IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCE HILL CIPHER* DENGAN KUNCI TERENKRIPSI ELGAMAL UNTUK ENKRIPSI CITRA DIGITAL BERWARNA

PROPOSAL
Diajukan Untuk Memenuhi Salah Satu Syarat Meraih Gelar
Sarjana Matematika Program Studi Matematika
Pada Fakultas Sains Dan Teknologi
UIN Alauddin Makassar

Oleh:

MUH. AFRIZAL NUR

NIM. 60600122061

JURUSAN MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI ALAUDDIN MAKASSAR

2025

DRAFT PROPOSAL

Nama : Muh. Afrizal Nur

NIM : 60600122061

Judul : Implementasi Algoritma Kriptografi Advance Hill Cipher Dengan Kunci Terenkripsi ElGamal Untuk Enkripsi Citra Digital Berwarna

---

I. PENDAHULUAN

A. *Latar Belakang*

Perkembangan teknologi informasi yang pesat terutama dalam era digital saat ini, telah mendorong penggunaan internet secara masif di berbagai bidang kehidupan. Menurut laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2024, jumlah pengguna internet di Indonesia diperkirakan mencapai 221.563.479 orang. Angka pengguna internet yang begitu tinggi ini telah mendorong pertumbuhan pesat berbagai layanan berbasis internet, seperti media sosial, *e-commerce*, dan layanan penyimpanan data (APJII, 2024).

Dengan begitu tingginya penggunaan layanan berbasis internet, tantangan terhadap keamanan data juga semakin serius. Data digital yang dikirim melalui internet, terutama yang bersifat sensitif seperti foto pribadi atau dokumen penting, sangat rentan terhadap ancaman seperti peretasan dan penyalahgunaan. Oleh karena itu, penting untuk menjaga data pribadi agar tidak jatuh ke tangan pihak yang tidak berwenang.

Al-Qur'an juga menganjurkan untuk menjaga rahasia yang seharusnya dijaga, anjuran ini terdapat dalam QS an-Nisa[4: 58]:

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَا ۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِ ۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖ ۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًا ۢ بَصِيْرًا

Terjemahnya: “Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat”

Menurut tafsir Tahlili, Ayat ini memerintahkan agar menyampaikan “amanat” kepada yang berhak. Amanah dalam hal ini dapat dimaknai sebagai kepercayaan yang diberikan kepada seseorang untuk menjaga sesuatu yang berharga, termasuk data atau informasi digital. Oleh karena itu, menjaga data yang sifatnya sensitif adalah bentuk dari melaksanakan amanah sebagaimana yang diperintahkan oleh Allah SWT.

Salah satu bentuk informasi digital yang paling umum digunakan adalah citra digital. Namun, penggunaan citra digital juga menghadirkan tantangan tersendiri dalam hal keamanan, terutama saat citra tersebut mengandung informasi sensitif dan dipertukarkan melalui jaringan yang tidak aman (Azam, 2020).

Keamanan citra digital menjadi isu yang sangat krusial, mengingat banyaknya ancaman yang muncul, seperti penyalahgunaan citra yang berisi informasi pribadi. Ancaman ini dapat menyebabkan citra yang bersifat rahasia yang dikirim dapat diakses oleh pihak - pihak yang tidak berwenang. Metode pengamanan data yang efektif sangat diperlukan untuk melindungi kerahasiaan dan integritas citra digital yang dikirimkan. Salah satu teknik yang dapat digunakan untuk menjaga keamanan citra digital yaitu menggunakan kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi seperti

kerahasiaan, integritas data, serta autentikasi. Dalam kriptografi, informasi yang bersifat rahasia akan disandikan sedemikian sehingga meskipun data tersebut dicuri oleh pihak yang tidak berwenang, mereka tidak dapat mengetahui data yang sebenarnya, karena informasi yang dicuri merupakan informasi yang telah disandikan (Jamaludin, 2018).

Pada dasarnya, terdapat tiga tipe algoritma kriptografi, yaitu algoritma simetri, asimetri, dan hybrid. Algoritma simetri menggunakan satu kunci tunggal yang sama untuk proses enkripsi dan dekripsi pesan. Sebaliknya, algoritma asimetri menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci publik bersifat terbuka dan dapat diketahui oleh banyak pihak, sedangkan kunci privat bersifat rahasia dan hanya diketahui oleh pihak yang berwenang. Sementara itu, algoritma hybrid menggabungkan keunggulan dari algoritma simetri dan asimetri untuk meningkatkan keamanan dan efisiensi dalam proses kriptografi.

Salah satu contoh algoritma kriptografi simetris adalah Hill Cipher, yang merupakan sandi polialfabetik berbasis metode substitusi dengan memanfaatkan perkalian matriks sebagai kunci untuk proses enkripsi dan dekripsi. Kunci dalam Hill Cipher berbentuk matriks bujur sangkar yang harus memiliki invers modulo terhadap jumlah alfabet yang digunakan. Invers ini diperlukan dalam proses dekripsi agar pesan dapat dikembalikan ke bentuk semula. Namun, pencarian matriks kunci yang memiliki invers dapat menjadi kompleks secara komputasi. Untuk mengatasi hal ini, digunakan matriks involutori, yaitu matriks yang merupakan invers dari dirinya sendiri, sebagai kunci dalam algoritma yang disebut *Advance Hill Cipher* (Acharya et al., 2009).

Menurut penelitian yang dilakukan Khazaei dan Ahmadi, algoritma Hill Cipher mampu dalam menghadapi serangan *Ciphertext-Only Attack* (COA).

Namun, COA telah mampu dipecahkan dengan *Chinese Remainder Theorem* (Khazaei & Ahmadi, 2017). Hal ini menunjukkan bahwa algoritma Hill Cipher memiliki kelemahan pada sisi keamanan kunci. Sehingga keamanan pada algoritma Hill Cipher harus ditingkatkan dan tetap mempertimbangkan kecepatan pada proses penyandian pesan.

Dalam penelitiannya, Fadlilah mengusulkan kombinasi Hill Cipher dan ElGamal untuk mengamankan pesan teks, didapatkan hasil bahwa penggabungan algoritma Hill Cipher dan ElGamal untuk mengamankan pesan teks dapat dilakukan dengan baik (Fadlilah et al., 2022). Namun, penelitian tersebut masih terbatas pada pengamanan pesan berbasis teks dan belum menyentuh aspek keamanan data berbentuk citra digital yang memiliki kompleksitas yang lebih tinggi.

Maka alasan utama penulis melakukan penelitian yang berjudul *"Implementasi Algoritma Kriptografi Advance Hill Cipher dengan Kunci Terenkripsi El-Gamal Untuk Enkripsi Citra Digital Berwarna"* bermaksud ingin melakukan penelitian yang bertujuan untuk meningkatkan keamanan suatu citra dengan menggabungkan dua algoritma yang disebut dengan algoritma hibrida.

B. *Rumusan Masalah*

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengimplementasikan metode kriptografi *Advance Hill Cipher* dengan kunci terenkripsi El Gamal untuk enkripsi dan dekripsi citra digital berwarna

2. Bagaimana hasil enkripsi dan dekripsi citra digital berwarna dengan metode kriptografi *Advance Hill Cipher* dengan kunci terenkripsi El Gamal
3. Bagaimana performa kecepatan enkripsi dan dekripsi Advance Hill Cipher dengan kunci terenkripsi ElGamal

C. *Tujuan Penelitian*

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini ialah sebagai berikut:

1. Untuk mengetahui proses enkripsi dan dekripsi citra digital berwarna menggunakan algoritma *Advance Hill Cipher* dengan kunci terenkripsi El Gamal
2. Untuk mengetahui hasil enkripsi dan dekripsi citra digital berwarna menggunakan algoritma *Advance Hill Cipher* dengan kunci terenkripsi El Gamal
3. Untuk mengetahui performa kecepatan enkripsi dan dekripsi Advance Hill Cipher dengan kunci terenkripsi ElGamal

D. *Manfaat Penelitian*

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Bagi Penulis, penelitian ini dapat menjadi sarana untuk memperdalam pemahaman tentang kriptografi algoritma Advance Hill Cipher dan ElGamal.
2. Bagi Pembaca, penelitian ini dapat memberikan wawasan tentang bagaimana implementasi algoritma Advance Hill Hipher dan ElGaman dalam mengenkripsi citra digital berwarna.

E. *Batasan Masalah*

Agar pembahasan pada penelitian ini tidak meluas, maka diperlukan batasan – batasan masalah sebagai berikut.

1. Matriks kunci *Advance Hill Cipher* menggunakan matriks ordo 3×3
2. Data yang dienkripsi berupa citra digital berwarna dengan format *.png* dengan ukuran 256×256

F. *Sistematika Penulisan*

I. PENDAHULUAN

Bagian ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian manfaat penelitian, batasan masalah dan sistematika penulisan.

II. TINJAUAN PUSTAKA

Bagian ini terdiri tentang landasan teori, yang berisikan teori-teori serta Pustaka yang digunakan pada saat penelitian. Teori – teori tersebut terkait dengan Algoritma kriptografi *Advance Hill Cipher*, *ElGamal*, dan metrics pengukuran *Structural Similarity Index Metrics* (SSIM) dan *Mean Square Error* (MSE) ini didapatkan dari buku literatur, jurnal, dan internet.

III. METODOLOGI PENELITIAN

Bagian ini dikemukakan metode penelitian yang mencangkup ruang lingkup kegiatan, waktu penelitiaan, jenis dan sumber data dan prosedur penelitiian

II. TINJAUAN PUSTAKA

A. *Matriks*

Matriks merupakan suatu susunan bilangan berbentuk persegi panjang yang disusun secara teratur dalam baris dan kolom. Setiap bilangan dalam susunan tersebut disebut sebagai entri matriks. Dalam konteks sistem persamaan linear, matriks digunakan untuk merepresentasikan koefisien-koefisien dari persamaan tersebut dalam bentuk entri-entri matriks.

Definisi 2.1.1 (Matriks)

Matriks **A** berukuran $\boldsymbol{m \times n}$ ialah suatu susunan angka dalam persegi empat ukuran $\boldsymbol{m \times n}$, sebagai berikut:

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

Matriks berukuran (ordo) $\boldsymbol{m \times n}$ atau $\boldsymbol{A} = (\boldsymbol{a_{ij}})$

Matriks ukuran $n \times n$ disebut sebagai matriks persegi. Matriks yang terdiri dari 1 baris dan n kolom ditulis $1 \times n$ disebut dengan matriks baris atau vektor baris dan yang terdiri dari n baris dan 1 kolom disebut matriks kolom atau vektor kolom.

1. **Operasi Matriks**

   Definisi 2.1.2 (Perkalian Matriks)

   Jika $\boldsymbol{A}$ adalah matriks $m \times r$ dan $\boldsymbol{B}$ adalah matriks $r \times n$ maka hasil kali $\boldsymbol{AB}$ adalah matriks $m \times n$ yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri pada baris i dan kolom j dari $\boldsymbol{AB}$, pilihlah baris i dari matriks $\boldsymbol{A}$ dan kolom j dari matriks $\boldsymbol{B}$. Kalikan entri-entri

yang bersesuaian dari baris dan kolom tersebut dan kemudian jumlahkan hasil yang diperoleh.

Contoh:

Misalkan diberikan dua buah matriks $\boldsymbol{A}$ dan $\boldsymbol{B}$, masing – masing berukuran 3×3, sebagai berikut:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}$$

Hasil perkalian dua matriks tersebut adalah matriks $\boldsymbol{C}$ berukuran 3×3 seperti berikut.

$$\boldsymbol{C} = \begin{bmatrix} 30 & 24 & 18 \\ 84 & 69 & 54 \\ 138 & 114 & 90 \end{bmatrix}$$

2. **Determinan Matriks**

Definisi 2.1.3 (Hasil Kali Elementer)

Suatu hasil kali elementer dari suatu matriks persegi $\boldsymbol{A_{n \times n}}$, adalah hasil kali $\boldsymbol{n}$ entri $\boldsymbol{A}$, yang tidak satu pun berasal dari baris atau kolom yang sama.

Definisi 2.1.4 (Determinan)

Misalkan $\boldsymbol{A}$ adalah suatu matriks persegi. Fungsi determinan dinyatakan oleh **det**, dan didefinisikan det(A) sebagai jumlah semua hasil kali elementer bertanda dari A. Jumlah det(A) dinamakan sebagai determinan A.

Teorema 2.1.1. Jika $\boldsymbol{A}$ adalah sebarang matriks persegi yang mengandung sebaris bilangan nol, maka $\det(\boldsymbol{A}) = 0$

Bukti:

Karena hasil kali elementer bertanda dari $\boldsymbol{A}$ mengandung satu faktor dari setiap baris $\boldsymbol{A}$, maka tiap-tiap hasil kali elementer bertanda mengandung faktor dari baris bilangan nol dan sebagai konsekuensinya juga akan mempunyai nilai nol.

Contoh:

Hitunglah determinan dari matriks: $\boldsymbol{A} = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$

$$\mathbf{det}(\boldsymbol{A}) = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$$

$$= (-1)^{1+1}2\begin{vmatrix} 1 & 5 \\ 2 & 2 \end{vmatrix} + (-1)^{1+2}4\begin{vmatrix} 3 & 5 \\ 1 & 2 \end{vmatrix} + (-1)^{1+3}1\begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix}$$

$$= 2(2-10) - 4(6-5) + 1(6-1)$$

$$= -15$$

3. **Invers Matriks**

Definisi 2.1.4 (Invers)

Jika $\boldsymbol{A}$ adalah matriks persegi, dan jika terdapat matriks $\boldsymbol{B}$ yang ukurannya sama sedemikian sehingga $\boldsymbol{AB} = \boldsymbol{BA} = \boldsymbol{I}$, maka $\boldsymbol{A}$ disebut dapat dibalik (*invertible*) dan $\boldsymbol{B}$ disebut sebagai invers dari $\boldsymbol{A}$.

Definisi 2.1.5 (Kofaktor-Adjoin)

Jika $\boldsymbol{A}$ adalah matriks persegi dan C_{ij} adalah kofaktor dari a_{ij}, maka matriks

$$\boldsymbol{C} = \begin{bmatrix} C_{11} & C_{12} & \dots & C_{1n} \\ C_{21} & C_{22} & \dots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \dots & C_{nn} \end{bmatrix}$$

Disebut matriks kofaktor dari $\boldsymbol{A}$. Transpos dari matriks ini disebut adjoin dari $\boldsymbol{A}$ dan dinyatakan sebagan $adj(\boldsymbol{A})$

Teorema 2.1.2. Jika $\boldsymbol{A}$ suatu matriks yang dapat dibalik, maka

$$\boldsymbol{A}^{-1} = \frac{1}{\det(\mathbf{A})} adj(\boldsymbol{A})$$

Bukti:

Akan ditunjukkan bahwa

$$\boldsymbol{A}adj(\boldsymbol{A}) = \det(\boldsymbol{A})\boldsymbol{I}$$

Perhatikan hasil kali

$$\boldsymbol{A}adj(\boldsymbol{A}) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} C_{11} & C_{21} & \dots & C_{j1} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{j2} & \dots & C_{n2} \\ \vdots & \vdots & & \vdots & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{jn} & \dots & C_{nn} \end{bmatrix}$$

Entri pada baris ke-i dan kolom ke-j dari hasil kali $\boldsymbol{A}adj(\boldsymbol{A})$ adalah

$$a_{i1}C_{j1} + a_{i2}C_{j2} + \cdots + a_{in}C_{jn}$$

Jika $i = j$, maka ..... adalah ekspansi kofaktor dari $\det(\boldsymbol{A})$ sepanjang baris ke-i dari $\boldsymbol{A}$ dan jika $i \neq j$, maka semua a dan kofaktor – kofaktornya berasal dari baris – baris yang berbeda dari $\boldsymbol{A}$, sehingga nilai dari .... adalah nol. Oleh karena itu,

$$\boldsymbol{A}adj(\boldsymbol{A}) = \begin{bmatrix} \det(\boldsymbol{A}) & 0 & \dots & 0 \\ 0 & \det(\boldsymbol{A}) & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det(\boldsymbol{A}) \end{bmatrix}$$

Karena $\boldsymbol{A}$ dapat dibalik, $\det(\boldsymbol{A}) \neq 0$. Karena itu, persamaan ..... dapat ditulis kembali sebagai.

$$\frac{1}{\det(\boldsymbol{A})}[\boldsymbol{A}adj(\boldsymbol{A})] = \boldsymbol{I}$$

Atau

$$\boldsymbol{A}\left[\frac{1}{\det(\boldsymbol{A})} adj(\boldsymbol{A})\right] = \boldsymbol{I}$$

Dengan mengalikan kedua sisi dengan $\boldsymbol{A}^{-1}$ menghasilkan

$$\boldsymbol{A}^{-1} = \frac{1}{\det(\boldsymbol{A})} adj(\boldsymbol{A})$$

Matriks $\boldsymbol{A}$ akan memiliki invers jika $\boldsymbol{A}$ adalah matriks persegi dan $\det(\boldsymbol{A}) \neq 0$. Jika $\det(\boldsymbol{A}) = 0$, maka $\boldsymbol{A}$ disebut matriks singular. Invers matriks $\boldsymbol{A}$ ditulis $\boldsymbol{A}^{-1}$.

Contoh:

Carilah invers dari matriks

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

B. *Aritmetika Modulo*

Aritmatika modulo merupakan bagian dari teori bilangan yang mempelajari operasi – operasi bilangan bulat berdasarkan pembagian terhadap suatu bilangan bulat positif tertentu, yang disebut modulus.

Aritmatika modular menggunakan operator modular, yaitu sebuah bilangan bulat a dan sebuah bilangan bulat n yang disebut modulus. Operasi modular disimbolkan dengan :

$$a \; mod \; n = r$$

Contoh:

Hasil dari 58 mod 7 adalah 2

Karena tujuan dari operasi modular adalah mengembalikan nilai r yang merupakan sisa bagi atas operasi a dibagi n, maka hasil dari 58 mod 7 = 2.

Definisi 2.2.1 (Kekongruenan)

Jika sebuah bilangan m yang tidak nol, membagi selisih $a - b$, maka dikatakan a kongruen dengan b modulo m, dan ditulis:

$$a \equiv b \ (mod\ m)$$

Jika $a - b$ tidak habis dibagi m, maka dikatakan a tidak kongruen dengan $b\ mod\ m$, dan ditulis:

$$a \not\equiv b \ (mod\ m)$$

Teorema 2.2.1 Misalkan m adalah bilangan bulat positif. Bilangan bulat a dan b kongruen modulo m jika dan hanya jika terdapat suatu bilangan bulat k sehingga.

$$a = b + km$$

Bukti:

Jika $a \equiv b \ (mod\ m)$, maka berdasarkan definisi kongruensi (Definisi 2.2.1), diketahui bahwa $m \mid (a - b)$. Ini berarti terdapat suatu bilangan bulat k sedemikian sehingga $a - b = km$, sehingga $a = b + km$. Sebaliknya, jika terdapat suatu bilangan bulat k sehingga $a = b + km$, maka $km = a - b$. Dengan demikian, m membagi $a - b$, sehingga $a \equiv b \ (mod\ m)$.

Contoh:

Periksa apakah $23 \equiv 5 \ (mod\ 6)$!

$$a - b = 23 - 5 = 18$$

Karena $6 \mid 18$, maka benar bahwa $23 \equiv 5 \ (mod\ 6)$, dapat ditulis sebagai.

$$23 = 5 + 3 \times 6$$

Definisi 2.2.2

Misalkan $\boldsymbol{A}$ dan $\boldsymbol{B}$ adalah matriks $n \times k$ dengan entri-entrinya bilangan bulat, dengan unsur ke (i, j) berturut-turut adalah a_{ij} dan b_{ij}. Matriks $\boldsymbol{A}$ dikatakan kongruen dengan $\boldsymbol{B}$ modulo m jika $a_{ij} \equiv b_{ij} \ (mod\ m)$ untuk setiap pasang (i, j) dengan $1 \leq i \leq n$ dan $i \leq j \leq k$ dan dinotasikan dengan

$$\boldsymbol{A} \equiv \boldsymbol{B} \ (mod\ m)$$

Contoh:

Definisi 2.2.3

Misalkan $\boldsymbol{A}'$ dan $\boldsymbol{A}$ adalah matriks $n \times n$ dari bilangan – bilangan bulat, dan $\boldsymbol{A}'\boldsymbol{A} = \boldsymbol{A}\boldsymbol{A}' = \boldsymbol{I}$ (mod m) dimana:

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

Adalah matriks identitas berorde n, maka $\boldsymbol{A}'$ dikatakan invers dari $\boldsymbol{A}$ modulo m. Jika $\boldsymbol{A}'$ invers dari $\boldsymbol{A}$ dan $\boldsymbol{B} \equiv \boldsymbol{A}' \ (mod\ m)$, maka $\boldsymbol{B}$ juga invers dari $\boldsymbol{A}$

C. *Kriptografi*

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata "*cryptós*" artinya *"secret"* (rahasia) dan *"gráphein"* artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi pada pengertian modern merupakan ilmu yang menggunakan teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data, dan autentikasi identitas.

1. **Terminologi dalam Kriptografi**

   a. Pesan

Pesan (message) adalah data atau informasi yang dapat dibaca, dan dimengerti artinya. Pesan dapat berupa teks, citra (image), suara/bunyi (audio), video, atau bentuk-bentuk biner lainnya, baik berbentuk digital maupun analog.

b. *Plaintext*

Plaintext merupakan pesan asli berupa kumpul karakter yang dapat berupa abjad, angka atau simbol yang dapat dibaca dan memiliki makna.

c. *Ciphertext*

Ciphertext merupakan pesan yang telah disandikan menjadi pesan yang tidak dapat dimengerti lagi maknanya, sehingga tidak dapat dimengerti oleh pihak lain.

d. Enkripsi

Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiannya menggunakan proses penyandian plainteks menjadi cipherteks. Proses enkripsi menerima masukan berupa plainteks dan kunci kemudian menghasilkan sebuah cipherteks.

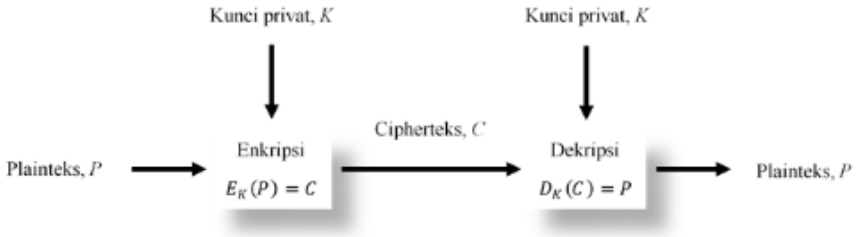
e. Dekripsi

Dekripsi merupakan proses mengembalikan cipherteks menjadi plainteks. Proses dekripsi menerima masukan berupa cipherteks dan kunci, kemudian menghasilkan plainteks.

2. **Algoritma Kriptografi**

a. Algoritma Simetri

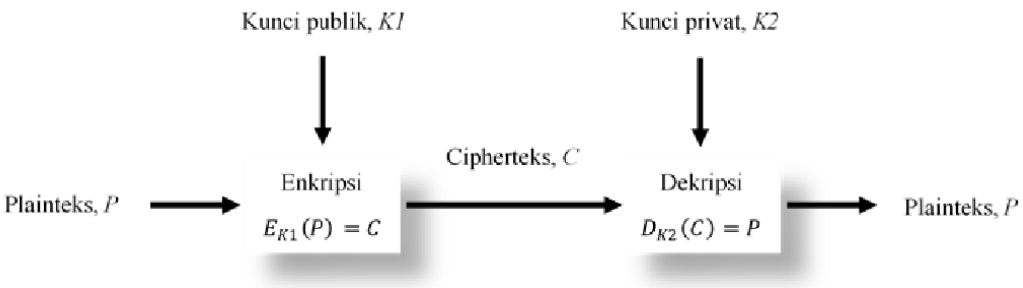
Algoritma simetri adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Untuk menggunakan algoritma ini, penerima pesan harus tahu kunci. Contoh algoritma yang memakai kunci simetri adalah *Hill Cipher, Advance Encryption Standard (AES), One Time Pad*, dan lain sebagainya.



Gambar 1. Proses enkripsi dan dekripsi algoritma simetri

b. Algoritma Asimetri

Algoritma asimetri adalah algoritma yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsinya. Algoritma asimetri memiliki kelebihan yaitu kunci untuk enkripsi dibuat umum (public key) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsinya hanya diketahui oleh orang yang berwenang atau sering disebut kunci pribadi (private key).



Gambar 2. Proses enkripsi dan dekripsi algoritma asimetri

D. *Hill Cipher*

Hill cipher dikembangkan oleh seorang matematikawan yaitu Lester S. Hill pada tahun 1929. *Hill cipher* termasuk kriptosistem polygrafik. Sebuah poly grafik adalah sebuah cipher dimana plaintext dibagi dalam sebuah group yang berdekatan dari panjang n, dan kemudian setiap group ditransformasikan ke dalam sebuah group yang berbeda dari n (Jamaludin, 2018).

Metode Hill Cipher menggunakan matriks kunci sebagai kunci enkripsi. eks yang akan dienkripsi dibagi menjadi blok-blok yang memiliki ukuran yang sama dengan matriks kunci. Setiap blok teks diubah menjadi vektor kolomdan dikalikan dengan matriks kunci. Hasil perkalian tersebut menghasilkan teks terenkripsi. Salah satu syarat penting dalam metode Hill Cipher adalah determinan matriks kunci harus relatif prima dengan ukuran alfabet yang digunakan. Misalkan untuk karakter ASCII 256 atau PBB(d, 256) = 1, dimana Jika determinan matriks kunci tidak memenuhi syarat ini, matriks invers dari matriks kunci tidak akan ada, dan metode Hill Cipher tidak dapat diterapkan. (Sylvinani dkk, 2024)

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

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

Keterangan:

C = *Ciphertext*

P = *Plaintext*

K = Matriks Kunci

N = Nilai modulo

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

$$K^{-1} = \frac{1}{\det A} Adj(A)$$

Keterangan:

Det A = Determinan matriks A

$Adj(A)$ = Adjoint matriks kunci

K^{-1} = Invers matriks

Jika invers matriks kunci berupa bilangan pecahan, konversikan matriks kunci menjadi bilangan bulat. Kemudian untuk mendapatkan *plaintext* Kembali menggunakan rumus.

$$P = K^{-1}C \ mod \ N$$

Keterangan:

P = *plaintext*

C = *ciphertext*

K = matriks kunci

N = nilai modulo

E. *Advance Hill Cipher*

Algoritma *Advance Hill Cipher* diusulkan Acharya, mereka mengklain bahwa algoritma Advance Hill Cipher lebih aman dibandingkan dengan Hill Cipher asli (Acharya et al., 2009). Pada kasus enkripsi, algoritma *AdvHill* menggunakan matriks kunci involutori. Suatu matriks A dikatakan suatu matrix involutori, jika matriks tersebut merupakan inversnya. Perkalian terhadap matriks A dikatakan involusi, jika $A^2 = I$. (Azam, 2020)

Berikut ini merupakan sifat – sifat dari matriks involutori.

1. $A = A^{-1}/A^2 = I$
2. $\det(A) = \pm 1$
3. A dikatakan involutori jika $\frac{1}{2}(A + I)$ idempoten
4. A involutori, B involutori maka AB juga involutori
5. Untuk n = genap $A^n = I$ dan untuk n = ganjil $A^n = A$
6. Matriks dengan periode 2 adalah involutori
7. A involutori jika $a_{11} + a_{22} \equiv 0$
8. $|A| = -1$ jika $a_{11} + a_{22} \equiv 0$
9. $\det(I) = 1 \Longrightarrow \det(A)$ harus berupa angka yang kuadratnya harus 1.

F. *El Gamal*

Algoritma ElGamal merupakan algoritma kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Algoritma ini didasarkan atas masalah logaritma diskrit. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Pada proses enkripsi dan dekripsi menggunakan algoritma ElGamal terdapat besaran perlu dipenuhi yaitu yang bersifat rahasia dan tidak rahasia.

Besaran yang bersifat tidak rahasia atau yang dapat diketahui pengirim dan penerima yaitu.

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

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

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

1. **Proses Pembentukan Kunci**

Algoritma ElGamal membutuhkan sepasang kunci yang dibangkitkan dengan menentukan bilangan prima p dan dua buah bilangan acak, yaitu g dan x dengan syarat $g < p$ dan $1 \leq x \leq p-2$ yang memenuhi persamaan.

$$y = g^x mod\ p$$

Keterangan:

y = kunci publik

g = generator (akar primitif dari bilangan prima)

p = bilangan prima

2. **Proses Enkripsi**

Proses enkripsi memanfaatkan kunci publik (y, g, p) dan bilangan acak k dengan syarat $1 \leq k \leq p-2$. Setiap karakter dalam pesan dilakukan enkripsi dengan bilangan k yang berbeda untuk meningkatkan keamanan dari *ciphertext* yang dihasilkan,

$$a = g^k mod\ p$$

$$b = m\ y^k mod\ p$$

Keterangan:

g = generator (akar primitif dari bilangan prima)

m = *Plaintext*

p = Bilangan prima

Proses enkripsi pada algoritnma ElGamal akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (a, b).

3. **Proses Dekripsi**

Pada proses dekripsi digunakan sepasang kunci pribadi (x, p) untuk mendekripsi (a, b) menjadi plaintext dengan persamaan:

$$m = b \cdot c \; mod \; p$$

Nilai dari variabel c didapat dengan menggunakan persamaan:

$$c = a^{p-1-x} \; mod \; p$$

Keterangan:

m = *Plaintext*

b = Ciphertext

p = Bilangan prima

G. *Citra Digital*

Citra Digital merupakan gambaran atau representasi dari suatu objek pada bidang dua dimensi. Dalam bentuk matematisnya citra digital didefiniskan pada fungsi dua dimensi $f(x, y)$, dimana x dan y merupakan koordinat spasial, dan amplitudo f di titik koordinat (x, y) dinamakan intensitas atau level keabuan pada citra di titik tersebut (Gonzalez, 2009).

Sebuah citra digital dapat dibentuk dalam sebuah matriks $M \times N$ berupa.

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,N-1} \\ \cdots & \cdots & \cdots & \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$

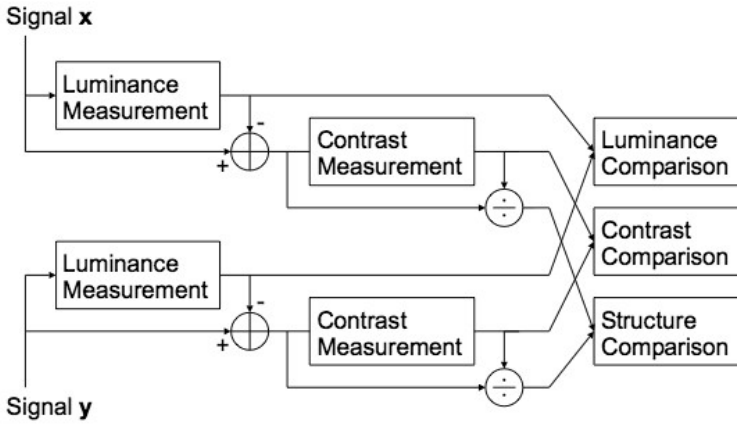
Setiap elemen dari matriks tersebut disebut dengan elemen piksel. Dalam sebuah citra digital terdapat komposisi antara koordinat dan tingkat keabuhan (Gray-Level). Koordinat diartikan sebagai posisi entri dalam matriks citra digital maka tingkat keabuhan merupakan entri/nilai dari setiap entri/piksel citra digital yang akan menentukan warna pada tiap piksel.

Tingkat keabuhan ini berkaitan dengan binary digit (bit) yang tersusun atas bilangan 0 dan 1. Semua varian warna untuk piksel diperoleh dari tiga warna dasar yaitu merah, hijau dan biru.

H. *Peak Signal-to-Noise Ratio* (PSNR)

SSIM merupakan kualitas metric yang digunakan untuk mengukur kemiripan diantara 2 citra dan dipercaya berkorelasi dengan kualitas persepsi *Human Visual System* (HVS) . Model SSIM dibuat dengan memperhatikan 3 faktor yaitu *loss of correlation*, *luminanced distortion* dan *contrast distortion*. Persamaan SSIM dapat dilihat pada.

$$SSIM(f,g) = l(f,g)c(f,g)s(f,g)$$



Gambar 3. Diagram sistem pengukuran SSIM

Dengan faktor – faktornya yaitu:

$$\begin{cases} l(f,g) = \dfrac{2\mu_f\mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f,g) = \dfrac{2\sigma_f\sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f,g) = \dfrac{2\sigma_{fg} + C_3}{\sigma_f\sigma_g + C_3} \end{cases}$$

$l(f, g)$ adalah perbandingan luminansi yang mengukur kemiripan nilai luminansi rerata 2 citra (μ_f dan μ_g). Nilai maksimal dari nilai $l(f, g)$ sama dengan 1. Nilai maksimal akan tercapai bila $\mu_f = \mu_g$.

$c(f, g)$ adalah perbandingan nilai kontras yang mengukur kemiripan nilai standar deviation 2 citra yaitu σ_f dan σ_g. Nilai maksimal dari nilai $c(f, g)$ sama dengan 1. Nilai maksimal akan tercapai bila $\sigma_f = \sigma_g$.

$s(f, g)$ adalah perbandingan struktur yang mengukur koefisien korelasi di antara 2 citra (f, g) σ_{fg} adalah nilai kovarian antara f dan g.

Jangkauan nilai SSIM adalah 0 sampai dengan 1. Nilai "0" menunjukkan kedua citra yang dibandingkan tidak berkorelasi sedangkan nilai "1" menunjukkan kedua citra yang dibandingkan sama persis $f = g$.

C_1, C_2 dan C_3 adalah suatu konstanta agar penyebut tidak sama dengan nol. (Wulandari, 2017).

I. Mean *Square* Error (MSE)

III. METODOLOGI PENELITIAN

A. *Jenis Penelitian*

Jenis penelitian yang digunakan adalah studi pustaka, didasarkan pada buku-buku dan jurnal ilmiah yang berhubungan dengan kriptografi dan aturan matematika yang berkaitan dengan *Hill cipher* dan ElGamal.

B. *Jenis dan Sumber Data*

Data yang digunakan dalam penelitian ini berupa data citra digital yang berukuran *N x N* dengan *N* merupakan bilangan genap positif dan format citra **.png* yang diperoleh dari *standard image test*

C. *Waktu dan Tempat Pengambilan Data*

Data penelitian tersebut diambil dari *standard image test*, pada bulan Januari 2025.

D. *Prosedur Penelitian*

Adapun langkah – langkah yang dilakukan untuk mendapatkan tujuan penelitian dengan menggunakan metode kriptografi Advance Hill Cipher dengan kunci terenkripsi El Gamal yaitu:

1. Persiapan Data
    a. Mengumpulkan beberapa citra digital berwarna yang akan digunakan sebagai data uji coba.
2. Penerapan Algoritma
    a. Pembangkitan Kunci
        1) Membangkitkan matriks kunci untuk algoritma Advance Hill Cipher yang invertibel modulo 256.

2) Menghasilkan pasangan kunci publik dan privat untuk algoritma ElGamal.

b. Proses Enkripsi

1) Mengenkripsi citra digital menggunakan Advance Hill Cipher dengan matriks kunci.

2) Mengenkripsi matriks kunci menggunakan ElGamal.

c. Proses Dekripsi

1) Mendekripsi matriks kunci menggunakan ElGamal.

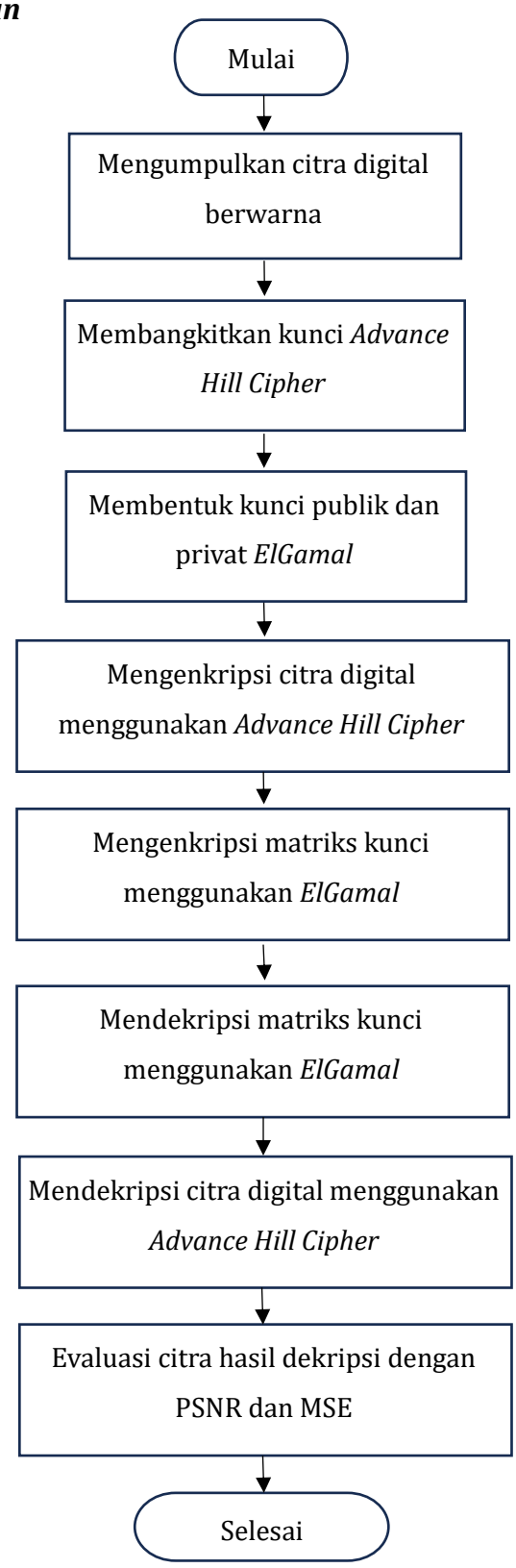
2) Mendekripsi citra menggunakan Advance Hill Cipher dengan matriks kunci dekripsi.

3. Evaluasi Hasil

a. Menilai kualitas citra hasil dekripsi menggunakan PSNR dan MSE.

b. Mengamati hasil visual untuk memastikan citra dapat dikenali.

E. *Flowchart Penelitian*



DAFTAR PUSTAKA

Acharya, B., Panigrahy, S. K., Patra, S. K., Kumar Panigrahy, S., & Panda, G. (2009). Image Encryption Using Advanced Hill Cipher Algorithm. In *International Journal of Recent Trends in Engineering* (Vol. 1, Issue 1). https://www.researchgate.net/publication/229012891

APJII. (2024). *Laporan Survei Pengguna Internet APJII 2024*.

Azam, T. (2020). *Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm*.

Fadlilah, S. N., Turmudi, T., & Khudzaifah, M. (2022). Penggabungan Algoritma Hill Cipher dan ElGamal untuk Mengamankan Pesan teks. *Jurnal Riset Mahasiswa Matematika*, *1*(5), 230–235. https://doi.org/10.18860/jrmm.v1i5.14496

Gonzalez, R. C. (2009). *Digital image processing*. Pearson education india.

Jamaludin, J. (2018). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *2*(2), 86–93.

Khazaei, S., & Ahmadi, S. (2017). Ciphertext-only attack on d × d Hill in O(d13d). *Information Processing Letters*, *118*, 25–29. https://doi.org/10.1016/j.ipl.2016.09.006

Wulandari, M. (2017). Index Quality Assesment Citra Terinterpolasi (SSIM dan FSIM). *Jurnal Terapan Teknologi Informasi*, *1*(1).