang tidak tercetak**.** Proses dekripsi menggunakan algoritma *Hill Cipher* dilakukan dengan mengalikan *ciphertext* dengan invers dari kunci simetris $\overline{K}$.

Dengan demikian pesan yang diterima sesuai dengan pesan yang telah dikirimkan. Baik dengan blok-blok *plaintext* yang sesuai dengan *ordo* matriks ataupun yang berbeda. Dapat diartikan bahwa pesan tidak diketahui oleh kriptanalis yang berusaha mengubah isi pesan. Sehingga mengamankan pesan menggunakan proses enkripsi dan dekripsi algoritma *Hill Cipher* dan *ElGamal* berhasil dilakukan.

3.4 Kesesuaian Agama dengan Konsep Enkripsi dan Dekripsi

Berdasarkan konsep kriptografi terdapat dalam al-Qur'an yaitu menjaga amanat, hal tersebut terdapat dalam surat an-Nisa' ayat 58, yaitu:

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

"*Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum diantara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah maha mendengar lagi maha melihat" (Q.S an-Nisa/4:58).*

Dari penjelasan surat an-Nisa' ayat 58 di atas dapat diketahui bahwa Allah Swt. memerintahkan agar amanat-amanat itu disampaikan pada orang yang berhak menerimanya. Sebagaimana pesan pada konsep kriptografi, bahwa pesan yang dikirim dari suatu tempat ke tempat lain haruslah terkirim dan terjaga kerahasiaannya. Sehingga pesan dapat dibaca oleh penerima dengan aman. Memanfaatkan kerumitan-kerumitan algoritma yang digunakan sehingga sebuah amanat tetap terjaga.

Pembentukan algoritma baru dengan menggabungkan algoritma *Hill Cipher* dan *ElGamal* dapat meningkatkan keamanan pada proses enkripsi dan dekripsi pada pesan teks. Sehingga penelitian ini dapat memudahkan pengirim dan penerima untuk menyembunyikan *plaintext* agar tidak diketahui oleh kriptanalis. Dengan demikian bahwa menggunakan pengetahuan yang dimiliki oleh peneliti bermanfaat bagi orang lain. Sebagaimana firman Allah Swt. pada QS. al-Zalzalah ayat 7, yaitu:

فَمَنْ يَّعْمَلْ مِثْقَالَ ذَرَّةٍ خَيْرًا يَّرَه ﴿٧﴾

"*Maka barang siapa yang mengerjakan kebaikan sebesar dzarrah-pun, ia akan mendapatkan balasan" (Q.S al-Zalzalah/30:7).*

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan hasil penelitian tentang proses enkripsi dan dekripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal* dapat ditarik kesimpulan sebagai berikut,

1. Proses enkripsi algoritma *Hill Cipher* dan *ElGamal* dengan menggunakan perhitungan matematika secara manual menghasilkan dua *ciphertext*. Menggunakan algoritma *Hill Cipher ciphertext* yang diperoleh melalui *plaintext* pesan. Sedangkan enkripsi menggunakan *ElGamal* menghasilkan *ciphertext* dari kunci simetris. Mengonversikan *plaintext* menggunakan tabel ASCII 256 sehingga dapat mengubah alfabet menjadi simbol-simbol yang tidak dimengerti. Dengan melakukan penyandian mengakibatkan *plaintext* memiliki tingkat keamanan yang tinggi dari serangan kriptanalis. Apabila kriptanalis dapat mengetahui potongan kunci memungkinkan dengan mudah dapat mengetahui *plaintext* asli. Namun pada penelitian ini kunci simetris dienkripsi menggunakan algoritma *ElGamal*.
2. Proses dekripsi menggunakan algoritma *Hill Cipher* dan *ElGamal* dapat mengubah *ciphertext* menjadi *plaintext* semula. Sehingga dapat diartikan bahwa proses dekripsi dapat dilakukan dengan baik. Karena *ciphertext* yang diperoleh adalah *ciphertext* pesan maka terlebih dahulu menentukan

plaintext dari kunci. Maka yang dilakukan mengubah *ciphertext* kunci menggunakan algoritma *ElGamal*. Kemudian menghasilkan kunci simetris yang digunakan sebagai kunci untuk melakukan dekripsi pada *ciphertext* pesan. Menggunakan algoritma *Hill Cipher* akan diperoleh *plaintext* asli yang sesuai dengan teks yang dikirimkan oleh pengirim. Sehingga proses dekripsi dapat dilakukan dengan menggunakan perhitungan matematika manual.

4.2 Saran

Setelah melakukan penelitian tentang proses enkripsi dan dekripsi pesan teks menggunakan algoritma *Hill Cipher* dan *ElGamal* peneliti memberikan saran kepada pembaca bahwa pada penelitian ini enkripsi dan dekripsi menggunakan perhitungan matematika manual dapat dilakukan dengan baik. Namun seiring dengan perkembangan teknologi diperlukan untuk meningkatkan kerumitan algoritma dalam melakukan pengamanan pesan teks. Tentunya dengan memodifikasi atau menggabungkan algoritma kriptografi yang lain.

DAFTAR PUSTAKA

Al-Qur'an dan Terjemah. 19998. Al Basyir. Semarang:ASY-SYIFA'

Ahmadi, S. K. (2016). *Ciphertext-only attack on d x d Hill in O(d13^d)*. 1-16.

Anton, H. (1987). *Aljabar Linear Elementer* (5 ed.). (R. Hutauruk, Penyunt., & I. N. Pantur Silaban, Penerj.) Jakarta: Erlangga.

Ariyus, D. (2008). *Pengantar Ilmu Komputer Teori Analisis dan Implementasi*. (F. S. Suryantoro, Penyunt.) Yogyakarta: C.V ANDI OFFSET.

Hamidah, S. N. (2009). *Konsep Matematis dan Konsep Penyandian Algoritma ElGamal*. Universitas Islam Negeri Maulana Malik Ibrahim Malang, Matematika, Malang.

Hill, L. S. (1929). *Cryptography in An Algebraic Alphabet*. The American Mathematical Monthly, 306 - 312.

Hondro, R. K. (2017). *Teknik Enkripsi dan Dekripsi Algoritma Hill Cipher*. STIMK Budi Darma, (hal. 1-5). Medan.

Irawan, W. H. (2014). *Pengantar Teori Bilangan* (1 ed.). (A. H. Fathani, Penyunt.) Malang: UIN-Maliki Press.

Jamaludin. (2018, April). *Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem*. *Sinkron, II*, 86 - 93.

Munir, R. (2010). *Matematika Diskrit* (Edisi 3 ed.). Bandung: Informatika Bandung.

Ramadani, S. (2020, April). *HYBIRD CRYPTOSYSTEM ALGORITMA HILL CIPHER DAN ALGORITMA. METHOMIKA, IV*, 1-9.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. (T. A. Prabawati, Penyunt.) Yogyakarta: C.V ANDI OFFSET.

Yusman, M. (2015). *Pengembangan Aplikasi Enkripsi dan Dekripsi Keamanan Data Menggunakan Metode ASCII*. Universitas Lampung, Matematika dan Ilmu Pengetahuan Alam, Lampung.

LAMPIRAN

a. Karakter ASCII 256 yang tidak terlihat simbolnya

Kode ASCII	Simbol	Deskripsi
00	NULL	Null char
01	SOH	Start of Heading
02	STX	Start of Text
03	ETX	End of Text
04	EOT	End of Transmission
05	ENQ	Enquiry
06	ACK	Acknowledgment
07	BEL	Bell
08	BS	Back Space
09	HT	Horizontal Tab
10	LF	Line Feed
11	VT	Vertical Tab
12	FF	Form Feed
13	CR	Carriage Return
14	SO	Shift Out
15	SI	Shift In
16	DLE	Data Line Escape
17	DC1	Device Control 1 (oft.XON)
18	DC2	Device Control 2
19	DC3	Device Control 3 (oft. XOFF)
20	DC4	Device Control 4
21	NAK	Negative Acknowledgement
22	SYN	Synchronous Idle
23	ETB	End of Transmit Block
24	CAN	Cancel
25	EM	End of Medium
26	SUB	Substitute
27	ESC	Escape
28	FS	File Separator
29	GS	Group Separator
30	RS	Record Separator
31	US	Unit Separator
127	DEL	Delete

b. Karakter ASCII 256 yang terlihat simbolnya

Kode ASCII	Simbol	Deskripsi
32		Space
33	!	Exclamation mark
34	"	Double quotes
35	#	Number
36	$	Dollar
37	%	Per cent sign
38	&	Ampersand
39	'	Single quote
40	(	Open parenthesis
41	)	Close parenthesis
42	*	Asterisk
43	+	Plus
44	,	Comma
45	-	Hyphen
46	.	dot
47	/	divide
48	0	Zero
49	1	One
50	2	Two
51	3	Three
52	4	Four
53	5	Five
54	6	Six
55	7	Seven
56	8	Eight
57	9	Nine
58	:	Colon
59	;	Semicolon
60	<	Less than
61	=	Equals
62	>	Greater than
63	?	Question mark
64	@	At symbol
65	A	Uppercase A
66	B	Uppercase B
67	C	Uppercase C

Kode ASCII	Simbol	Deskripsi
68	D	Uppercase D
69	E	Uppercase E
70	F	Uppercase F
71	G	Uppercase G
72	H	Uppercase H
73	I	Uppercase I
74	J	Uppercase J
75	K	Uppercase K
76	L	Uppercase L
77	M	Uppercase M
78	N	Uppercase N
79	O	Uppercase O
80	P	Uppercase P
81	Q	Uppercase Q
82	R	Uppercase R
83	S	Uppercase S
84	T	Uppercase T
85	U	Uppercase U
86	V	Uppercase V
87	W	Uppercase W
88	X	Uppercase X
89	Y	Uppercase Y
90	Z	Uppercase Z
91	[	Opening bracket
92	\	Backslash
93	]	Closing bracket
94	^	Caret - circumflex
95	_	Underscore
96	`	Grave accent
97	a	Lowercase a
98	b	Lowercase b
99	c	Lowercase c
100	d	Lowercase d
101	e	Lowercase e
102	f	Lowercase f
103	g	Lowercase g

Kode ASCII	Simbol	Deskripsi
104	h	Lowercase h
105	i	Lowercase i
106	j	Lowercase j
107	k	Lowercase k
108	l	Lowercase l
109	m	Lowercase m
110	n	Lowercase n
111	o	Lowercase o
112	p	Lowercase p
113	q	Lowercase q
114	r	Lowercase r
115	s	Lowercase s
116	t	Lowercase t
117	u	Lowercase u
118	v	Lowercase v
119	w	Lowercase w
120	x	Lowercase x
121	y	Lowercase y
122	z	Lowercase z
123	{	Opening brace
124	|	Vertical bar
125	}	Closing brace
126	~	Equivalency sign - tilde

c. Karakter ASCII 256 yang tidak tercantum pada keyboard tapi dapat ditampilkan

Kode ASCII	Simbol	Deskripsi
128	Ç	Majuscule C-cedilla
129	ü	Letter u with umlaut
130	é	Letter e with acute accent
131	â	Letter a with circumflex accent
132	ä	Letter a with umlaut
133	à	Letter a with grave accent
134	å	Letter a with a ring
135	ç	Minuscule c-cedilla
136	ê	Letter e with circumflex accent

Kode ASCII	Simbol	Deskripsi
137	ë	Letter e with umlaut
138	è	Letter e with grave accent
139	ï	Letter i with umlaut
140	î	Letter i with circumflex accent
141	ì	Letter i with grave accent
142	Ä	Letter A with umlaut
143	Å	Capital letter A with a ring
144	É	Capital letter E with acute accent
145	æ	Latin diphthong ae in lowercase
146	Æ	Latin diphthong AE in uppercase
147	ô	Letter o with circumflex accent
148	ö	Letter o with umlaut
149	ò	Letter o with grave accent
150	û	Letter u with circumflex accent
151	ù	Letter u with grave accent
152	ÿ	Lowercase letter y with diaeresis
153	Ö	Letter O with umlaut
154	Ü	Letter U with umlaut
155	Ø	Empty set
156	£	Pound sign : symbol for the pound sterling
157	Ø	Empty set
158	×	Multiplication sign
159	ƒ	Function sign
160	á	Lowercase letter a with acute accent
161	í	Lowercase letter i with acute accent
162	ó	Lowercase letter o with acute accent
163	ú	Lowercase letter u with acute accent
164	ñ	Lowercase n with tilde
165	Ñ	Uppercase N with tilde
166	ª	Feminine ordinal indicator
167	º	Masculine ordinal indicator
168	¿	Inverted question marks
169	®	Registered trademark symbol
170	¬	Logical negation symbol
171	½	One half
172	¼	Quarter
173	¡	Inverted exclamation marks

Kode ASCII	Simbol	Deskripsi
174	«	Right-pointing quotation mark
175	»	Left-pointing quotation marks
176	░	Graphic character, low density dotted
177	▒	Graphic character, medium density dotted
178	▓	Graphic character, high density dotted
179	│	Box drawing character single vertical line
180	┤	Box drawing character single vertical and left line
181	Á	Capital letter A with acute accent or A-acute
182	Â	Letter A with circumflex accent or A-circumflex
183	À	Letter A with grave accent
184	©	Copyright symbol
185	╣	Box drawing character double line vertical and left
186	║	Box drawing character double vertical line
187	╗	Box drawing character double line upper right corner
188	╝	Box drawing character double line lower right corner
189	¢	Cent symbol
190	¥	YEN and YUAN sign
191	┐	Box drawing character single line upper right corner
192	└	Box drawing character single line lower left corner
193	┴	Box drawing character single line horizontal and up
194	┬	Box drawing character single line horizontal down
195	├	Box drawing character single line vertical and right
196	─	Box drawing character single horizontal line
197	┼	Box drawing character single line horizontal vertical
198	ã	Lowercase letter a with tilde
199	Ã	Capital letter A with tilde
200	╚	Box drawing character double line lower left corner
201	╔	Box drawing character double line upper left corner
202	╩	Box drawing character double line horizontal and up
203	╦	Box drawing character double line horizontal down
204	╠	Box drawing character double line vertical and right
205	═	Box drawing character double horizontal line
206	╬	Box drawing character double line horizontal vertical
207	¤	Generic currency sign
208	Đ	Lowercase letter eth

Kode ASCII	Simbol	Deskripsi
209	Ð	Capital letter Eth
210	Ê	Letter E with circumflex accent
211	Ë	Letter E with umlaut
212	È	Capital letter E with grave accent
213	I	Lowercase dot less i
214	Í	Capital letter I with acute accent or I-acute
215	Î	Letter I with circumflex accent
216	Ï	Letter I with umlaut
217	┘	Box drawing character single line lower right corner
218	┌	Box drawing character single line upper left corner
219	█	Block, graphic character
220	▄	Bottom half block
221	¦	Vertical broken bar
222	Ì	Capital letter I with grave accent
223	▀	Top half block
224	Ó	Capital letter O with acute accent
225	ß	Letter Eszett
226	Ô	Letter O with circumflex accent
227	Ò	Capital letter O with grave accent
228	õ	Lowercase letter o with tilde
229	Õ	Capital letter O with tilde
230	µ	Lowercase letter Mu
231	þ	Lowercase letter Thorn
232	Þ	Capital letter Thorn
233	Ú	Capital letter U with acute accent
234	Û	Letter U with circumflex accent
235	Ù	Capital letter U with grave accent
236	ý	Lowercase letter y with acute accent
237	Ý	Capital letter Y with acute accent
238	¯	Macron symbol
239	´	Acute accent
240	≡	Congruence relation symbol
241	±	Plus-minus sign
242	‗	Underline

Kode ASCII	Simbol	Deskripsi
243	¾	Three quarters
244	¶	Paragraph sign
245	§	Section sign
246	÷	The division sign
247	¸	Cedilla
248	°	Degree symbol
249	¨	Diaresis
250	·	Space dot
251	¹	Exponent 1
252	³	Exponent 3
253	²	Exponent 2
254	■	Black square
255	Nbsp	No-breaking space

RIWAYAT HIDUP

Siti Nur Fadlilah adalah nama penulis skripsi ini. Penulis lahir dari orang tua Nurhuda dan Rusiati sebagai anak pertama dari dua bersaudara. Penulis dilahirkan di Desa Candiwatu Kecamatan Pacet Kabupaten Mojokerto pada tanggal 13 Februari 1999. Penulis menempuh pendidikan dimulai dari Taman Kanak-kanak PGRI Candiwatu (lulus tahun 2005), melanjutkan ke Sekolah Dasar Negeri (SDN) Candiwatu dan Madrasah Tsanawiyah (Mts) Miftahul Ulum Gondang (lulus tahun 2014). Kemudian melanjutkan ke jenjang Sekolah Menengah Atas (SMA) di SMA Islam Diponegoro Gondang (lulus tahun 2017) dan melanjutkan studi di Universitas Islam Negeri Maulanan malik Ibrahim Malang pada tahun 2017. Penulis mengambil fakultas Sains dan Teknologi Program Studi Matematika.

Penulis mengenal organisasi sejak duduk di bangku Sekolah Dasar Negeri (SDN) sebagai Pradana dalam kegiatan pramuka tahun 2008. Kemudian di Mts. menjabat sebagai sekretaris II periode 2011/ 2012, kemudian sebagai ketua Organisasi Siswa Intra Seolah (OSIS) dan melanjutkan di extrakurikuler pramuka. Pada tahun 2014 di SMA sebagai Sekretaris periode 2014/2015. Penulis tetap aktif dalam dunia kepramukaan sebagai pembina pramuka di Mts. Toriqul Ulum. Pada tahun 2015 sebagai ketua OSIS periode 2015/2016. Setelah melanjutkan ke jenjang Universitas mendalami organisasi di Keluarga Besar Mahasiswa Bidikmisi (KBMB) dengan mengemban amanah sebagai Sekretaris II periode 2018/2019 dan bendahara umum periode 2019/2020.

Ketika memasuki semester delapan penulis fokus dengan skripsi yang sedang dikerjakan. Dengan ketekunan, motivasi tinggi untuk terus berusaha dan belajar sehingga penulis dapat menyelesaikan pengerjaan tugas akhir skripsi ini. Semoga dengan penulisan tugas akhir skripsi ini mampu memberikan kontribusi positif bagi dunia pendidikan. Akhir kata penulis mengucapkan rasa syukur yang sebesar-besarnya atas terselesaikannya skripsi yang berjudul "Enkripsi dan Dekripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal* untuk Mengamankan Pesan Teks".

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

BUKTI KONSULTASI SKRIPSI

Nama : Siti Nur Fadlilah
NIM : 17610003
Fakultas/Program Studi: Sains dan Teknologi/ Matematika
Judul Skripsi : Enkripsi dan Dekripsi Menggunakan Algoritma *Hill Cipher* dan *ElGamal* untuk Mengamankan Pesan Teks
Pembimbing I : Prof. Dr. H. Turmudi, M.Si., Ph.D
Pembimbing II : Muhammad Khudzaifah, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	09 Maret 2021	Konsultasi BAB I,II dan III	1.
2.	19 Maret 2021	Konsultasi BAB I, II dan Kajian Keislaman	2.
3.	22 Maret 2021	Revisi BAB I,II dan III	3.
4.	30 Maret 2021	Konsultasi BAB III	4.
5.	16 April 2021	Revisi BAB III	5.
6.	27 April 2021	Konsultasi BAB IV	6.
7.	04 Mei 2021	ACC BAB I sampai BAB IV untuk diseminarkan	7.
8.	05 Mei 2021	ACC BAB I sampai BAB IV untuk diseminarkan	8.
9.	18 Mei 2021	Revisi BAB I dan III	9.
10.	04 Agustus 2021	Konsultasi BAB IV dan Abstrak	10.
11.	19 Agustus 2021	Konsultasi BAB III dan Kajian Keislaman	11.
12.	6 September 2021	ACC keseluruhan untuk disidangkan	12.
13.	6 September 2021	ACC keseluruhan untuk disidangkan	13.

Malang, 06 Desember 2021
Mengetahui,
Ketua Program Studi Matematika

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