SKRIPSI

SKEMA ENKRIPSI BERBASIS GRAF *SUN*, BIPARTIT, DAN BINTANG DENGAN SUBSTITUSI DAN PERMUTASI

ARDHA CARLINDA PUTRI

22106010050

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2026

SKEMA ENKRIPSI BERBASIS GRAF *SUN*, BIPARTIT, DAN BINTANG DENGAN SUBSTITUSI DAN PERMUTASI

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

ARDHA CARLINDA PUTRI

22106010050

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2026

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Ardha Carlinda Putri
NIM	: 22106010050
Judul Skripsi	: Skema Enkripsi Berbasis Graf *Sun*, Bipartit, dan Bintang dengan Substitusi dan Permutasi

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 2 Februari 2026

Pembimbing II

Deddy Rahmadi, M.Sc.
NIP. 199308072022031001

Pembimbing I

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 198401132015031001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-434/Un.02/DST/PP.00.9/02/2026

Tugas Akhir dengan judul : SKEMA ENKRIPSI BERBASIS GRAF SUN, BIPARTIT, DAN BINTANG DENGAN SUBSTITUSI DAN PERMUTASI

yang dipersiapkan dan disusun oleh:

Nama : ARDHA CARLINDA PUTRI
Nomor Induk Mahasiswa : 22106010050
Telah diujikan pada : Selasa, 10 Februari 2026
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 69a054418eba1

Penguji I

Deddy Rahmadi, M.Sc.
SIGNED

Valid ID: 699bbd783c097

Penguji II

Pipit Pratiwi Rahayu, S.Si., M.Sc.
SIGNED

Valid ID: 699695384488b

Yogyakarta, 10 Februari 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 69a129d2aaf15

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Ardha Carlinda Putri
NIM	: 22106010050
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 2 Maret 2026

Ardha Carlinda Putri

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk kedua orang tua dan Almamater UIN Sunan Kalijaga Yogyakarta.

HALAMAN MOTTO

"Dan bahwa manusia hanya memperoleh apa yang telah diusahakannya."

(QS. An-Najm: 39)

"Dua hal saja: Usahakan doamu, dan doakan usahamu."

PRAKATA

Allhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT yang telah memberikan rahmat, nikmat, serta hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi dengan judul "Skema Enkripsi Berbasis Graf *Sun*, Bipartit, dan Bintang dengan Substitusi dan Permutasi". Penulisan skripsi ini diselesaikan sebagai salah satu prasyarat mencapai gelar Sarjana Matematika.

Penulis menyadari bahwa penulisan skripsi ini terdapat banyak hambatan dan halangan. Namun berkat adanya motivasi, bantuan, bimbingan, dan dorongan dari berbagai pihak, *alhamdulillah* skripsi ini dapat terselesaikan. Oleh karena itu, dengan kerendahan hati penulis mengucapkan terima kasih kepada:

1. Prof. Noorhaidi, M.A., M.Phil., Ph.D., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Dr. Epha Diana Supandi, S.Si., M.Sc., selaku Ketua Program Studi Matematika.
4. Noor Saif Muhammad Mussafi, S.Si., M.Sc., Ph.D., selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama menempuh pendidikan.
5. Muhamad Zaki Riyanto, S.Si., M.Sc., dan Deddy Rahmadi, M.Sc., selaku dosen pembimbing skripsi yang telah meluangkan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.

6. Pipit Pratiwi Rahayu, S.Si., M.Sc., selaku dosen penguji yang telah memberikan saran dan masukan yang berharga dalam penyempurnaan skripsi ini.

7. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.

8. Bapak dan Ibu tercinta, dua orang yang sangat berjasa dalam hidup penulis. Terima kasih atas doa, cinta, kepercayaan, dan segala bentuk dukungan yang telah diberikan, sehingga penulis selalu merasa dikuatkan dalam setiap proses dan keputusan yang diambil. Terima kasih pula atas kesediaan Bapak dan Ibu yang tanpa lelah mendengarkan setiap keluh kesah penulis hingga sampai pada titik ini. Semoga karya ini menjadi kebanggaan kecil bagi Bapak dan Ibu, sebagaimana kalian selalu menjadi kebanggaan terbesar dalam hidup penulis.

9. Kakak penulis, Arga Aryanto, terima kasih atas perhatian dan dukungan yang telah diberikan selama ini. Penulis menyadari bahwa setiap orang memiliki cara yang berbeda dalam menunjukkan kepedulian, dan hal tersebut tetap menjadi bagian dari dukungan yang berarti dalam perjalanan penulis hingga tahap ini.

10. Keluarga besar penulis, khususnya kakak sepupu penulis Dyah Retno Setyaningrum, Sinta Amalia Sari, dan Fitriana Novita Sari, terima kasih atas doa, perhatian, dan kebersamaan yang selalu diberikan meskipun terpisah oleh jarak. Dukungan tersebut menjadi penyemangat tersendiri bagi penulis dalam menyelesaikan skripsi ini.

11. Sahabat penulis, Dea Iswari, Fernanda Devita Sukma, dan Jaqueline Widad Zuha, terima kasih atas kebersamaan, dukungan, dan bantuan yang diberikan

sejak awal perkuliahan hingga proses penyusunan skripsi ini. Kehadiran kalian menjadikan perjalanan penulis selama masa perkuliahan terasa lebih berwarna.

12. Teman-teman seperjuangan selama proses penyusunan skripsi ini, terima kasih atas kebersamaan, dukungan, dan semangat yang saling diberikan selama belajar dan berdiskusi bersama di perpustakaan.
13. Teman-teman seperjuangan Program Studi Matematika angkatan 2022.
14. Semua pihak yang tidak bisa penulis sebutkan yang secara langsung maupun tidak langsung membantu terselesaikannya skripsi ini.

Penulis berharap semoga skripsi ini dapat memberikan manfaat bagi semua yang membacanya. Penulis juga berharap kritik dan saran yang membangun.

Yogyakarta, 28 Januari 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$\mathbb{Z}$	:	himpunan semua bilangan bulat
$\mathbb{Z}_n$	:	himpunan semua bilangan bulat modulo n
$\mathbb{Z}_{>0}$	:	Himpunan semua bilangan bulat positif
P_n	:	himpunan n bilangan prima
S_n	:	grup permutasi dari n elemen
$\bar{G}$	:	komplemen dari graf G
C_n	:	graf siklus (*cycle graph*) dengan n verteks
K_n	:	graf lengkap (*complete graph*) dengan n verteks
Su_n	:	graf *sun* dengan $2n$ verteks
B_n	:	graf bintang (*star graph*) dengan $n+1$ verteks
$\odot$	:	operasi korona (*corona product*)
$\gcd(a,b)$	:	pembagi persekutuan terbesar (*greatest common divisor*) dari a dan b
$a \equiv b \pmod{m}$	:	a kongruen dengan b modulo m
$a \mid b$	:	a membagi habis b
$a \nmid b$	:	a tidak membagi habis b
$\lceil x \rceil$	:	fungsi atap (*ceiling function*) dari x (bilangan bulat terkecil yang lebih besar atau sama dengan x)
■	:	tanda akhir pembuktian

INTISARI

SKEMA ENKRIPSI BERBASIS GRAF *SUN*, BIPARTIT, DAN BINTANG DENGAN SUBSTITUSI DAN PERMUTASI

Oleh

Ardha Carlinda Putri

22106010050

Perkembangan kemampuan komputasi modern dan munculnya berbagai ancaman baru, mendorong adanya eksplorasi terhadap pendekatan baru dalam perancangan algoritma kriptografi. Salah satu inovasi yang berkembang adalah penggunaan teori graf sebagai dasar pembentukan algoritma. Namun, salah satu skema enkripsi berbasis graf yang menjadi fokus penelitian ini masih memiliki beberapa keterbatasan, terutama pada aspek ruang kunci, mekanisme difusi, dan konsistensi algoritma. Berdasarkan hal tersebut, rumusan masalah dalam penelitian ini adalah bagaimana mengembangkan algoritma enkripsi dan dekripsi yang konsisten pada graf *sun*, graf bipartit, dan graf bintang dengan meningkatkan aspek keamanan dan ruang kuncinya.

Penelitian ini bertujuan untuk mengkaji dan mengembangkan skema enkripsi kriptografi simetris berbasis tiga jenis graf tersebut. Metode yang digunakan adalah studi literatur dengan melakukan modifikasi pada struktur algoritma. Pengembangan dilakukan dengan menggunakan *Vigenere cipher* sebagai metode substitusi untuk memperluas ruang kunci dan *permutation cipher* sebagai mekanisme difusi untuk memperkuat kerahasiaan pesan.

Hasil penelitian menunjukkan bahwa skema enkripsi yang dikembangkan memiliki ruang kunci yang lebih luas dan bersifat polialfabetik sehingga lebih tahan terhadap analisis frekuensi. Selain itu, penyesuaian aturan enkripsi menghasilkan alur algoritma yang jelas, konsisten, dan tetap memenuhi sifat keterbalikan (*invertibility*). Pengembangan ini dapat menjadi alternatif pendekatan dalam perancangan skema kriptografi simetris berbasis graf serta menjadi dasar bagi penelitian lanjutan dalam pengembangan algoritma kriptografi berbasis struktur graf lainnya.

Kata kunci : graf bipartit, graf bintang, graf *sun*, kriptografi simetris.

ABSTRACT

AN ENCRYPTION SCHEME BASED ON SUN, BIPARTITE, AND STAR GRAPHS WITH SUBSTITUTION AND PERMUTATION

By

Ardha Carlinda Putri

22106010050

The development of modern computing capabilities and the emergence of various new threats have encouraged exploration of new approaches in cryptographic algorithm design. One of the innovations that has developed is the use of graph theory as the basis for algorithm formation. However, one of the graph-based encryption schemes that is the focus of this research still has several limitations, particularly in terms of key space, diffusion mechanisms, and algorithm consistency. Based on this, the problem formulation in this study is how to develop consistent encryption and decryption algorithms on sun graphs, bipartite graphs, and star graphs by improving their security and key space aspects.

This study aims to examine and develop a symmetric cryptographic encryption scheme based on these three types of graphs. The method used is a literature study with modifications to the algorithm structure. The development was carried out using the Vigenere cipher as a substitution method to expand the key space and a permutation cipher as a diffusion mechanism to strengthen message confidentiality.

The results of the study show that the developed encryption scheme has a wider key space and is polyalphabetic, making it more resistant to frequency analysis. In addition, adjustments to the encryption rules result in a clearer, more consistent algorithm flow that still satisfies the invertibility property. This development can be an alternative approach in the design of graph-based symmetric cryptography schemes and serve as a basis for further research in the development of other graph-based cryptography algorithms.

Keyword : bipartite graph, star graph, sun graph, symmetric cryptography.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, digitalisasi telah menjadi bagian dari hampir seluruh aspek kehidupan manusia. Pemanfaatan internet sebagai media komunikasi memungkinkan pertukaran data dilakukan dengan cepat, mudah, dan tanpa batas geografis. Namun, jalur komunikasi digital yang bersifat terbuka tersebut rentan terhadap berbagai ancaman keamanan, seperti penyadapan, pencurian data, peretasan, maupun manipulasi informasi oleh pihak yang tidak berwenang. Kondisi ini menunjukkan bahwa proses komunikasi digital memerlukan mekanisme yang mampu menjamin kerahasiaan dan keamanan data selama proses pengiriman berlangsung.

Salah satu solusi pengamanan data dalam bidang matematika adalah kriptografi. Secara etimologis, istilah *kriptografi* berasal dari bahasa Yunani, yaitu *cryptos* yang berarti "rahasia" dan *graphein* yang berarti "tulisan". Secara terminologis, kriptografi didefinisikan sebagai ilmu yang mempelajari teknik-teknik matematis untuk menjaga aspek keamanan informasi, meliputi kerahasiaan (*confidentiality*), integritas data (*integrity*), autentikasi entitas (*entity authentication*), dan autentikasi pesan (*data authentication*) (Menezes et al., 1996).

Dalam praktiknya, algoritma kriptografi modern umumnya melibatkan tiga fungsi utama, yaitu proses enkripsi, dekripsi, dan kunci (*key*). Enkripsi merupakan proses mengubah pesan asli yang dapat dimengerti, disebut dengan plainteks,

menjadi kode yang sulit dimengerti oleh pihak yang tidak memiliki kunci, disebut cipherteks. Sementara itu, proses mengembalikan cipherteks menjadi plainteks disebut dekripsi (Stinson & Paterson, 2019). Adapun syarat untuk menjalankan kedua proses tersebut, yaitu dibutuhkan suatu kunci rahasia yang hanya diketahui oleh pihak yang melakukan komunikasi.

Secara umum, klasifikasi kriptografi berdasarkan kunci dibedakan menjadi dua jenis, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris atau disebut juga kriptografi kunci publik. Pada kriptografi kunci simetris, proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci yang sama, sedangkan kriptografi kunci asimetris menggunakan pasangan kunci berbeda, yaitu kunci publik dan kunci privat. Kedua jenis ini memiliki kelebihan dan kekurangan masing-masing. Pada kriptografi kunci simetris, kecepatan pemrosesan data berjalan lebih cepat, termasuk pesan berukuran besar. Namun, terdapat pula kelemahannya, yaitu menimbulkan masalah bagaimana untuk mendistribusikan kunci rahasia antar pengguna (*key distribution problem*). Sementara itu, kriptografi kunci asimetris mempunyai tingkat keamanan kunci lebih tinggi, tetapi kecepatan proses enkripsi maupun dekripsi cenderung lebih lambat dibandingkan dengan kriptografi kunci simetris (Arizal et al., 2022). Oleh karena itu, pada penelitian ini digunakan kriptografi kunci simetris dengan mempertimbangkan efisiensi proses enkripsi.

Perkembangan kemampuan komputasi modern dan munculnya ancaman baru, termasuk potensi serangan dari komputer kuantum, mendorong adanya eksplorasi terhadap pendekatan baru dalam perancangan algoritma kriptografi. Salah satu pendekatan yang berkembang dalam beberapa tahun terakhir adalah pemanfaatan teori graf sebagai dasar pembentukan algoritma enkripsi. Pendekatan ini memanfaatkan kompleksitas struktur graf dan ruang kunci yang luas sehingga

diharapkan dapat meningkatkan kekuatan sistem kriptografi.

Salah satu pendekatan awal yang memperkenalkan penggunaan teori graf dalam kriptografi adalah penelitian oleh Ustimenko (2007). Dalam penelitiannya, Ustimenko mengusulkan bahwa struktur graf khususnya graf dengan sifat aljabar tertentu, seperti graf bireguler dan graf dengan *girth* besar dapat dimanfaatkan untuk membangun skema enkripsi yang aman. Meskipun penelitian tersebut belum memberikan rancangan algoritma enkripsi dan dekripsi yang dapat langsung diimplementasikan, konsep-konsep yang diberikan membuka perspektif baru bahwa teori graf memiliki potensi dalam pengembangan sistem kriptografi yang aman.

Seiring dengan berkembangnya penelitian dalam bidang ini, berbagai pendekatan kriptografi yang memanfaatkan teori graf mulai dikembangkan oleh beberapa peneliti. Salah satu penelitian tersebut adalah karya Selvakumar & Gupta (2012) yang mengusulkan inovasi skema enkripsi dan dekripsi menggunakan graf terhubung (*connected graph*) dan konsep subgraf pohon (*spanning tree*). Penelitian selanjutnya dilakukan oleh Etaiwi (2014) yang menerapkan konsep graf siklus *(cycle graph)*, graf komplit, dan *minimum spanning tree* dalam perancangan algoritma enkripsi. Penelitian lain yang relevan dilakukan oleh Chandrasekaran (2017) yang mengusulkan skema enkripsi berbasis graf bipartit lengkap. Pada algoritma enkripsi tersebut, alfabet direpresentasikan melalui tabel numerik yang berfungsi sebagai dasar proses enkripsi. Penelitian lebih lanjut oleh Ni et al. (2021) yang mengembangkan tiga algoritma enkripsi dan dekripsi berbasis struktur graf, yaitu graf *sun*, graf bipartit, dan graf bintang.

Penelitian ini mengkaji dan mengembangkan skema enkripsi berbasis graf yang diusulkan oleh Ni et al. (2021). Dalam penelitiannya, Ni et al. membangun algoritma enkripsi dan dekripsi menggunakan tiga jenis graf, yaitu graf *sun*, graf

bipartit, dan graf bintang. Meskipun memberikan pendekatan yang inovatif dalam menghubungkan kriptografi dengan teori graf, skema tersebut masih memiliki beberapa keterbatasan, seperti ruang kunci yang relatif kecil, tidak adanya mekanisme difusi tambahan, serta beberapa inkonsistensi penulisan dalam algoritma enkripsi.

Penelitian ini memiliki aspek kebaruan yang berfokus pada pengembangan skema enkripsi dan dekripsi sistem kriptografi simetris berbasis graf. Pertama, algoritma dasar yang digunakan adalah *Vigenere cipher* yang memiliki ruang kunci lebih besar dan proses enkripsi dan dekripsi bersifat polialfabetik. Kedua, pada penelitian ini ditambahkan tahap difusi melalui permutasi sehingga mengurangi korelasi langsung antara posisi plainteks dan cipherteks. Ketiga, diberikan batasan dan beberapa penyesuaian pada algoritma enkripsi sehingga skema enkripsi berbasis graf yang dihasilkan diharapkan memiliki konsistensi algoritma yang lebih baik.

1.2. Batasan Masalah

Pembatasan masalah dalam penelitian diperlukan untuk memfokuskan pembahasan sehingga lebih terarah. Penelitian ini dibatasi hanya membahas skema enkripsi yang diperkenalkan pada penelitian sebelumnya serta pengembangan algoritma enkripsi dan dekripsi menggunakan tiga jenis graf, yaitu graf *sun*, graf bipartit, dan graf bintang. Pengembangan dibatasi pada penggunaan *Vigenere cipher*, tahap difusi berupa permutasi, serta penyesuaian aturan konversi numerik pada masing-masing graf.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diuraikan di atas, kemudian dirumuskan masalah sebagai berikut:

1. Bagaimana algoritma enkripsi dan dekripsi pada pengamanan pesan menggunakan graf *sun* serta pengembangannya?
2. Bagaimana algoritma enkripsi dan dekripsi pada pengamanan pesan menggunakan graf bipartit serta pengembangannya?
3. Bagaimana algoritma enkripsi dan dekripsi pada pengamanan pesan menggunakan graf bintang serta pengembangannya?

1.4. Tujuan Penelitian

Tujuan penulis dalam penyusunan penelitian ini adalah sebagai berikut:

1. Mengkaji dan mengembangkan algoritma enkripsi dan dekripsi menggunakan graf *sun*.
2. Mengkaji dan mengembangkan algoritma enkripsi dan dekripsi menggunakan graf bipartit.
3. Mengkaji dan mengembangkan algoritma enkripsi dan dekripsi menggunakan graf bintang.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dalam penyusunan penelitian ini adalah sebagai berikut:

1. Memberikan pengetahuan mengenai proses enkripsi dan dekripsi yang menggunakan tiga jenis graf, yaitu graf *sun*, graf bipartit, dan graf bintang.
2. Memberikan referensi tentang pengembangan skema enkripsi menggunakan *Vigenere cipher* dan permutasi sebagai mekanisme penyandian.

1.6. Tinjauan Pustaka

Referensi utama dalam penyusunan tugas akhir ini adalah penelitian oleh Ni et al. (2021) berjudul *Some Graph-Based Encryption Schemes*. Penelitian tersebut mengusulkan tiga algoritma enkripsi dan dekripsi yang dibangun menggunakan tiga jenis graf, yaitu graf *sun*, graf bipartit, dan graf bintang dengan metode enkripsi menggunakan sandi geser *(shift cipher)*. Persamaan penelitian oleh Ni et al. (2021) dengan penelitian yang dilakukan penulis terletak pada pemanfaatan tiga jenis graf tersebut sebagai media transformasi data dalam proses enkripsi dan dekripsi. Adapun perbedannya terletak pada fokus pengembangan, penelitian ini memperluas ruang kunci menggunakan *Vigenere cipher* sebagai algoritma dasar, menambahkan tahap difusi menggunakan sandi permutasi *(permutation cipher)*, serta melakukan penyesuaian terhadap beberapa inkonsistensi penulisan dalam algoritma enkripsi serta aturan konversi numerik agar struktur graf yang dihasilkan lebih konsisten.

Penelitian lain dilakukan oleh Buzarbarua et al. (2024) dengan judul *An Encryption Algorithm Employing Graphs*. Penelitian tersebut mengembangkan skema enkripsi menggunakan graf bintang sebagai representasi pesan, dengan memetakan karakter pesan ke himpunan bilangan prima dan membangun konektivitas graf berdasarkan pasangan nilai yang diperoleh dari proses enkripsi. Persamaan dengan penelitian yang dilakukan oleh penulis terletak pada pemanfaatan struktur graf, khususnya graf bintang untuk merepresentasikan cipherteks. Adapun perbedaannya, penelitian Buzarbarua et al. (2024) hanya berfokus pada satu jenis graf dan menggunakan skema enkripsi numerik sederhana, sedangkan penelitian ini mengembangkan tiga skema graf sekaligus, yaitu graf *sun*, graf bipartit, dan graf bintang, serta ditambahkan *Vigenere cipher* dan sandi permutasi *(permutation cipher)* untuk memperkuat proses enkripsi.

Perbedaaan dan persamaan penelitian yang dilakukan penulis dengan penelitian sebelumnya dapat dilihat pada tabel berikut.

Tabel 1.1 Tinjauan Pustaka

No	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
1	Ni et al. (2021)	*Some Graph-Based Encryption Schemes*	Menggunakan tiga jenis graf, yaitu graf *sun*, graf bipartit, dan graf bintang sebagai dasar pembentukan cipherteks.	Menggunakan shift cipher dengan ruang kunci terbatas dan tanpa permutasi. Sementara itu, penelitian ini mengembangkan ruang kunci dengan menggunakan *Vigenere cipher*, menambah tahap permutasi, dan memperbaiki inkonsistensi proses enkripsi sehingga lebih stabil.

No	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
2	Buzarbaruah et al. (2024)	*An Encryption Algorithm Employing Graphs*	Memanfaatkan graf untuk representasi cipherteks, khususnya graf bintang.	Penelitian tersebut hanya menggunakan graf bintang dan pemetaan ke bilangan prima, sedangkan penelitian ini menggunakan tiga graf dan menambahkan penggunaann *Vigenere cipher* serta permutasi.

Penulisan tugas akhir ini juga memerlukan beberapa literatur pendukung sebagai landasan teori. Konsep dasar kriptografi, sistem kriptografi, dan mekanisme penyandian merujuk pada *Handbook of Applied Cryptography* oleh Menezes, van Oorschot, dan Vanstone (Menezes et al., 1996) serta buku Stinson & Paterson (2019). Selanjutnya, materi mengenai teori bilangan dan struktur aljabar diperoleh dari buku Rosen (2011). Sementara itu, pemahaman mengenai teori graf, termasuk jenis-jenis graf yang digunakan dalam penelitian ini mengacu pada buku karya Munandar (2022).

1.7. Metode Penelitian

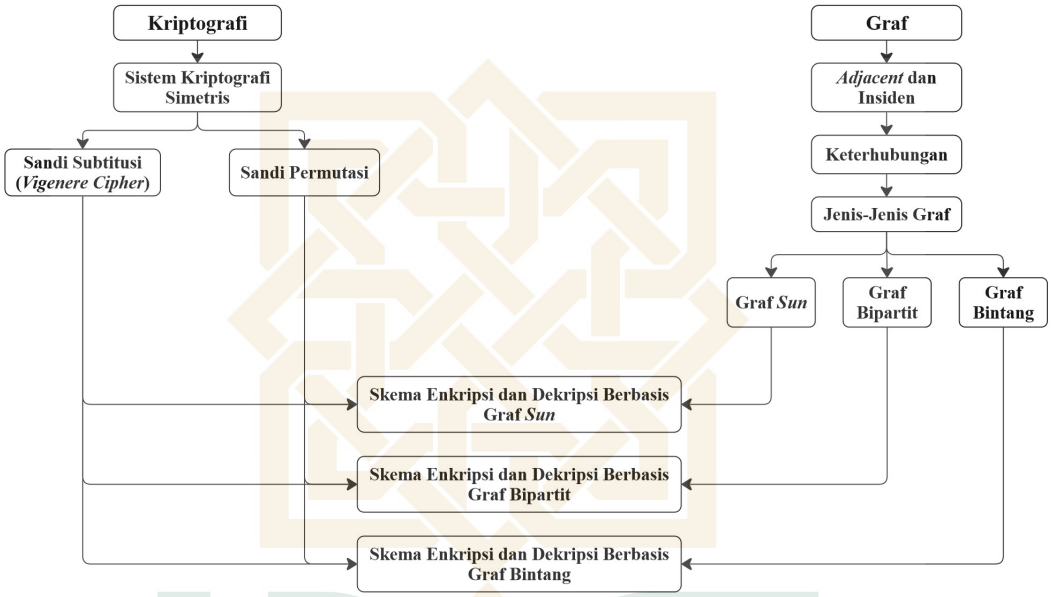
Penelitian ini menggunakan metode studi literatur *(library research)*. Metode ini dilakukan dengan mengumpulkan, mengkaji, dan menganalisis berbagai referensi terkait kriptografi klasik, teori bilangan, teori graf, serta penelitian-penelitian sebelumnya yang membahas tentang skema enkripsi berbasis graf. Adapun sumber literatur yang digunakan oleh penulis mencakup buku, artikel jurnal, dan publikasi ilmiah lain yang relevan dengan topik yang diangkat.

Pembahasan dimulai dari kajian mengenai kriptografi simetris sebagai dasar skema enkripsi yang digunakan dalam penelitian ini. Materi kriptografi diawali dengan membahas sistem kriptografi klasik yang kemudian difokuskan pada dua jenis *cipher*, yaitu *Vigenere cipher* sebagai metode subtitusi dan *permutation cipher* sebagai metode difusi. Kedua teknik ini menjadi komponen utama dalam pengembangan skema enkripsi yang diajukan. Selanjutnya, pembahasan teori graf dimulai dari konsep dasar himpunan verteks dan *edge*, *adjacent* dan insiden, serta keterhubungan. Materi kemudian diarahkan pada tiga jenis graf yang menjadi fokus penelitian, yaitu graf *sun*, graf bipartit, dan graf bintang. Ketiga graf ini digunakan sebagai struktur pembentuk cipherteks sesuai dengan rancangan skema enkripsi yang dikembangkan.

Berdasarkan pembahasan mengenai konsep kriptografi dan teori graf yang telah diuraikan sebelumnya. Penelitian dilanjutkan dengan merancang algoritma enkripsi dan dekripsi berdasarkan tiga jenis graf yang digunakan. Tahapan ini meliputi, pertama penyusunan ulang proses enkripsi agar konsisten untuk setiap graf. Kedua, penerapan *Vigenere cipher* sebagai dasar subtitusi. Ketiga, penambahan tahap difusi. Keempat, konstruksi graf *sun*, graf bipartit, dan graf bintang untuk membentuk cipherteks. Keseluruhan proses ini menghasilkan skema enkripsi dan

dekripsi yang telah dikembangkan dari penelitian sebelumnya.

Langkah-langkah penelitian yang telah dijelaskan dapat divisualisasikan pada bagan alur penelitian sebagai berikut.



Gambar 1.1 Alur Penelitian

1.8. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penulisan tugas akhir ini terbagi menjadi empat bab, yaitu sebagai berikut:

BAB 1 : Bab ini membahas tentang latar belakang masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, serta sistematika penulisan.

BAB 2 : Bab ini berisi landasan teori yang mencakup materi-materi pendukung penelitian, meliputi teori bilangan, konsep dasar teori graf, serta konsep dasar kriptografi klasik.

BAB 3 : Bab ini menyajikan pembahasan utama penelitian, yaitu penyusunan ulang algoritma enkripsi dan dekripsi berbasis graf, pengembangan mekanisme enkripsi, implementasi algoritma pada masing-masing jenis graf, serta analisis hasil yang diperoleh.

BAB 4 : Bab ini memuat penutup yang berisi kesimpulan dari penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya.

BAB IV

PENUTUP

Bab penutup ini akan diberikan kesimpulan dan saran-saran yang dapat diambil berdasarkan materi-materi yang telah dibahas pada bab-bab sebelumnya.

4.1. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut.

1. Algoritma enkripsi yang dikembangkan pada graf *sun* (Su_n) diawali dengan tahap substitusi menggunakan *Vigenere Cipher* untuk menghasilkan enkripsi awal. Selanjutnya, dilakukan tahap permutasi pertama pada hasil substitusi tersebut berdasarkan urutan nilai kunci yang dipilih. Setelah dilakukan perhitungan invers modulo untuk memperoleh label verteks, Alice mengonstruksi graf *sun* (Su_n) menggunakan operasi korona $C_n \odot K_1$. Sebagai tahap akhir keamanan, dilakukan permutasi kembali terhadap label-label tersebut sehingga diperoleh graf *sun* hasil permutasi sebagai *cipherteks*. Pada algoritma ini, permutasi dilakukan sebanyak dua kali. Permutasi pertama bertujuan untuk mengacak urutan pesan setelah proses substitusi, sedangkan permutasi kedua bertujuan untuk menghilangkan korelasi langsung antara label pada verteks siklus C_n dengan *pendant vertex*.

2. Algoritma enkripsi pada graf bipartit diawali dengan tahap substitusi menggunakan *Vigenere Cipher* dan permutasi kunci sebagaimana pada graf

sun. Perbedaan utama terletak pada proses pelabelan yang memanfaatkan tabel bilangan prima untuk memetakan karakter pesan menjadi hasil kali dua bilangan prima unik. Selanjutnya, konstruksi graf bipartit dilakukan dengan memecah nilai numerik tersebut menjadi dua bagian untuk membentuk partisi verteks V_1 dan V_2. Tahap akhir dilakukan dengan memberikan bobot acak yang terurut pada setiap *edge*) sehingga dihasilkan graf bipartit berbobot sebagai cipherteks. Pada algoritma ini, diterapkan batasan berupa pengecualian bilangan prima 11 pada proses pembentukan tabel pemetaan bilangan prima untuk memastikan graf bipartit yang dihasilkan tetap memenuhi sifat bipartit.

3. Algoritma enkripsi pada graf bintang (B_n) diawali dengan tahap substitusi menggunakan *Vigenere Cipher* dan permutasi kunci sebagaimana pada graf *sun* dan graf bipartit. Selanjutnya, Alice mengonstruksi graf bintang menggunakan operasi korona $K_1 \odot \overline{K_n}$ yang terdiri dari satu verteks pusat dan n verteks daun. Proses kemudian dilanjutkan dengan pembobotan *edge* yang merupakan perbedaan utama algoritma ini dibandingkan dua algoritma sebelumnya karena informasi pesan disimpan pada *edge*. Pada tahap akhir, Alice menyembunyikan seluruh label verteks sehingga dihasilkan graf bintang dengan hanya bobot pada *edge* yang terlihat sebagai *cipherteks*. Pada algoritma ini, dilakukan penyesuaian pada aturan pembobotan *edge* sehingga setiap langkah dekripsi bersesuaian langsung dengan langkah enkripsi dan proses mengembalikan cipherteks menjadi plainteks dapat dilakukan secara tepat.

4.2. Saran

Berdasarkan hasil penelitian yang dilakukan, beberapa saran untuk pengembangan lebih lanjut dapat disampaikan sebagai berikut.

1. Skema enkripsi berbasis graf pada skripsi ini masih menggunakan struktur aljabar sederhana, yaitu $\mathbb{Z}_{26}$. Penelitian selanjutnya dapat mengkaji pengembangan skema dengan menggunakan struktur aljabar yang lebih umum, seperti ring polinomial, guna memperluas ruang pesan dan kunci serta meningkatkan kompleksitas skema kriptografi.
2. Penelitian selanjutnya dapat mengembangkan variasi struktur graf atau mengombinasikan skema yang diusulkan dengan metode kriptografi lain.

DAFTAR PUSTAKA

Arizal, A., Sidabutar, J., & Yulianti, N. (2022). *Kriptografi: Teknik Keamanan Data*. ISBN: 9786233424554.

Buzarbarua, B., Phukan, P., Das, M., & Barman, B. (2024). An encryption algorithm employing graphs. *Journal of Mechabics of Continua and Mathematical Sciences*, 19:11–17.

Chandrasekaran, V. M. Praba, B. M. A. K. G. (2017). Data transfer using complete bipartite graph. *IOP Conference Series: Materials Science and Engineering*, 263.

D.S. Malik, John N. Mordeson, M. S. (1997). *Fundamentals of Abstract Algebra*. McGraw-Hill Companies, ISBN: 0070400350.

Etaiwi, W. M. A. (2014). Encryption algorithm using graph theory. *Journal of Scientific Research & Reports*, 3:2519–2527.

Frucht, R. & Harary, F. (1970). On the corona of two graphs. *Aequationes Mathematicae*, 4:322–325, DOI: 10.1007/BF01844162.

Khoiriah, S. & Kusmayadi, T. A. (2018). Dimensi metrik lokal pada graf antiprisma dan graf sun. *Journal of Mathematics and Mathematics Education*, 8:9–15.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Munandar, A. (2022). *Pengantar Matematika Diskrit dan Teori Graf*. Sleman : Deepublish (CV Budi Utama).

Ni, B., Qazi, R., Rehman, S. U., & Farid, G. (2021). Some graph-based encryption schemes. *Journal of Mathematics*, 1:6614172.

Rosen, K. H. (2011). *Elementary Number Theory and Its Applications*. Pearson Education, USA, 6th edition.

Selvakumar, R. & Gupta, N. (2012). Fundamental circuits and cut-sets used in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, 15:287–301.

Stinson, D. R. & Paterson, M. B. (2019). *Cryptography: Theory and Practice*. CRC Press, Boca Raton, 4th edition.

Ustimenko, V. A. (2007). On graph-based cryptography and symbolic computations. *Serdica Journal of Computing*, 1:131–156.