# KOMBINASI METODE *VIGÈNERE CIPHER* DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA

**SKRIPSI**

**OLEH:**
**LUDYAWATI**
**NIM. 19610036**

**PROGRAM STUDI MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2023**

# KOMBINASI METODE *VIGÈNERE CIPHER* DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA

**SKRIPSI**

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

**Oleh**
**Ludyawati**
**NIM. 19610036**

**PROGRAM STUDI MATEMATIKA**
**FAKULTAS SAINS DAN TEKNOLOGI**
**UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM**
**MALANG**
**2023**

# KOMBINASI METODE *VIGÈNERE CIPHER* DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA

**SKRIPSI**

**Oleh**
**Ludyawati**
**NIM. 19610036**

Telah Diperiksa dan Disetujui Untuk Diuji

Malang, 6 Juni 2023

| Dosen Pembimbing I | Dosen Pembimbing II |
|---|---|
| Muhammad Khudzaifah, M.Si | Erna Herawati, M.Pd |
| NIDT. 19900511 20160801 1 057 | NIDT. 19760723 20180201 2 222 |

Mengetahui,
Ketua Program Studi Matematika,

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

# KOMBINASI METODE *VIGÈNERE CIPHER* DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA

**SKRIPSI**

**Oleh**
**Ludyawati**
**NIM. 19610036**

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

Tanggal 8 Juni 2023

| | | | |
|---|---|---|---|
| Ketua Penguji | : | Dr. Hairur Rahman, M.Si | ..... |
| Anggota Penguji 1 | : | Juhari, M.Si | ..... |
| Anggota Penguji 2 | : | Muhammad Khudzaifah, M.Si | ..... |
| Anggota Penguji 3 | : | Erna Herawati, M.Pd | ..... |

Mengetahui,
Ketua Program Studi Matematika,

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

## PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

| | |
|---|---|
| Nama | : Ludyawati |
| NIM | : 19610036 |
| Program Studi | : Matematika |
| Fakultas | : Sains dan Teknologi |
| Judul Skripsi | : Kombinasi Metode *Vigènere Cipher* Dan Elgamal Pada Pengamanan Pesan Rahasia |

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

Malang, 8 Juni 2023

Yang membuat pernyataan,


Ludyawati

NIM. 19610036

## MOTO

“Orang yang meraih kesuksesan tidak selalu orang yang pintar, tapi orang yang selalu meraih kesuksesan adalah orang yang gigih dan pantang menyerah.”
(Susi Pudjiastuti)

## PERSEMBAHAN

Skripsi ini, penulis persembahkan kepada seluruh pihak yang telah berperan bagi penulis sejak awal masa perkuliahan hingga selesainya penelitian ini. Penulis mengucapkan terimakasih dengan segala ketulusan hati kepada kedua orang tua penulis Ayahanda Kariono dan Ibunda Suwarni, serta adik penulis Lucky Aprilia yang telah memberikan do'a, semangat, motivasi, serta dorongan moril dan materil serta kasih saying yang tak terhingga kepada penulis.

Sahabat dan teman-teman penulis semasa perkuliahan, Fairuz Nadhif Izdhihar, Sukmawati Indah Safitri, Tre Hayu Ria Sageta, dan Synta Shofiatul Khusniah yang telah memberikan memberikan bantuan dan dorongan saat menyelesaikan penulisan dan penyusunan skripsi ini.

Kepada saudara Yoga Dipayana Putra yang yang telah memberikan do'a, semangat, motivasi, serta dorongan moril dan materil sehingga penulis dapat menyelesaikan penyusunan dan penulisan skripsi ini.

Diri saya sendiri yang sudah berjuang dengan keras secara fisik dan mental, untuk menuntaskan segala tanggung jawab perkuliahan dengan semaksimal mungkin.

# KATA PENGANTAR

*Assalamu'alaikum Warahmatullahi Wabarakatuh*

Segala puji bagi Allah Swt. Atas segala rahmat yang telah diberikan sehingga penulis mampu menyelesaikan penulisan dan penyusunan skripsi dengan judul "Kombinasi Metode *Vigènere Cipher* Dan ElGamal pada Pengamanan Pesan Rahasia" sebagai syarat untuk memperoleh gelar sarjana Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sholawat serta salam senantiasa tercurahkan kepada baginda Rasulullah Muhammad Saw. yang telah membimbing umatnya dari jaman yang gelap gulita menuju jaman yang terang benderang yakni agama Islam.

Dalam proses penulisan dan penyusunan skripsi ini tidak lepas dari bimbingan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu patutlah penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

Ucapan terima kasih dituliskan sebagai berikut:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I yang telah meluangkan waktunya untuk memberikan bimbingan, arahan, nasehat, serta ilmu sehingga penulis dapat menyelesaikan penelitian ini.
5. Erna Herawati, M.Pd., selaku dosen pembimbing II yang telah memberikan bimbingan dan arahan kepada penulis dengan baik.
6. Dr. Hairur Rahman, M.Si., selaku Penguji Utama dalam Ujian Skripsi yang telah memberikan kritik dan saran yang membangun kepada penulis.
7. Juhari, M.Si., selaku Ketua Penguji dalam Ujian Skripsi yang telah memberikan kritik dan saran yang membangun kepada penulis.

8. Seluruh dosen dan staf administrasi Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim yang telah memberikan ilmu dan bimbingan kepada penulis.
9. Ayahanda Kariono, Ibunda Suwarni, dan adik penulis Lucky Aprilia yang telah memberikan do'a, semangat, motivasi, serta dorongan moril dan materil sehingga penulis dapat menyelesaikan penyusunan dan penulisan skripsi ini.
10. Kepada saudara Yoga Dipayana Putra yang telah memberikan do'a, semangat, motivasi, serta dorongan moril dan materil sehingga penulis dapat menyelesaikan penyusunan dan penulisan skripsi ini.
11. Seluruh mahasiswa matematika angkatan 2019 terutama Fairuz Nadhif Izdhihar, Sukmawati Indah Safitri, Tre Hayu Ria Sageta, dan Synta Shofiatul Khusniah yang telah memberikan bantuan dan dorongan saat menyelesaikan penulisan dan penyusunan skripsi ini.
12. Semua pihak yang tidak dapat disebutkan satu-persatu yang telah membantu dalam menyelesaikan skripsi ini.

Malang, 8 Juni 2023

Penulis

**DAFTAR ISI**

## DAFTAR TABEL

## DAFTAR GAMBAR

## DAFTAR SIMBOL

$C$ = Cipherteks
$P$ = Plainteks
$K$ = Kunci
$E$ = Enkripsi
$D$ = Dekripsi
$\alpha$ = Akar primitif Acak
$\beta$ = Kunci Publik
$d$ = Kunci Rahasia
$i$ = Urutan ke-
$k$ = Bilangan bulat Acak
$p$ = Bilangan Prima
$\gamma$ = Cipherteks ElGamal
$\delta$ = Cipherteks ElGamal
$\mathbb{Z}_p^*$ = Himpunan bilangan Bulat yang membentuk grup perkalian modulo $p$

## DAFTAR LAMPIRAN

# ABSTRAK

Ludyawati. 2023. **Kombinasi Metode *Vigènere Cipher* Dan ElGamal pada Pengamanan Pesan Rahasia**. Skripsi Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Pembimbing (1): Muhammad Khudzaifah, M.Si, Pembimbing (2): Erna Herawati, M.Pd.

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

*Vigènere Cipher* adalah salah satu kriptografi algoritma simetris yang menggunakan satu jenis kunci yang sama pada proses enkripsi dan dekripsi. Keamanan dari metode *Vigènere Cipher* terletak pada perhitungan modulo yang digunakan. ElGamal adalah salah satu kriptografi algoritma asimetris yang menggunakan dua jenis kunci yang berbeda pada proses enkripsi dan dekripsi. Keamanan dari algoritma ElGamal adalah terletak pada kerumitan perhitungan bilangan prima besar. *Vigènere Cipher* dan ElGamal memiliki kelebihan dan kekurangan masing-masing. Oleh karena itu peneliti tertarik untuk mengkombinasikan kelebihan dari dua metode tersebut. Pada penelitian ini dilakukan dua kali penguncian pada proses enkripsi dan dekripsi. Pada proses enkripsi menggunakan kunci publik dan pada proses dekripsi menggunakan kunci publik $(p, \alpha, \beta)$ dan kunci rahasia $(d)$. Kunci yang digunakan berasal dari pembentukan kunci menggunakan algoritma ElGamal. Keamanan kunci yang dibentuk dari algoritma ElGamal terletak pada bilangan prima besar aman $p$, akar primitif $\alpha$ dari bilangan prima $p$, dan bilangan bulat acak $d$ yang berasal dari tiga digit terakhir dari Nomor Induk Mahasiswa. Kesimpulan dari penelitian ini adalah kombinasi dari metode *Vigènere Cipher* dan ElGamal dapat meningkatkan keamanan pesan rahasia karena menghasilkan cipherteks dengan ukuran dua kali lipat $(\gamma, \delta)$ dari pesan asli.

# ABSTRACT

Ludyawati. 2023. **Combination of the Vigènere Cipher and ElGamal Methods for Securing Secret Messages**. Thesis Mathematics Study Program, Faculty of Science and Technology, UIN Maulana Malik Ibrahim Malang, Supervisor (1): Muhammad Khudzaifah, M.Sc, Supervisor (2): Erna Herawati, M.Pd.

**Keywords**: Encryption, Decryption, Vigènere Cipher, ElGamal.

Vigènere Cipher is a symmetric cryptographic algorithm that uses the same type of key in the encryption and decryption process. The security of the Vigènere Cipher method lies in the modulo calculation used. ElGamal is an asymmetric cryptographic algorithm that uses two different types of keys in the encryption and decryption process. The security of the ElGamal algorithm lies in the complexity of calculating large prime numbers. The Vigènere Cipher and ElGamal have their advantages and disadvantages. Therefore researchers are interested in combining the advantages of the two methods. In this study, two locks were carried out in the encryption and decryption process. The encryption process uses a public key and the decryption process uses a public key $(p, \alpha, \beta)$ and a secret key $(d)$. The key used comes from key formation using the ElGamal algorithm. The key security formed from the ElGamal algorithm lies in the large prime $p$, the primitive root $\alpha$ of the prime number $p$, and the random integer $d$ which comes from the last three digits of Student Number. The conclusion of this study is that the combination of the Vigènere Cipher and ElGamal methods can increase the security of secret messages because it produces a ciphertext with twice the size $(\gamma, \delta)$ of the original message.

# مستخلص البحث

لودياواتي. ٢٠٢٣. مزيج من طرق تشفير ***Vigènere*** و تشفير ***ElGamal*** لتأمين الرسائل السرية. البحث العلمي الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج، المشرف (١): محمد حد يفة ، الما جستير ، المشرف (٢): اير نا هيرا وا تي ، الما جستير.

الكلمات المفتاحية: التشفير ، فك التشفير ، تشفير *Vigènere* ، تشفير *ElGamal*.

تشفير *Vigènere* هو خوارزمية تشفير متماثلة تستخدم نفس النوع من المفاتيح في عمليات التشفير وفك التشفير. يكمن أمان طريقة تشفير *Vigènere* في حساب *modulo* المستخدم. تشفير *ElGamal* هو من احد ى خوارزمية تشفير غير متماثلة تستخدم مفتحين مختلفين في عمليات التشفير وفك التشفير. يكمن أمان خوارزمية تشفير *ElGamal* في تعقيد حساب الأعداد الأولية الكبرى. تشفير *Vigènere* و تشفير *ElGamal* مزاياهما وعيوبهما. لذلك ، يهتم كا نت البا حثة تجلب كثيرا في البحث عن مزا يا هد ين الشفرين. ثم إجراء قفلين في عملية التشفير وفك التشفير. في عملية التشفير باستخدام المفتاح العام وفي عملية فك التشفير باستخدام المفتاح العام $(p, \alpha, \beta)$ والمفتاح السري $(d)$. يأتي المفتاح المستخدم من تشكيل المفاتيح باستخدام خوارزمية الجمل. يكمن الأمان الرئيسي المتكون من خوارزمية الجمل في العدد الأولي الكبرى الآمن $p$ ، والجذر البدائي $\alpha$ للعدد الأولي $p$ ، والعدد الصحيح العشوائي $d$ المشتق من الأرقام الثلاثة الأخيرة من رقم تعريف الطالب. استنتاج هذه الدراسة هو أن الجمع بين طريقتي تشفير *Vigènere* و تشفير *ElGamal* يمكن أن يحسن أمان الرسائل السرية لأنه ينتج نصا مشفرا بضعف حجم الرسالة الأصلية $(\gamma, \delta)$.

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Pada zaman seperti saat ini, salah satu aset yang berharga dan harus dilindungi adalah informasi. Pengaksesan informasi menjadi lebih mudah dengan adanya jaringan komputer seperti internet. Hal ini termasuk kedalam sisi positif dari kemajuan sistem informasi. Di sisi lain, sisi negatif dari kemajuan sistem informasi berkaitan dengan masalah kemanan. Salah satu contoh dari masalah keamanan adalah jatuhnya informasi ke tangan pihak tidak terkait, hal tersebut dapat menyebabkan kerugian bagi pemilik informasi. Jatuhnya informasi ke pihak tidak terkait menjadi ancaman yang cukup serius bagi pihak-pihak penting seperti pemerintahan, militer, perbankan, pendidikan, dan lain-lain. Bagi pihak tersebut faktor utama yang harus terpenuhi dalam menggunakan internet sebagai alat pengirim pesan rahasia adalah tingkat keamanan informasi. Perintah untuk menjaga kerahasiaan pesan tercantum di firman Allah Swt. Q.S An-Nisa ayat 58 yang berbunyi :

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

*"Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat."(Q.S An Nisa:58)*

Pesan tersirat yang dapat diambil dari ayat tersebut adalah pentingnya menjaga kerahasiaan pesan dan menyampaikan pesan kepada yang berhak sesuai dengan amanah yang telah diberikan. Hal tersebut sesuai dengan prinsip

Kriptografi, yaitu mengamankan pesan atau informasi sampai kepada penerima agar tidak bocor ke pihak tidak terkait. Pengubahan pesan rahasia menjadi kode-kode yang sulit dimengerti oleh pihak tidak terkait umumnya menggunakan metode penyandian. Pada awal pembentukan metode penyandian, fokus utama dari metode ini adalah pada kerahasiaan algoritma. Akan tetapi hal ini dianggap kurang pada aspek kenyamanan karena mengingat sebelum melakukan pertukaran pesan rahasia setiap pengguna diharuskan untuk membuat algoritma baru. Kemudian, muncul perkembangan dengan menggunakan metode penyandian baru. Metode penyandian memiliki fokus yang berbeda, yaitu lebih difokuskan kepada kerahasiaan kunci atau yang dikenal dengan Kriptografi. Walaupun memiliki fokus utama yang berbeda, akan tetapi metode Kriptografi dapat dengan baik menjaga pesan rahasia dari pihak tidak terkait yang akan melakukan pencurian informasi.

Kriptografi menurut (Munir, 2019) memiliki 2 algoritma yang didasarkan pada kuncinya, diantaranya Algoritma simetris (*symmetric-key cryptography*) dan algoritma asimetris (*asymmetric-key cryptography*). Algoritma simetris memiliki satu jenis kunci yang digunakan untuk proses enkripsi dan proses dekripsi. Sedangkan untuk algoritma asimetris memiliki dua jenis kunci. Kunci yang digunakan terdiri dari kunci publik dan kunci rahasia. Kunci publik digunakan pada proses enkripsi dan kunci rahasia digunakan pada proses dekripsi. Keamanan algoritma simestris terletak pada kerahasiaan kuncinya. Sedangkan kelemahan algoritma simetri adalah untuk memulihkan pesan yang telah disandikan, kunci yang digunakan penerima harus sama dengan kunci pengirim pesan. Berbeda dengan algoritma simetris, algoritma asimetris memiliki 2 kelebihan yaitu tidak

perlu untuk mengirimkan kunci rahasia sebagaimana algoritma simetris dan jumlah kunci dapat ditekan. Kunci rahasia tidak dikirimkan karena kunci tersebut dapat dibuat sendiri oleh pihak penerima pesan dengan mengacu pada kunci publik yang diberikan dan bilangan acak. Kelebihan kedua terletak pada banyaknya jumlah kunci yang dapat dibuat sebanyak jumlah pihak yang diajak berkorespondesni (Munir, 2019). Salah satu contoh dari algoritma simetris seperti *Vigènere Cipher* dan algortima asimetris seperti ElGamal.

Ada beberapa penelitian yang telah dilakukan dengan mengkombinasikan kedua algoritma tersebut untuk mengamankan informasi yang berupa pesan rahasia maupun citra(gambar). Misalnya menurut penelitian Bella Ariska, Suroso, dan Jon Endri tahun 2018 tentang kombinasi algoritma simetris yaitu *Vigènere Cipher* dan algoritma asimetris yaitu ElGamal yang diterapkan pada pengamanan pesan rahasia. Penelitian tersebut berjudul *Rancangan Kriptografi Hybrid Kombinasi Metode Vigènere Cipher dan Elgamal pada Pengamanan Pesan Rahasia*. Pada penelitian tersebut ditunjukkan bahwa ditunjukan bahwa algoritma Elgamal dan *Vigènere Cipher* dapat melakukan proses enkripsi dan dekripsi pesan rahasia serta mempunyai kemampuan yang baik dalam mengatasi masalah pada proses pendistribusian kunci. Dengan memanfaatkan Kriptografi *hybrid* kombinasi ini dapat meningkatan kecepatan proses enkripsi dan dekripsi tanpa mengurangi kenyamanan dan kemanan.

Penelitian kedua yaitu Divananda Zikry Fadilla tahun 2017 tentang kombinasi algoritma simetris yaitu *Vigènere Cipher* dan algoritma asimetris yaitu ElGamal yang diterapkan pada pengamanan citra. Penelitian tersebut berjudul *Implementasi Algoritma ElGamal dan Vigènere Cipher untuk Enkripsi dan*

*Dekripsi Data Citra Digital*. Pada penelitian tersebut ditunjukan bahwa algoritma Elgamal dan *Vigènere Cipher* melakukan enkripsi dan dekripsi pada citra atau gambar. Kekurangan dari penelitian ini yaitu pada proses dekripsi hasil gambar tidak bisa kembali 100% seperti *pixel* awal. Penyebab kekurangan ini berada pada perhitungan algoritma ElGamal yang menggunakan modulo bilangan prima.

Berdasarkan penelitian-penelitian yang telah dilakukan pada algoritma simetris yaitu *Vigènere Cipher* dan algoritma asimetris yaitu ElGamal dapat disimpulkan bahwa kedua algoritma tersebut memiliki kelebihan dan kekurangan masing-masing. Kelebihan dari kedua algoritma tersebut dapat dikombinasikan sehingga dapat meningkatkan tingkat keamanan pesan dan juga meminimalisir kekurangan dari kombinasi tersebut. Oleh karenanya penulis tertarik untuk melakukan penelitian tentang penerapan kombinasi algoritma *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia.

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses enkripsi dari kombinasi metode *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia?
2. Bagaimana proses dekripsi dari kombinasi metode *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia?

## 1.3 Tujuan Penelitian

Berdasarkan uraian rumusan masalah, tujuan penelitian dalam penelitian ini adalah sebagai berikut:

1. Mengetahui proses enkripsi kombinasi metode *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia.
2. Mengetahui proses dekripsi kombinasi metode *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia.

## 1.4 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penulisan penelitian ini adalah sebagai berikut:

1. Menambah pemahaman dan wawasan tentang proses enkripsi dan dekripsi kombinasi metode *Vigenère Cipher* dan ElGamal dengan menggunakan pendekatan matematika.
2. Sebagai tambahan referensi pembelajaran mata kuliah Kriptografi, khususnya yang berkaitan dengan *Vigènere Cipher* dan ElGamal.
3. Menambah pemahaman dan wawasan keilmuwan Kriptografi pada proses enkripsi dan dekripsi untuk pengamanan pesan melalui kombinasi metode *Vigènere Cipher* dan ElGamal.

## 1.5 Batasan Masalah

Agar penelitian ini tidak meluas, maka diberikan batasan masalah. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Plainteks berdasarkan pada tabel *ASCII printable*.

2. Bilangan acak yang digunakan dalam proses enkripsi berasal dari *Microsoft Excel*.
3. Perhitungan modulo dalam metode *Vigènere Cipher* dan ElGamal dilakukan dengan *software Python.*
4. Bilangan bulat acak $d$ diperoleh dari tiga digit terakhir NIM.

## 1.6 Definisi Istilah

Penelitian ini memiliki beberapa istilah, diantaranya sebagai berikut:

1. Pesan

   Pesan adalah informasi yang pengirim inmgin sampaikan kepada penerima. Pesan ini dapat berbentuk teks, suara/bunyi, citra/gambar, video, atau bentuk biner lainnya yang berbentuk digital maupun analog. Dalam ilmu Kriptografi terdapat istilah plainteks dan cipherteks. Plainteks adalah pesan rahasia yang akan disandikan dan cipherteks adalah pesan yang telah disandikan.

2. Pengirim dan penerima

   Dalam sistem komunikasi, terdapat dua pihak yaitu pihak pengirim dan pihak penerima. Pihak yang akan mengirimkan pesan atau informasi disebut dengan pengirim. Sedangkan orang yang menerima pesan atau informasi yang telah dikirimkan oleh pihak pengirim disebut dengan penerima.

3. Enkripsi dan Dekripsi

   Enkripsi adalah proses menyandikan pesan menjadi kode-kode yang sulit dimengerti. Pada proses enkripsi ini melakukan perubahan plainteks menjadi

cipherteks. Sedangkan dekripsi adalah proses pengembalian atau pemulihan pesan terkodekan atau cipherteks menjadi pesan asli atau plainteks.

4. Cipher, kode, dan kunci

   Cipher adalah algoritma Kriptografi yang digunakan untuk proses enkripsi dan dekripsi. Cipher dapat diartikan sebagai aturan yang digunakan untuk menyandikan pesan atau plainteks. Kode adalah prosedur yang diacu untuk mengganti setiap plainteks dengan satu kata kode. Perubahan dari plainteks menjadi kode disebut *encoding*, sebaliknya perubahan kode menjadi plainteks disebut *decoding*. Kunci dalam Kriptografi ada dua yaitu kunci rahasia dan kunci publik. Kunci rahasia biasanya digunakan pada Kriptografi modern. Hal ini sejalan dengan prinsip Kreckhoff yang berbunyi "Semua algoritma Kriptografi harus publik; hanya kunci yang rahasia" (Munir, 2019).

5. Sistem Kriptografi

   Sistem Kriptografi adalah sistem yang terbentuk untuk menyandikan pesan dengan fokus utamanya adalah kerahasiaan kunci. Sistem ini mengubah pesan rahasia atau plainteks menjadi kode-kode pesan atau cipherteks atau sebaliknya.

6. Kriptanalisis

   Kriptanilisis berbanding terbalik dengan Kriptografi. Jika Kriptografi menyandikan pesan agar tidak diketahui oleh pihak tidak terkait, kriptanalisis adalah memecahkan pesan yang telah disandikan. Kriptanalisis adalah seni memecahkan cipherteks menjadi plainteks tanpa mengetahui

kunci yang digunakan dalam proses enkripsi-dekripsi. Orang yang melakukan kriptanalisis disebut kriptanalis.

# BAB II

# KAJIAN TEORI

## 2.1 Kriptografi

### 2.1.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *crypto* dan *graphia*. *Crypto* yang berarti rahasia(*secret*) atau menyembunyikan dan *graphia* yang berarti tulisan(*writting*). Secara harfiah Kriptografi adalah "*secret writing*" yang berarti tulisan rahasia. Sebelum tahun 1980-an definisi yang digunakan untuk Kriptografi adalah ilmu dan seni yang digunakan yang bertujuan menjaga kerahasiaan pesan dengan cara mengubahnya menggunakan proses penyandian menjadi bentuk yang tidak dapat dipahami maknanya (Munir, 2019).

Kriptografi dalam pengertian modern adalah ilmu yang dipergunakan dalam aspek keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas dengan berdasarkan teknik matematika. Dapat disimpulkan bahwa menurut pengertian modern, Kriptografi tidak hanya berhubungan dengan penyembunyian pesan rahasia tetapi sekumpulan teknik yang digunakan untuk mengamankan pesan (Sadikin, 2012).

### 2.1.2 Sejarah Kriptografi

Sejarah Kriptografi sudah dimulai sejak ribuan tahun yang lalu. Bahkan Kriptografi sudah ada sejak zaman Mesir kuno (*ancient cryptography*) yang jauh sebelum abad Masehi. Bangsa Mesir kuno, Cina, India Kuno, Romawi dan Yunani menggunakan kriptografi sebagai cara menyamarkan pesan dari pihak

musuh. Bangsa Arab pun ikut andil dalam sejarah Kriptografi. Bangsa Arab menggunakan Kriptografi pada abad 9 sampai 15 Masehi yang pada saat itu adalah masa kejayaan peradaban Islam di Baghdad (Munir, 2019).

Kriptografi juga digunakan pada zaman Reisans di Eropa. Asal mula kriptografi di saman Reisans ini adalah berasal dari Baghdad atau Bangsa Arab. Para mahasiswa yang telah selesai menuntut ilmu di Baghdad pulang kembali ke Eropa. Mereka membawa pulang semua ilmu yang telah mereka dapatkan termasuk Kriptografi, oleh karenanya saat itu dinamakan jaman Reisans atau jaman kebangkitan Eropa. Pada jaman ini tercatat 2 *cipher* subtitusi yang terkenal yaitu *Vigenère Cipher* (Tahun 1586) dan *Playfair Cipher* (Tahun 1854). Sejarah Kriptografi juga tercatat pada abad ke-17 yaitu pada saat ratu Skotlandia, Queen Marry dihukum mati setelah surat (sudah dienkripsi) yang dikirimnya berhasil terpecahkan. Surat tersebut berisi tentang rencananya untuk membunuh Ratu Elizabeth I. Sejarah kriptografi juga tercatat saat perang dunia I dan II. Saat itu Jerman menggunakan enigma (mesin enkripsi) sebagai salah satu strategi perang. Akan tetapi, hal tersebut tidak bertahan lama karena pihak Sekutu berhasil memecahkannya.

Salah satu pemicu kemunculan kriptografi modern adalah perkembangan peralatan komputer digital (Munir, 2019). Perkembangan komputer digital menyebabkan *cipher* yang dihasilkan lebih kompleks dan berbentuk biner. Oleh karena itu Kriptografi modern tidak hanya berkaitan dengan pengamanan pesan rahasia, akan tetapi juga memunculkan konsep seperti tanda tangan digital dan sertifikat digital.

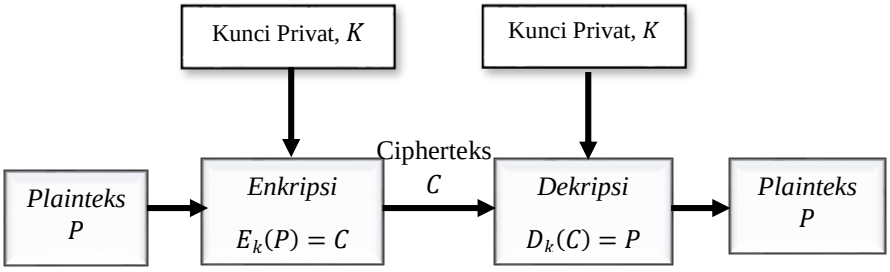
### 2.1.3 Macam-macam Algoritma Kriptografi

Menurut (Munir, 2019) algortima dikelompokkan berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, diantaranya:

1. Algoritma Simetris

   Algoritma simetris memiliki satu kunci yang digunakan untuk proses enkripsi dan proses dekripsi (Ariyus, 2008).Sistem dari algoritma simetris dapat berjalan jika pengirim dan penerima memiliki kunci yang sama saat bertukar pesan.

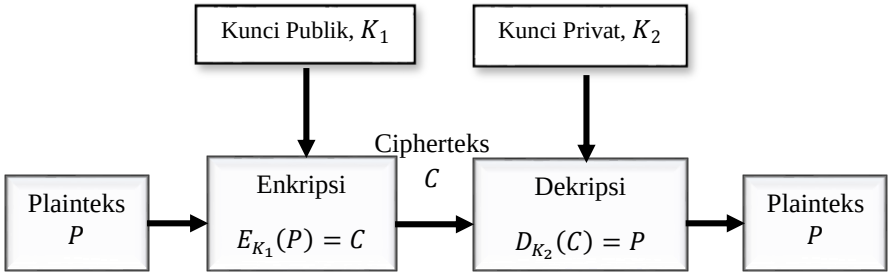
***Gambar 2.1*** *Skema Kriptografi Simetri*




2. Algoritma Asimetris

   Algortima asimetris adalah algoritma yang menggunakan dua kunci berbeda pada proses enkripsi dan dekripsi. Kunci yang digunakan saat proses enkripsi adalah kunci publik sedangakn kunci yang digunakan saat proses dekripsi adalah kunci publik. Algortima asimetris disebut juga dengan kriptografi kunci publik (Ariyus, 2006). Pada Kriptografi kunci publik, pengirim dan penerima memegang sepasang kunci. Pengirim mengenkripsi pesan rahasia menggunakan kunci publik dan penerima mendekripsi pesan yang sudah disandikan menggunakan kunci rahasia.

***Gambar 2.2*** *Skema Algoritma Asimetris.*




### 2.1.4 Kriptografi Klasik dan Modern

1. Kriptografi Klasik

   Kriptografi klasik termasuk ke dalam algoritma simetris. Oleh karena itu dapat di simpulkan bahwa Kriptografi klasik menggunakan satu kunci untuk proses enkripsi dan dekripsi. Kriptografi klasik terdiri dari dua teknik dasar, diantaranya (Munir, 2019):

   a. Teknik subtitusi (*substitution ciphers*)

      Teknik substitusi adalah teknik mengganti setiap karakter dengan karakter lain (Ariyus, 2006). Teknik substitusi terdiri dari beberapa jenis, yaitu monoalphabet (*cipher* abjad-tunggal), polyalphabet (*cipher* abjad-banyak), monograf (*cipher* subtitusi homofonik), dan *polygraph* (*cipher* subtitusi poligram). Beberapa metode yang termasuk di teknik substitusi diantaranya *Caesar cipher*, *Affine cipher*, *Vigenere Cipher*, *Playfair Cipher*, dan *Hill Cipher* (Munir, 2019)

   b. Teknik transposisi (*transposition ciphers*)

      Teknik transposisi adalah teknik memindahkan posisi karakter teks asli ke posisi lain tanpa mengubah nilai aslinya. Dengan kata lain, teknik ini melakukan *transpose* terhadap rangkaian karakter asli pada plainteks. Nama lain dari tenik ini adalah teknik mutasi, karena *transpose* setiap

karakter asli pada plainteks sama dengan mempermutasikan karakter-karakter tersebut (Munir, 2019).

2. Kriptografi Modern

   Kriptografi modern adalah kriptografi yang ada di era komputer digital, sehingga data yang direpresentasikan dalam bentuk biner. Jika syarat tersebut terpenuhi maka informasi dalam bentuk apapun dapat dienkripsi. Berbeda dengan kriptografi klasik, kriptografi modern dapat mengenkripsi berbagai jenis data digital seperti citra/gambar, suara, video, objek 3-D, atau sebagainya. Kriptografi modern termasuk kedalam algoritma asimetris. Oleh karena itu dapat disimpulkan bahwa kriptografi modern menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Selain itu, konsep fungsi *hash* muncul dalam kriptografi modern. Fungsi *hash* melahirkan konsep tanda tangan digital yang berguna sebagai otentikasi dan nirpenyangkalan (Munir, 2019).

## 2.2 Penggunaan Konsep Matematika pada metode *Vigenère cipher*

### 2.2.1 Teori Bilangan

Teori bilangan adalah ilmu yang mempelajari tentang bilangan dan sifat-sifatnya. Oleh karenanya teori bilangan disebut sebagai aritmatika lanjut atau *advanced arithmetic* (Kraft, 2015). Teori bilangan atau *number theory* adalah teori yang berperan penting dalam Kriptografi. Bilangan yang digunakan dalam Kriptografi adalah bilangan bulat (*integer*). Bilangan bulat digunakan dalam algoritma simetris dan asimetris.

### 2.2.2 Bilangan Bulat

Bilangan yang tidak memiliki pecahan desimal disebut dengan bilangan bulat. $\mathbb{Z}$ atau *Zahlen* digunakan sebagai simbol dari himpunan dari semua bilangan bulat. $\mathbb{Z}$ atau *Zahlen* berasal dari bahasa Jerman. Notasi lain dari bilangan bulat adalah *I* atau *Integer* yang berasal dari bahasa Inggris. Himpunan bilangan bulat terdiri dari bilangan bulat positif dan bilangan bulat negatif. Bilangan bulat positif adalah bilangan bulat yang lebih besar dari nol yang dinotasikan dengan $\mathbb{Z}^+$. Sedangkan bilangan bulat negatif adalah bilangan bulat yang lebih kecil dari nol yang dinotasikan dengan $\mathbb{Z}^-$(Kraft, 2015).

### 2.2.3 Keterbagian

**Definisi 2.1**

Misalkan $a, b \in \mathbb{Z}$ dengan $a \neq 0$. $a$ dikatakan habis membagi $b$ jika tidak memiliki sisa bagi ($r = 0$) atau $a = bx$ untuk suatu $x \in \mathbb{Z}$ (Ariyus, 2006).

Notasi keterbagian bilangan bulat dapat ditulis sebagai beikut:

1. Simbol $a|b$ dipakai untuk menyatakan bahwa $b$ habis dibagi $a$, $a$ membagi habis $b$, $b$ kelipatan $a$
2. Simbol $a \nmid b$ dipakai untuk menyatakan bahwa $b$ tidak habis dibagi $a$, $a$ tidak membagi habis $b$, $b$ bukan kelipatan $a$

**Teorema 2.2**

Diberikan $a, b, c \in \mathbb{Z}$ (Ariyus, 2006).

1. Jika $a|b$ maka $a|bx$, untuk setiap bilangan bulat $x$;
2. Jika $a|b$ dan $b|c$, maka $a|c$;
3. Jika $a|b$ dan $a|c$, maka $a|(bx + cy)$ untuk setiap $x, y \in \mathbb{Z}$

4. Jika $a|b$ dan $b|a$, maka $a \equiv \pm b$;
5. Jika $a|b$, $a > 0, b > 0$, maka $a \leq b$;
6. Untuk setiap bilangan bulat $x \neq 0$, $a|b$ jika dan hanya jika $xa|xb$;

**Bukti:**

1. Jika $a|b$ maka ada $m \in \mathbb{Z}$ sedemikian sehingga $b = a \cdot m$. Akibatnya untuk setiap $n \in \mathbb{Z}$ diperoleh $bn = (an)m = a(nm)$. Pada bilangan bulat terdapat aturan sifat tertutup terhadap perkalian maka terdapat $p = nm$. Sehingga $bn = ap$, maka $a|bx$.
2. Jika $a|b$ maka $b = am$ untuk $m \in \mathbb{Z}$ dan $b|c$ maka $c = bn$ untuk $m \in \mathbb{Z}$. Sedemikian sehingga diperoleh $c = bn = (am)n = a(mn)$, untuk suatu $m, n \in \mathbb{Z}$. Maka $a|c$.
3. Jika $a|b$ maka $b = am$ untuk $m \in \mathbb{Z}$ dan dan $a|c$ maka $c = an$ untuk $n \in \mathbb{Z}$. Sehingga $bx = (am)x$ untuk setiap $x \in \mathbb{Z}$ dan $cy = (an)y$ untuk setiap $y \in \mathbb{Z}$. Diperoleh $bx + cy = (am)x + (an)y = a(mx + ny)$ untuk suatu $mx + ny \in \mathbb{Z}$. Maka $a|(bx + cy)$.
4. Jika $a|b$ maka $b = am$ untuk $m \in \mathbb{Z}$ dan dan $b|a$ maka $a = bn$ untuk $n \in \mathbb{Z}$. Diperoleh $b = am = (bn)m = b(nm)$ maka $b - b(nm) = b(1 - nm) = 0$. Karena $b \neq 0$ maka $1 - nm = 0$ atau $nm = 1$. Sedemikian sehingga $n = m = 1$ atau $n = m = -1$. Maka $a \equiv \pm b$.
5. Jika $a|b$ maka $b = am$ untuk $m \in \mathbb{Z}$. Jika $a > 0, b > 0$ dan $b = am$ maka untuk $m = 1$ terpenuhi $a = b$. Sedangkan untuk $m > 1$ maka $b > a$. Maka $a \leq b$.
6. Jika $a|b$ maka $b = am$ untuk $m \in \mathbb{Z}$. Akibatnya untuk $x \in \mathbb{Z}$ dan $x \neq 0$ berlaku $xb = x(am) = (xa)m$. Sehingga $xa|xb$. Jika $xa|xb$ dan $x \neq 0$,

maka $xb = (xa)m$ untuk suatu $x \in \mathbb{Z}$. $xb = (xa)m = x(am)$ atau $xb - (xa)m = x(b - am) = 0$. Karena $m \neq 0$, maka $b - am = 0$ atau $b = am$ untuk $m \in \mathbb{Z}$. Maka $a|b$.

### 2.2.4 Aritmatika Modulo

**Definisi 2.3**

Misalkan $a$ adalah bilangan bulat dan $c$ adalah bilangan bulat dan $c > 0$. Operasi $a\ mod\ c$. Bilangan $c$ disebut dengan modulo atau modulus. Dalam aritmatika modulo $c$ terletak pada himpunan $\{0,1,2, \dots, m - 1\}$. Dengan kata lain $a\ mod\ c = e$ sedemikian sehingga $a = cf + e$ dengan $0 \leq e < c$ (Munir, 2019).

Operasi modulo dapat diartikan mencari sisa $r$ yang merupakan sisa bagi atas operasi $a$ atas $c$. Bilangan $c$ disebut moldulus atau modulo dan hasil operasi modulo $c$ terletak di dalam himpunan $\{0,1,2, \dots, c - 1\}$ (Munir, 2019).

**Contoh 2.4**

Temukan hasil operasi berikut:

1. $45\ mod\ 7$
2. $35\ mod\ 6$
3. $12\ mod\ 5$

Jawab:

1. $45\ mod\ 7 = 3$

   45 dibagi 7 adalah 6 dengan sisa 3, $45 = (7 \times 6) + 3$. Sehingga $45\ mod\ 7 = 3$
2. $35\ mod\ 6 = 5$

35 dibagi 6 adalah 5 dengan sisa 5, $35 = (6 \times 5) + 5$. Sehingga $35\ mod\ 6 = 5$

3. $12\ mod\ 5 = 2$

   12 dibagi 5 adalah 2 dengan sisa 2, $12 = (5 \times 2) + 2$. Sehingga $12\ mod\ 5 = 2$

### 2.2.5 Kongruensi

**Definisi 2.5**

Misalkan $a$ dan $b$ adalah bilangan bulat dan $n > 0$, ditulis $a \equiv b\ (mod\ n)$ jika $n|(a - b)$. Jika $a$ tidak kongruen dengan $b$ dalam modulus $n$, maka dituliskan $a \not\equiv b(mod\ n)$ (Munir, 2019).

**Contoh 2.6**

Beberapa contoh kekongruenan:

1. $63 \equiv 8(mod\ 5)$ (5 habis membagi $63 - 8 = 55$)
2. $43 \equiv 3(mod\ 8)$ (8 habis membagi $43 - 3 = 40$)
3. $59 \equiv 5(mod\ 9)$ (9 habis membagi $59 - 5 = 54$)

Berdasarkan definisi operasi modulo, $a\ mod\ n = b$ sedemikian hingga $a = b + nc$ dengan $0 \leq b < n$ sehingga dapat ditulis juga sebagai $a \equiv b(mod\ n)$

**Contoh 2.7**

1. $75\ mod\ 9 = 3$ dapat dituliskan sebagai $75 \equiv 3(mod\ 9)$
2. $53\ mod\ 7 = 4$ dapat dituliskan sebagai $53 \equiv 4(mod\ 7)$
3. $89\ mod\ 9 = 8$ dapat dituliskan sebagai $89 \equiv 8(mod\ 9)$

## 2.3 *Vigenère Cipher*

*Vigenère Cipher* adalah salah satu contoh Kriptografi klasik teknik substitusi *cipher polyalphabet* (abjad-banyak). Pertama kali dipublikasikan oleh *Blaisè de Vigenère* seorang diplomat Prancis sekaligus kriptologis pada abad 16 yaitu tahun 1586. Digambarkan pertama kali oleh Giovian Batista Belaso pada tahun 1553 pada bukunya yang berjudul *La Cifra del Sig*. Ide dasar dari metode ini adalah sama seperti metode *Caesar cipher*, akan tetapi jumlah pergeseran tiap huruf berbeda-beda. Untuk mengenkripsi pesan rahasia biasanya dapat menggunakan *tabula recta* (Ariyus, 2006).

*Tabula recta* digunakan untuk memperoleh cipherteks dari kunci yang sudah ditentukan. Kunci dari *Vigenère Cipher* ini bersifat fleksibel, maksud dari fleksibel ini adalah kunci yang digunakan dapat menyesuaikan panjang dari plainteks. Jika plainteks lebih panjang dari kunci maka kunci dapat diulang sampai semua plainteks memiliki kunci.

Enkripsi dengan menggunakan *Vigenère cipher* dapat diformulasikan secara matematis. Misalkan kunci dengan panjang $i$ adalah rangkaian $k_1, k_2, \dots, k_i$. Plainteks adalah rangkaian $p_1, p_2, \dots, p_i$. Dan cipherteks adalah rangkaian $c_1, c_2, \dots, c_i$, maka proses Enkripsi menggunakan metode *Vigènere Cipher* dengan modifikasi modulo *ASCII Printable* menggunakan perhitungan sebagai berikut (Putri, 2021):

$$C_i = ((P_i + K_i - 32) mod\ 95) + 32 \qquad (2.1)$$

**Bukti:**

Misalkan plainteks adalah $C = C_1, C_2, \dots, C_i$, kunci adalah $K = K_1, K_2, \dots, K_i$ dan cipherteks adalah $P = P_1, P_2, \dots, P_i$. Langkah pembuktiannya adalah sebagai berikut:

a. Letakkan teks asli, kunci, dan teks terenkripsi dalam bentuk numerik berdasarkan karakter dengan kode ASCII *printable*. Konversi plainteks dan kunci menjadi urutan dengan kode karakter dalam ASCII *printable*. pastikan untuk membatasi karakter yang digunakan hanya pada karakter ASCII *printable*, yaitu karakter dengan kode ASCII antara 32 hingga 126.
b. Rumus enkripsi *Vigenère cipher* dengan menggunakan ASCII *printable* adalah $C_i = (P_i + K_i - 32) mod\ 95 + 32$, dimana 95 adalah jumlah karakter dalam ASCII *printable* dan penambahan 32 dilakukan untuk menggeser hasil modulo ke rentang karakter ASCII *printable* (32 hingga 126).
c. Perhitungan tersebut memastikan bahwa karakter-karakter dalam cipherteks didapatkan dengan melakukan penjumlahan modulo 95 dari karakter-karakter plainteks dan karakter kunci, dan kemudian menggeser hasil modulo ke rentang karakter ASCII *printable*.
d. Dengan demikian telah dibuktikan bahwa $C_i = (P_i + K_i - 32) mod\ 95 + 32$.

Proses Dekripsi menggunakan metode *Vigènere Cipher* dengan modifikasi modulo *ASCII Printable* menggunakan perhitungan sebagai berikut: (Putri, 2021)

$$P_i = ((P_i - K_i - 32) mod\ 95) + 32 \qquad (2.2)$$

**Bukti:**

Misalkan plainteks adalah $P = P_1, P_2, \dots, P_i$, kunci adalah $K = K_1, K_2, \dots, K_i$ dan cipherteks adalah $C = C_1, C_2, \dots, C_i$. Langkah pembuktiannya adalah sebagai berikut:

a. Letakkan teks asli, kunci, dan teks terenkripsi dalam bentuk numerik berdasarkan karakter dengan kode ASCII *printable*. Konversi plainteks dan kunci menjadi urutan dengan kode karakter dalam ASCII *printable*. pastikan untuk membatasi karakter yang digunakan hanya pada karakter ASCII *printable,* yaitu karakter dengan kode ASCII antara 32 hingga 126

b. Rumus dekripsi *Vigenère cipher* dengan menggunakan ASCII *printable* adalah $P_i = (P_i - K_i - 32) mod\ 95 + 32$, dimana $95$ adalah jumlah karakter dalam ASCII *printable* dan penambahan 32 dilakukan untuk menggeser hasil modulo ke rentang karakter ASCII *printable* (32 hingga 126).

c. Perhitungan tersebut memastikan bahwa karakter-karakter dalam cipherteks didapatkan dengan melakukan penjumlahan modulo 95 dari karakter-karakter plainteks dan karakter kunci, dan kemudian menggeser hasil modulo ke rentang karakter ASCII *printable*.

d. Dengan demikian telah dibuktikan bahwa $P_i = ((P_i - K_i - 32) mod\ 95) + 32$.

**Contoh 2.8**

Proses Enkripsi:

***Tabel 2.3*** *Proses Enkripsi Vigenère cipher*

| **Plainteks** | I | N | D | O | N | E | S | I | A |
|---|---|---|---|---|---|---|---|---|---|
| **Indeks** | 73 | 78 | 68 | 79 | 78 | 69 | 83 | 73 | 65 |
| **Kunci** | L | E | M | A | R | I | L | E | M |
| **Indeks** | 76 | 69 | 77 | 65 | 82 | 73 | 76 | 69 | 77 |
| $C_i = ((P_i + K_i - 32) mod\ 95) + 32$ | 54 | 52 | 50 | 49 | 65 | 47 | 64 | 47 | 47 |
| **Cipherteks** | 6 | 4 | 2 | 1 | A | / | @ | / | / |

Proses Dekripsi:

***Tabel 2.4*** *Proses* Dekripsi *Vigenère cipher*

| **Cipherteks** | 6 | 4 | 2 | 1 | A | / | @ | / | / |
|---|---|---|---|---|---|---|---|---|---|
| **Indeks** | 54 | 52 | 50 | 49 | 65 | 47 | 64 | 47 | 47 |
| **Kunci** | L | E | M | A | R | I | L | E | M |
| **Indeks** | 76 | 69 | 77 | 65 | 82 | 73 | 76 | 69 | 77 |
| $P_i = ((P_i - K_i - 32) mod\ 95) + 32$ | 73 | 78 | 68 | 79 | 78 | 69 | 83 | 73 | 65 |
| **Plainteks** | I | N | D | O | N | E | S | I | A |

## 2.4 Penggunaan Konsep Matematika pada algoritma ElGamal

### 2.4.1 Bilangan Prima

Bilangan bulat positif $p$ lebih dari 1 yang pembaginya hanya 1 dan $p$ disebut dengan bilangan prima. Kecuali 2 yang merupakan bilangan genap, semua bilangan prima adalah bilangan ganjil. Bilangan prima sangat penting didalam Kriptografi. Penggunaan bilangan prima dalam Kriptografi terdapat dalam algoritma asimetris atau algoritma kunci-publik (Munir, 2019).

Untuk menguji apakah bilangan bulat tersebut termasuk bilangan prima atau bukan, maka digunakan suatu teorema. Teorema tersebut adalah teorema

Fermat. Nama Fermat sendiri berasal dari matematikawan Perancis pada tahun 1640 (Ariyus, 2006).

**Teorema 2.9**

Jika $p$ adalah bilangan prima dan $a$ adalah bilangan bulat yang tidak habis dibagi dengan $p$, dengan $\gcd(a, p) = 1$, maka

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

Untuk sebarang $a \in \mathbb{Z}_p$(Munir, 2019).

**Bukti:**

Jika $a \in \mathbb{Z}_p$ dan $n$ adalah bilangan bulat maka berlaku $a^{\varphi(n)} \equiv 1(mod\ n)$. Diambil $n = p$ sehingga diperoleh $a^{p-1} \equiv a^{\varphi(n)} \equiv 1(mod\ p)$.

**Contoh 2.10**

Buktikan apakah $127$ adalah bilangan prima dengan menggunakan teorema Fermat.

Bukti:

$2^{127-1} = (2^7)^{17} \times 2^7$ (Dipilih $2^7 = 128$ karena dekat dengan 127)

$2^{126} = 1^{17} \cdot 2^7 (mod\ 123)$ $(2^7 = 128 \equiv 1\ mod\ (127))$

$2^{126} = 1 \cdot 2^7 (mod\ 123)$ $(1^{17} = 1)$

$2^{126} = 1 \cdot 1(mod\ 123)$ $(2^7 = 128 \equiv 1\ mod\ (127))$

$2^{126} = 1$

Karena $2^{127-1} \equiv 1(mod\ 127)$, maka $127$ adalah bilangan prima

### 2.4.2 Keprimaan Aman

Fungsi dari keprimaan aman adalah mengecek bilangan prima yang telah dipilih benar-benar aman dan memiliki kekuatan yang cukup dalam membentuk

kunci kriptografi ElGamal (Andrian, 2014). Hal ini sejalan dengan letak keamanan kriptografi ElGamal adalah pada kerumitan perhitungan bilangan prima. Maka, untuk mengecek keamanan bilangan prima dapat dilakukan melalui uji keprimaan aman berikut (Basyiah, 2017):

$$p = 2q + 1$$

**Bukti:**

Untuk membuktikan uji keprimaan aman dengan menggunakan persamaan 2.3, dimana $p$ dan $q$ adalah bilangan prima, dapat menggunakan pendekatan berikut:

1. Anggap $p$ bukanlah bilangan prima, artinya $p$ dapat difaktorkan menjadi $p = ab$, dimana $a$ dan $b$ adalah bilangan bulat positif yang lebih kecil dari $p$.
2. Jika $a = b$, maka $a^2 = p$, yang berarti $p$ bukanlah bilangan prima. Oleh karena itu, diasumsikan $a \neq b$.
3. Karena $a$ dan $b$ adalah faktor dari $p$, dapat dituliskan persamaan tersebut menjadi $p \equiv 0\ (mod\ a)$ dan $p \equiv 0\ (mod\ b)$. Karena $p = 2q + 1$, sehingga dapat dituliskan $2q \equiv -1\ (mod\ a)$ dan $2q \equiv -1\ (mod\ b)$. Perhatikan bahwa $2q + 1 \equiv 1\ (mod\ a)$ dan $2q + 1 \equiv 1\ (mod\ b)$. Dapat disimpulkan bahwa $2q \equiv 0\ (mod\ a)$ dan $2q \equiv 0\ (mod\ b)$.
4. Namun, hal ini berarti $a$ dan $b$ adalah faktor dari $2q$. Karena $q$ adalah bilangan prima, maka faktor-faktor dari $2q$ adalah $1, 2, q, 2q$. Oleh karena itu, untuk $a$ dan $b$ hanya memiliki 4 kemungkinan yaitu:
   a. Jika $a = 1$, maka persamaannya menjadi $p \equiv 0\ (mod\ 1)$, bernilai benar untuk semua bilangan $p$.

b. Jika $a = 2$, maka persamaannya menjadi $p \equiv 0\ (mod\ 2)$, bernilai benar untuk semua bilangan genap $p$.
c. Jika $a = q$, maka persamaannya menjadi $p \equiv 0\ (mod\ q)$, bernilai benar karena $p$ adalah kelipatan dari $q$.
d. Jika $a = 2q$, maka persamaannya menjadi $p \equiv 0\ (mod\ 2q)$, bernilai benar karena $p = 2q$.

5. Dalam semua kasus, tidak ditemukan faktor yang berbeda dari 1 dan $p$ untuk $p = 2q + 1$. Oleh karena itu dapat disimpulkan bahwa $p$ adalah bilangan prima. Dalam konteks uji keprimaan aman jika $p = 2q + 1$, dengan $p$ dan $q$ sebagai bilangan prima maka $p$ adalah bilangan prima.

Bilangan prima dapat dikatakan bilangan prima aman jika memenuhi syarat (Basyiah, 2017):

1. Hitung $q$ dengan persamaan penentuan bilangan prima aman.
2. Jika $q$ merupakan bilangan prima, maka $p$ merupakan bilangan prima aman.
3. Jika $q$ bukan merupakan bilangan prima aman, maka $p$ bukan merupakan bilangan prima aman

### *2.4.3 Great Common Divisor (GCD)*

**Definisi 2.11**

Misalkan $a, b \in \mathbb{Z}$ dan $a, b \neq 0$. Bilangan $d$ disebut faktor persekutuan dari $a, b$ jika $d|a$ dan $d|b$. Faktor persekutuan besar atau *great common divisior(gcd)* dari $a$ dan $b$ jika $d$ adalah bilangan bulat positif terbesar sehingga $d|a$ dan $d|b$. Karena *gcd* dari $a$ dan $b > 0$ maka gcd dari $a$ dan $b \geq 1$ (Kraft, 2014).

**Definisi 2.12**

Jika $b$ adalah bilangan prima dan $a$ adalah bilangan bulat yang tidak habis dibagi dengan $b$**,** sehingga $gcd(a, b) = 1$. Maka

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

Untuk sebarang $a \in \mathbb{Z}_b$ (Kraft, 2014).

**Contoh 2.13**

Pembagi dari 12 adalah 1,2,3,4,6, dan 12. Sedangkan pembagi dari 18 adalah 1,2,3,6,9, dan 12. Maka {1,2,3,6}adalah himpunan persekutuan pembagi dari 12 dan 18. Dapat dilihat bahwa himpunan ini memiliki elemen terbesar yaitu 6.

### 2.4.4 Fungsi $\phi - Euler$ dan Teorema Euler

Fungsi ϕ-Euler merupakan fungsi yang memulihkan jumlah bilangan integer $a$ yang $0 < \alpha < p$ dan $\alpha$ adalah prima relatif dengan $p$ bila $\gcd(\alpha, p) = 1$(Sadikin, 2012).

**Definisi 2.14**

Jika diberikan $p$ adalah bilangan prima, maka $\phi(p) = \phi\big(\phi(p)\big) = \phi(p-1)$ (Ariyus, 2008).

**Teorema 2.15**

Jika $(\alpha, p) = 1$ maka $\alpha^{\phi(p)} \equiv 1(mod\ p)$ (Irawan, 2017).

**Bukti:**

Andaikan $r_1, r_2, \dots, r_{\phi(p)}$ merupakan suatu sistem residu modulo $p$. Sehingga $\alpha r_1, \alpha r_2, \dots, \alpha r_{\phi(p)}$ juga merupakan sistem residu modulo $p$. Oleh sebab itu, untuk setiap $r_i$ tentu ada $\alpha r_j$ sedemikian sehingga $r_i \equiv \alpha r_j (mod\ p)$. Akibatnya bilangan – bilangan $\alpha r_1, \alpha r_2, \dots, \alpha r_{\phi(p)}$ tidak lain adalah sisa atau residu modulo dari $p$

walaupun kemungkinan urutan yang dihasilkan tidak sama. Maka diperoleh $\alpha r_1, \alpha r_2, \dots, \alpha r_{\phi(p)} = r_1, r_2, \dots, r_{\phi(p)} (mod\ p)$. Akibatnya $\alpha^{\phi(p)}(r_1, r_2, \dots, r_{\phi(p)}) \equiv (r_1, r_2, \dots, r_{\phi(p)}) (mod\ p)$. Karena $(r_i, p) = 1$ maka $\alpha^{\phi(p)}(r_1, r_2, \dots, r_{\phi(p)}) \equiv 1 (mod\ p)$

**Contoh 2.16**

1. $\phi(10) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$
2. $\phi(13) = \phi\big(\phi(13)\big) = \phi(13 - 1) = 12$ (Karena 13 adalah bilangan prima)
3. $\phi(32) = \phi(2^4) = 2^4 - 2^{4-1} = 32 - 8 = 24$

### 2.4.5 Akar Primitif

**Definisi 2.17**

Jika $n$ adalah bilangan bulat, dan $\alpha$ disebut akar primitif dari $p$ jika berpangkatan $\alpha, \alpha^1, \dots, \alpha^{\phi(p)}$ menghasilkan nilai yang berbeda dan semua relatif prima dengan $p$. Jika $p$ adalah bilangan prima, maka $a$ disebut akar primitif dari $p$ jika perpangkatan $\alpha, \alpha^1, \dots, \alpha^{p-1}$ dalam modulus $p$ (Munir, 2019).

**Teorema 2.18**

Suatu elemen yang membangun $\mathbb{Z}_p{}^*$ disebut akar primitif (*primitif root) mod p*. (Kraft, 2014).

**Bukti:**

Jika $p$ adalah bilangan prima maka $\alpha \in \mathbb{Z}_p^*$ disebut sebagai akar primitif (*primitif root*) $modulo\ p$. Jika setiap bilangan relatif prima $p$ maka kongruen dengan $\alpha\ modulo\ p$. $\alpha$ adalah akar primitif $modulo\ p$ jika dan hanya jika untuk setiap bilangan bulat $\alpha$ sehingga $\gcd(\alpha, p) = 1$, dimana terdapat $k$ bilangan bulat maka:

$$a^k \equiv a (mod\ p) \Leftrightarrow a = a^k (mod\ p)$$

Nilai $k$ disebut logaritma diskrit dari $a$ dengan basis $a\ modulo\ p$. Jadi $a$ adalah akar primitif $modulo\ p$ jika dan hanya jika $a$ adalah generator dari $\mathbb{Z}_p^*$.

Langkah penentuan akar primitif $\alpha$ dinyatakan sebagai berikut:

1. Menentukan $\alpha$ dengan catatan $\alpha \in \mathbb{Z}_p{}^*$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan $p$ atau menggunakan *software Python*.
2. Melakukan pengecekan dengan menggunakan pengujian elemen primitif yaitu $\alpha^2 mod\ p$ dan $\alpha^q mod\ p$ (Basyiah, 2017).
3. Jika $\alpha^2 mod\ p = 1$ dan $\alpha^q mod\ p = 1$, maka $\alpha$ adalah bukan akar primitif.
4. Jika $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka $\alpha$ adalah akar primitif.

   **Teorema 2.19**

   Jika $p$ adalah bilangan prima dan $a$ adalah bilangan relatif prima dengan $p$, maka jika $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, $\alpha$ adalah akar primitif dari $\mathbb{Z}_p{}^*$(Basyiah, 2017).

   **Bukti:**

   a. Asumsikan $a$ adalah akar primitif modulo $p$.
   b. Untuk membuktikan bahwa $\alpha^2 mod\ p \neq 1$, kita asumsikan sebaliknya pembuktian kontradiksi yaitu $\alpha^2 mod\ p = 1 \Leftrightarrow \alpha^2 \equiv 1(mod\ p)$.
   c. Jika $\alpha^2 \equiv 1(mod\ p)$, maka dapat dituliskan $\alpha^2 - 1 \equiv 0(mod\ p)$. Langkah selanjutnya dapat melakukan pemfaktoran sehingga menjadi $(a+1)(a-1) \equiv 0(mod\ p)$. Karena $p$ adalah bilangan prima, maka harus ada salah satu faktor yang kongruen dengan $0(mod\ p)$. Artinya harus ada dua kemungkinan yaitu, $a + 1 \equiv 0(mod\ p)$ atau $a - 1 \equiv 0(mod\ p)$.

d. Jika $a + 1 \equiv 0(mod\ p)$, maka $a \equiv -1(mod\ p)$. Namun berarti $a$ bukanlah akar primitif modulo $p$ karena $a$ tidak memiliki orde $q$ yang membagi $\varphi(p)$. Jika $a - 1 \equiv 0(mod\ p)$, maka $a \equiv 1(mod\ p)$. Namun, ini berarti $a$ bukanlah akar primitif modulo $p$, yang berarti $q$ bukan orde dari $a$ modulo $p$.

e. Oleh karena itu, jika $a$ adalah akar primitif, maka $\alpha^2 \not\equiv 1(mod\ p) \Leftrightarrow \alpha^2 mod\ p \neq 1$.

f. Untuk membuktikan bahwa $\alpha^q mod\ p \neq 1 \Leftrightarrow \alpha^q \not\equiv 1(mod\ p)$ digunakan sifat orde $a$ modulo $a$.

g. Jika $a$ adalah akar primitif modulo $p$, maka orde $a$ yang diberi tanda $q$, adalah bilangan terkecil dimana $\alpha^q \equiv 1(mod\ p)$. Jika $\alpha^q \equiv 1(mod\ p)$, maka $q$ bukanlah orde dari $a$ modulo $p$ karena $q < \varphi(p)$ dan $q$ tidak membagi $\varphi(p)$. Oleh karena itu, jika $a$ adalah akar primitif modulo $p$, maka $\alpha^q \not\equiv 1(mod\ p) \Leftrightarrow \alpha^q mod\ p \neq 1$.

Dengan demikian, dengan menggunakan logika kontradiksi dan sifat-sifat akar primitif dan orde dalam himpunan bilangan bulat yang membentuk grup perkalian modulo $p$, terbukti bahwa $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka $\alpha$ adalah akar primitif.

**Contoh 2.20**

Misalkan $p = 67$, maka $a = 13$ adalah akar primitif 67 dari karena

1. $13^2 mod\ 97$

   $13^2 mod\ 67 \quad = \quad 35$

2. $13^q mod\ p \neq 1$

$13^{33} mod\ 67 \quad = \quad 66$

Karena $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka $\alpha$ adalah akar primitif

### 2.4.6 Logaritma Diskrit

Keamanan Algoritma ElGamal terletak pada kesuliatan perhitungan logaritma diskrit (Munir, 2019). Dapat disimpulkan bahwa logaritma diskrit memiliki peranan yang penting dalam melakukan pengamanan suatu informasi atau pesan rahasia yang menggunakan kriptografi ElGamal (Hamidah, 2009).

**Definisi 2.21**

Misalkan diberikan suatu bilangan prima dengan notasi $p$, akar primitif dengan notasi $a$, dan $h \not\equiv 0$. Maka untuk mencari $x$ atau bisa disebut dengan log diskrit adalah dengan perhitungan berikut:

$$a^x \equiv h\ (mod\ p) \Leftrightarrow h = a^x (mod\ p)$$

$x$ tersebut yang disebut dengan masalah logaritma diskrit (Sadikin, 2012).

**Contoh 2.22**

Temukan $x$ dari $2^x \equiv 10\ mod\ 13$

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

***Tabel** 2.5 Perhitungan Logaritma Diskrit*

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $2^i \equiv 10\ mod\ 13$ | 2 | 4 | 8 | 3 | 6 | 12 | 11 |
| $i$ | 8 | 9 | **10** | 11 | 12 | | |
| $2^i \equiv 10\ mod\ 13$ | 9 | 5 | **10** | 7 | 1 | | |

Karena ketika $i = 10$ nilai $2^i \equiv 10 \, mod \, 13$ maka $log_2(10) = 10$ pada $\mathbb{Z}^*_{13}$. Maka nilai $x = 10$.

### 2.4.7 Eksponensial Modulo

Operasi modulo pada sistem Kriptografi yang sering digunakan yaitu perhitungan eksponensial. Dalam sistem Kriptografi modern khususnya ElGamal dalam proses enkripsi dan dekripsi menggunakan operasi eksponensial modulo. Ekponensial modulo yang digunakan dalam Algortima ElGamal adalah sebagai berikut (Munir, 2019):

$$y = g^x mod \, n \tag{2.4}$$

**Bukti:**

Misalkan $y = a^x mod \, n$, dan akan dibuktikan bahwa persamaan ini benar. berikut adalah langkah-langkah pembuktian:

1. Diasumsikan bahwa $g$, $x$, dan $n$ adalah bilangan bulat positif. Akan dibuktikan bahwa $y = g^x mod \, n$. Ini berarti bahwa $y$ adalah sisa hasil bagi pembagian $g^x$ dengan $n$.
2. Digunakan induksi matematika pada nilai $x$. Basis induksi: jika $x = 1$, maka $y = g^1 mod \, n = g \, mod \, n$. Ini adalah sisa hasil bagi $g$ dengan $n$ dan bernilai benar. Langkah induksi: Diasumsikan bahwa persamaan ini benar untuk suatu nilai $k$, yaitu $y = g^k mod \, n$. Akan dibuktikan bahwa persamaan ini juga benar untuk suatu nilai $k + 1$, yaitu $y = g^{k+1} mod \, n$.
3. Dari asumsi induksi, diketahui bahwa $y = g^k mod \, n$. Dapat ditulis $g^{k+1}$ sebagai $g^k \cdot g$. Jadi dimiliki $y = g^k \cdot g \, mod \, n$. Karena perkalian dalam aritmatika modulo dapat diubah urutannya, dapat dituliskan sebagai $y = g \cdot$

$g^k \, mod \, n$. Diketahui bahwa $y = g^k mod \, n$, sehingga dapat dituliskan menjadi $y = (y \cdot g) \, mod \, n$. Ini berarti $y$ adalah sisa hasil bagi dengan $n$. Karena digunakan aritmatika modulo, sisa hasil bagi perkalian $g$ dan $y$ tetap sama dengan sisa hasil bagi perkalian $g^k$ dan $g$ yaitu $g^{k+1}$.

4. Oleh karena itu dapat disimpulkan bahwa persamaan ini benar untuk $k + 1$. Dengan menggunakan prinsip induksi, dapat dibuktikan bahwa persamaan ini benar untuk setiap nilai $x$ positif.
5. Dengan demikian telah dibuktikan bahwa eksponensial modulo $y = g^x mod \, n$ berlaku. Ini adalah dasar operasi modulo dalam kriptografi.

**Contoh 2.23**

$2^{125} mod \, 527$

$2^0 \equiv 1 \, mod \, 257$

$2^4 = 4^2 \equiv 16 \, mod \, 257$

$2^8 = 16^2 \equiv 256 \, mod \, 257$

$2^{16} = 256^2 \equiv 1 \, mod \, 257$

$2^{32} \equiv 1 \, mod \, 257$

$2^{64} \equiv 1 mod \, 257$

Karena $125 = 64 + 32 + 16 + 8 + 4 + 2$ maka didapatkan

$2^{125} = 1 \cdot 16 \cdot 256 \cdot 1 \cdot 1 \cdot 1 \equiv 241 \, mod \, 257$

## 2.5 ElGamal

Algoritma ElGamal termasuk kedalam algoritma asimetris. Algoritma ini pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Algoritma ElGamal ini pada awalnya digunakan untuk *digital signature*, akan tetapi

kemudian dimodifikasi untuk melakukan enkripsi dan dekripsi pesan (Munir, 2019). Keamanan dari algoritma ElGamal ini terletak pada rumitnya perhitungan logaritma diskrit pada bilangan modulo prima yang besar sehingga upaya untuk melakukan pembobolan menjadi sangat sukar (Andrian, 2014). Algoritma ElGamal tidak dipatenkan oleh pembuatnya akan tetapi didasarkan kepada kriptografi Diffie-Hellman atau dengan kata lain melakukan penyempurnaan terhadap kriptografi Diffie-Hellman (Ariyus, 2006). Pada algoritma ini terdiri atas 3 proses yaitu proses pembentukan kunci, proses enkripsi, dan proses dekripsi (Munir, 2019).

### 2.5.1 Pembentukan Kunci

Pembentukan Kunci terdiri dari pembentukan kunci publik dan rahasia. proses pembentukan kunci dibutuhkan sebuah bilangan prima besar $p$ yang digunakan untuk membentuk $\mathbb{Z}_p{}^*$, akar primitif $\alpha$ dan sebarang bilangan bulat $d$, $0 < d < p - 1$ (ElGamal, 1985). Sedangkan untuk kunci rahasianya adalah $d$. Proses pembentukan kunci menggunakan algoritma ElGamal terdiri atas:

1. Penentuan bilangan prima $p$ aman yang bernilai besar (Ifanto, 2009)

   Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan akar primitif. Untuk menguji keprimaan aman yaitu sebagai berikut (Basyiah, 2017):

   $$p = 2q + 1 \qquad \text{(Berdasarkan Persamaan 2.3)}$$

   Langkah penentuan bilangan aman tersebut dinyatakan sebagai berikut:

   a. Tentukan bilangan $100 < p < 999$ (Ummi, 2013).

Penggunaan interval $100 < p < 999$ adalah berdasarkan peneilitian yang dilakukan oleh Khairul Ummi dengan judul penelitian Analisis Penggunaan Bilangan Prima Aman Besar pada Algoritma ElGamal. Pada penelitian tersebut dapat ditarik kesimpulan bahwa perbandingan cipherteks yang menggunakan bilangan prima 3 digit memiliki kapasitas mencapai lebih dari 500% dibanding plainteksnya. Semakin besar nilai bilangan prima maka kapasitas cipherteks juga semakin besar. Sehingga dapat disimpulkan pembobolan pesan akan semakin sulit dilakukan. Penentuan bilangan prima ini dapat dilakukan dengan menggunakan bantuan *software Python* (Ummi, 2013).

b. Hitung $q$ dengan persamaan penentuan bilangan prima aman (Basyiah, 2017).
c. Jika $q$ merupakan bilangan prima, maka $p$ merupakan bilangan prima aman (Basyiah, 2017).
d. Jika $q$ bukan merupakan bilangan prima, maka $p$ bukan merupakan bilangan prima aman (Basyiah, 2017).

2. Penentuan akar primitif

Langkah penentuan akar primitif dinyatakan sebagai berikut:

a. Menentukan $\alpha$ dengan catatan $\alpha \in \mathbb{Z}_p{}^*$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan $p$ atau menggunakan *software Python*.
b. Melakukan pengecekan dengan menggunakan perhitungan $\alpha^2 mod\ p$ dan $\alpha^2 mod\ p$ berdasarkan Teorema 2.19.

c. Jika $\alpha^2 mod\ p = 1$ dan $\alpha^2 mod\ p = 1$, maka $\alpha$ adalah bukan akar primitif (Basyiah, 2017).

d. Jika $\alpha^2 mod\ p \neq 1$ dan $\alpha^2 mod\ p \neq 1$, maka $\alpha$ adalah akar primitif (Basyiah, 2017).

3. Pembentukan kunci berdasarkan bilangan prima dan akar primitif

Kunci publik ElGamal berupa 3 pasangan yaitu $(p, \alpha, \beta)$, dengan $p$ adalah bilangan prima, $\alpha$ adalah akar primitif dari $p$ dan dengan persamaan berikut (ElGamal, 1985):

$$\beta = \alpha^d mod\ p \tag{2.5}$$

**Bukti:**

Misalkan $\beta = \alpha^d mod\ p$, dan akan dibuktikan bahwa persamaan ini benar menggunakan pembuktian eksponensial modulo. Berikut adalah langkah-langkah pembuktian:

a. Diasumsikan bahwa $a$, $d$, dan $p$ adalah bilangan bulat positif. Akan dibuktikan bahwa $\beta = \alpha^d mod\ p$. Ini berarti bahwa $\beta$ adalah sisa hasil bagi pembagian $\alpha^d mod\ p$.

b. Digunakan induksi matematika pada nilai $d$. Basis induksi: jika $d = 1$, maka $\beta = \alpha^1 mod\ p = a\ mod\ p$. Ini adalah sisa hasil bagi $a$ dengan $p$ dan bernilai benar. Langkah induksi: Diasumsikan bahwa persamaan ini benar untuk suatu nilai $k$, yaitu $\beta = \alpha^k mod\ p$. Akan dibuktikan bahwa persamaan ini juga benar untuk suatu nilai $k + 1$, yaitu $\beta = \alpha^{k+1} mod\ p$.

c. Dari asumsi induksi, diketahui bahwa $\beta = \alpha^k mod\ p$. Dapat ditulis $a^{k+1}$ sebagai $a^k \cdot a$. Jadi dimiliki $\beta = a^k \cdot a\ mod\ p$. Karena perkalian dalam aritmatika modulo dapat diubah urutannya, dapat dituliskan sebagai $\beta =$

$a \cdot a^k \ mod\ p$. Diketahui bahwa $\beta = a^k mod\ p$, sehingga dapat dituliskan menjadi $\beta = (\beta \cdot a)\ mod\ p$. Ini berarti $\beta$ adalah sisa hasil bagi dengan $p$. Karena digunakan aritmatika modulo, sisa hasil bagi perkalian $a$ dan $\beta$ tetap sama dengan sisa hasil bagi perkalian $a^k$ dan $a$ yaitu $a^{k+1}$.

d. Oleh karena itu dapat disimpulkan bahwa persamaan ini benar untuk $k+1$. Dengan menggunakan prinsip induksi, dapat dibuktikan bahwa persamaan ini benar untuk setiap nilai $d$ positif.

e. Dengan demikian telah dibuktikan bahwa eksponensial modulo $\beta = a^d mod\ p$ berlaku. Ini adalah dasar operasi modulo dalam kriptografi.

Sedangkan kunci rahasia ElGamal berupa pasangan bilangan $(p, d)$ dengan $d$ adalah bilangan acak $1 < d < p - 1$. Dengan menggunakan kunci publik yang dihasilkan, pesan dapat dienkripsi menggunakan skema enkripsi ElGamal (ElGamal, 1985).

**Contoh 2.24**

Pembentukan Kunci publik dan rahasia

1. Pilih bilangan prima $p = 579$ untuk membentuk grup perkalian$(\mathbb{Z}^*_{579}, \times)$

   Melakukan pengecekan terhadap 579

   $$p = 2q + 1$$
   $$579 = 2q + 1$$
   $$2q = 579 - 1$$
   $$q = \frac{578}{2}$$
   $$q = 289$$

   Karena $p = 579$ dan $q = 289$ adalah biolangan prima, maka 579 termasuk kedalam bilangan prima aman

2. Pilih akar primitif pada $(\mathbb{Z}_{579}^{*},\times)$, maka $\varphi(579) = \varphi(\varphi(579)) = 578$, karena $579$ merupakan bilangan prima. Sehingga terdapat $758$ kandidat akar primitif, kemudian dipilih 27.

   Melakukan pengecekan terhadap 27, menggunakan perhitungan berikut

   a. $\alpha^2 mod\ p$

   $$\alpha^2 mod\ p = 27^2 mod\ 579$$
   $$= 729\ mod\ 579$$
   $$= 150$$

   b. $\alpha^q mod\ p$

   $$\alpha^q mod\ p = 27^{289} mod\ 579$$
   $$= 27$$

   Karena $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka $27$ termasuk akar primitif dari $\mathbb{Z}_{579}^{*}$

3. Pilih sebarang bilangan bulat dengan syarat $0 < d < p - 1$ sehingga dipilih $d = 891$.

4. Mencari $\beta$

   $$\beta = \alpha^d mod\ p$$
   $$= 27^{891} mod\ 579$$
   $$= 3$$

   Sehingga diperoleh kunci publik $(p, \alpha, \beta) = (579, 27, 3)$

### 2.5.2 Proses Enkripsi menggunakan Algoritma ElGamal

Proses Enkripsi pesan (cipherteks) dengan Algoritma ElGamal menggunakan kunci publik $(p, \alpha, \beta)$ adalah pasangan $(\gamma, \delta)$, dimana

$$\gamma = \alpha^k mod\ p \qquad \delta = \beta^k \cdot m\ mod\ p \tag{2.6}$$

dengan $k$ adalah bilangan acak $(1 \leq k \leq p-1)$, $m$ yang berasal dari plainteks yang akan disandikan dan $\beta$ dihitung di persamaan 2.5 (ElGamal, 1985).

**Bukti:**

1. Misalkan $\gamma$ adalah hasil enkripsi, $a$ adalah generator kelompok modulo $p$, $k$ adalah bilangan acak, dan $p$ adalah modulus prima.
   a. Dalam enkripsi ElGamal, $\gamma$ dihitung sebagai $\gamma = \alpha^k mod\ p$.
   b. Dengan menggunakan sifat eksponensial, dapat dituliskan $\alpha^k$ sebagai $\alpha \cdot a \cdot \ldots \cdot a$ (sebanyak $k$ kali). Dengan menggunakan sifat modulo, dapat diambil hasil modulo $p$ untuk setiap perkalian $a$.
   c. Gunakan langkah a dan b untuk mengubah $\gamma = \alpha^k$menjadi bentuk yang menggunakan sifat eksponensial modulo. Tulis $\gamma = (\alpha\ mod\ p) \cdot (a\ mod\ p) \cdot \ldots \cdot (a\ mod\ p)(mod\ p)$, sebanyak $k$ kali. Karena $\alpha\ mod\ p$ akan menghasilkan nilai antara 0 dan $p-1$, dapat dituliskan $\gamma = (a_1, a_2, \ldots, a_k)(mod\ p)$ dengan $a_i$ adalah hasil modulo setiap $a$. Namun karena $a$ adalah generator kelompok modulo $p$, maka $a_i$ akan mencakup semua anggota kelompok dan tidak ada pengulangan. Oleh karena itu dapat dituliskan $\gamma = (a_1, a_2, \ldots, a_k)(mod\ p) = \alpha^k mod\ p$ menggunakan definisi matematika dan sifat eksponensial modulo.
   d. Dengan demikian, telah dibuktikan $\gamma = \alpha^k mod\ p$.
2. Misalkan $\delta$ adalah hasil enkripsi, $\beta$ adalah kunci publik, $k$ adalah bilangan acak, $m$ adalah pesan yang akan dienkripsi, dan $p$ adalah modulus prima.
   a. Dalam enkripsi ElGamal, $\delta$ dihitung sebagai $\delta = \beta^k \cdot m\ mod\ p$.

b. Dengan menggunakan sifat eksponensial, dapat dituliskan $\beta^k$ sebagai $\beta \cdot \beta \cdot \ldots \cdot \beta$ (sebanyak $k$ kali). Dengan menggunakan sifat modulo, dapat diambil hasil modulo $p$ untuk setiap perkalian $\beta$.

c. Gunakan langkah a dan b untuk mengubah $\delta = \beta^k$ menjadi bentuk yang menggunakan sifat eksponensial modulo. Tulis $\delta = ((\beta \cdot \ldots \cdot \beta) \cdot m) mod\ p$, sebanyak $k$ kali. Terapkan sifat modulo setelah perkalian, sehingga dapat dituliskan $\delta = ((\beta_1, \beta_2, \ldots, \beta_k)) \cdot m) mod\ p$ dengan $\beta_i$ adalah hasil modulo setiap $a$. Namun karena $\beta$ adalah kunci publik dan merupakan elemen kelompok modulo $p$, maka $\beta_i$ akan mencakup semua anggota kelompok dan tidak ada pengulangan. Oleh karena itu dapat dituliskan $\delta = ((\beta_1, \beta_2, \ldots, \beta_k)) \cdot m) mod\ p = \beta^k \cdot m\ mod\ p$.

d. Dengan demikian, telah dibuktikan $\delta = \beta^k \cdot m\ mod\ p$.

Tidak disarankan untuk menggunakan nilai $k$ yang sama untuk menyandikan lebih dari satu blok pesan, karena jika digunakan lebih dari sekali, memungkinkan penyusup untuk menghitung pesan lain dengan menggunakan $k$ yang sama tersebut. Ukuran cipherteks yang dihasilkan dari proses ini adalah dua kali dari ukuran pesan asli (ElGamal, 1985).

**Contoh 2.25**

Misalkan didapatkan diperoleh kunci publik $(p, \alpha, \beta) = (1759, 28, 37)$, kunci rahasia $d = 891$, dan $p = 1759$, enkripsi pesan rahasia yang berupa bilangan berikut:

1. $(P_1) = 193$
2. $(P_2) = 103$
3. $(P_3) = 9$

4. $(P_4) = 63$

Jawab:

1. Plainteks 1, $(P_1) = 193$

$$\gamma_1 = \alpha^{k_1} \, mod \, p \qquad \delta_1 = \beta^{k_1} \cdot m_1 mod p$$
$$= 28^{40} \, mod \, 1759 \qquad = 37^{40} \cdot 193 mod 1579$$
$$= 1225 \qquad = 322$$

2. Plainteks 2, $(P_2) = 103$

$$\gamma_2 = \alpha^{k_2} \, mod \, p \qquad \delta_2 = \beta^{k_2} \cdot m_2 mod p$$
$$= 28^{1178} \, mod \, 1759 \qquad = 37^{1178} \cdot 103 mod 1579$$
$$= 1690 \qquad = 1356$$

3. Plainteks 3, $(P_3) = 9$

$$\gamma_3 = \alpha^{k_3} \, mod \, p \qquad \delta_3 = \beta^{k_3} \cdot m_3 mod p$$
$$= 28^{205} \, mod \, 1759 \qquad = 37^{205} \cdot 9 mod 1579$$
$$= 1704 \qquad = 1168$$

4. Plainteks 4, $(P_4) = 63$

$$\gamma_4 = \alpha^{k_4} \, mod \, p \qquad \delta_4 = \beta^{k_4} \cdot m_4 mod p$$
$$= 28^{1167} \, mod \, 1759 \qquad = 37^{1167} \cdot 63 mod 1579$$
$$= 385 \qquad = 251$$

Sehingga cipherteks yang berasal dari plainteks diatas adalah sebagai berikut

$$C_1 = (1225, 322)$$
$$C_2 = (1690, 1356)$$
$$C_3 = (1704, 1168)$$
$$C_4 = (385, 251)$$

### 2.5.3 Proses Dekripsi menggunakan Algoritma ElGamal

Setelah menerima cipherteks $(\gamma, \delta)$ dari pihak pengirim, proses selanjytnya adalah proses dekripsi dari cipherteks menggunakan kunci publik $p$ dan kunci rahasia $d$ (Munir, 2019).

**Teorema 2.26**

Diberikan $(p, \alpha, \beta)$ sebagai kunci publik dan $d$ adalah kunci rahasia pada kriptografi ElGamal. jika diberikan cipherteks $(\gamma, \delta)$, maka

$$m = \delta(\gamma^d)^{-1} mod\ p = \delta \cdot \gamma^{p-1-d} mod\ p$$

Dengan $m$ adalah plainteks (Stinson, 1995).

**Bukti:**

Diketahui kunci publik $(p, \alpha, \beta)$ dan kunci rahasia $d$ pada Kriptografi ElGamal. Diberikan cipherteks $(\gamma, \delta)$ , sehingga diperoleh bahwa

$m = \left(\frac{\delta}{\gamma^d}\right) mod\ p$

$= \delta(\gamma^d)^{-1} mod\ p$ (Ingat pembagian jika dinaikan menjadi invers)

$= m \cdot \beta \cdot (\alpha^d)^{-1} mod\ p$ Subtitusi perhitungan $\delta$ dan $\gamma$

$= m \cdot \alpha^d \cdot (\alpha^d)^{-1} mod\ p$ Subtitusi perhitungan $\beta$

$= m \cdot mod\ p$ $\alpha^d \cdot (\alpha^d)^{-1} = \alpha^{d-d}$ (aturan eksponensial)

Dengan demikian didapatkan $m = \delta(\gamma^d)^{-1} mod\ p$. Karena $\mathbb{Z}_p$ memiliki orde $p - 1$. Maka :

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

**Contoh 2.27**

Misalkan didapatkan diketahui, kunci rahasia $d = 891$, dan $p = 1759$ dekripsikan cipherteks yang berupa bilangan berikut:

$$C_1 = (\gamma_1, \delta_1) = (1225, 322)$$

$$C_2 = (\gamma_2, \delta_2) = (1690, 1356)$$

$$C_3 = (\gamma_3, \delta_3) = (1704, 1168)$$

$$C_4 = (\gamma_4, \delta_4) = (385, 251)$$

Jawab:

Perhitungan untuk mendekripsikan pesan menjadi:

$$m_i = \delta_i \cdot {\gamma_i}^{(p-1-d)} mod\ p$$

$$= \delta_i \cdot {\gamma_i}^{(1759-1-891)} mod\ 1759$$

$$= \delta_i \cdot {\gamma_i}^{867} mod\ 1759$$

Proses Dekripsi ditunjukkan sebagai berikut:

1. $C_1 = (\gamma_1, \delta_1) = (1225, 322)$, sehingga

$$m_1 = \delta_1 \cdot {\gamma_1}^{867} mod\ 1759$$

$$= 322 \cdot 1225^{867} mod\ 1759$$

$$= 193$$

2. $C_2 = (\gamma_2, \delta_2) = (1690, 1356)$, sehingga

$$m_2 = \delta_2 \cdot {\gamma_2}^{867} mod\ 1759$$

$$= 1356 \cdot 1690^{867} mod\ 1759$$

$$= 103$$

3. $C_3 = (\gamma_3, \delta_3) = (1704, 1168)$, sehingga

$$m_3 = \delta_3 \cdot {\gamma_3}^{867} mod\ 1759$$

$$= 1168 \cdot 1704^{867} mod\ 1759$$

$$= 9$$

4. $C_4 = (\gamma_4, \delta_4) = (385, 251)$, sehingga

$$m_4 = \delta_4 \cdot {\gamma_4}^{867} mod\ 1759$$
$$= 251 \cdot 385^{867} mod\ 1759$$
$$= 63$$

### *2.6 ASCII*

*ASCII* atau *American Standard Code for Information Interchange* adalah format umum yang digunakan pada komputer dan internet. *ASCII* ini dikembangkan oleh *American National Standards Institute* (ANSI). *ASCII* digunakan sebagai kode Standar Amerika untuk Pertukaran Informasi (/ˈæski/ (simak) ass-kee) untuk sarana karakter komunikasi digital. *ASCII* dikembangkan pada awal tahun 1960-an ketika komunikasi jaringan awal sedang dikembangkan.

*ASCII* digunakan kompoter untuk mewakili karakter-karakter seperti huruf atau angka. Dalam kode ASCII terdapat 95 karakter diantaranya terdiri dari 26 huruf alphabet kapital (A-Z), 26 huruf alfabet kecil (a-z), 10 karakter angka (0-9) dan 33 karakter khusus yang berisi simbol matematika, tanda baca, dan karakter spasi(Fadlillah, 2021).

Pengaruh perkembangan *ASCII* berkaitan juga dengan perkembangan teknologi yaitu dalam banyaknya karakter yang dgunakan menjadi delapan bit atau sering disebut US-*ASCII*-8. *ASCII* terdiri dari bilangan biner 00000000 sampai 11111111 yang mewakili karakter 256. Pengelompokan kode *ASCII* menjadi beberapa bagian diantaranya sebagai berikut:

1. Kode *ASCII* seperti kode 10 (Line Feed), 13 (Carriage return), 8 (Tab), 32 (Space) termasuk kedalam kode yang tidak terlihat simbolnya.

2. Kode *ASCII* seperti kode abjad (A,…,Z), numerik (0,…,9), karakter khusus (~!@#$%^&*()_+?:”{}) termasuk kedalam kode yang terlihat simbolnya.
3. Kode *ASCII* yang digunakan untuk kode grafik. Kode ini tidak tercantum pada *keyboard*.

Selain itu, *ASCII* dapat dikelompokkan menjadi 3 jenis berdasarkan penggunaannya pada media komunikasi, diantaranya (Fadlillah, 2021):

1. *ASCII Control Characters*, yaitu kode control yang tidak dapat dicetak dan digunakan untuk mengontrol perifeal seperti printer
2. *ASCII Printable Characters*, yaitu umum untuk semua variasi tabel *ASCII* yang berbeda, mereka disebut karakter yang dapat dicetak. Dan karaktrer ini dapat ditemui di *keyboard* komputer.
3. *The Extended ASCII* atau kode *ASCII* yang diperluas. Kode *ASCII extended* digunakan untuk mempresentasikan kode-kode khusus. Contoh dari kode *ASCII extended* adalah kode pada tombol F1 sampai dengan F12 yang ada pada *keyboard* computer.

## 2.7 Kajian Agama

Al-Qur’an adalah wahyu dan kalam Allah yang disampaikan melalui malaikat Jibril kepada Nabi Muhammad SAW. Al-Qur’an menjadi tuntunan dan pedoman bagi seluruh umat manusia. Pedoman seluruh aspek kehidupan di dunia termuat dalam Al-Qur’an. Salah satu aspek kehidupan yang termuat dalam Al-Qur’an adalah menjaga amanah. Amanah adalah menunaikan segala sesuatu yang telah diberikan atau ditugaskan kepada seseorang terkait urusan agama maupun urusan dunia akhirat. Menjaga amanah sesuai dengan konsep Kriptografi. Konsep

Kriptografi sendiri adalah mengamankan pesan atau informasi sampai kepada penerima agar tidak bocor ke pihak yang tidak terkait. Hal tersebut sejalan dengan pengertian amanah yaitu menyampaikan pesan dari pengirim kepada yang berhak yang dalam konteks Kriptografi dikenal sebagai penerima. Perintah menjaga amanah tercantum di firman Allah Swt. Q.S Al Anfal ayat 27 yang berbunyi:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ

*"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul dan janganlah kamu mengkhianati amanah-amanah yang dipercayakan kepada kamu, sedang kamu mengetahui."(Q.S Al Anfal:27)*

Dalam pandangan islam, amanah dapat diartikan secara luas. Arti yang cukup umum dari amanah adalah perasaan manusia yang terkait dengan perbuatan yang didasarkan kepada kesadaran diri dan tanggung jawab kepada diri masing-masing dan kepada Allah Swt. dalam melakukan sesuatu yang telah dipercayakan kepadanya (Dewi, 2022). Menurut Muhammad Naasib Ar-rifai'I dalam buku ringkasan Ibnu Katsir, orang dapat dikatakan amanah jika diberikan kepercayaan tidak akan mengkhianati, jika dititipkan sesuatu tidak berkhianat, dan jika berjanji tidak akan mengingkari. Seluruh amanah baik terkait urusan agama maupun urusan dunia akhirat haram hukumnya jika diingkari atau dikhianati (Dalimunthe, 2016).

Perintah untuk menyampaikan atau menunaikan amanah juga diperintahkan oleh Rasulullah dalam hadits riwayat Abu Daud yang berbunyi:

حَدَّثَنَا أَبُو كَامِلٍ أَنَّ يَزِيدَ بْنَ زُرَيْعٍ حَدَّثَهُمْ حَدَّثَنَا حُمَيْدٌ يَعْنِي الطَّوِيلَ عَنْ يُوسُفَ بْنِ مَاهَكَ الْمَكِّيِّ قَالَ كُنْتُ أَكْتُبُ لِفُلَانٍ نَفَقَةَ أَيْتَامٍ كَانَ وَلِيَّهُمْ فَغَالَطُوهُ بِأَلْفِ دِرْهَمٍ فَأَدَّاهَا إِلَيْهِمْ فَأَدْرَكْتُ لَهُمْ مِنْ مَالِهِمْ مِثْلَيْهَا قَالَ قُلْتُ أَقْبِضُ الْأَلْفَ الَّذِي ذَهَبُوا بِهِ مِنْكَ قَالَ لَا حَدَّثَنِي أَبِي أَنَّهُ سَمِعَ رَسُولَ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ: يَقُولُ أَدِّ الْأَمَانَةَ إِلَى مَنْ ائْتَمَنَكَ وَلَا تَخُنْ مَنْ خَانَكَ

*"Tunaikanlah amanah kepada orang yang mempercayaimu dan janganlah engkau mengkhianati orang yang mengkhianatimu!" (H.R Abu Daud)*

Dalam hadis tersebut, Rasulullah memerintahkan untuk menunaikan amanah yang telah diberikan. Hal ini juga sesuai dengan hasil dan pembahasan dalam penelitian ini. Dalam hal ini kombinasi metode *Vigènere Cipher* dan ElGamal berperan sebagai alat untuk menyampaikan amanah. Peran dari kombinasi metode *Vigènere Cipher* dan ElGamal juga sebagai alat pengaman dari pesan rahasia. Tujuan dari alat pengaman pesan rahasia adalah agar isi pesan tidak bisa diketahui oleh orang yang tidak terkait. Selain itu modifikasi kombinasi metode *Vigènere Cipher* dan ElGamal mengamankan pesan asli dengan sangat baik sehingga dapat mengurangi kemungkinan terjadinya pembobolan pesan rahasia.

Menurut hadis riwayat Al-Syaibaniy, amanah dapat disama artikan kepada menjaga titipan, hadis tersebut berbunyi:

*"Barangsiapa mendengar suatu berita dari seseorang dia tidak berkenan untuk menyebarkannya maka itu adalah amanah walaupun orang tersebut tidak meminta untuk disembunyikan"(H.R Ahmad)*

Dalam hadis tersebut menjelaskan salah satu kriteria seseorang dapat dikatakan amanah adalah jika memperoleh berita atau informasi, seseorang tersebut tidak menyampaikan berita kepada orang yang tidak terkait atau menyebarkannnya (Dalimunthe, 2016).

# BAB III

# METODE PENELITIAN

## 3.1 Jenis Penelitian

Jenis penelitian ini adalah penelitain kualitatif karena memiliki fokus terhadap pemahaman yang mendalam dan pengembangan teori mengenai kombinasi Kriptografi metode *Vigènere Cipher* dan ElGamal dalam mengamankan pesan rahasia. Data yang dikumpulkan dalam penelitian ini bersifat deskriptif yang berasal dari beberapa sumber diantaranya buku, jurnal, laporan hasil penelitian, artikel, dan skripsi.

## 3.2 Pra Penelitian

Tahapan pertama dalam penelitian ini adalah menentukkan latar belakangan dan rumusan masalah. Tahapan selanjutnya adalah dengan mencari referensi terkait penelitian dimana sumber penelitian ini berasal dari jurnal, laporan hasil penelitian, artikel, dan skripsi. Tahapan terakhir adalah menganalisis masalah dan merancang penyelesaian masalah sesuai dengan penelitian ini yaitu kombinasi Kriptografi metode *Vigènere Cipher* dan ElGamal dalam mengamankan pesan rahasia.

## 3.3 Tahapan Penelitian

Melakukan simulasi kombinasi metode *Vigènere Cipher* dan algoritma ElGamal diantaranya sebagai berikut:

1. Algoritma pembentukan Kunci

Membentuk kunci publik dan kunci rahasia. Pembentukan kunci ini menggunakan Algoritma ElGamal. Untuk membentuk kunci publik dan rahasia dibutuhkan bilangan acak, bilangan prima, dan akar primitif. Untuk bilangan bulat acak dipilih melalui 3 angka terakhir pada NIM. Pada proses menentukan bilangan prima, bilangan prima dapat dikatakan bilangan prima aman jika memenuhi syarat:

a. Pilih bilangan prima $p$ dengan syarat $100 < p < 999$ (Ummi, 2013). Pemilihan bilangan prima $p$ dapat dilakukan secara acak menggunakan *software Python.*
b. Melakukan pengecekan bilangan prima aman dengan menggunakan perhitungan $q$ dengan persamaan 2.3 yaitu $p = 2q + 1$.
c. Jika $q$ merupakan bilangan prima, maka $p$ merupakan bilangan prima aman.
d. Jika $q$ bukan merupakan bilangan prima, maka $p$ bukan merupakan bilangan prima aman.

Dan pada proses menentukan akar primitif dilakukan beberapa langkah diantaranya:

a. Menentukan $\alpha$ dengan catatan $\alpha \in \mathbb{Z}_p{}^*$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan $p$ atau dipilih secara acak menggunakan *software Python*.
b. Melakukan pengecekan dengan menggunakan perhitungan $\alpha^2 mod\ p$ dan $\alpha^2 mod\ p$ berdasarkan teorema 2.19.
c. Jika $\alpha^2 mod\ p = 1$ dan $\alpha^q mod\ p = 1$, maka $\alpha$ adalah bukan akar primitif.

d. Jika $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka $\alpha$ adalah akar primitif.

2. Algoritma Enkripsi Pesan

a. Menetukan pesan asli atau plainteks yang digunakan

b. Proses enkripsi tahap pertama ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo *ASCII printable*. Proses enkripsi tahap pertama ini menghasilkan cipherteks yang berupa angka.

c. Langkah selanjutnya adalah melakukan proses enkripsi tahap kedua pada cipherteks yang telah didapatkan dari proses enkripsi tahap pertama menggunakan algoritma ElGamal. Pada proses enkripsi tahap kedua ini diperlukan bilangan acak yang didapatkan melalui *Microsoft Excel*. Proses enkripsi tahap kedua ini menghasilkan cipherteks yang berupa pasangan angka .

d. Selanjutnya pengirim mengirimkan kunci publik kepada penerima untuk proses deksripsi pesan rahasia.

3. Algoritma Dekripsi Pesan

a. Setelah menerima pesan, langkah selanjutnya adalah proses dekripsi tahap pertama menggunakan metode ElGamal. Dalam proses dekripsi tahap pertama ini membutuhkan kunci rahasia yang telah didapatkan dan bilangan acak yang didapatkan melalui *Microsoft Excel*. Pada proses dekripsi tahap pertama ini menghasilkan plainteks yang berupa angka.

b. Melakukan proses deksripsi tahap kedua pada plainteks yang telah didapatkan pada tahap pertama menggunakan metode *Vigènere Cipher*. Dalam proses dekripsi tahap kedua ini dilakukan dengan menggunakan

modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo *ASCII printable*. Proses dekripsi tahap kedua ini menggunakan kunci publik.

c. Mengubah plainteks yang didapatkan menjadi karakter berdasarkan tabel *ASCII printable*.

# BAB IV

# HASIL DAN PEMBAHASAN

## 4.1 Proses Enkripsi

Proses Enkripsi adalah proses pengubahan pesan asli(plainteks) menjadi pesan rahasia(cipherteks) (Munir, 2019). Pada penelitian ini dilakukan proses Enkripsi sebanyak dua kali. Enkripsi pertama menggunakan metode *Vigènere Cipher* dan enkripsi kedua menggunakan algoritma ElGamal. Sebelum melakukan enkripsi, pihak pengirim pesan harus menentukkan pesan asli yang akan diubah menjadi indeks karakter menggunakan tabel *ASCII printable*. Proses Enkripsi dapat dilakukan dengan adanya kunci. Dalam kriptografi terdapat dua jenis kunci yaitu kunci publik dan kunci rahasia (Ariyus, 2008). Pada penelitian ini kunci yang digunakan adalah kunci publik dan kunci rahasia. Kunci tersebut didasarkan kepada kombinasi dari dua algoritma yang digunakan. Kombinasi yang digunakan adalah algoritma simetris yaitu *Vigènere Cipher* dan algoritma asimetris yaitu ElGamal. Oleh karena itu dibutuhkan kunci publik untuk algoritma simetris dan kunci rahasia untuk algorima asimestris (Munir, 2019).

### 4.1.1 Simulasi Pembentukan Kunci

Berikut adalah simulasi pembentukan kunci publik dan rahasia menggunakan algoritma ElGamal:

1. Penentuan bilangan prima $p$ aman yang bernilai besar (Ifanto, 2009). Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan akar primitif. Bilangan prima $p$ dengan interval $100 < p < 999$

atau 3 digit. Pemilihan bilangan prima $p$ dapat dilakukan secara acak dengan menggunakan bantuan *software Python* (Ummi, 2013).

Dipilih $p = 827$

2. Melakukan pengecekan bilangan prima aman $p$ dengan perhitungan pada persamaan 2.3 (Basyiah, 2017).

$$\begin{aligned} p &= 2q + 1 \\ 827 &= 2q + 1 \\ 2q &= 827 - 1 \\ q &= \frac{826}{2} \\ q &= 413 \end{aligned}$$

Karena $q = 413$ adalah bilangan prima, maka p merupakan bilangan prima aman.

3. Menentukan akar primitif $\alpha \in \mathbb{Z}_p{}^*$. Langkah penentuan akar primitif dinyatakan sebagai berikut:

   a. Menentukan $\alpha$ dengan catatan $\alpha \in \mathbb{Z}_p{}^*$. Untuk menentukan akar primtif acak ini dapat dilakukan dengan menggunakan bilangan yang relatif prima dengan $p$ atau menggunakan bantuan *software Python*. Berdasarkan definisi 2.14 untuk mencari akar primitif dapat dilakukan dengan perhitungan berikut

$$\varphi(827) = \varphi(\varphi(827)) = \varphi(827 - 1) = 826$$

Dipilih $\alpha = 37$, karena $\gcd(37, 826) = 1$. Oleh karena itu 37 relatif prima dengan 826.

b. Untuk memastikan 37 adalah akar primtitif dari perlu dilakukan pengecekan terhadap 827 dengan menggunakan perhitungan $\alpha^2 mod\ p$ dan $\alpha^q mod\ p$ berdasarkan Teorema 2.19 (Basyiah, 2017).

- $\alpha^2 mod\ p$

$$\alpha^2 mod\ p = 37^2 mod\ 827$$
$$= 1369\ mod\ 827$$
$$= 524$$

- $\alpha^q mod\ p$

$$\alpha^q mod\ p = 37^{413} mod\ 827$$
$$= 826$$
$$= 826$$

Karena $\alpha^2 mod\ p \neq 1$ dan $\alpha^q mod\ p \neq 1$, maka 37 termasuk akar primitif dari $\mathbb{Z}_{827}^*$

4. Pilih bilangan bulat acak $d$, berdasarkan penggabungan 3 bilangan terakhir pada NIM atau nomer identitas mahasiswa.

   NIM yang digunakan adalah 19610036. Sehingga 3 bilangan terakhir NIM tersebut adalah 036. Berdasarkan aturan yang telah ditetapkan maka $d = 36$.

5. Pembentukan kunci berdasarkan bilangan prima dan akar primitif.

   Untuk mencari nilai $\beta$ menggunakan perhitungan $\beta = \alpha^d mod\ p$ berdasarkan persamaan 2.5 sehingga (ElGamal, 1985)

$$\beta = \alpha^d mod\ p$$
$$= 37^{36} mod\ 827$$
$$= 276$$

Diperoleh kunci publik $(p, \alpha, \beta)$ dan kunci rahasia $(p, d)$

Sehingga didapatkan kunci publik $(p, \alpha, \beta) = (827, 37, 276)$ dan kunci rahasia $(p, d = 827, 36)$

### 4.1.2 Algoritma Enkripsi *Vigènere Cipher* dan ElGamal

Algoritma Enkripsi *Vigènere Cipher* dan ElGamal dijelaskan sebagai berikut:

1. Proses enkripsi tahap pertama menggunakan kunci publik$(p, \alpha, \beta)$ yang telah didapatkan melalui proses pembentukan kunci menggunakan algoritma ElGamal. Sesuai dengan algoritma dari *Vigènere Cipher*, untuk melakukan enkripsi diperlukan pengubahan pesan rahasia dan kunci publik menjadi indeks angka. Untuk proses Enkripsi dilakukan perhitungan dengan menambahkan indeks pesan rahasia dan kunci publik. Setelah didapatkan hasil dari penambahan tersebut langkah selanjutnya adalah melakukan perhitungan modulo. Dalam penelitian ini modulo yang digunakan adalah modulo ASCII *printable*. Proses Enkripsi menggunakan metode *Vigènere Cipher* dengan modifikasi modulo *ASCII Printable* menggunakan perhitungan sebagai berikut (Putri, 2021):

   $$C_i = ((P_i + K_i - 32) mod\ 95) + 32$$ ( Berdasarkan persamaan 2.1)

2. Enkripsi tahap kedua adalah dengan menggunakan algoritma ElGamal. Algoritma ini membutuhkan dua jenis kunci yaitu kunci publik dan kunci rahasia (Munir, 2019). Dalam proses tahap kedua cipherteks didapatkan melalui $(\gamma_i, \delta_i)$ dengan menggunakan perhitungan enkripsi algoritma ElGamal pada persamaan 2.6 yaitu sebagai berikut (ElGamal, 1985):

   $$\gamma_i = \alpha^{k_i} mod p \quad \delta_i = \beta^{k_i} \cdot m_i mod p$$ (Berdasarkan Persamaan 2.6)

Dengan keterangan notasi $\alpha, \beta$ dan $p$ adalah kunci publik. Bilangan acak dinotasikan sebagai $k$. Bilangan acak yang akan digunakan berasal dari *Microsoft Excel* dengan aturan $1 \leq k \leq p-1$. Sedangkan untuk notasi $m$ adalah cipherteks yang telah didapatkan dari proses Enkripsi tahap pertama. *Output* dari proses enkripsi tahap kedua adalah dalam bentuk pasangan bilangan $(\gamma_i, \delta_i)$.

### 4.1.3 Simulasi Enkripsi *Vigènere Cipher* dan ElGamal

Proses Enkripsi diawali oleh proses enkripsi tahap pertama. Proses Enkripsi tahap pertama adalah dengan menggunakan metode *Vigènere Cipher*. Berikut adalah langkah-langkah Enkripsi tahap pertama:

1. Menentukkan plainteks atau pesan asli

   Pada penelitian ini pesan asli atau (plainteks)-nya yang digunakan adalah Ludyawati-19610036. Peneliti memilih Plainteks tersebut karena berdasarkan nama lengkap serta nomor induk mahasiswa (NIM) dari peneliti. Plainteks tersebut dapat dirubah sesuai dengan kebutuhan dan keinginan penelitian selanjutnya.

2. Menentukkan indeks karakter dari plainteks yang telah dibuat

***Tabel 4.1*** *Indeks Plainteks*

| **Plainteks** | **Indeks** |
|---|---|
| L | 76 |
| u | 117 |
| d | 100 |
| y | 121 |
| a | 97 |
| w | 119 |

| **Plainteks** | **Indeks** |
|---|---|
| - | 45 |
| 1 | 49 |
| 9 | 57 |
| 6 | 54 |
| 1 | 49 |
| 0 | 48 |

| | |
|---|---|
| a | 97 |
| t | 116 |
| i | 105 |

| | |
|---|---|
| 0 | 48 |
| 3 | 51 |
| 6 | 54 |

3. Menentukkan indeks karakter dari kunci publik $(827, 37, 276)$

***Tabel 4.2*** *Indeks Kunci Publik*

| Kunci | Indeks |
|---|---|
| 8 | 56 |
| 2 | 50 |
| 7 | 55 |
| , | 44 |
| 3 | 51 |
| 7 | 55 |

| Kunci | Indeks |
|---|---|
| , | 44 |
| 2 | 50 |
| 7 | 55 |
| 6 | 54 |

4. Melakukan Enkripsi Tahap Pertama dengan metode *Vigènere Cipher.*

   Proses Enkripsi tahap pertama ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo *ASCII printable*.

***Tabel 4.3*** *Proses Enkripsi Tahap Pertama*

| $i$ | Plainteks | Kunci | $E = ((P_i + K_i - 32) mod\ 95) + 32$ | Cipherteks |
|---|---|---|---|---|
| 1 | 76 | 56 | $((76 + 56 - 32) mod\ 95) + 32$ | 37 |
| 2 | 117 | 50 | $((117 + 50 - 32) mod\ 95) + 32$ | 72 |
| 3 | 100 | 55 | $((100 + 55 - 32) mod\ 95) + 32$ | 60 |
| 4 | 121 | 44 | $(121 + 44 - 32) mod\ 95) + 32$ | 70 |
| 5 | 97 | 51 | $((97 + 51 - 32) mod\ 95) + 32$ | 53 |
| 6 | 119 | 55 | $((119 + 55 - 32) mod\ 95) + 32$ | 79 |
| 7 | 97 | 44 | $((97 + 44 - 32) mod\ 95) + 32$ | 46 |
| 8 | 116 | 50 | $((116 + 50 - 32) mod\ 95) + 32$ | 71 |
| 9 | 105 | 55 | $((105 + 55 - 32) mod\ 95) + 32$ | 65 |
| 10 | 45 | 54 | $((45 + 54 - 32) mod\ 95) + 32$ | 99 |
| 11 | 49 | 56 | $((49 + 56 - 32) mod\ 95) + 32$ | 105 |

| | | | | |
|---|---|---|---|---|
| 12 | 57 | 50 | $((57+50-32) mod\ 95)+32$ | 107 |
| 13 | 54 | 55 | $((54+55-32) mod\ 95)+32$ | 109 |
| 14 | 49 | 44 | $((49+44-32) mod\ 95)+32$ | 93 |
| 15 | 48 | 51 | $((48+51-32) mod\ 95)+32$ | 99 |
| 16 | 48 | 55 | $((48+55-32) mod\ 95)+32$ | 103 |
| 17 | 51 | 44 | $((51+44-32) mod\ 95)+32$ | 95 |
| 18 | 54 | 50 | $((54+50-32) mod\ 95)+32$ | 104 |

Setelah mendapatkan cipherteks dari proses Enkripsi yang pertama, cipherteks tersebut kemudian dienkripsi kembali dengan menggunakan Algoritma ElGamal. Proses ini disebut dengan proses enkripsi tahap kedua. Pada proses enkripsi tahap kedua kunci yang digunakan adalah kunci publik $(p, \alpha, \beta) = (827, 37, 276)$. Pada proses ini juga dibutuhkan bilangan bulat acak $k$ yang berasal dari *Microsoft Excel* dengan aturan $1 \leq k \leq p-1$. Notasi $m$ adalah cipherteks yang telah didapatkan dari proses Enkripsi tahap pertama. Berikut adalah proses Enkripsi tahap kedua:

***Tabel 4.4*** *Proses Enkripsi Tahap Kedua*

| $\boldsymbol{i}$ | $\boldsymbol{m_i}$ | $\boldsymbol{k_i}$ | $\boldsymbol{\gamma_i = 37^{k_i} mod\ 827}$ | $\boldsymbol{\gamma_i}$ | $\boldsymbol{\delta_i = 276^{k_i} \cdot m_i mod\ 827}$ | $\boldsymbol{\delta_i}$ |
|---|---|---|---|---|---|---|
| 1 | 37 | 173 | $37^{173} mod\ 827$ | 345 | $276^{173} \cdot 37\ mod\ 827$ | 384 |
| 2 | 72 | 251 | $37^{251} mod\ 827$ | 280 | $276^{251} \cdot 72\ mod\ 827$ | 45 |
| 3 | 60 | 799 | $37^{799} mod\ 827$ | 451 | $276^{799} \cdot 60\ mod\ 827$ | 70 |
| 4 | 70 | 525 | $37^{525} mod\ 827$ | 24 | $276^{525} \cdot 70\ mod\ 827$ | 813 |
| 5 | 53 | 797 | $37^{797} mod\ 827$ | 631 | $276^{797} \cdot 53\ mod\ 827$ | 143 |
| 6 | 79 | 728 | $37^{728} mod\ 827$ | 496 | $276^{728} \cdot 79\ mod\ 827$ | 372 |
| 7 | 46 | 447 | $37^{447} mod\ 827$ | 384 | $276^{447} \cdot 46\ mod\ 827$ | 769 |
| 8 | 71 | 790 | $37^{790} mod\ 827$ | 3 | $276^{790} \cdot 71\ mod\ 827$ | 805 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | 65 | 821 | $37^{821} mod\ 827$ | 709 | $276^{821} \cdot 65\ mod\ 827$ | 82 |
| 10 | 99 | 269 | $37^{269} mod\ 827$ | 746 | $276^{269} \cdot 99\ mod\ 827$ | 671 |
| 11 | 105 | 256 | $37^{256} mod\ 827$ | 306 | $276^{256} \cdot 105\ mod\ 827$ | 729 |
| 12 | 107 | 418 | $37^{418} mod\ 827$ | 820 | $276^{418} \cdot 107\ mod\ 827$ | 579 |
| 13 | 109 | 770 | $37^{770} mod\ 827$ | 93 | $276^{770} \cdot 109\ mod\ 827$ | 715 |
| 14 | 93 | 543 | $37^{543} mod\ 827$ | 442 | $276^{543} \cdot 93\ mod\ 827$ | 504 |
| 15 | 99 | 494 | $37^{494} mod\ 827$ | 504 | $276^{494} \cdot 99\ mod\ 827$ | 31 |
| 16 | 103 | 184 | $37^{184} mod\ 827$ | 273 | $276^{184} \cdot 103\ mod\ 827$ | 513 |
| 17 | 95 | 266 | $37^{266} mod\ 827$ | 108 | $276^{266} \cdot 95\ mod\ 827$ | 18 |
| 18 | 104 | 65 | $37^{65} mod\ 827$ | 218 | $276^{65} \cdot 104\ mod\ 827$ | 190 |

Cipherteks yang dihasilkan dari enkripsi tahap kedua ini berbentuk pasangan angka$(\gamma_i, \delta_i)$. Cipherteks yang telah dihasilkan ditunjukkan sebagai berikut:

***Tabel 4.5*** *Cipherteks yang Dihasilkan*

| | | | | | |
|---|---|---|---|---|---|
| C1 | $(345, 384)$ | C7 | $(384, 805)$ | C13 | $(93, 715)$ |
| C2 | $(280, 45)$ | C8 | $(3, 805)$ | C14 | $(442, 504)$ |
| C3 | $(451, 70)$ | C9 | $(709, 82)$ | C15 | $(504, 31)$ |
| C4 | $(24, 813)$ | C10 | $(746, 671)$ | C16 | $(273, 513)$ |
| C5 | $(631, 143)$ | C11 | $(306, 729)$ | C17 | $(108, 18)$ |
| C6 | $(496, 372)$ | C12 | $(820, 579)$ | C18 | $(218, 190)$ |

## 4.2 Proses Dekripsi Pesan

Proses Deskripsi merupakan proses mengubah pesan rahasia(chiperteks) menjadi pesan asli(plainteks) (Munir, 2019). Pada penelitian ini terjadi 2 tahap proses deskripsi. Tahap pertama adalah proses dekripsi menggunakan algoritma ElGamal. Algoritma ElGamal termasuk kedalam algoritma asimetris, oleh

karenanya kunci yang digunakan pada proses dekripsi adalah kunci rahasia (Ariyus, 2006). Proses dekripsi tahap pertama menggunakan kunci rahasia yang telah didapatkan pada proses pembentukan kunci sebelumnya. *Output* atau hasil dari proses dekripsi tahap pertama adalah dalam bentuk angka.

Setelah mendapatkan plainteks dari proses dekripsi tahap pertama, plainteks tersebut didekripsi kembali menggunakan metode *Vigènere Cipher*. Proses ini disebut dengan proses enkripsi tahap kedua. Pada proses dekripsi tahap kedua, kunci yang digunakan tidak menggunakan kunci rahasia, akan tetapi menggunakan kunci publik. Hal tersebut berdasarkan kepada metode *Vigènere Cipher* yang termasuk kedalam algoritma simetris (Ariyus, 2006). Algoritma simetris hanya menggunakan satu jenis kunci yaitu kunci publik.

### 4.2.1 Algoritma Dekripsi *Vigènere Cipher* dan ElGamal

1. Proses dekripsi dimulai dengan proses dekripsi tahap pertama. Proses dekripsi tahap pertama menggunakan metode ElGamal dan kunci rahasia$(d, p)$.
2. Pada proses dekripsi dilakukan menggunakan perhitungan (Stinson, 1995):

   $$m_i = \delta_i \cdot {\gamma_i}^{(p-1-d)} mod\ p$$ (Berdasarkan Teorema 2.26)

   Dengan keterangan $m_i$ adalah plainteks yang dihasilkan, sedangkan $(\gamma_i, \delta_i)$ adalah cipherteks yang diperoleh dari pihak pengirim.
3. Pada proses dekripsi tahap pertama ini kunci yang digunakan adalah $(p, \alpha, \beta)$. Proses dekripsi tahap kedua ini dilakukan dengan menggunakan modifikasi perhitungan modulo dalam metode *Vigènere Cipher*, yaitu dengan menggunakan modulo *ASCII printable*. Sebelum melakukan proses

dekripsi, langkah pertama dalam proses dekripsi metode *Vigènere Cipher* adalah menentukkan indeks karakter dari kunci publik. Proses Dekripsi menggunakan metode *Vigènere Cipher* dengan modifikasi modulo *ASCII Printable* menggunakan perhitungan sebagai berikut: (Putri, 2021)

$$P_i = ((P_i - K_i - 32) mod\ 95) + 32 \qquad (2.2)$$

4. Langkah terakhir untuk mendapatkan pesan asli adalah melakukan pengindeksan terhadap plainteks yang telah didapatkan.

### 4.2.2 Simulasi Dekripsi *Vigènere Cipher* dan ElGamal

Proses dekripsi dimulai dengan proses dekripsi tahap pertama. Proses dekripsi tahap pertama menggunakan metode ElGamal dan kunci rahasia. Kunci rahasia yang digunakan dalam penelitian ini adalah $(p, d = 827, 36)$.

Sehingga jika disubtitusikan nilai $d, p$ menjadi

$$m_i = \delta_i \cdot {\gamma_i}^{(827-1-36)} mod\ 827$$

$$m_i = \delta_i \cdot {\gamma_i}^{(790)} mod\ 827$$

Berikut adalah proses dekripsi tahap pertama:

***Tabel 4.6*** *Proses Dekripsi Tahap Pertama*

| $\boldsymbol{i}$ | $\boldsymbol{\gamma_i}$ | $\boldsymbol{\delta_i}$ | $\boldsymbol{m_i = \delta_i \cdot {\gamma_i}^{(790)} mod\ 827}$ | $\boldsymbol{m_i}$ |
|---|---|---|---|---|
| 1 | 345 | 384 | $384 \cdot 345^{(790)} mod\ 827$ | 37 |
| 2 | 280 | 45 | $45 \cdot 280^{(790)} mod\ 827$ | 72 |
| 3 | 451 | 70 | $70 \cdot 451^{(790)} mod\ 827$ | 60 |
| 4 | 24 | 813 | $813 \cdot 24^{(790)} mod\ 827$ | 70 |
| 5 | 631 | 143 | $143 \cdot 631^{(790)} mod\ 827$ | 53 |
| 6 | 496 | 372 | $372 \cdot 496^{(790)} mod\ 827$ | 79 |
| 7 | 384 | 769 | $769 \cdot 384^{(790)} mod\ 827$ | 46 |
| 8 | 3 | 805 | $805 \cdot 3^{(790)} mod\ 827$ | 71 |

| | | | | |
|---|---|---|---|---|
| 9 | 709 | 82 | $82 \cdot 709^{(790)} mod\ 827$ | 65 |
| 10 | 746 | 671 | $671 \cdot 746^{(790)} mod\ 827$ | 99 |
| 11 | 306 | 729 | $729 \cdot 306^{(790)} mod\ 827$ | 105 |
| 12 | 820 | 579 | $579 \cdot 820^{(790)} mod\ 827$ | 107 |
| 13 | 93 | 715 | $715 \cdot 93^{(790)} mod\ 827$ | 109 |
| 14 | 442 | 504 | $504 \cdot 442^{(790)} mod\ 827$ | 93 |
| 15 | 504 | 31 | $31 \cdot 504^{(790)} mod\ 827$ | 99 |
| 16 | 273 | 513 | $513 \cdot 273^{(790)} mod\ 827$ | 103 |
| 17 | 108 | 18 | $18 \cdot 108^{(790)} mod\ 827$ | 95 |
| 18 | 218 | 190 | $190 \cdot 218^{(790)} mod\ 827$ | 104 |

Setelah mendapatkan plainteks dari proses dekripsi tahap pertama, plainteks tersebut didekripsi kembali menggunakan metode *Vigènere Cipher*. Sebelum melakukan proses dekripsi, langkah pertama dalam proses dekripsi metode *Vigènere Cipher* adalah menentukkan indeks karakter dari kunci publik $(p, \alpha, \beta) = (827, 37, 276)$. Indeks karakter dari kunci publik ditampilkan pada tabel:

***Tabel 4.7*** *Indeks Karakter Kunci Publik*

| **Kunci** | **Indeks** |
|---|---|
| 8 | 56 |
| 2 | 50 |
| 7 | 55 |
| , | 44 |
| 3 | 51 |
| 7 | 55 |

| **Kunci** | **Indeks** |
|---|---|
| , | 44 |
| 2 | 50 |
| 7 | 55 |
| 6 | 54 |

Sehingga proses dekripsi tahap kedua adalah sebagai berikut:

***Tabel 4.8*** *Proses Dekripsi Tahap Kedua*

| $i$ | **Cipherteks** | **Kunci** | $D = ((C_i - K_i - 32) mod\ 95) + 32$ | **Plainteks** |
|---|---|---|---|---|
| 1 | 37 | 56 | $((37 - 56 - 32) mod\ 95) + 32$ | 76 |
| 2 | 72 | 50 | $((72 - 50 - 32) mod\ 95) + 32$ | 117 |
| 3 | 60 | 55 | $((60 - 55 - 32) mod\ 95) + 32$ | 100 |
| 4 | 70 | 44 | $((70 - 44 - 32) mod\ 95) + 32$ | 121 |
| 5 | 53 | 51 | $((53 - 51 - 32) mod\ 95) + 32$ | 97 |
| 6 | 79 | 55 | $((79 - 55 - 32) mod\ 95) + 32$ | 119 |
| 7 | 46 | 44 | $((46 - 44 - 32) mod\ 95) + 32$ | 97 |
| 8 | 71 | 50 | $((71 - 50 - 32) mod\ 95) + 32$ | 116 |
| 9 | 65 | 55 | $((65 - 55 - 32) mod\ 95) + 32$ | 105 |
| 10 | 99 | 54 | $((99 - 54 - 32) mod\ 95) + 32$ | 45 |
| 11 | 105 | 56 | $((105 - 56 - 32) mod\ 95) + 32$ | 49 |
| 12 | 107 | 50 | $((107 - 50 - 32) mod\ 95) + 32$ | 57 |
| 13 | 109 | 55 | $((109 - 55 - 32) mod\ 95) + 32$ | 54 |
| 14 | 93 | 44 | $((93 - 44 - 32) mod\ 95) + 32$ | 49 |
| 15 | 99 | 51 | $((99 - 51 - 32) mod\ 95) + 32$ | 48 |
| 16 | 103 | 55 | $((103 - 55 - 32) mod\ 95) + 32$ | 48 |
| 17 | 95 | 44 | $((95 - 44 - 32) mod\ 95) + 32$ | 51 |
| 18 | 104 | 50 | $((104 - 50 - 32) mod\ 95) + 32$ | 54 |

Langkah selanjutnya plainteks yang dihasilkan dari proses dekripsi tahap kedua dibuah menjadi karakter menggunakan tabel *ASCII printable*. Plainteksnya adalah

***Tabel 4.9*** *Proses Pengubahan Indeks menjadi Karakter*

| **Plainteks** | **Simbol** |
|---|---|
| 76 | L |
| 117 | u |
| 100 | d |

| **Plainteks** | **Simbol** |
|---|---|
| 45 | - |
| 49 | 1 |
| 57 | 9 |

| | |
|---|---|
| 121 | y |
| 97 | a |
| 119 | w |
| 97 | a |
| 116 | t |
| 105 | i |

| | |
|---|---|
| 54 | 6 |
| 49 | 1 |
| 48 | 0 |
| 48 | 0 |
| 51 | 3 |
| 54 | 6 |

Pesan asli atau plainteks yang dihasilkan yaitu Ludyawati-19610036.

## 4.3 Kajian Integrasi Agama

Berdasarkan hasil dan pembahasan yang telah didapatkan dapat ditarik kesimpulan bahwa, kombinasi metode *Vigènere Cipher* dan ElGamal dapat mengamankan pesan rahasia serta menyampaikan pesan dengan aman kepada pihak penerima. Maksud dari menyampaikan dengan benar kepada penerima adalah isi pesan yang disampaikan sesuai dengan isi pesan yang dikirim oleh pengirim. Dalam hal ini makna menyampaikan sejalan dengan prinsip amanah, yaitu menyampaikan atau memberikan kepada yang berhak menerimanya. Amanah tidak hanya berfokus kepada menyampaikan kepada yang berhak menerima, akan tetapi juga menyampaikan isi amanah atau menjalankan amanah sesuai dengan yang diberikan tanpa mengubahnya.

Sifat amanah sangat penting bagi kehidupan manusia, bahkan Allah SWT menjanjikan surga kepada orang yang senantiasa menjaga amanah kepada-Nya maupun amanah kepada sesama umat manusia. Menurut Tafsir Al-Madinah Al-Munawwarah/Markaz Ta'dzhim al-Qur'an, ayat Q.S Al Mu’minun ayat 9 menjelaskan orang-orang yang selalu menjaga amanah dan menepati janji, dan orang-orang yang senantiasa mendirikan shalat pada waktunya dengan

menyempurnakan rukun-rukunnya. Mereka yang memiliki derajat yang tinggi itu akan mewarisi surga, mewarisi tempatnya yang paling mulia, dan mereka akan tinggal di dalamnya selama-lamanya.

Menjaga informasi termasuk dalam kategori amanah. Amanah adalah salah satu sifat wajib Rasulullah. Sifat wajib rasulullah adalah cerminan dari karakter yang dimiliki oleh Rasulullah Saw. dalam menjalankan tugasnya menjadi pemimpin dari seluruh umat manusia. Pada dasarnya sifat amanah sudah dimiliki Nabi Muhammad jauh sebelum menerima wahyu. Sifat amanah Rasulullah memberi bukti bahwa, Rasulullah memiliki karakter yang dapat dipercaya karena dapat menjaga kepercayaan dengan merahasiakan sesuatu atau hal yang harus dirahasiakan dan juga menyampaikan sesuatu atau hal yang harus disampaikan. Sesuatu atau hal yang akan disampaikan, disampaikan dengan apa adanya tanpa ada yang diubah atau dikurangi informasinya (Fajriyah, 2021).

Selain sifat amanah, 3 sifat wajib Rasulullah yang lain juga berkaitan dengan Kriptografi. Sifat wajib Rasulullah tersebut diantaranya shiddiq(jujur), fathanah(cerdas), dan tabligh(menyampaikan). Shiddiq adalah sifat Rasulullah yang memiliki arti benar atau jujur. Dalam menyampaikan informasi, sifat shiddiq sangat diperlukan. Informasi harus disampaikan dengan benar, akurat, dan tepat. Dalam era informasi digital saat ini, implementasi sifat shiddiq adalah informasi yang diterima dalam bentuk pesan akan sama isinya dengan pesan yang dikirim (Fajriyah, 2021). Oleh karena itu diperlukan sistem keamanan seperti Kriptografi yang mengamankan pesan, agar pesan atau informasi yang dikirimkan tidak dimanipulasi oleh pihak tidak terkait.

Sifat wajib Rasulullah selanjutnya adalah fathanah. Fathanah artinya pandai atau cerdas. Sifat fathanah wajib dimiliki oleh nabi dan rasul dalam mendakwahkan kebenaran. Sifat fathanah diperlukan untuk melakukan dakwah kebenaran karena mengajak umat manusia menuju kebenaran diperlukan kecerdasan. Rasulullah merupakan seorang yang memiliki keistimewaan dengan ketetapan ucapannya. Berbeda dengan manusia biasa, Rasulullah mendapat ilmu bukan melalui membaca kitab akan tetapi karena wahyu yang diberikan oleh Allah Swt. Kecerdasan tersebut diperlukan untuk memahami dan menjelaskan wahyu yang diterima dari Allah Swt. kepada umat manusia sebagai pedoman, petunjuk, nasihat, dan bimbingan. Implementasi sifat fathanah di era informasi digital ini adalah dalam penyampaian pesan atau informasi diperlukan cara yang tepat dan cerdas agar informasi yang disampaikan tidak jatuh ketangan yang tidak terkait (Fajriyah, 2021). Salah satu cara tepat dan cerdas yang dapat dilakukan untuk melindungi informasi adalah dengan menggunakan Kriptografi.

Sifat wajib Rasulullah yang terakhir adalah tabligh. Tabligh artinya menyampaikan atau sekaligus mengajak orang lain ke jalan yang benar dan lurus. Dalam artian lain, sifat tabligh diartikan sebagai menyampaikan segala informasi yang baik kepada siapapun (Fajriyah, 2021). Dapat disimpulkan bahwa menyampikan sebuah informasi harus dilakukan secara tepat tanpa meninggalkan kejujuran dan juga kebenaran kepada yang layak menerimanya. Kriptografi memiliki konsep yang sama dengan sifat tabligh yaitu menyampaikan pesan kepada yang berhak dengan informasi yang benar dan sesuai.

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut:

1. Proses Enkripsi kombinasi metode *Vigènere Cipher* dan ElGamal diawali dengan proses pembentukan kunci menggunakan Algoritma Elgamal. Kunci yang dibentuk adalah kunci publik$(p, \alpha, \beta)$ dan kunci rahasia $d$. Proses pembentukan kunci dipengaruhi beberapa komponen yang harus dipenuhi, yaitu bilangan prima aman besar $p$ yang dihasilkan dari *software Python*, akar primitif $\alpha$ dari bilangan prima $p$, dan bilangan bulat $d$ yang berasal dari tiga digit terakhir dari NIM. Untuk lebih memperkuat kunci publik dilakukan pengecekan keprimaan aman dan juga akar primitif. Proses enkripsi dilakukan sebanyak dua kali yaitu proses enkripsi menggunakan metode *Vigènere Cipher* dan ElGamal. Kekuatan dari proses enkripsi tergantung pada kunci publik dan perhitungan modulo yang digunakan. Terlebih lagi pada proses enkripsi dengan Algoritma ElGamal karena kekuatan keamanan Enkripsi dari ElGamal tergantung pada bilangan prima besar dan juga akar primitif dari bilangan prima tersebut. Pada enkripsi metode *Vigènere Cipher* cipherteks diperkuat dengan menggunakan perhitungan modulo *ASCII printable.* Perhitungan dari modulo ini dapat meningkatkan keamanan dari cipherteks karena perhitungan yang digunakan berbeda dengan perhitungan modulo *tabula recta* atau tabel *ASCII* keseluruhan.

2. Proses Dekripsi kombinasi metode *Vigènere Cipher* dan ElGamal diawali dengan melakukan proses dekripsi tahap pertama. Proses dekripsi tahap pertama dilakukan menggunakan Algoritma ElGamal. Pada proses ini kunci yang digunakan adalah kunci rahasia$(p, d)$. Setelah proses tersebut dilanjutkan dengan proses dekripsi tahap kedua dengan menggunakan metode *Vigènere Cipher*. Perhitungan yang digunakan pada proses ini adalah menggunakan perhitungan modulo *ASCII printable*. Dan proses dekripsi kombinasi metode *Vigènere Cipher* dan ElGamal dapat mengembalikan atau memulihkan cipherteks menjadi pesan asli seperti semula.

## 5.2 Saran untuk penelitian Lanjutan

Penelitian ini membahas mengenai kombinasi metode *Vigènere Cipher* dan ElGamal pada pengamanan pesan rahasia. Pada kombinasi ini menggunakan modifikasi terhadap perhitungan modulo dalam metode *Vigènere Cipher* yaitu menggunakan modulo *ASCII printable*. Saran untuk penelitian selanjutnya adalah dengan menambah modifikasi terhadap Algoritma ElGamal agar kombinasi yang dihasilkan memiliki tingkat keamanan yang lebih kuat atau dapat mengubah modifikasi metode *Vigènere Cipher* dengan modifikasi yang lain.

# DAFTAR PUSTAKA


Andrian, Y., (2014). Perbandingan Penggunaan Bilangan Prima Aman dan Tidak Aman pada Proses Pembentukan Kunci Algoritma ElGamal. *Citec Journal* Vol. 1, No. 3, 194-203.

Ariska, B., & Endri, J. (2018). Rancangan Kriptografi Hybrid Kombinasi Metode *Vigenere Cipher* Dan Elgamal Pada Pengamanan Pesan Rahasia. Seminar Nasional Inovasi dan Aplikasi di Industri, 328-336.

Ariyus, D. (2006). KRIPTOGRAFI (Edisi Pertama). Yogyakarta: Penerbit Graha Ilmu.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori, Analisis, dam Implementasi. Yogyakarta: C.V ANDI OFFSET.

Basyiah, Syahputra. F., (2017). Perancangan Aplikasi Penyandian Pesan Teks Menggunakan *Vigenere Cipher* dan Algoritma ElGamal. http://ejournal.ust.ac.id/index.php/Jurnal_Means, 80-85.

Dalimunthe, P. R. (2016). AMANAH DALAM PRESPEKTIF HADIS. Jurnal Universitas Sunan Gunung Djati Bandung, 7-16.

Dewi, A. V., Wibisono. M. Y., & Hernawan, W. (2022). Amanah dalam Pandangan Hadis: Studi Tahkrij, Syarah, dan Tematik. Gunung Djati *Conference Series*, Volume 8, 914-925.

ElGamal, T. (1985). *A Publik Key Cryptosystem and a Signature Scheme Based on Discrete Logaritms*. IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO.4.

Fadilla, D. V. (2017). Implementasi Algoritma Elgamal Dan *Vigenere Cipher* Untuk Enkripsi Dan Dekripsi Data Citra Digital. Jurnal Universitas Teknologi Yogyakarta.

Fadlillah, S. N. (2021). Enkripsi dan Dekripsi menggunakan Algoritma *Hill Cipher* dan ElGamal untuk Mengamankan Pesan Teks. Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Fadlillah, S. N., Turmudi, & Khudzaifah, M,. (2022). Penggabungan Algoritma Hill Cipher dan ElGamal untuk Mengamankan Pesan Teks. Jurnal Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Fajriyah, N. H., Sari, P., & Nurhidayati, N. (2021). Upaya Penerapan Sifat Wajib Rasul Di Era Digital Melalui Pemanfaatan Kriptografi Dalam Pengiriman Pesan. Prosiding Konferensi Integrasi Interkoneksi Islam dan Sains, Volume 3, 37-41.

Hamidah, S. N. (2009). Konsep Matematis dan Proses Penyandian Kriptografi ElGamal. Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Ifanto, M. (2009). Metode Enkripsi dan Dekripsi Menggunakan Algoritma ElGamal. Jurnal Institut Teknologi Bandung.

Irawan, D. M. (2017). Implementasi Kriptografi *Vigenere Cipher* dengan Php. Jurnal teknologi Informasi Volume 1, 11-21.

Kraft, J.S., Washington, L.C., (2014). *An Introduction to Number Theory with Cryptography*. U.S: CRC Press.

Kraft, J.S., Washington, L.C., (2015). *Elementary Number Theory*. U.S: CRC Press.

Kementrian Agama RI. (2019). Al Qur'an dan Terjemahannya.

Khadir, O. (2011). *Conditions on The Generator For Forging ElGamal Signature.* International Journal of Pure and Applied Mathematics Vol. 70 No.7, 939-949.

Khumaidi, A. (2020). Algoritma Hybrid RSA (Rivest, Shamir, Adleman) dan Vigenere Cipher untuk Mengamankan Pesan. Jurnal Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Massandy, D. T. (2009). Algoritma ElGamal dalam Pengamanan Pesan Rahasia. Jurnal Institut Teknologi Bandung, 1-5.

Munir, R. (2019). KRIPTOGRAFI (Edisi Kedua). Bandung: Informatika Bandung.

Putri, R. A., Santoso, K. A., & Kamsyakawumi, A. (2021). Pengkodean *Polyalphabetic* dengan Modifikasi Algoritma ElGamal-*Caesar Cipher*. Prosiding Seminar Nasional Matematika, 540-547.

Sadikin, R. (2012). Kriptografi untuk Keamanan jaringan. Yogyakarta: C.V ANDI OFFSET.

Stinson, D.R., (1995). *Cryptography Theory and Practice*. Florida: CRC Press, Inc.

Ummi, K. (2013). Analisis Penggunaan Bilangan Prima Aman Besar Pada Algoritma ElGamal. *Proceedings* Konferensi Nasional Sistem Informasi, 1-5.

Yani, E. C. (2009). Analisis dampak Pemilihan Nilai Bilangan Prima pada Properti Algoritma ElGamal *p* terhadap Kekuatan Pengamanan Data. Jurnal Institut Teknologi Bandung.

# LAMPIRAN

## Lampiran 1. Tabel *ASCII* 0-126

### 1. Tabel *ASCII* 0-32

| Indeks | Simbol | Dekripsi |
|---|---|---|
| 00 | NULL | *NULL char* |
| 01 | SOH | *Start of Heading* |
| 02 | STX | *Start of Text* |
| 03 | ETX | *End of text* |
| 04 | EOT | *End if 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* |

| Indeks | Simbol | Dekripsi |
|---|---|---|
| 16 | DLE | *Data Line Escape* |
| 17 | DC1 | *Device Control 1* |
| 18 | DC2 | *Device Control 2* |
| 19 | DC3 | *Device Control 3* |
| 20 | DC4 | *Device Control 4* |
| 21 | NAK | *Negative Acknowledgemnt* |
| 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* |

### 2. Tabel *ASCII* 32-126

| Indeks | Simbol | Dekripsi |
|---|---|---|
| 32 | *Space* | *(Space)* |
| 33 | ! | *(Exclamation Mark)* |
| 34 | " | *(Quotation Mark)* |
| 35 | # | *(Number Sign)* |

| Indeks | Simbol | Dekripsi |
|---|---|---|
| 80 | P | *(Capital Letter P)* |
| 81 | Q | *(Capital Letter Q)* |
| 82 | R | *(Capital Letter R)* |
| 83 | S | *(Capital Letter S)* |

| 36 | $ | *(Dollar Sign)* |
|---|---|---|
| 37 | % | *(Percent Sign)* |
| 38 | & | *(Ampersand)* |
| 39 | ' | *(Apostrophe)* |
| 40 | ( | *(Round Brackets)* |
| 41 | ) | *(Round Brackets)* |
| 42 | * | *(Asterisk)* |
| 43 | + | *(Plus Sign)* |
| 44 | , | *(Comma)* |
| 45 | - | *(Hyphen)* |
| 46 | . | *(Dot, Full Stop)* |
| 47 | / | *(Slash)* |
| 48 | 0 | *(Number Zero)* |
| 49 | 1 | *(Number One)* |
| 50 | 2 | *(Number Two)* |
| 51 | 3 | *(Number Three)* |
| 52 | 4 | *(Number Four)* |
| 53 | 5 | *(Number Five)* |
| 54 | 6 | *(Number Six)* |
| 55 | 7 | *(Number Seven)* |
| 56 | 8 | *(Number Eight)* |
| 57 | 9 | *(Number Nine)* |
| 58 | : | *(Colon)* |
| 59 | ; | *(Semicolon)* |

| 84 | T | *(Capital Letter T)* |
|---|---|---|
| 85 | U | *(Capital Letter U)* |
| 86 | V | *(Capital Letter V)* |
| 87 | W | *(Capital Letter W)* |
| 88 | X | *(Capital Letter X)* |
| 89 | Y | *(Capital Letter Y)* |
| 90 | Z | *(Capital Letter Z)* |
| 91 | [ | *(Square Brackets)* |
| 92 | \ | *(Backslash)* |
| 93 | ] | *(Square Brackets)* |
| 94 | ^ | *(Circumflex Accent)* |
| 95 | _ | *(Underscore)* |
| 96 | ` | *(Grave Accent)* |
| 97 | a | *(Lowercase Letter A)* |
| 98 | b | *(Lowercase Letter B)* |
| 99 | c | *(Lowercase Letter C)* |
| 100 | d | *(Lowercase Letter D)* |
| 101 | e | *(Lowercase Letter E)* |
| 102 | f | *(Lowercase Letter F)* |
| 103 | g | *(Lowercase Letter G)* |
| 104 | h | *(Lowercase Letter H)* |
| 105 | i | *(Lowercase Letter I)* |
| 106 | j | *(Lowercase Letter J)* |
| 107 | k | *(Lowercase Letter K)* |

| 60 | < | *(Less-Than Sign)* |
|---|---|---|
| 61 | = | *(Equals Sign)* |
| 62 | > | *(Greater-Than Sign)* |
| 63 | ? | *(Question Mark)* |
| 64 | @ | *(At Sign)* |
| 65 | A | *(Capital Letter A)* |
| 66 | B | *(Capital Letter B)* |
| 67 | C | *(Capital Letter C)* |
| 68 | D | *(Capital Letter D)* |
| 69 | E | *(Capital Letter E)* |
| 70 | F | *(Capital Letter F)* |
| 71 | G | *(Capital Letter G)* |
| 72 | H | *(Capital Letter H)* |
| 73 | I | *(Capital Letter I)* |
| 74 | J | *(Capital Letter J)* |
| 75 | K | *(Capital Letter K)* |
| 76 | L | *(Capital Letter L)* |
| 77 | M | *(Capital Letter M)* |
| 78 | N | *(Capital Letter N)* |
| 79 | O | *(Capital Letter O)* |

| 108 | l | *(Lowercase Letter L)* |
|---|---|---|
| 109 | m | *(Lowercase Letter M)* |
| 110 | n | *(Lowercase Letter N)* |
| 111 | o | *(Lowercase Letter O)* |
| 112 | p | *(Lowercase Letter P)* |
| 113 | q | *(Lowercase Letter Q)* |
| 114 | r | *(Lowercase Letter R)* |
| 115 | s | *(Lowercase Letter S)* |
| 116 | t | *(Lowercase Letter T)* |
| 117 | u | *(Lowercase Letter U)* |
| 118 | v | *(Lowercase Letter V)* |
| 119 | w | *(Lowercase Letter W)* |
| 120 | x | *(Lowercase Letter X)* |
| 121 | y | *(Lowercase Letter Y)* |
| 122 | z | *(Lowercase Letter Z)* |
| 123 | { | *(Curly Brackets Or Braces)* |
| 124 | \| | *(Vertical Bar Or Vertical Slash)* |
| 125 | } | *(Curly Brackets Or Braces)* |
| 126 | ~ | *(Tilde Or Swung Dash)* |

## RIWAYAT HIDUP

Ludyawati, lahir di Malang, 28 Juni 2001. Memiliki nama panggilan Ludya. Merupakan putri pertama dari bapak Kariono dan ibu Suwarni serta kakak dari seorang adik Lucky Aprilia. Bertempat tinggal di Jalan Hayam Wuruk Gang 2 No.3 Rt 02 Rw 07, Desa Oro Oro Ombo, Kecamatan Batu Kota Batu, Jawa Timur.

Penulis memulai pendidikan dari TK PGRI 05 Kota Batu dan lulus pada tahun 2007. Kemudian melanjutkan pendidikan sekolah dasar di SDN Oro-Oro Ombo 01 dan lulus pada tahun 2013. Penulis kemudian melanjutkan pendidikan sekolah menengah pertama di SMPN 02 Kota Batu dan lulus pada tahun 2016. Pendidikan selanjutnya adalah pendidikan sekolah menengah atas di MAN Kota Batu dan lulus pada tahun 2019. Pada tahun yang sama, penulis memulai jenjang pendidikan selanjutnya yaitu perguruan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang, Fakultas Sains dan Teknologi pada Program Studi matematika.

Selama menempuh pendidikan pada jenjang perguruan tinggi, penulis aktif mengikuti beberapa kepanitiaan dan organisasi. Organisasi yang diikuti penulis diantaranya PMII Rayon Pencerahan Galileo tahun 2019-2022 serta Himpunan Mahasiswa Prodi Matematika pada tahun 2020 dan 2021. Selain itu penulis juga mengikuti beberapa kepanitiaan diantaranya KOMET XIX pada tahun 2019 dan KOMET XX pada tahun 2020.

**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 : Ludyawati
NIM : 19610036
Fakultas / Program Studi : Sains dan Teknologi / Matematika
Judul Skripsi : Kombinasi Metode *Vigènere Cipher* dan ElGamal Pada Pengamanan Pesan Rahasia
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Erna Herawati, M.Pd

| No | Tanggal | Hal | Tanda Tangan |
|---|---|---|---|
| 1. | 14 Desember 2022 | Konsultasi BAB I, II, dan III | 1. |
| 2. | 11 Januari 2023 | Konsultasi BAB I, II, dan Kajian Agama | 2. |
| 3. | 11 Januari 2023 | Konsultasi Revisi BAB I, II, dan III | 3. |
| 4. | 18 Januari 2023 | Konsultasi Revisi BAB I, II, dan Kajian Agama | 4. |
| 5. | 24 Januari 2023 | ACC Seminar Proposal | 5. |
| 6. | 28 Maret 2023 | Konsultasi revisi Seminar Proposal | 6. |
| 7. | 29 Maret 2023 | Konsultasi Bab IV dan V | 7. |
| 8. | 3 April 2023 | Konsultasi Bab IV dan Kajian Integrasi Agama | 8. |
| 9. | 4 April 2023 | ACC Seminar Hasil | 9. |
| 10. | 16 Mei 2023 | Konsultasi Revisi Seminar Hasil dan Abstrak | 10. |
| 11. | 19 Mei 2023 | Konsultasi Revisi Kajian Agama Bab IV | 11. |
| 12. | 19 Mei 2023 | ACC Sidang Skripsi | 12. |
| 13. | 23 Mei 2023 | ACC Sidang Skripsi | 13. |
| 14. | 08 Juni 2023 | ACC Keseluruhan | 14. |

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

Malang, 8 Juni 2023
Mengetahui,
Ketua Program Studi Matematika

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