e-ISSN 2722-7774

# CGANT

## Journal of Mathematics and Applications

CGANT University of Jember

# EDITORIAL TEAM

## HONORARY EDITOR

Prof, Drs Dafik, M.Sc, Ph.D, University of Jember, Indonesia

## EDITOR IN CHIEF

Zainur Rasyid Ridlo, S.Pd, M.Pd, University of Jember, Indonesia

## MANAGING EDITORS

Dr. Ika Hesti Agustin, S.Si., M.Si., University of Jember, Indonesia
Dr. Arika Indah Kristiana, S.Si., M.Pd., University of Jember, Indonesia
Ridho Alfarisi, S.Pd., M.Si., University of Jember, Indonesia
Rafiantika Megahnia Prihandini, S.Pd., M.Si., University of Jember, Indonesia
Robiatul Adawiyah, S.Pd., M.Si., University of Jember, Indonesia

## GRAPHICAL EDITORS

Rosanita Nisviasari, S.Si., M.Si., University of Jember, Indonesia
Ika Nur Maylisa, S.Pd., M.Pd., University of Jember, Indonesia

## LAYOUTING EDITORS

Elsa Yuli Kurniawati, S.Pd., M,Si., University of Jember, Indonesia
Dwi Agustin Retno Wardani, S.Si., M.Si., University of Jember, Indonesia
Rifki Ilham Baihaqi, S.Si, M.Mat, University of Jember, Indonesia

# VOL 2, NO 1 (2021)

# CGANT JOURNAL OF MATHEMATICS AND APPLICATIONS

DOI: https://doi.org/10.25037/cgantjma.v2i1

Available Online Since June 2021

## TABLE OF CONTENTS

### ARTICLES

CGANT JMA
http://www.jcgantunej.or.id
Volume 2, No 1, 2021
DOI:
10.25037/cgantjma.v2i1.52

Journal of
MATHEMATICS AND APPLICATIONS

e-ISSN 2722-7774

# Analisa *Antimagic* Total *Covering* Super pada Eksponensial Graf Khusus dan Aplikasinya dalam Mengembangkan *Chipertext*

Hani'ah Zakin[1,2], Ika Hesti A.[1,2], Kusbudiono[1,2], Dafik[1,3]
[1]CGANT - Universitas Jember
[2]Jurusan Matematika FMIPA Universitas Jember
[3]Program Studi Pendidikan Matematika FKIP Universitas Jember
haniahzakin@gmail.com, hestyarin@gmail.com, Kusbudiono@unej.ac.id,
d.dafik@unej.ac.id

**Abstract**

Let $H_i$ be a finite collection of simple, nontrivial and undirected graphs and let each $H_i$ have a fixed vertex $v_j$ called a terminal. The amalgamation $H_i$ as $v_j$ as a terminal is formed by taking all the $H_i$'s and identifying their terminal. When $H_i$ are all isomorphic graphs, for any positif integer $n$, we denote such amalgamation by $G = \mathrm{Amal}(H, v, n)$, where $n$ denotes the number of copies of $H$. The graph $G$ is said to be an $(a, d)$-$H$-antimagic total graph if there exist a bijective function $f : V(G) \cup E(G) \to \{1, 2, \ldots, |V(G)| + |E(G)|\}$ such that for all subgraphs isomorphic to $H$, the total $H$-weights $w(H) = \sum_{v \in V(H)} f(v) + \sum_{e \in E(H)} f(e)$ form an arithmetic sequence $\{a, a + d, a + 2d, ..., a + (t - 1)d\}$, where $a$ and $d$ are positive integers and $t$ is the number of all subgraphs isomorphic to $H$. An $(a, d)$-$H$-antimagic total labeling $f$ is called super if the smallest labels appear in the vertices. In this paper, we study a super $(a, d)$-$H$ antimagic total labeling of $G = \mathrm{Amal}(H, v, n)$ and its disjoint union when $H$ is a complete graph.

**Keywords :** *Super $H$-antimagic total graph, Amalgamation of graph, Complete graph*
Mathematics Subject Classification: 05C78

## Pendahuluan

Aplikasi pada graf meliputi berbagai macam, yaitu dalam transparansi, komunikasi, pewarnaan peta, ikatan kimia, desain arsitektur. Untuk aplikasi graf yang lain adalah untuk kristografi, pengaturan jadwal, dan astronomi, dan sebagainya. Aplikasi graf mulai berkembang lagi pada pengembangan *chiphertext*. *Chiphertext* merupakan proses pengembangan dari *cryptosystem*. *Chiphertext* adalah kalimat rahasia yang dikembangkan. Sedangkan *cryptosystem* merupakan suatu fasilitas yang mengkonversikan *plaintext* ke dalam bentuk *chiphertext* dan sebaliknya. Di dalam *cryptosystem* menyangkut *cryptography* yang merupakan skema yang mungkin untuk *encryption* dan *decryption* [1]. *Encryption* adalah proses pengubahan *plaintext* (pesan yang akan dikirim) menjadi *chiphertext* (pesan rahasia) sedangkan *decryption* adalah proses untuk memperoleh kembali *plainttext* dari *chiphertext*. Dalam proses ini dibutuhkan sebuah kunci rahasia untuk mengatur beberapa atau semua yang digunakan dalam proses *encryption* maupun *decryption*. Secara umum kunci-kunci yang digunakan untuk proses pengenkripsian dan pendeskripsian tidak perlu identik dan tergantung pada sistem yang digunakan [2]. Berikut adalah alur kerja pada pengembangan *chiphertext* yang ditunjukkan pada gambar 1.

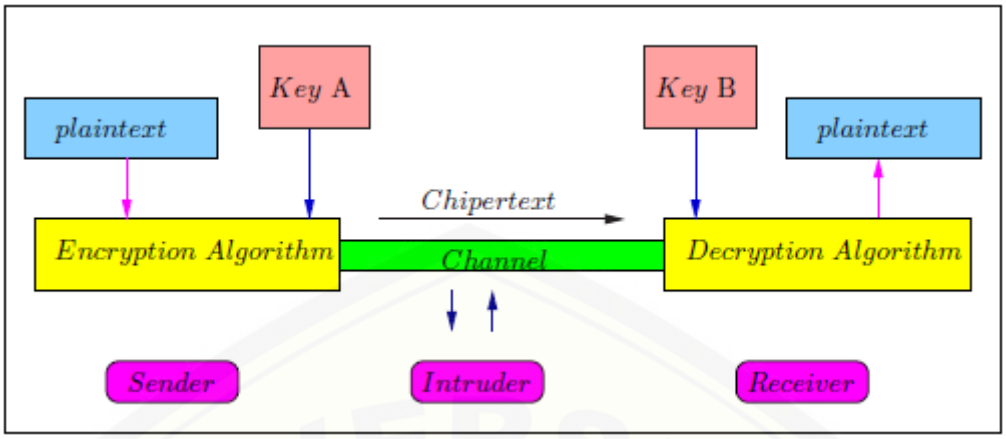


Figure 1: Alur Kerja Kriptografi

Terdapat banyak metode yang dapat digunakan untuk memperoleh *chiphertext* seperti *affine ciphers*, *vigenere ciphers*, *the one-time pad*, Caesar *system*, dan sebagainya. Metode yang digunakan pada penelitian ini merupakan aplikasi pelabelan total *covering*. Metode ini merujuk pada Caesar *system* yaitu menggunakan sistem (mod 26), atau disebut dengan aturan Julius Caesar. Berikut akan ditunjukkan aturan Julius Caesar pada tabel 1

Table 1: Aturan Julius Caesar.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

## Hasil Penelitian

Sebagai ilustrasi akan diberikan tiga contoh eksponensial dari graf lintasan dan amalgamasi graf *cycle* $P_{n+1}^{Amal(C_{m+2},e,s)}$ beserta keterangan label titk, label sisi dan bobot total selimutnya sebagai berikut.

1. Gambar 2 merupakan contoh dari Super (*1692,22*)-$\mathcal{H}$-*antimagic* Total *covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle* $P_4^{Amal(C_{11},e,3)}$. Dari gambar tersebut terlihat jelas label titik, label sisi dan bobot total selimut pada eksponensial dari graf lintasan dan amalgamasi graf $cycle$ dengan $n = 3$, $s = 3$, $m = 9$ dan $t = 10$ sehingga didapat nilai $a = 1692$ dan $d = 22$.

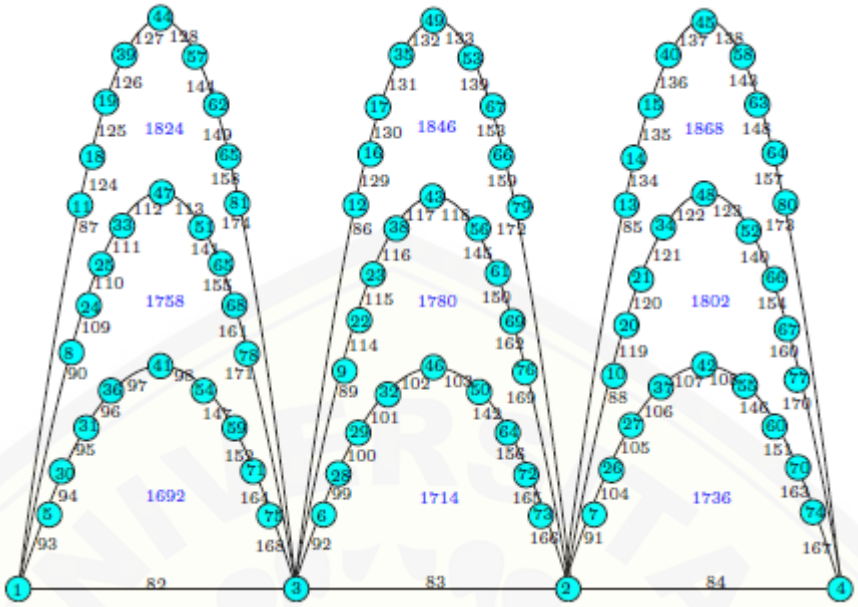


Figure 2: Graf $P_4^{Amal(C_{11},e,3)}$

2. Gambar 3 merupakan contoh dari Super (*1411,15*)-$\mathcal{H}$-*antimagic* Total *covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle* $P_4^{Amal(C_{10},e,3)}$. Dari gambar tersebut terlihat jelas label titik, label sisi dan bobot total selimut pada eksponensial dari graf lintasan dan amalgamasi graf $cycle$ dengan $n = 3$, $s = 3$, $m = 8$ dan $t = 9$ sehingga didapat nilai $a = 1411$ dan $d = 15$.

3. Gambar 4 merupakan contoh dari Super (*1142,9*)-$\mathcal{H}$-*antimagic* Total *covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle* $P_4^{Amal(C_9,e,3)}$. Dari gambar tersebut terlihat jelas label titik, label sisi dan bobot total selimut pada eksponensial dari graf lintasan dan amalgamasi graf $cycle$ dengan $n = 3$, $s = 3$, $m = 7$ dan $t = 8$ sehingga didapat nilai $a = 1142$ dan $d = 9$.

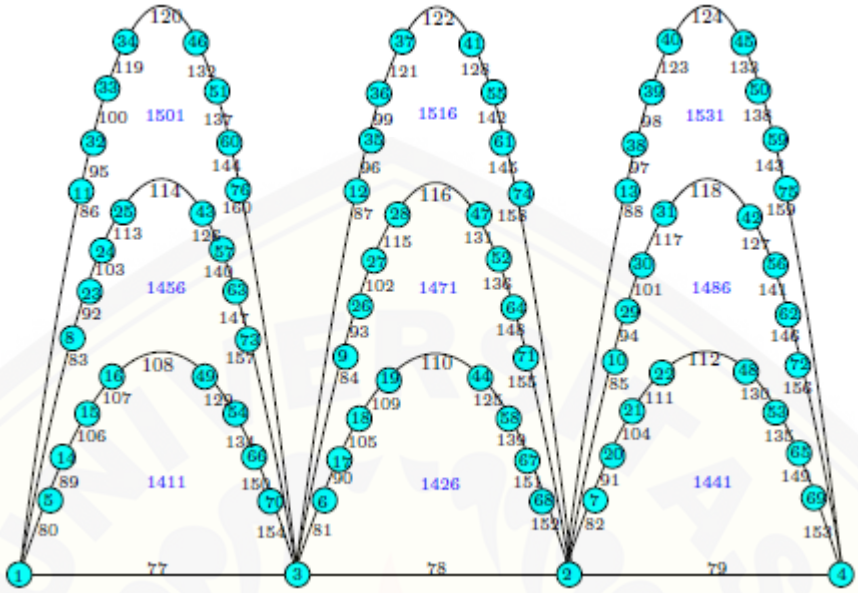

Figure 3: Graf $P_4^{Amal(C_{10},e,3)}$

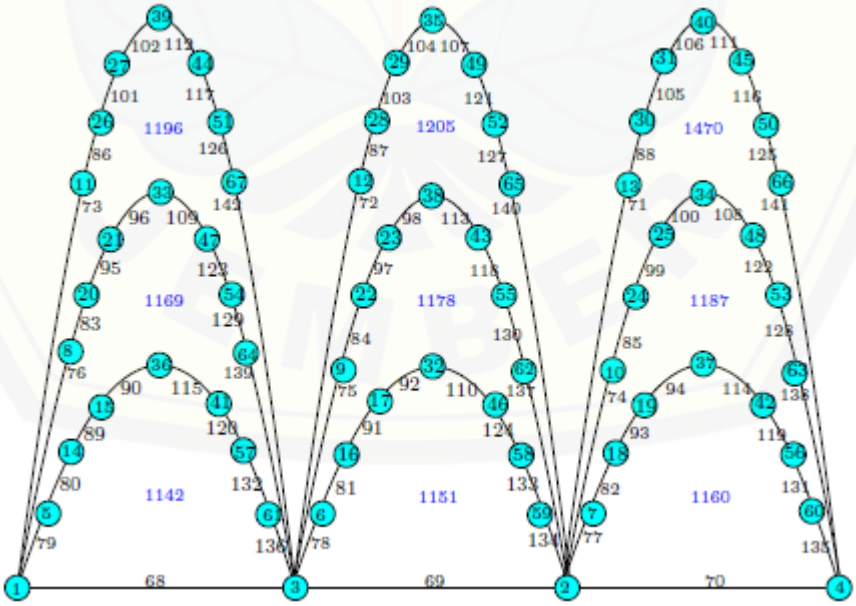

Figure 4: Graf $P_4^{Amal(C_9,e,3)}$

## Pengembangan *Chiphertext* Super $(a,d)$-$\mathcal{H}$-*Antimagic* Total *Covering* pada Eksponensial Dari Graf Lintasan dan dari Amalgamasi Graf *Cycle* $P_{n+1}^{Amal(C_{m+2},e,s)}$

Sebelumnya telah disajikan sebuah teorema Super (*a,d*)-$\mathcal{H}$-*antimagic* Total *covering* pada Eksponensial dari Graf Lintasan dan Amalgamasi Graf *Cycle* $P_{n+1}^{Amal(C_{m+2},e,s)}$ beserta ilustrasi grafnya. Ilustrasi yang telah disajikan tersebut akan digunakan untuk membentuk *Chiphertext*. Metode yang digunakan untuk membentuk *Chiphertext* adalah metode eliminasi yaitu metode yang menitik beratkan pada pengeliminasian sisi yang labelnya tidak memenuhi syarat. Metode eliminasi pada pembentukan *Chiphertext* disini berbeda dengan metode eliminasi yang biasa digunakan pada bahasan matematika. Adapun langkah-langkah metode eliminasi sebagai berikut:

1. Menentukan karakter yang akan dibuat *Chiphertext*.
   Misalkan $r$ adalah banyaknya karakter yang akan dibuat *Chiphertext*.

2. Menentukan dan memilih graf yang memenuhi syarat $|E(G)| \geq r$.
   Graf yang dipilih harus memenuhi $|E(G)| \geq r$ karena terdapat $r$ karakter dimana setiap karakter diwakili oleh sebuah sisi. Tidak boleh ada satupun karakter yang tidak dikorespondensikan terhadap sisi. Karakter yang dikorespondensi satu-satu dengan sisi secara eksplisit menyatakan bahwa karakter tersebut dikorespondensi satu-satu terhadap label sisi yang akan dibentuk *Chiphertext*.

3. Melabeli titik dan sisi sehingga membentuk super $(a,d)\mathcal{H}-$ *antimagic* total *covering* pada Eksponensial dari Amalgamasi Graf *Cycle* $P_{n+1}^{Amal(C_{m+2},e,s)}$.
   Graf yang sudah ditentukan berdasarkan label titik dan sisi berdasarkan ilustrasi gambar yang sudah ada. Label titik dan sisi ini mempunyai peran yang sangat penting dalam pembentukan *Chiphertext*.

4. Mengeliminasi sisi yang memiliki label $f_e > |V(G)| + r$.
   Karakter yang digunakan sebanyak $r$ sehingga *Chiphertext* yang dibutuhkan adalah sebanyak $r$. Kode awal yang didapat berupa angka sehingga perlu dibuat aturan untuk mentransformasikan angka ke *Chiphertext* sehingga menggunakan bilangan modulo (mod $r$). Salah satu aturan yang sudah ada adalah aturan Julius Caesar dimana setiap alfabet dikorespondensikan secara berurutan dengan bilangan (mod 26). Sisi yang memiliki label $f_e > |V(G)|+r$ dieliminasi. Pengeliminasian ini dilakukan agar tidak terjadi kesamaan atau pengulangan bilangan mod $r$ dengan demikian tidak terjadi kesamaan *Chiphertext*. Bila sisi sudah dieliminasi maka sisi tidak digunakan untuk diagram pohon.

5. Membuat diagram pohon sesuai dengan super $(a,d)\mathcal{H}-$ *antimagic* total *covering* pada Graf Eksponensial dari Graf Lintasan dan Amalgamasi Graf *Cycle* $P_{n+1}^{Amal(C_{m+2},e,s)}$.
   Pembangunan diagram pohon dengan utama label titik terkecil, pada penelitian ini label titik yang dipilih yaitu 1 (satu), sedangkan akar selanjutnya mengikuti pola graf. Sisi yang sudah dieliminasi tidak perlu digunakan.

6. Membentuk tabel *Chiphertext*. Tabel yang terdiri dari *plaintext*, label sisi yang bersesuaian dengan *plaintext*, (mod $r$) dari label sisi, dan *Chiphertext* yang bersesuaian dengan (mod $r$).

**Pembentukan *Chiphertext* Alfabet Super (*1142,9*)-$\mathcal{H}$-*Antimagic* Total *Covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle*** $P_4^{Amal(C_9,e,3)}$

Gambar 4 merupakan Graf $P_4^{Amal(C_9,e,3)}$ dengan $d = 9$ yang akan diterapkan untuk membentuk *Chiphertext* alfabet. Pada Gambar 4 ditunjukkan bahwa label titik dimulai dari 1 sampai 67 dan label sisi dimulai dari 68 sampai 142. Langkah awal pada metode eliminasi adalah menjumlahkan banyaknya titik dengan banyaknya abjad yang digunakan dan mengeliminasi label sisi yang lebih besar dari jumlah tersebut, sehingga label sisi yang lebih besar dari $67 + 26 = 93$ yaitu $94, 95 \cdots, 142$ harus dieliminasi agar tidak ada bilangan mod 26 yang berulang. Selanjutnya adalah membangun diagram pohon yang berakar 1 (satu) dan akar selanjutnya mengikuti pola graf serta dilengkapi dengan label sisi. Langkah selanjutnya adalah mencantumkan abjad dari A sampai Z. Penempatan abjad harus berurutan dari kiri ke kanan dan dimulai dari layer teratas. Sehingga diagram pohon terbentuk seperti Gambar 5. Tahapan terakhir adalah membuat tabel *Chiphertext* dari abjad seperti pada Tabel 2.

Sebuah pesan *(plaintext)* **"PASSWORD WIFI ANDA TELAH DIBAJAK. MOHON KALI INI DIJAGA DENGAN BENAR, PASSWORD WIFI ANDA ADALAH ZGFACLORP."** akan dirubah menjadi *Chiphertext*. Langkah awal yang dilakukan adalah menghapus tanda baca selain spasi karena pentingnya tanda spasi maka untuk pengkodean dari alfabet ke alfabet tanda spasi selalu dikodekan dengan "@" dan mengganti angka dengan huruf. Sehingga pesan menjadi **"PASSWORD WIFI ANDA TELAH DIBAJAK MOHON KALI INI DIJAGA DENGAN BENAR PASSWORD WIFI ANDA ADALAH ZGFACLORP"**. Dengan menggunakan Tabel 2 maka dilakukan proses *encryption* sehingga didapatkan *Chiphertext* **"DQLLNTJV@NCAC@QWVQ@LRSQU@VCBQFQI @ZTUT@VCFQXQ@VRWXQW@BRWQJ@NCAC@DQLLNTJV@QWVQ@QVQ SQU@OXAQYSTJD"**

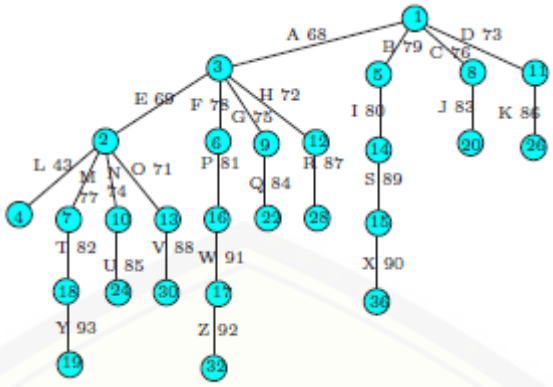


Figure 5: Diagram Pohon $P_4^{Amal(C_9,e,3)}$

**Pembentukan *Chiphertext* Simbol Super (*1692,22*)-$\mathcal{H}$-*Antimagic* Total *Covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle*** $P_4^{Amal(C_{11},e,3)}$

Gambar 2 merupakan Graf $P_4^{Amal(C_{11},e,3)}$ dengan $d = 22$ yang akan diterapkan untuk membentuk *Chiphertext* simbol. Pada Gambar 2 ditunjukkan bahwa label titik dimulai dari 1 sampai 81 dan label sisi dimulai dari 82 sampai 174. Karakter yang digunakan sebanyak 45 yang terdiri dari abjad dari A sampai Z, angka dari 0 sampai 9, tanda baca spasi (sp.), tanda baca titik (.), tanda baca koma (,), tanda tanya (?), tanda seru(!), tanda baca (@), tanda baca (#), tanda baca($), tanda baca (&). Langkah awal pada metode eliminasi adalah menjumlahkan banyaknya titik dengan banyaknya karakter yang digunakan dan mengeliminasi label sisi yang lebih besar dari jumlah tersebut, sehingga label sisi yang lebih besar dari $81 + 45 = 126$ yaitu $127, 128 \cdots, 174$ harus dieliminasi agar tidak ada bilangan mod 45 yang berulang. Selanjutnya adalah membangun diagram pohon yang berakar 1 (satu) dan akar selanjutnya mengikuti pola graf serta dilengkapi dengan label sisi. Langkah selanjutnya adalah mencantumkan karakter sesuai dengan urutan yang telah ditentukan. Penempatan karakter harus berurutan dari kiri ke kanan dan dimulai dari layer teratas. Sehingga diagram pohon terbentuk seperti Gambar 6. Tahapan terakhir adalah membuat tabel *Chiphertext* sesuai karakter seperti pada Tabel 4.

Sebuah pesan *(plaintext)* **"PASSWORD NIM ANDA MULAI SEKARANG SUDAH TIDAK BERLAKU, NIM ANDA ADALAH 121810101049 DENGAN PASSWORD Z4PB8HIJ@#."** akan diubah langsung menjadi *Chiphertext*. Dengan menggunakan Tabel 4 maka dilakukan proses *encryption* sehingga didapatkan *Chiphertext* "∀ ✠ ∠ ∠ ℘ □ ∇ ∗ ♡ ✠ ∓ ∗ ✠ ♡ ∞ ♋ ⋄ ✠ ι ♡ ∠ ¥ £ ✠ ∇ ✠ ∓ ⋆ ♡ ∠ ♋ ∗ ✠ ℧ ♡ ✓ ι ∗ ✠ £ ♡ ∂ ¥ ∇ ⋄ ✠ £ ♋ ♣ ♡ ∓ ι ∞ ♡ ✠ ∓ ∗ ✠ ♡ ✠ ∗ ✠ ⋄ ✠ ℧ ✓ ¶ ✓ ‡ ✓ ® ✓ ® ✓ ® ♯ ℜ ∗ ¥ ∓ ⋆ ✠ ∓ ∀ ✠ ∠ ∠ ℘ □ ∇ ∗ \ ♯ ∀ ‡ ℧ ι ⊥ ¬ ∥ ℓ".

Table 2: Pembentukan *Chiphertext* alfabet dari Gambar 4.

| *Plaintext* | Label Sisi | (Mod 26) | *Chiphertext* |
|---|---|---|---|
| A | 68 | 16 | Q |
| B | 79 | 1 | B |
| C | 76 | 24 | Y |
| D | 73 | 21 | V |
| E | 69 | 17 | R |
| F | 78 | 0 | A |
| G | 75 | 23 | X |
| H | 72 | 20 | U |
| I | 80 | 2 | C |
| J | 83 | 5 | F |
| K | 86 | 8 | I |
| L | 70 | 18 | S |
| M | 77 | 25 | Z |
| N | 74 | 22 | W |
| *Plaintext* | Label Sisi | (Mod 26) | *Chiphertext* |
| O | 71 | 19 | T |
| P | 81 | 3 | D |
| Q | 84 | 6 | G |
| R | 87 | 9 | J |
| S | 89 | 11 | L |
| T | 82 | 4 | E |
| U | 85 | 7 | H |
| V | 88 | 10 | K |
| W | 91 | 13 | N |
| X | 90 | 12 | M |
| Y | 93 | 15 | P |
| Z | 92 | 14 | O |
| sp | | | @ |

Table 3: Aturan pengkodean untuk bilangan mod 45.

| (mod 45) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Simbol | ℵ | ∞ | ℏ | ∂ | ı | ∇ | ȷ | △ | ℓ | ∀ | ℘ | ∃ | ℜ | ¬ | ℑ |
| (mod 45) | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| Simbol | √ | ′ | ⊤ | ∅ | ⊥ | ∠ | \ | ♭ | ♣ | ♮ | ♢ | ♯ | ♡ | ‖ | ♠ |
| (mod 45) | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 |
| Simbol | ¶ | ‡ | © | § | £ | ✓ | ® | ✠ | ¥ | ⋄ | □ | ℧ | ∗ | ∓ | ⋆ |

Table 4: Pembentukan *Chiphertext* alfabet dari Gambar 2.

| *Plain-text* | Label Sisi | (Mod 45) | *Chipher-text* | *Plain-text* | Label Sisi | (Mod 45) | *Chipher-text* |
|---|---|---|---|---|---|---|---|
| A | 82 | 37 | ✠ | N | 88 | 43 | ∓ |
| B | 93 | 3 | ∂ | O | 85 | 40 | □ |
| C | 90 | 0 | ℵ | P | 99 | 9 | ∀ |
| D | 87 | 42 | ∗ | Q | 114 | 24 | ♮ |
| E | 83 | 38 | ¥ | R | 95 | 5 | ∇ |
| F | 92 | 2 | ℏ | S | 110 | 20 | ∠ |
| G | 89 | 44 | ⋆ | T | 125 | 35 | ✓ |
| H | 86 | 41 | ℧ | U | 104 | 14 | ☪ |
| I | 94 | 4 | ı | V | 119 | 29 | ♠ |
| J | 109 | 19 | ⊥ | W | 100 | 10 | ℘ |
| K | 124 | 34 | £ | X | 115 | 25 | ♢ |
| L | 84 | 39 | ⋄ | Y | 96 | 6 | ȷ |
| M | 91 | 1 | ∞ | Z | 111 | 21 | \ |
| *Plain-text* | Label Sisi | (Mod 45) | *Chipher-text* | *Plain-text* | Label Sisi | (Mod 45) | *Chipher-text* |
| 0 | 126 | 36 | ® | sp. | 117 | 27 | ♡ |
| 1 | 105 | 15 | √ | . | 98 | 8 | ℓ |
| 2 | 120 | 30 | ¶ | , | 113 | 23 | ♣ |
| 3 | 101 | 11 | ∃ | ? | 107 | 17 | ⊤ |
| 4 | 116 | 26 | ♯ | ! | 122 | 32 | © |
| 5 | 97 | 7 | △ | @ | 103 | 13 | ¬ |
| 6 | 112 | 22 | ♭ | # | 118 | 28 | ‖ |
| 7 | 106 | 16 | ′ | $ | 108 | 18 | ∅ |
| 8 | 121 | 31 | ‡ | & | 123 | 33 | § |
| 9 | 102 | 12 | ℜ | | | | |

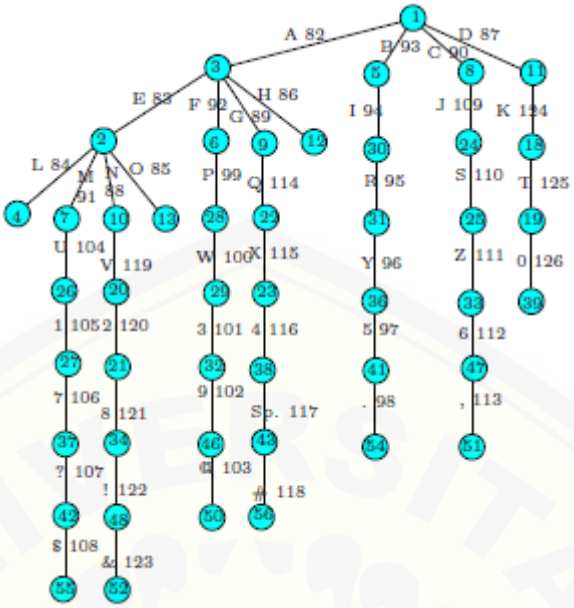


Figure 6: Diagram Pohon $P_4^{Amal(C_11,e,3)}$

**Pembentukan *Stream Chipher* Super (*11411,15*)-$\mathcal{H}$-*Antimagic* Total *Covering* pada Eksponensial dari Graf Lintasan dan Graf Lintasan dan Amalgamasi Graf *Cycle*** $P_4^{Amal(C_{10},e,3)}$

Gambar 3 merupakan Graf $P_4^{Amal(C_{10},e,3)}$ dengan $d = 15$ yang akan diterapkan untuk membentuk *Stream Chipher*. *Stream Chipher* disebut juga dengan sandi aliran. *Stream Chipher* ini yang didasarkan pada fungsi *chaos*. Fungsi *chaos* dalam matematika merupakan suatu fungsi yang mempunyai sifat bahwa nilai fungsinya sensitif terhadap nilai awal, artinya perubahan kecil pada nilai awal akan mengakibatkan perubahan besar pada nilai fungsinya. Penerapan fungsi *chaos* dalam *stream chipher* tentu menguntungkan, karena sifat sensitif pada nilai awal tersebut, sehingga diharapkan dapat meningkatkan keamanan dari *stream chipher*. Keuntungan dari *stream chipher* adalah tidak dibatasi oleh panjang *plaintext*. Sama seperti metode eliminasi, *stream chipher* juga menggunakan aturan Julius Caesar. Sehingga *plaintext* $y_1, y_2, y_3, \ldots$ dengan $y_i \in Z_{26}$ dan kunci aliran $k_1, k_2, k_3, \ldots$ dengan $k_i \in Z_{26}$. *Chiphertext* $z_1, z_2, z_3, \ldots$ diperoleh dengan proses enkripsi sebagai berikut: $z_i = y_i + k_i (\mathrm{mod}\ 26)$. Kemudian untuk memperoleh *plaintext* $y_1, y_2, y_3, \ldots$ kembali, digunakanlah fungsi invers dari $z_i = y_i + k_i (\mathrm{mod}\ 26)$.

Sebuah pesan *plaintext*: "**bismillahirahmanirrahim dengan ini saya nyatakan mahasiswa atas nama haniah zakin lulus tepat waktu dengan bidang skripsi teori graf**", akan diubah menjadi *Chiphertext* dengan mengabaikan spasi dan tanda baca lainnya, menjadi "**bismillahirahmanirrahimdenganinisayanyatakanmahasis waatasnamahaniahzakinlulustepatwaktu denganbidangskripsiteorigraf**". Dengan menggunakan Tabel 5 maka dilakukan proses *encryption* sehingga didapatkan *chiphertext* sebagai berikut: "**clxa xbicvaucndsgaxgqjmtxzjcbazolaxwzedlodmjnnccaebuakdxfirkgbkltpibb iilpxdvfhwnlcxjmxhnblkfcwbjfxpyokusovmmlhljkcyk**"

Table 5: Proses enkripsi *stream chipher* dari *plaintext* menjadi *chiphertext*.

| *Plaintext* | $y_i$ | $k_i$ | $z_i = y_i + k_i(Mod26)$ | *Chiphertext* |
|---|---|---|---|---|
| b | 1 | 1 | 2 | c |
| i | 8 | 3 | 11 | l |
| s | 18 | 5 | 23 | x |
| m | 12 | 14 | 0 | a |
| i | 8 | 15 | 23 | x |
| l | 11 | 16 | 1 | b |
| l | 11 | 49 | 8 | i |
| a | 0 | 54 | 2 | c |
| h | 7 | 66 | 21 | v |
| i | 8 | 70 | 0 | a |
| r | 17 | 3 | 20 | u |
| a | 0 | 2 | 2 | c |
| h | 7 | 6 | 13 | n |
| m | 12 | 17 | 3 | d |
| a | 0 | 18 | 18 | s |
| n | 13 | 19 | 6 | g |
| i | 8 | 44 | 0 | a |
| r | 17 | 58 | 23 | x |
| r | 17 | 67 | 6 | g |
| a | 0 | 68 | 16 | q |
| h | 7 | 2 | 9 | j |
| i | 8 | 4 | 12 | m |
| m | 12 | 7 | 19 | t |
| d | 3 | 20 | 23 | x |
| e | 4 | 21 | 25 | z |
| n | 13 | 22 | 9 | j |
| g | 6 | 48 | 2 | c |
| a | 0 | 53 | 1 | b |
| n | 13 | 65 | 0 | a |
| i | 8 | 69 | 25 | z |
| n | 13 | 1 | 14 | o |
| i | 8 | 3 | 11 | l |
| s | 18 | 8 | 0 | a |
| a | 0 | 23 | 23 | x |
| y | 24 | 24 | 22 | w |
| a | 0 | 25 | 25 | z |

| *Plaintext* | $y_i$ | $k_i$ | $z_i = y_i + k_i(Mod26)$ | *Chiphertext* |
|---|---|---|---|---|
| n | 13 | 43 | 4 | e |
| y | 24 | 57 | 3 | d |
| a | 0 | 63 | 11 | l |
| t | 19 | 73 | 14 | o |
| a | 0 | 3 | 3 | d |
| k | 10 | 2 | 12 | m |
| a | 0 | 9 | 9 | j |
| n | 13 | 26 | 13 | n |
| m | 12 | 27 | 13 | n |
| a | 0 | 28 | 2 | c |
| h | 7 | 47 | 2 | c |
| a | 0 | 52 | 0 | a |
| s | 18 | 64 | 4 | e |
| i | 8 | 71 | 1 | b |
| s | 18 | 2 | 20 | u |
| w | 22 | 4 | 0 | a |
| a | 0 | 10 | 10 | k |
| a | 0 | 29 | 3 | d |
| t | 19 | 30 | 23 | x |
| a | 0 | 31 | 5 | f |
| s | 18 | 42 | 8 | i |
| n | 13 | 56 | 17 | r |
| a | 0 | 62 | 10 | k |
| m | 12 | 72 | 6 | g |
| a | 0 | 1 | 1 | b |
| h | 7 | 3 | 10 | k |
| a | 0 | 11 | 11 | l |
| n | 13 | 32 | 19 | t |
| i | 8 | 33 | 15 | p |
| a | 0 | 34 | 8 | i |
| h | 7 | 46 | 1 | b |
| z | 25 | 51 | 1 | b |
| a | 0 | 60 | 8 | i |
| k | 10 | 76 | 8 | i |
| i | 8 | 3 | 11 | l |
| n | 13 | 2 | 15 | p |

| *Plaintext* | $y_i$ | $k_i$ | $z_i = y_i + k_i(Mod26)$ | *Chiphertext* |
|---|---|---|---|---|
| l | 11 | 12 | 23 | x |
| u | 20 | 35 | 3 | d |
| l | 11 | 36 | 21 | v |
| u | 20 | 37 | 5 | f |
| s | 18 | 41 | 7 | h |
| t | 19 | 55 | 22 | w |
| e | 4 | 61 | 13 | n |
| p | 15 | 74 | 11 | l |
| a | 0 | 2 | 2 | c |
| t | 19 | 4 | 23 | x |
| w | 22 | 13 | 9 | j |
| a | 0 | 38 | 12 | m |
| k | 10 | 39 | 23 | x |
| t | 19 | 40 | 7 | h |
| u | 20 | 45 | 13 | n |
| d | 3 | 50 | 1 | b |
| e | 4 | 59 | 11 | l |
| n | 13 | 75 | 10 | k |
| g | 6 | 77 | 5 | f |
| a | 0 | 80 | 2 | c |
| n | 13 | 87 | 22 | w |
| b | 1 | 104 | 1 | b |
| i | 8 | 105 | 9 | j |
| d | 3 | 106 | 5 | f |
| a | 0 | 127 | 23 | x |
| n | 13 | 132 | 15 | p |
| g | 6 | 148 | 24 | y |
| s | 18 | 152 | 14 | o |
| k | 10 | 78 | 10 | k |
| r | 17 | 81 | 20 | u |
| i | 8 | 88 | 18 | s |
| p | 15 | 103 | 14 | o |
| s | 18 | 107 | 21 | v |
| i | 8 | 108 | 12 | m |

| *Plaintext* | $y_i$ | $k_i$ | $z_i = y_i + k_i(Mod26)$ | *Chiphertext* |
|---|---|---|---|---|
| t | 19 | 123 | 12 | m |
| e | 4 | 137 | 11 | l |
| o | 14 | 149 | 7 | h |
| r | 17 | 150 | 11 | l |
| i | 8 | 79 | 9 | j |
| g | 6 | 82 | 10 | k |
| r | 17 | 89 | 2 | c |
| a | 0 | 102 | 24 | y |
| f | 5 | 109 | 10 | k |

Table 6: Proses deskripsi *stream chipher* dari *chiphertext* menjadi *plaintext*.

| *Chiphertext* | $z_i$ | $k_i$ | $y_i = z_i - k_i(Mod26)$ | *Plaintext* |
|---|---|---|---|---|
| c | 2 | 1 | 1 | b |
| l | 11 | 3 | 8 | i |
| x | 23 | 5 | 18 | s |
| a | 0 | 14 | 12 | m |
| x | 23 | 15 | 8 | i |
| b | 1 | 16 | 11 | l |
| i | 8 | 49 | 11 | l |
| c | 2 | 54 | 0 | a |
| v | 21 | 66 | 7 | h |
| a | 0 | 70 | 8 | i |
| u | 20 | 3 | 17 | r |
| c | 2 | 2 | 0 | a |
| n | 13 | 6 | 7 | h |
| d | 3 | 17 | 12 | m |
| s | 18 | 18 | 0 | a |
| g | 6 | 19 | 13 | n |
| a | 0 | 44 | 8 | i |
| x | 23 | 58 | 17 | r |
| g | 6 | 67 | 17 | r |
| q | 16 | 68 | 0 | a |
| j | 9 | 2 | 7 | h |
| m | 12 | 4 | 8 | i |
| t | 19 | 7 | 12 | m |

| *Chiphertext* | $z_i$ | $k_i$ | $y_i = z_i - k_i(Mod26)$ | *Plaintext* |
|---|---|---|---|---|
| x | 23 | 20 | 3 | d |
| z | 25 | 21 | 4 | e |
| j | 9 | 22 | 13 | n |
| c | 2 | 48 | 6 | g |
| b | 1 | 53 | 0 | a |
| a | 0 | 65 | 13 | n |
| z | 25 | 69 | 8 | i |
| o | 14 | 1 | 13 | n |
| l | 11 | 3 | 8 | i |
| a | 0 | 8 | 18 | s |
| x | 23 | 23 | 0 | a |
| w | 22 | 24 | 24 | y |
| z | 25 | 25 | 0 | a |
| e | 4 | 43 | 13 | n |
| d | 3 | 57 | 24 | y |
| l | 11 | 63 | 0 | a |
| o | 14 | 73 | 19 | t |
| d | 3 | 3 | 0 | a |
| m | 12 | 2 | 10 | k |
| j | 9 | 9 | 0 | a |
| n | 13 | 26 | 13 | n |
| n | 13 | 27 | 12 | m |
| c | 2 | 28 | 0 | a |
| c | 2 | 47 | 7 | h |
| a | 0 | 52 | 0 | a |
| e | 4 | 64 | 18 | s |
| b | 1 | 71 | 8 | i |
| u | 20 | 2 | 18 | s |
| a | 0 | 4 | 22 | w |
| k | 10 | 10 | 0 | a |
| d | 3 | 29 | 0 | a |
| x | 23 | 30 | 19 | t |
| f | 5 | 31 | 0 | a |
| i | 8 | 42 | 18 | s |

| *Chiphertext* | $z_i$ | $k_i$ | $y_i = z_i - k_i(Mod26)$ | *Plaintext* |
|---|---|---|---|---|
| r | 17 | 56 | 13 | n |
| k | 10 | 62 | 0 | a |
| g | 6 | 72 | 12 | m |
| b | 1 | 1 | 0 | a |
| k | 10 | 3 | 7 | h |
| l | 11 | 11 | 0 | a |
| t | 19 | 32 | 13 | n |
| p | 15 | 33 | 8 | i |
| i | 8 | 34 | 0 | a |
| b | 1 | 46 | 7 | h |
| b | 1 | 51 | 25 | z |
| i | 8 | 60 | 0 | a |
| i | 8 | 76 | 10 | k |
| l | 11 | 3 | 8 | i |
| p | 15 | 2 | 13 | n |
| x | 23 | 12 | 11 | l |
| d | 3 | 35 | 20 | u |
| v | 21 | 36 | 11 | l |
| f | 5 | 37 | 20 | u |
| h | 7 | 41 | 18 | s |
| w | 22 | 55 | 19 | t |
| n | 13 | 61 | 4 | e |
| l | 11 | 74 | 15 | p |
| c | 2 | 2 | 0 | a |
| x | 23 | 4 | 19 | t |
| j | 9 | 13 | 22 | w |
| m | 12 | 38 | 0 | a |
| x | 23 | 39 | 10 | k |
| h | 7 | 40 | 19 | t |
| n | 13 | 45 | 20 | u |
| b | 1 | 50 | 3 | d |
| l | 11 | 59 | 4 | e |
| k | 10 | 75 | 13 | n |
| f | 5 | 77 | 6 | g |
| c | 2 | 80 | 0 | a |
| w | 22 | 87 | 13 | n |
| b | 1 | 104 | 1 | b |
| j | 9 | 105 | 8 | i |
| f | 5 | 106 | 3 | d |
| x | 23 | 127 | 0 | a |
| p | 15 | 132 | 13 | n |
| y | 24 | 148 | 6 | g |

| *Chiphertext* | $z_i$ | $k_i$ | $y_i = z_i - k_i(Mod26)$ | *Plaintext* |
|---|---|---|---|---|
| o | 14 | 152 | 18 | s |
| k | 10 | 78 | 10 | k |
| u | 20 | 81 | 17 | r |
| s | 18 | 88 | 8 | i |
| o | 14 | 103 | 15 | p |
| v | 21 | 107 | 18 | s |
| m | 12 | 108 | 8 | i |
| m | 12 | 123 | 19 | t |
| l | 11 | 137 | 4 | e |
| h | 7 | 149 | 14 | o |
| l | 11 | 150 | 17 | r |
| j | 9 | 79 | 8 | i |
| k | 10 | 82 | 6 | g |
| c | 2 | 89 | 17 | r |
| y | 24 | 102 | 0 | a |
| k | 10 | 109 | 5 | f |

*Plaintext* $y_1, y_2, y_3, \ldots$ diperoleh dengan proses deskripsi $y_i = z_i - k_i(\mathrm{mod}\ 26)$. Dari Tabel 6 tersebut dapat dilihat bahwa *chiphertext* dapat diubah kembali menjadi *plaintext* sehingga *chiphertext* "**clxaxbicvaucndsgaxgqjmtxzjcbazoaxwzedlodmjnnccaebuakdxfirkgbkltpibbiilpxdvfhwnlcxjmxhnblkfcwbjfxp yokusovmmlhljkcyk**" dapat diubah kembali menjadi kalimat plaintext "**bismillahirahmanirrahimdenganinisayanyatakanmahasiswaatasnamahaniahza kinlulustepatwaktudenganbidangskripsiteorigraf**" yang apabila diberi spasi plaintext akan menjadi "**bismillahirahmanirrahim dengan ini saya nyatakan mahasiswa atas nama haniah zakin lulus tepat waktu dengan bidang skripsi teori graf**".

## Kesimpulan

Eksponensial dari Graf Lintasan dan Amalgamasi Graf $Cycle$ yang dinotasikan dengan $P_{n+1}^{Amal(C_{m+2},e,s)}$ memiliki macam-macam *chiphertext* bergantung pada nilai $m, n, t, s$ yang disajikan pada contoh berikut

Table 7: *Chiphertext* alfabet dari Graf $P_4^{Amal(C_9,e,3)}$ dengan d=9.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Plaintext* | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| *Chiphertext* | Q | B | Y | V | R | A | X | U | C | F | I | S | Z | W |
| *Plaintext* | O | P | Q | R | S | T | U | V | W | X | Y | Z | sp | |
| *Chiphertext* | T | D | G | J | L | E | H | K | N | M | P | O | @ | |

*Stream Chipher* disebut juga dengan sandi aliran. *Stream Chipher* ini yang didasarkan pada fungsi *chaos*. Fungsi *chaos* dalam matematika merupakan suatu fungsi yang mempunyai sifat bahwa nilai fungsinya sensitif terhadap nilai awal, artinya perubahan kecil pada

Table 8: *Chiphertext* simbol dari Graf $P_4^{Amal(C_{11},e,3)}$ dengan d=22.

| *Plaintext* | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Chiphertext* | ✠ | $\partial$ | $\aleph$ | $*$ | ¥ | $\hbar$ | $\star$ | $\mho$ | $\imath$ | $\perp$ | £ | $\diamond$ | $\infty$ | $\mp$ | $\square$ |
| *Plaintext* | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 |
| *Chiphertext* | $\forall$ | $\natural$ | $\nabla$ | $\angle$ | ✓ | $\Im$ | ♠ | $\wp$ | $\diamondsuit$ | $\jmath$ | \ | ® | $\surd$ | ¶ | $\exists$ |
| *Plaintext* | 4 | 5 | 6 | 7 | 8 | 9 | sp. | . | , | ? | ! | @ | # | $ | & |
| *Chiphertext* | $\sharp$ | $\triangle$ | $\flat$ | $\prime$ | ‡ | $\Re$ | ♡ | $\ell$ | ♣ | $\top$ | © | ¬ | $\|$ | $\emptyset$ | § |

nilai awal akan mengakibatkan perubahan besar pada nilai fungsinya. Penerapan fungsi *chaos* dalam *stream chipher* tentu menguntungkan, karena sifat sensitif pada nilai awal tersebut, sehingga diharapkan dapat meningkatkan keamanan dari *stream chipher*. Keuntungan dari *stream chipher* adalah tidak dibatasi oleh panjang *plaintext*. Sama seperti metode eliminasi, *stream chipher* juga menggunakan aturan Julius Caesar. Sehingga *plaintext* $y_1, y_2, y_3, \ldots$ dengan $y_i \in Z_{26}$ dan kunci aliran $k_1, k_2, k_3, \ldots$ dengan $k_i \in Z_{26}$. *Chiphertext* $z_1, z_2, z_3, \ldots$ diperoleh dengan proses enkripsi sebagai berikut:
$z_1 = y_1 + k_1, z_2 = y_2 + k_2, \ldots, z_n = y_n + k_n, z_{n+1} = y_{n+1} + k_{n+1} \ldots \pmod{26}$.
*Plaintext* $y_1, y_2, y_3, \ldots$ diperoleh dengan proses deskripsi sebagai berikut:
$y_1 = z_1 + k_1, y_2 = z_2 + k_2, \ldots, y_n = z_n + k_n, y_{n+1} = z_{n+1} + k_{n+1} \ldots \pmod{26}$.

## Referensi

[1] Kak, Avi. 2015. *Lecture 2: Classical Encryption Techniques*. Purdue University.

[2] Pearson, E. 2006. *Introduction To Cryptography With Coding Theory*. America: United States of America.