JIKO (JURNAL INFORMATIKA DAN KOMPUTER)
Juni 2025, Volume: **9**, No. **2** | Pages 449–462
doi: 10.26798/jiko.v9i2.1921
e-ISSN : 2477-3964 – p-ISSN : 2477-4413

ARTICLE

Integrasi Tangga Nada Diatonis Mayor pada Kriptografi dalam Merancang Skema Transposisi

Integration of Major Diatonic Scale in Cryptography in Designing Transposition Schemes

Kadek Widiana* dan Alz Danny Wowor

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
*Penulis Korespondensi: kadekwidiana16@gmail.com

(Disubmit 22-03-25; Diterima 02-05-25; Dipublikasikan online pada 20-06-25)

Abstrak

Di era digital yang semakin maju, keamanan data menjadi aspek krusial yang memerlukan perhatian serius. Metode transposisi yang digunakan pada algoritma AES dan DES memiliki kerentanan pada indeks transposisinya membentuk pola dan tidak sepenuhnya acak, sehingga berpotensi memudahkan kriptanalis mencari relasi cipherteks. Penelitian ini mengeksplorasi pendekatan baru dalam merancang skema transposisi pada algoritma *square transposition* dengan mengintegrasikan teori musik, khususnya tangga nada diatonis mayor kedalam kotak skema. Pendekatan ini diharapkan menghasilkan pola transposisi yang unik dan lebih acak. Penelitian ini merancang kotak skema diatonis mayor sebagai acuan dalam mengatur urutan indeks dan memodifikasi tiga skema yang digunakan pada penelitian terdahulu, yaitu skema papan catur, spiral dan cermin. Pola pada ketiga skema tersebut diimplementasikan ke dalam kotak skema diatonis mayor, sehingga urutan indeks yang dihasilkan menjadi berbeda. Nilai keacakan dan korelasi yang dihasilkan pada modifikasi skema tersebut dibandingkan dengan hasil pengujian penelitian terdahulu. Diperoleh bahwa dari dua modifikasi skema tersebut menghasilkan uji keacakan dan uji korelasi yang lebih baik. Penelitian ini menunjukkan bahwa penggabungan konsep musik ke dalam algoritma *square transposition* merupakan pendekatan baru yang menjanjikan.

Kata kunci: Kriptografi; *Square transposition*; Tangga nada; Diatonis mayor

Abstract

In the increasingly advanced digital era, data security is a crucial aspect that requires serious attention. The transposition method used in the AES and DES algorithms has a vulnerability in its transposition index forming a pattern and not completely random, so it has the potential to make it easier for cryptanalysts to find ciphertext relationships. This study explores a new approach in designing a transposition scheme in the square transposition algorithm by integrating music theory, especially the major diatonic scale, into the scheme box. This approach is expected to produce a unique and more random transposition pattern. This study designs a major diatonic scheme box as a reference in arranging the index sequence and modifying three schemes used in previous studies, namely the chessboard, spiral and mirror schemes. The patterns in the three schemes are implemented into the major diatonic scheme box, so that the resulting index sequence is different. The randomness and correlation values produced in the scheme modification are compared with the results of previous research tests. It was found that the two scheme modifications produced better randomness and correlation tests. This study shows that the integration of musical concepts into the square transposition algorithm is a promising new approach.

KeyWords: Cryptography; Square transposition, Scale, Diatonic mayor

How to Cite: K. Widiana *et al.*, "Integrasi Tangga Nada Diatonis Mayor pada Kriptografi dalam Merancang Skema Transposisi", *JIKO (JURNAL INFORMATIKA DAN KOMPUTER)*, Volume: **9**, No.**2**, Pages 449–462, Juni 2025, doi: 10.26798/jiko.v9i2.1921.

1. Pendahuluan

Pertukaran informasi melalui jaringan internet memiliki berbagai kerentanan terhadap serangan siber. Keamanan data menjadi aspek krusial yang memerlukan perhatian serius ditengah pesatnya perkembangan teknologi. Kriptografi memainkan peran penting sebagai disiplin ilmu dan seni mengamankan data digital [1], [2]. Kriptografi memastikan kerahasiaan, integritas dan keaslian informasi melalui berbagai teknik enkripsi, salah satunya adalah metode transposisi [3], [4]. Metode transposisi bekerja dengan mengubah posisi atau urutan karakter pada pesan asli untuk menghasilkan cipherteks [5]. Penggunaan metode transposisi pada kriptografi modern bertujuan untuk meningkatkan efe difusi dan kebingungan [6].

Meskipun metode transposisi merupakan komponen penting dalam menciptakan kriptografi modern, cipher tersebut memiliki memiliki kelemahan. Permasalahan utama yang teridentifikasi adalah nilai indeks transposisi yang berpola. Algoritma AES dan DES merupakan algoritma kriptografi modern yang memanfaatkan metode transposisi dengan nilai indeks berpola [7], [8], [9]. Pola yang teratur ini dapat dieksploitasi oleh kriptanalis melalui berbagai metode analisis pola atau serangan kriptanalisis lainnya. Oleh karena itu, diperlukan pengembangan metode transposisi untuk menghasilkan pola perpindahan karakter yang lebih acak.

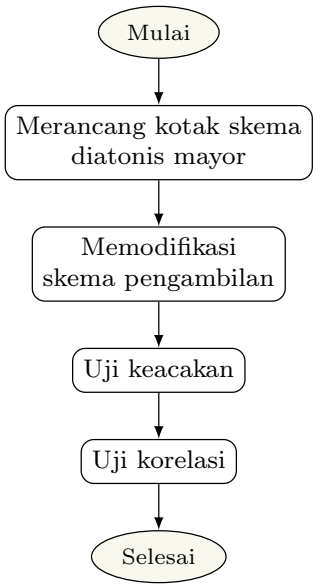
Penelitian ini menjelajahi pendekatan baru dalam merancang skema transposisi pada algoritma *square transposition*, yaitu mengintegrasikan teori musik, khususnya tangga nada diatonis mayor ke dalam kotak skema *square transposision*. Pendekatan ini diharapkan dapat menghasilkan pola transposisi yang unik dan memiliki tingkat keacakan yang tinggi dibandingkan metode transposisi yang sudah dikembangkan. Penelitian ini akan memodifikasi skema papan catur, skema spiral dan skema cermin dengan mengkombinasikan aturan urutan indeks yang sudah kedalam aturan kotak skema diatonis mayor. Hasil statistik dari modifikasi tersebut akan dibandingkan dengan skema asli untuk mengetahui seberapa optimal pendekatan yang diusulkan dengan terhadap skema asli.

Peninjauan penelitian terdahulu diperlukan untuk menunjukkan keterbaruan, serta mengetahui keterkaitan terhadap penelitian-penelitian sebelumnya yang dapat dijadikan sebagai pembanding dan/atau acuan pada penelitian yang sedang dilakukan. Penelitian [7] secara khusus mengkaji tentang pengembangan algoritma transposisi baru, yaitu algoritma *square transposition*. Penelitian tersebut membandingkan hasil uji keacakan skema transposisi berukuran 64-bit terhadap algoritma AES dan DES. Penelitian tersebut merancang dua skema pemasukan dengan nilai indeks acak dan empat skema pengambilan, yaitu horizontal, vertikal, zig-zag, dan bajak sawah. Secara keseluruhan, hasil uji keacakan nilai indeks serta uji korelasi terhadap plainteks dan cipherteks menunjukkan bahwa algoritma *square transposition* menghasilkan nilai indeks lebih acak dan mampu menyamarkan plainteks lebih baik dibandingkan AES dan DES.

Penelitian [10] merancang algoritma *square transposition* dengan skema pemasukan papan catur. Rata-rata uji keacakan *monobit*, *block bit* dan *runs* yang dihasilkan skema pemasukan papan catur secara berturut-turut adalah 1.0, 0.9003 dan 0.6043, sedangkan nilai rata-rata uji korelasi yang dihasilkan skema pemasukan papan catur adalah 0.3752. Penelitian [11] merancang algoritma *square transposition* dengan skema pemasukan spiral, dimana pola urutan indeks membentuk beberapa pola lingkaran yang dimulai dari tengah kotak skema. Rata-rata uji keacakan *monobit*, *block bit* dan *runs* yang dihasilkan skema pemasukan spiral secara berturut-turut adalah 0.9222, 0.9999 dan 0.0000, sedangkan nilai rata-rata uji korelasi yang dihasilkan skema pemasukan spiral adalah 0.2595. Penelitian [12] melakukan implementasi pola pembiasan cermin dalam merancang algoritma *square transposition*. Rata-rata uji keacakan *monobit*, *block bit* dan *runs* yang dihasilkan skema pemasukan cermin secara berturut-turut adalah 0.1805, 0.1905 dan 0.1824, sedangkan nilai rata-rata uji korelasi yang dihasilkan skema pemasukan cermin adalah 0.2052. Secara umum, rancangan penelitian pada ketiga penelitian terdahulu tersebut terdiri dari merancang kotak skema, uji keacakan dan uji korelasi.

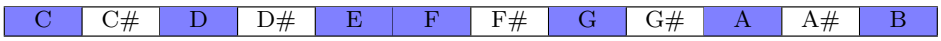
2. Metode

Secara garis besar rancangan penelitian ini terdiri dari proses perancangan kotak skema diatonis mayor, memodifikasi skema pemasukan dan skema pengambilan, pengujian keacakan serta pengujian korelasi. Diagram alir rancangan secara lengkap dapat dilihat pada Gambar 1.



Gambar 1. Diagram alir rancangan penelitian

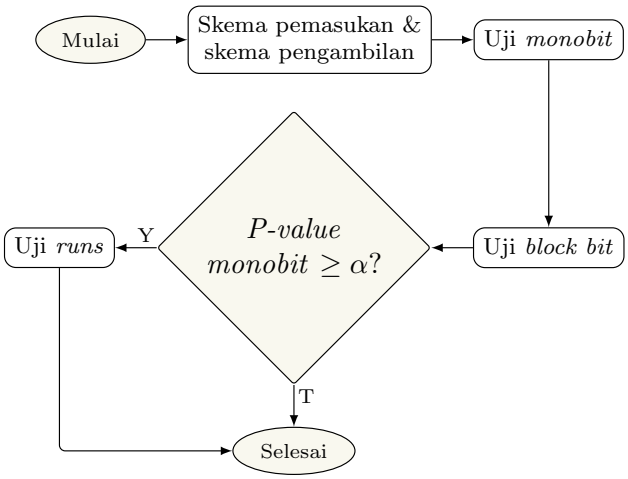
Tahap perancangan kotak skema diatonis mayor merupakan tahapan merancang kotak skema dengan mengintegrasikan nada-nada diatonis mayor ke dalam kotak skema. Kotak skema diatonis mayor menjadi acuan dalam memasukan urutan indeks, dengan memprioritaskan posisi nada-nada diatonis mayor dalam urutan indeks sesuai dengan aturan skema tertentu. Tangga nada diatonis mayor merupakan bagian dari tangga nada kromatis yang memiliki susunan 7 nada dari 12 nada per-oktaf [13]. Interval dari ketujuh nada tersebut meliputi 1-1-½-1-1-1-½. Dimisalkan nada *do* = *C*, berdasarkan struktur interval tersebut, maka nada tangga nada diatonis mayor akan tersusun dari nada *C*, *D*, *E*, *F*, *G*, *A*, *B* dan kembali ke nada *C* [13], [14], [15]. Ilustrasi secara lengkap dapat dilihat pada Gambar 2.



Gambar 2. Tangga nada diatonis mayor dalam 1 oktaf dengan nada *do* = *C*

Tahapan selanjutnya adalah melakukan modifikasi skema papan catur, spiral dan cermin sebagai skema pengambilan pada penelitian ini. Diperlukan analisa terlebih dahulu untuk mengetahui pola urutan indeks pada skema tersebut. Setelah itu, pola urutan indeks pada setiap skema tersebut dimasukan kedalam kotak skema diatonis mayor dengan memprioritaskan nada tangga nada diatonis mayor saat memasukan indeks, sehingga posisi indeks menjadi berbeda dengan skema asli.

Pengujian keacakan dilakukan untuk mengetahui nilai keacakan yang dihasilkan pada kombinasi modifikasi skema pemasukan dan skema pengambilan. Metode uji keacakan yang digunakan meliput *monobit*, *block bit* dan *runs*. Apabila pengujian *monobit* menghasilkan *P-value* < 0.01, maka pengujian *runs* tidak perlu dilakukan dikarenakan kegagalan pada pengujian *monobit* [16]. Kombinasi skema pemasukan dan pengambilan dapat dikatakan acak apabila *P-value* dari dua atau tiga pengujian tersebut ≥ 0.01 [17], [7]. Diagram alir uji keacakan skema tertera pada Gambar 3.



Gambar 3. Diagram alir uji keacakan skema

Tahapan uji korelasi dilakukan untuk menghitung nilai korelasi antar plainteks dan cipherteks yang dihasilkan pada setiap kombinasi skema pemasukan dan skema pengambilan. Uji korelasi dilakukan untuk mengetahui seberapa optimal skema transposisi dalam menyamarkan plainteks. Dalam konteks kriptografi, nilai korelasi yang baik adalah r yang mendekati angka 0 atau hubungan korelasi yang sangat rendah, dikarenakan algoritma kriptografi dapat dikatakan algoritma kriptografi yang baik adalah algoritma yang dapat menyembunyikan plainteks dengan optimal [18].

3. Hasil dan Pembahasan

3.1 Kotak Skema Diatonis Mayor

Berdasarkan ilustrasi pada Gambar 2, apabila susunan nada tangga nada diatonis mayor dalam satu oktaf diimplementasikan pada kotak skema transposisi berukuran 8×8, maka kotak skema akan tersusun dari 6 oktaf (kelebihan 8 nada kromatis pada oktaf terakhir akan diabaikan). Setiap nada kromatis ke-i dengan $(i-1)|8$, akan disusun ke baris baru pada kotak skema (ilustrasi secara lengkap dapat dilihat pada Gambar 4).

C	C#	D	D#	E	F	F#	G
G#	A	A#	B	C	C#	D	D#
E	F	F#	G	G#	A	A#	B
C	C#	D	D#	E	F	F#	G
G#	A	A#	B	C	C#	D	D#
E	F	F#	G	G#	A	A#	B
C	C#	D	D#	E	F	F#	G
G#	A	A#	B	C	C#	D	D#

Gambar 4. Integrasi tangga nada diatonis mayor pada kotak skema

3.2 Skema Pemasukan

Rancangan skema pemasukan pada penelitian ini merupakan modifikasi dari skema pemasukan penelitian terdahulu. Modifikasi dilakukan dengan mengatur ulang pola urutan indeks pada skema ke dalam kotak skema diatonis mayor. Berikut merupakan hasil modifikasi skema pemasukan tersebut.

3.2.1 Modifikasi Skema Pemasukan Papan Catur

Skema pemasukan papan catur pada penelitian [10], memiliki pola memasukan indeks kedalam kotak skema terbagi menjadi empat bagian, meliputi bagian (a) terdiri dari kolom 1 dan 2 kotak skema, bagian (b) terdiri dari kolom 3 dan 4 hingga bagian (d) terdiri dari kolom 7 dan 8. Indeks terlebih dahulu dimasukkan pada kotak berwarna putih pada setiap bagian, dimulai dari bagian (a) hingga bagian (d) dengan arah dari bawah ke atas kotak skema. Sehingga a_{01} terletak pada kiri-bawah kotak skema dan a_{32} berakhiran pada kanan-atas kotak skema. Jika semua kotak putih sudah terisi indeks, urutan indeks dilanjutkan pada kotak

berwarna abu yang dimulai dari bagian (a) hingga bagian(d) dengan arah dari bawah ke atas kotak skema. Ilustrasi pola urutan indeks papan catur terlihat pada Gambar 5.

a_{40}	a_{08}
a_{07}	a_{39}
a_{38}	a_{06}
a_{05}	a_{37}
a_{36}	a_{04}
a_{03}	a_{35}
a_{34}	a_{02}
a_{01}	a_{33}

(a) Bagian 1

a_{48}	a_{16}
a_{15}	a_{47}
a_{46}	a_{14}
a_{13}	a_{45}
a_{44}	a_{12}
a_{11}	a_{43}
a_{42}	a_{10}
a_{09}	a_{41}

(b) Bagian 2

a_{56}	a_{24}
a_{23}	a_{55}
a_{54}	a_{22}
a_{21}	a_{53}
a_{52}	a_{20}
a_{19}	a_{51}
a_{50}	a_{18}
a_{17}	a_{49}

(c) Bagian 3

a_{64}	a_{32}
a_{31}	a_{63}
a_{62}	a_{30}
a_{29}	a_{61}
a_{60}	a_{28}
a_{27}	a_{59}
a_{58}	a_{26}
a_{25}	a_{57}

(d) Bagian 4

Gambar 5. Skema papan catur yang dipecah menjadi empat bagian

Jika pola urutan indeks pada skema papan catur diatas diterapkan pada kotak skema diatonis mayor, maka indeks pada kotak putih bagian (a) skema pemasukan 1 dengan arah dari bawah ke atas terdiri dari $\{a_{38}, a_{39}, a_{01}, \ldots, a_{43}\}$ dan diakhiri dengan indeks $\{a_{60}, a_{61}, a_{35}, \ldots, a_{64}\}$ pada kotak abu bagian (d).

a_{40}	a_{08}	a_{48}	a_{16}	a_{56}	a_{24}	a_{64}	a_{32}
a_{07}	a_{39}	a_{15}	a_{47}	a_{23}	a_{55}	a_{31}	a_{63}
a_{38}	a_{06}	a_{46}	a_{14}	a_{54}	a_{22}	a_{62}	a_{30}
a_{05}	a_{37}	a_{13}	a_{45}	a_{21}	a_{53}	a_{29}	a_{61}
a_{36}	a_{04}	a_{44}	a_{12}	a_{52}	a_{20}	a_{60}	a_{28}
a_{03}	a_{35}	a_{11}	a_{43}	a_{19}	a_{51}	a_{27}	a_{59}
a_{34}	a_{02}	a_{42}	a_{10}	a_{50}	a_{18}	a_{58}	a_{26}
a_{01}	a_{33}	a_{09}	a_{41}	a_{17}	a_{49}	a_{25}	a_{57}

(a) Skema papan catur [10]

a_{24}	a_{43}	a_{29}	a_{48}	a_{34}	a_{13}	a_{64}	a_{18}
a_{42}	a_{23}	a_{47}	a_{28}	a_{12}	a_{59}	a_{17}	a_{63}
a_{22}	a_{04}	a_{56}	a_{07}	a_{58}	a_{11}	a_{62}	a_{16}
a_{03}	a_{41}	a_{06}	a_{55}	a_{10}	a_{33}	a_{53}	a_{37}
a_{40}	a_{02}	a_{54}	a_{05}	a_{32}	a_{50}	a_{36}	a_{52}
a_{01}	a_{21}	a_{46}	a_{27}	a_{49}	a_{31}	a_{51}	a_{35}
a_{20}	a_{39}	a_{26}	a_{45}	a_{30}	a_{09}	a_{61}	a_{15}
a_{38}	a_{19}	a_{44}	a_{25}	a_{08}	a_{57}	a_{14}	a_{60}

(b) Modifikasi skema papan catur (skema pemasukan 1)

Gambar 6. Skema papan catur dan modifikasinya

3.2.2 Modifikasi Skema Pemasukan Spiral

Skema pemasukan spiral yang dirancang pada penelitian [11], memiliki pola urutan indeks membentuk beberapa pola lingkaran yang dimulai dari titik tengah kotak skema. Berdasarkan Gambar 7 (a), skema ini terdiri dari tujuh lingkaran dengan indeks saling berurutan. Pada lingkaran 1 terdiri dari indeks $\{a_{01}, a_{02}, a_{03}, a_{04}\}$, lingkaran 2 terdiri dari indeks $\{a_{05}, a_{06}, \ldots, a_{12}\}$, lingkaran 3 terdiri dari indeks $\{a_{13}, a_{14}, \ldots, a_{24}\}$, lingkaran 4 terdiri dari indeks $\{a_{25}, a_{26}, \ldots, a_{40}\}$, lingkaran 5 terdiri dari indeks $\{a_{41}, a_{42}, \ldots, a_{52}\}$, lingkaran 6 terdiri dari indeks $\{a_{53}, a_{54}, \ldots, a_{60}\}$ dan lingkaran 7 terdiri dari indeks $\{a_{61}, a_{62}, a_{63}, a_{64}\}$.

Ketujuh pola lingkaran diatas menjadi pola memasukan indeks pada skema pemasukan 2 (spiral diatonis mayor). Sehingga, lingkaran 1 pada skema pemasukan 2 terdiri dari indeks $\{a_{01}, a_{02}, a_{38}, a_{03}\}$, lingkaran 2 terdiri dari indeks $\{a_{39}, a_{40}, a_{04}, \ldots, a_{07}\}$, lingkaran 3 $\{a_{08}, a_{09}, a_{10}, \ldots, a_{47}\}$ dan seterusnya. Skema pemasukan 2 secara lengkap dapat dilihat pada Gambar 7.

a_{63}	a_{57}	a_{47}	a_{33}	a_{32}	a_{46}	a_{56}	a_{62}
a_{58}	a_{48}	a_{34}	a_{19}	a_{18}	a_{31}	a_{45}	a_{55}
a_{49}	a_{35}	a_{20}	a_{09}	a_{08}	a_{17}	a_{30}	a_{44}
a_{36}	a_{21}	a_{10}	a_{03}	a_{02}	a_{07}	a_{16}	a_{29}
a_{37}	a_{22}	a_{11}	a_{04}	a_{01}	a_{06}	a_{15}	a_{28}
a_{50}	a_{38}	a_{23}	a_{12}	a_{05}	a_{14}	a_{27}	a_{43}
a_{59}	a_{51}	a_{39}	a_{24}	a_{13}	a_{26}	a_{42}	a_{54}
a_{64}	a_{60}	a_{52}	a_{40}	a_{25}	a_{41}	a_{53}	a_{61}

(a) Skema spiral [11]

a_{37}	a_{61}	a_{28}	a_{52}	a_{18}	a_{27}	a_{60}	a_{36}
a_{62}	a_{29}	a_{53}	a_{13}	a_{12}	a_{51}	a_{26}	a_{59}
a_{30}	a_{19}	a_{44}	a_{05}	a_{41}	a_{11}	a_{50}	a_{25}
a_{20}	a_{45}	a_{06}	a_{38}	a_{02}	a_{04}	a_{43}	a_{17}
a_{54}	a_{14}	a_{42}	a_{03}	a_{01}	a_{40}	a_{10}	a_{49}
a_{31}	a_{21}	a_{46}	a_{07}	a_{39}	a_{09}	a_{48}	a_{24}
a_{34}	a_{57}	a_{22}	a_{47}	a_{08}	a_{16}	a_{56}	a_{33}
a_{64}	a_{35}	a_{58}	a_{23}	a_{15}	a_{55}	a_{32}	a_{63}

(b) Modifikasi skema spiral (skema pemasukan 2)

Gambar 7. Skema spiral dan modifikasinya

3.2.3 Modifikasi Skema Pemasukan Cermin

Penelitian [12], merancang skema pemasukan berdasarkan pola pembiasan cermin. Berdasarkan skema cermin pada Gambar 9, skema cermin terbagi menjadi dua pola besar, yaitu pola Objek dan pola Bayangan. Dimisalkan pada kolom 1 hingga kolom 4 adalah pola Objek dan kolom 5 hingga kolom 8 adalah pola Bayangan. Masing-masing pola besar tersebut terdiri dari empat bagian kecil yang terdiri dari 8 indeks. Indeks pada pola Objek terdiri dari $\{a_{01}, a_{02}, \ldots, a_{33}\}$, sedangkan indeks pada pola Bayangan terdiri dari $\{a_{33}, a_{34}, \ldots, a_{64}\}$.

a_{10}	a_{09}	a_{02}	a_{01}
a_{11}	a_{16}	a_{03}	a_{08}
a_{12}	a_{15}	a_{04}	a_{07}
a_{13}	a_{14}	a_{05}	a_{06}
a_{26}	a_{25}	a_{18}	a_{17}
a_{27}	a_{32}	a_{19}	a_{24}
a_{28}	a_{31}	a_{20}	a_{23}
a_{29}	a_{30}	a_{21}	a_{22}

(a) Pola Objek

a_{33}	a_{34}	a_{41}	a_{42}
a_{40}	a_{35}	a_{48}	a_{43}
a_{39}	a_{36}	a_{47}	a_{44}
a_{38}	a_{37}	a_{46}	a_{45}
a_{49}	a_{50}	a_{57}	a_{58}
a_{56}	a_{51}	a_{64}	a_{59}
a_{55}	a_{52}	a_{63}	a_{60}
a_{54}	a_{53}	a_{62}	a_{61}

(b) Pola Bayangan

Gambar 8. Skema cermin yang dipecah menjadi dua bagian

Pada skema pemasukan 3 (cermin diatonis mayor), empat pola kecil dari pola Objek meliputi $\{a_{38}, a_{01}, a_{39}, \ldots, a_{04}\}$, $\{a_{42}, a_{05}, a_{43}, \ldots, a_{09}\}$, …, dan $\{a_{14}, a_{49}, a_{15}, \ldots, a_{18}\}$. Sedangkan empat pola kecil dari pola Bayangan meliputi $\{a_{19}, a_{20}, a_{52}, \ldots, a_{24}\}$, $\{a_{54}, a_{25}, a_{55}, \ldots, a_{28}\}$, …, dan $\{a_{34}, a_{61}, a_{35}, \ldots, a_{64}\}$. Delapan pola kecil pada skema pemasukan 3 secara lengkap tertera pada Gambar 9.

a_{10}	a_{09}	a_{02}	a_{01}	a_{33}	a_{34}	a_{41}	a_{42}
a_{11}	a_{16}	a_{03}	a_{08}	a_{40}	a_{35}	a_{48}	a_{43}
a_{12}	a_{15}	a_{04}	a_{07}	a_{39}	a_{36}	a_{47}	a_{44}
a_{13}	a_{14}	a_{05}	a_{06}	a_{38}	a_{37}	a_{46}	a_{45}
a_{26}	a_{25}	a_{18}	a_{17}	a_{49}	a_{50}	a_{57}	a_{58}
a_{27}	a_{32}	a_{19}	a_{24}	a_{56}	a_{51}	a_{64}	a_{59}
a_{28}	a_{31}	a_{20}	a_{23}	a_{55}	a_{52}	a_{63}	a_{60}
a_{29}	a_{30}	a_{21}	a_{22}	a_{54}	a_{53}	a_{62}	a_{61}

(a) Skema cermin [12]

a_{05}	a_{42}	a_{01}	a_{38}	a_{19}	a_{20}	a_{54}	a_{25}
a_{43}	a_{09}	a_{39}	a_{04}	a_{24}	a_{52}	a_{28}	a_{55}
a_{06}	a_{08}	a_{40}	a_{03}	a_{53}	a_{21}	a_{57}	a_{26}
a_{07}	a_{44}	a_{02}	a_{41}	a_{23}	a_{22}	a_{56}	a_{27}
a_{49}	a_{14}	a_{45}	a_{10}	a_{29}	a_{58}	a_{34}	a_{61}
a_{15}	a_{18}	a_{45}	a_{13}	a_{60}	a_{30}	a_{64}	a_{35}
a_{16}	a_{51}	a_{11}	a_{47}	a_{33}	a_{31}	a_{63}	a_{36}
a_{50}	a_{17}	a_{46}	a_{12}	a_{32}	a_{59}	a_{37}	a_{62}

(b) Modifikasi skema cermin (skema pemasukan 3)

Gambar 9. Skema cermin dan modifikasinya

3.3 Skema Pengambilan

Setiap modifikasi skema pemasukan dipasangkan dengan skema pemasukan yang berbeda, menyesuaikan skema pengambilan yang digunakan pada penelitian terdahulu. Tabel 1 menunjukan bahwa skema pengambilan yang digunakan pada skema papan catur adalah skema horizontal (kiri-kanan), vertikal (kiri-kanan), bajak sawah (kanan-kiri), spiral dan zig-zag [10]. Maka pasangan skema pengambilan pada modifikasi skema pemasukan papan catur mengikuti skema pengambilan yang digunakan pada penelitian [10]. Demikian juga pada modifikasi skema pengambilan spiral dan cermin.

Tabel 1. Daftar skema pengambilan pada penelitian terdahulu

No.	Skema Pengambilan	Skema Pemasukan		
		Papan Catur[10]	Spiral[11]	Cermin[12]
1.	Horizontal (kiri-kanan)	✓	✓	✓
2.	Horizontal (kanan-kiri)		✓	
3.	Vertikal (atas-bawah)	✓	✓	✓
4.	Vertikal (bawah-atas)		✓	
5.	Bajak sawah (kiri-kanan)		✓	
6.	Bajak sawah (kanan-kiri)	✓	✓	✓
7.	Spiral	✓		
8.	Zig-zag	✓	✓	✓
9.	Tanam Padi		✓	
10.	Acak			✓

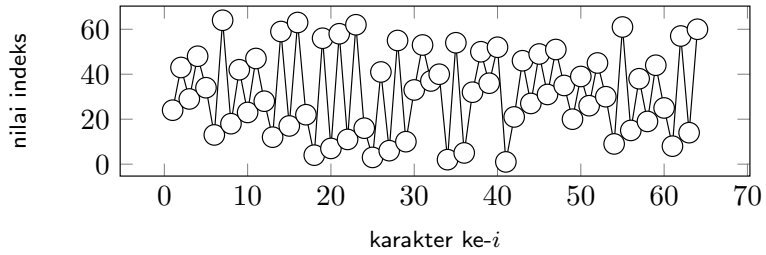
Setiap skema pengambilan akan dijabarkan dengan satu kombinasi skema pemasukkan, untuk skema pemasukkan lain dapat menyesuaikan dengan skema yang telah dijabarkan. Berikut hasil kombinasi serta grafik nilai indeks skema pemasukan terhadap skema pengambilan.

3.3.1 Skema Pengambilan Horizontal (Kiri-kanan)

Skema pengambilan ini merupakan pola pengambilan indeks secara horizontal kiri ke kanan yang dimulai dari kiri-atas dan berakhir di kanan-bawah kotak skema. Koordinat Cartesius dapat digunakan sebagai visualisasi perpindahan indeks kombinasi skema tersebut, dimana setiap indeks pemasukan (i) sebagai ordinat dan indeks pengambilan (j) sebagai absis. Kombinasi indeks dan grafik indeks skema pemasukan 1 dan pengambilan horizontal (kiri-kanan) tertera pada Gambar 10 dan Gambar 11.

$a_{24(01)}$	$a_{43(02)}$	$a_{29(03)}$	$a_{48(04)}$	$a_{34(05)}$	$a_{13(06)}$	$a_{64(07)}$	$a_{18(08)}$
$a_{42(09)}$	$a_{23(10)}$	$a_{47(11)}$	$a_{28(12)}$	$a_{12(13)}$	$a_{59(14)}$	$a_{17(15)}$	$a_{63(16)}$
$a_{22(17)}$	$a_{04(18)}$	$a_{56(19)}$	$a_{07(20)}$	$a_{58(21)}$	$a_{11(22)}$	$a_{62(23)}$	$a_{16(24)}$
$a_{03(25)}$	$a_{41(26)}$	$a_{06(27)}$	$a_{55(28)}$	$a_{10(29)}$	$a_{33(30)}$	$a_{53(31)}$	$a_{37(32)}$
$a_{40(33)}$	$a_{02(34)}$	$a_{54(35)}$	$a_{05(36)}$	$a_{32(37)}$	$a_{50(38)}$	$a_{36(39)}$	$a_{52(40)}$
$a_{01(41)}$	$a_{21(42)}$	$a_{46(43)}$	$a_{27(44)}$	$a_{49(45)}$	$a_{31(46)}$	$a_{51(47)}$	$a_{35(48)}$
$a_{20(49)}$	$a_{39(50)}$	$a_{26(51)}$	$a_{45(52)}$	$a_{30(53)}$	$a_{09(54)}$	$a_{61(55)}$	$a_{15(56)}$
$a_{38(57)}$	$a_{19(58)}$	$a_{44(59)}$	$a_{25(60)}$	$a_{08(61)}$	$a_{57(62)}$	$a_{14(63)}$	$a_{60(64)}$

Gambar 10. Indeks skema pemasukan 1 dan pengambilan horizontal (kiri-kanan)



Gambar 11. Grafik indeks skema pemasukan 1 dan pengambilan horizontal (kiri-kanan)

Berdasarkan Gambar 10, hasil kombinasi skema pemasukan 1 dan pengambilan horizontal dimulai dari a_{24}, dimana indeks pengambilan j = 01 hingga j = 64 untuk a_{60}. Kombinasi skema pemasukan 1 dan skema pengambilan horizontal menghasilkan indeks bit pada *bytes* cipherteks dengan l_1 ={a_{24}, a_{43}, a_{29}, …, a_{18}}, l_2 ={a_{42}, a_{23}, a_{47}, …, a_{63}}, …, l_8 ={a_{38}, a_{19}, a_{44}, …, a_{60}}.

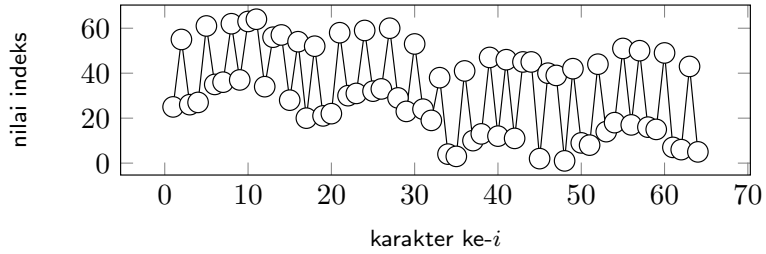
3.3.2 Skema Pengambilan Vertikal (Atas-bawah)

Skema pengambilan ini merupakan pola pengambilan indeks secara vertikal atas ke bawah yang dimulai dari kanan-atas dan berakhir di kiri-bawah kotak skema. Nilai indeks dan grafik indeks skema pemasukan

3 dan pengambilan vertikal (atas-bawah) tertera pada Gambar 12 dan Gambar 13.

$a_{05(64)}$	$a_{42(49)}$	$a_{01(48)}$	$a_{38(33)}$	$a_{19(32)}$	$a_{20(17)}$	$a_{54(16)}$	$a_{25(01)}$
$a_{43(63)}$	$a_{09(50)}$	$a_{39(47)}$	$a_{04(34)}$	$a_{24(31)}$	$a_{52(18)}$	$a_{28(15)}$	$a_{55(02)}$
$a_{06(62)}$	$a_{08(51)}$	$a_{40(46)}$	$a_{03(35)}$	$a_{53(30)}$	$a_{21(19)}$	$a_{57(14)}$	$a_{26(03)}$
$a_{07(61)}$	$a_{44(52)}$	$a_{02(45)}$	$a_{41(36)}$	$a_{23(29)}$	$a_{22(20)}$	$a_{56(13)}$	$a_{27(04)}$
$a_{49(60)}$	$a_{14(53)}$	$a_{45(44)}$	$a_{10(37)}$	$a_{29(28)}$	$a_{58(21)}$	$a_{34(12)}$	$a_{61(05)}$
$a_{15(59)}$	$a_{18(54)}$	$a_{45(43)}$	$a_{13(38)}$	$a_{60(27)}$	$a_{30(22)}$	$a_{64(11)}$	$a_{35(06)}$
$a_{16(58)}$	$a_{51(55)}$	$a_{11(42)}$	$a_{47(39)}$	$a_{33(26)}$	$a_{31(23)}$	$a_{63(10)}$	$a_{36(07)}$
$a_{50(57)}$	$a_{17(56)}$	$a_{46(41)}$	$a_{12(40)}$	$a_{32(25)}$	$a_{59(24)}$	$a_{37(09)}$	$a_{62(08)}$

Gambar 12. Indeks skema pemasukan 3 dan pengambilan vertikal (atas-bawah)



Gambar 13. Grafik indeks skema pemasukan 3 dan pengambilan vertikal (atas-bawah)

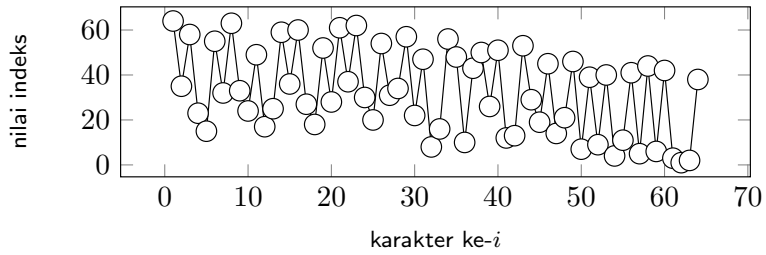
Berdasarkan Gambar 12, Hasil kombinasi indeks skema pemasukan 3 dan skema pengambilan vertikal dimulai dari a_{25}, dimana indeks pengambilan j = 01 hingga j = 64 untuk a_{05}. Keluaran indeks bit pada *bytes* cipherteks yang dihasilkan meliputi l_1 ={a_{25}, a_{55}, a_{26}, …, a_{62}}, l_2 ={a_{37}, a_{63}, a_{64}, …, a_{54}}, …, l_8 ={a_{50}, a_{16}, a_{15}, …, a_{05}}.

3.3.3 Skema Pengambilan Bajak Sawah (Kiri-kanan)

Skema pengambilan ini merupakan pola pengambilan indeks dengan teknik membajak sawah yang dimulai dari tepi sawah dan mengerucut ke tengah sawah. Pada skema pengambilan ini dimulai dari kiri-bawah kotak yang mengarah ke kanan dan berakhir di tengah kotak. Nilai indeks dan grafik indeks skema pemasukan 2 dan pengambilan bajak sawah (kiri-kanan) tertera pada Gambar 14 dan Gambar 15.

$a_{37(22)}$	$a_{61(21)}$	$a_{28(20)}$	$a_{52(19)}$	$a_{18(18)}$	$a_{27(17)}$	$a_{60(16)}$	$a_{36(15)}$
$a_{62(23)}$	$a_{29(44)}$	$a_{53(43)}$	$a_{13(42)}$	$a_{12(41)}$	$a_{51(40)}$	$a_{26(39)}$	$a_{59(14)}$
$a_{30(24)}$	$a_{19(45)}$	$a_{44(58)}$	$a_{05(57)}$	$a_{41(56)}$	$a_{11(55)}$	$a_{50(38)}$	$a_{25(13)}$
$a_{20(25)}$	$a_{45(46)}$	$a_{06(59)}$	$a_{38(64)}$	$a_{02(63)}$	$a_{04(54)}$	$a_{43(37)}$	$a_{17(12)}$
$a_{54(26)}$	$a_{14(47)}$	$a_{42(60)}$	$a_{03(61)}$	$a_{01(62)}$	$a_{40(53)}$	$a_{10(36)}$	$a_{49(11)}$
$a_{31(27)}$	$a_{21(48)}$	$a_{46(49)}$	$a_{07(50)}$	$a_{39(51)}$	$a_{09(52)}$	$a_{48(35)}$	$a_{24(10)}$
$a_{34(28)}$	$a_{57(29)}$	$a_{22(30)}$	$a_{47(31)}$	$a_{08(32)}$	$a_{16(33)}$	$a_{56(34)}$	$a_{33(09)}$
$a_{64(01)}$	$a_{35(02)}$	$a_{58(03)}$	$a_{23(04)}$	$a_{15(05)}$	$a_{55(06)}$	$a_{32(07)}$	$a_{63(08)}$

Gambar 14. Indeks skema pemasukan 2 dan pengambilan bajak sawah (kiri-kanan)



Gambar 15. Grafik indeks skema pemasukan 2 dan pengambilan bajak sawah (kiri-kanan)

Berdasarkan Gambar 14, hasil kombinasi indeks skema pemasukan 2 dan pengambilan bajak sawah (kiri-kanan) dimulai dari a_{64}, dimana indeks pengambilan j = 01 hingga j = 64 untuk a_{38}. Skema pemasukan

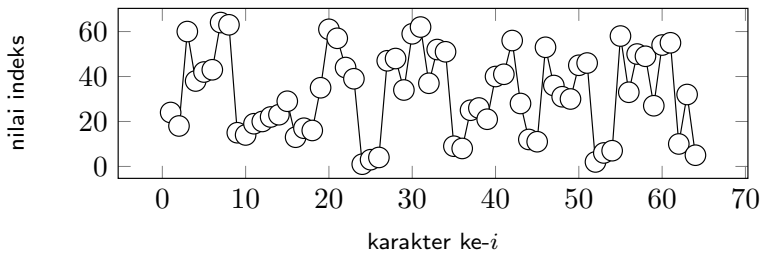
2 dan skema pengambilan bajak-sawah (kiri-kanan) menghasilkan indeks bit l_1 ={a_{64}, a_{35}, a_{58}, …, a_{63}}, l_2 ={a_{33}, a_{24}, a_{49}, …, a_{60}}, …, l_8 ={a_{05}, a_{44}, a_{06}, …, a_{38}}.

3.3.4 Skema Pengambilan Spiral

Skema pengambilan spiral merupakan skema pengambilan yang digunakan pada penelitian [10] mirip dengan skema pengambilan spiral pada penelitian [11]. Perbedaan terletak pada arah indeks, dimana indeks pada skema pengambilan ini dimulai dari luar kiri-atas kotak skema dan berakhir di tengah kotak skema. Indeks pada skema ini diawali dari kiri-atas kotak skema dan berakhir di tengah kotak skema. Kombinasi indeks dan grafik indeks skema pemasukan 1 dan pengambilan spiral secara lengkap tertera pada Gambar 16 dan Gambar 17.

$a_{24(01)}$	$a_{43(06)}$	$a_{29(15)}$	$a_{48(28)}$	$a_{34(29)}$	$a_{13(16)}$	$a_{64(07)}$	$a_{18(02)}$
$a_{42(05)}$	$a_{23(14)}$	$a_{47(27)}$	$a_{28(43)}$	$a_{12(44)}$	$a_{59(30)}$	$a_{17(17)}$	$a_{63(08)}$
$a_{22(13)}$	$a_{04(26)}$	$a_{56(42)}$	$a_{07(54)}$	$a_{58(55)}$	$a_{11(45)}$	$a_{62(31)}$	$a_{16(18)}$
$a_{03(25)}$	$a_{41(41)}$	$a_{06(53)}$	$a_{55(61)}$	$a_{10(62)}$	$a_{33(56)}$	$a_{53(46)}$	$a_{37(32)}$
$a_{40(40)}$	$a_{02(52)}$	$a_{54(60)}$	$a_{05(64)}$	$a_{32(63)}$	$a_{50(57)}$	$a_{36(47)}$	$a_{52(33)}$
$a_{01(24)}$	$a_{21(39)}$	$a_{46(51)}$	$a_{27(59)}$	$a_{49(58)}$	$a_{31(48)}$	$a_{51(34)}$	$a_{35(19)}$
$a_{20(12)}$	$a_{39(23)}$	$a_{26(38)}$	$a_{45(50)}$	$a_{30(49)}$	$a_{09(35)}$	$a_{61(20)}$	$a_{15(09)}$
$a_{38(04)}$	$a_{19(11)}$	$a_{44(22)}$	$a_{25(37)}$	$a_{08(36)}$	$a_{57(21)}$	$a_{14(10)}$	$a_{60(03)}$

Gambar 16. Indeks skema pemasukan 1 dan pengambilan spiral



Gambar 17. Grafik indeks skema pemasukan 1 dan pengambilan spiral

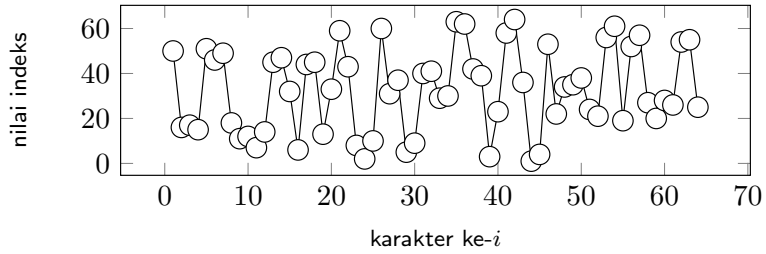
Hasil kombinasi indeks skema pemasukan 1 dan skema pengambilan spiral dimulai dari a_{24}, dimana indeks pengambilan j = 01 hingga j = 64 untuk a_{05}. Keluaran indeks bit pada *bytes* cipherteks yang dihasilkan meliputi l_1 ={a_{24}, a_{18}, a_{60}, …, a_{63}}, l_2 ={a_{15}, a_{14}, a_{19}, …, a_{13}}, …, l_8 ={a_{50}, a_{49}, a_{27}, …, a_{05}}.

3.3.5 Skema Pengambilan Zig-zag

Skema pengambilan zig-zag merupakan skema pengambilan yang mengarah dari kiri ke bawah kotak dan dimulai dari kiri-bawah kotak hingga ke kanan-atas kotak. Kombinasi indeks dan grafik indeks skema pemasukan 3 dan pengambilan zig-zag secara lengkap tertera pada Gambar 18 dan Gambar 19.

$a_{05(29)}$	$a_{42(37)}$	$a_{01(44)}$	$a_{38(50)}$	$a_{19(55)}$	$a_{20(59)}$	$a_{54(62)}$	$a_{25(64)}$
$a_{43(22)}$	$a_{09(30)}$	$a_{39(38)}$	$a_{04(45)}$	$a_{24(51)}$	$a_{52(56)}$	$a_{28(60)}$	$a_{55(63)}$
$a_{06(16)}$	$a_{08(23)}$	$a_{40(31)}$	$a_{03(39)}$	$a_{53(46)}$	$a_{21(52)}$	$a_{57(57)}$	$a_{26(61)}$
$a_{07(11)}$	$a_{44(17)}$	$a_{02(24)}$	$a_{41(32)}$	$a_{23(40)}$	$a_{22(47)}$	$a_{56(53)}$	$a_{27(58)}$
$a_{49(07)}$	$a_{14(12)}$	$a_{45(18)}$	$a_{10(25)}$	$a_{29(33)}$	$a_{58(41)}$	$a_{34(48)}$	$a_{61(54)}$
$a_{15(04)}$	$a_{18(08)}$	$a_{45(13)}$	$a_{13(19)}$	$a_{60(26)}$	$a_{30(34)}$	$a_{64(42)}$	$a_{35(49)}$
$a_{16(02)}$	$a_{51(05)}$	$a_{11(09)}$	$a_{47(14)}$	$a_{33(20)}$	$a_{31(27)}$	$a_{63(35)}$	$a_{36(43)}$
$a_{50(01)}$	$a_{17(03)}$	$a_{46(06)}$	$a_{12(10)}$	$a_{32(15)}$	$a_{59(21)}$	$a_{37(28)}$	$a_{62(36)}$

Gambar 18. Indeks skema pemasukan 3 dan pengambilan zig-zag



Gambar 19. Grafik indeks skema pemasukan 3 dan pengambilan zig-zag

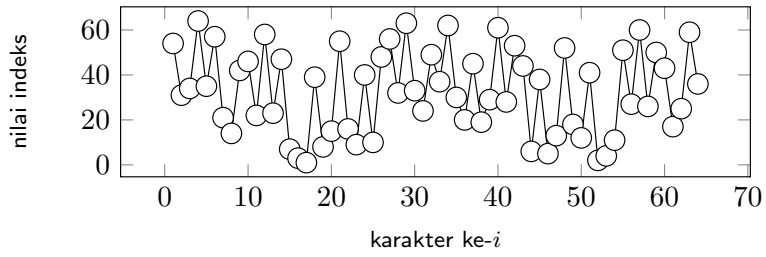
Hasil kombinasi indeks skema pemasukan 3 dan skema pengambilan zig-zag dimulai dari a_{50}, dimana indeks pengambilan $j = 01$ hingga $j = 64$ untuk a_{25}. Keluaran indeks bit pada *bytes* cipherteks yang dihasilkan meliputi $l_1 = \{a_{50}, a_{16}, a_{17}, \ldots, a_{18}\}$, $l_2 = \{a_{11}, a_{12}, a_{07}, \ldots, a_{06}\}$, $\ldots$, $l_8 = \{a_{57}, a_{27}, a_{20}, \ldots, a_{25}\}$.

3.3.6 Skema Pengambilan Tanam Padi

Skema pengambilan tanam padi merupakan skema pengambilan dengan urutan indeks mengikuti pola petani menanam padi yang dimulai dari tengah-kiri dan berakhir di kanan-atas kotak skema. Kombinasi indeks dan grafik indeks skema pemasukan 2 dan pengambilan tanam padi secara lengkap tertera pada Gambar 20 dan Gambar 21.

$a_{37(33)}$	$a_{61(40)}$	$a_{28(41)}$	$a_{52(48)}$	$a_{18(49)}$	$a_{27(56)}$	$a_{60(57)}$	$a_{36(64)}$
$a_{62(34)}$	$a_{29(39)}$	$a_{53(42)}$	$a_{13(47)}$	$a_{12(50)}$	$a_{51(55)}$	$a_{26(58)}$	$a_{59(63)}$
$a_{30(35)}$	$a_{19(38)}$	$a_{44(43)}$	$a_{05(46)}$	$a_{41(51)}$	$a_{11(54)}$	$a_{50(59)}$	$a_{25(62)}$
$a_{20(36)}$	$a_{45(37)}$	$a_{06(44)}$	$a_{38(45)}$	$a_{02(52)}$	$a_{04(53)}$	$a_{43(60)}$	$a_{17(61)}$
$a_{54(01)}$	$a_{14(08)}$	$a_{42(09)}$	$a_{03(16)}$	$a_{01(17)}$	$a_{40(24)}$	$a_{10(25)}$	$a_{49(32)}$
$a_{31(02)}$	$a_{21(07)}$	$a_{46(10)}$	$a_{07(15)}$	$a_{39(18)}$	$a_{09(23)}$	$a_{48(26)}$	$a_{24(31)}$
$a_{34(03)}$	$a_{57(06)}$	$a_{22(11)}$	$a_{47(14)}$	$a_{08(19)}$	$a_{16(22)}$	$a_{56(27)}$	$a_{33(30)}$
$a_{64(04)}$	$a_{35(05)}$	$a_{58(12)}$	$a_{23(13)}$	$a_{15(20)}$	$a_{55(21)}$	$a_{32(28)}$	$a_{63(29)}$

Gambar 20. Indeks skema pemasukan 2 dan pengambilan tanam padi



Gambar 21. Grafik indeks skema pemasukan 2 dan pengambilan tanam padi

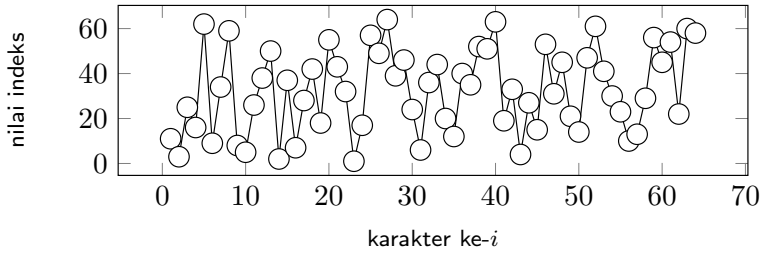
Hasil kombinasi indeks skema pemasukan 2 dan skema pengambilan tanam padi dimulai dari a_{54}, dimana indeks pengambilan $j = 01$ hingga $j = 64$ untuk a_{36}. Keluaran indeks bit pada *bytes* cipherteks yang dihasilkan meliputi $l_1 = \{a_{54}, a_{31}, a_{34}, \ldots, a_{14}\}$, $l_2 = \{a_{42}, a_{46}, a_{22}, \ldots, a_{03}\}$, $\ldots$, $l_8 = \{a_{60}, a_{26}, a_{50}, \ldots, a_{36}\}$.

3.3.7 Skema Pengambilan Acak

Skema pengambilan ini merupakan skema pengambilan yang digunakan pada penelitian [12], dengan urutan indeks acak. Kombinasi indeks dan grafik indeks skema pemasukan 3 dan pengambilan acak secara lengkap tertera pada Gambar 22 dan Gambar 23.

$a_{05(10)}$	$a_{42(18)}$	$a_{01(23)}$	$a_{38(12)}$	$a_{19(41)}$	$a_{20(34)}$	$a_{54(61)}$	$a_{25(03)}$
$a_{43(21)}$	$a_{09(06)}$	$a_{39(28)}$	$a_{04(43)}$	$a_{24(30)}$	$a_{52(38)}$	$a_{28(17)}$	$a_{55(20)}$
$a_{06(31)}$	$a_{08(09)}$	$a_{40(36)}$	$a_{03(02)}$	$a_{53(46)}$	$a_{21(49)}$	$a_{57(25)}$	$a_{26(11)}$
$a_{07(16)}$	$a_{44(33)}$	$a_{02(14)}$	$a_{41(53)}$	$a_{23(55)}$	$a_{22(62)}$	$a_{56(59)}$	$a_{27(44)}$
$a_{49(26)}$	$a_{14(50)}$	$a_{45(60)}$	$a_{10(56)}$	$a_{29(58)}$	$a_{58(64)}$	$a_{34(07)}$	$a_{61(52)}$
$a_{15(45)}$	$a_{18(19)}$	$a_{45(48)}$	$a_{13(57)}$	$a_{60(63)}$	$a_{30(54)}$	$a_{64(27)}$	$a_{35(37)}$
$a_{16(04)}$	$a_{51(39)}$	$a_{11(01)}$	$a_{47(51)}$	$a_{33(42)}$	$a_{31(47)}$	$a_{63(40)}$	$a_{36(32)}$
$a_{50(13)}$	$a_{17(24)}$	$a_{46(29)}$	$a_{12(35)}$	$a_{32(22)}$	$a_{59(08)}$	$a_{37(15)}$	$a_{62(05)}$

Gambar 22. Indeks skema pemasukan 3 dan pengambilan acak



Gambar 23. Grafik indeks skema pemasukan 3 dan pengambilan acak

Hasil kombinasi indeks skema pemasukan 3 dan skema pengambilan acak dimulai dari a_{11}, dimana indeks pengambilan $j = 01$ hingga $j = 64$ untuk a_{36}. Keluaran indeks bit pada *bytes* cipherteks yang dihasilkan meliputi $l_1 = \{a_{11}, a_{03}, a_{25}, \ldots, a_{59}\}$, $l_2 = \{a_{08}, a_{05}, a_{26}, \ldots, a_{07}\}$, $\ldots$, $l_8 = \{a_{13}, a_{29}, a_{56}, \ldots, a_{58}\}$.

3.4 Hasil Uji Keacakan

Pengujian keacakan pada kombinasi skema pemasukan dan skema pengambilan dilakukan untuk mengetahui seberapa acak indeks yang dihasilkan. Setiap hasil uji dikatakan acak apabila *P-value* yang dihasilkan $\geq \alpha$, dimana $\alpha = 0.01$ [19, 20, 21]. Hasil pengujian keacakan terhadap tiga skema pemasukan diatonis mayor tertera pada Tabel 2.

Tabel 2. Hasil uji keacakan modifikasi skema pemasukan

No.	Kombinasi Skema (Pemasukan-Pengambilan)	*P-value*			Mean
		Monobit	*Block Bit*	*Runs*	
1.	1 & horizontal (kiri-kanan)	1.0000	0.0591	0.2113	0.4235
2.	1 & vertikal (atas-bawah)	1.0000	0.0301	0.8026	0.6109
3.	1 & zig-zag	1.0000	0.9810	0.0801	0.6870
4.	1 & bajak sawah (kanan-kiri)	1.0000	0.8571	0.0244	0.6272
5.	1 & spiral	1.0000	0.7576	0.0124	0.5900
6.	2 & horizontal (kanan-kiri)	1.0000	0.8571	0.2113	0.6895
7.	2 & horizontal (kiri-kanan)	1.0000	0.8571	0.2113	0.6895
8.	2 & vertikal (atas-bawah)	1.0000	0.0103	0.6171	0.5425
9.	2 & vertikal (bawah-atas)	1.0000	0.0103	0.3173	0.4425
10.	2 & zig-zag	1.0000	0.9344	0.0801	0.6715
11.	2 & bajak sawah (kanan-kiri)	1.0000	0.8571	1.0000	0.9524
12.	2 & bajak sawah (kiri-kanan)	1.0000	0.5366	0.8026	0.7797
13.	2 & alur tanam padi	1.0000	0.9810	0.2113	0.7308
14.	3 & horizontal (kiri-kanan)	0.8026	0.9617	0.6112	0.7919
15.	3 & vertikal (atas-bawah)	0.8026	0.8992	0.7964	0.8327
16.	3 & zig-zag	0.8026	0.8992	0.6112	0.7710
17.	3 & bajak sawah (kanan-kiri)	0.8026	0.2317	0.6222	0.5522
18.	3 & acak	0.8026	0.4838	0.6222	0.6362

Berdasarkan hasil uji keacakan pada Tabel 2, skema pemasukan spiral diatonis mayor dan skema pengambilan bajak sawah memperoleh rata-rata *P-value* tertinggi, yaitu 0.9524. Sedangkan *P-value* terendah diha-

silkan oleh kombinasi skema pemasukan papan catur diatonis mayor dan skema pengambilan horizontal, yaitu sebesar 0.4235. Secara keseluruhan hasil modifikasi skema pemasukan papan catur, spiral dan cermin memenuhi kriteria acak.

3.5 Perbandingan Uji Keacakan

Perbandingan pengujian uji keacakan terhadap penelitian terdahulu dilakukan untuk mengetahui skema transposisi paling optimal antara skema pemasukan penelitian terdahulu dan modifikasinya. Tabel 3 merupakan hasil rata-rata uji keacakan untuk membandingkan skema penelitian terdahulu terhadap skema modifikasi.

Tabel 3. Perbandingan uji keacakan penelitian terdahulu terhadap skema modifikasi

No.	Skema Pemasukan	*P-value*			Mean
		Monobit	*Block Bit*	*Runs*	
1.	Papan Catur Diatonis Mayor	1.0000	0.5370	0.2262	0.5877
2.	Papan Catur [10]	1.0000	0.9003	0.6043	0.8348
3.	Spiral Diatonis Mayor	1.0000	0.6305	0.4314	0.6873
4.	Spiral [11]	0.7675	0.8998	0.0000	0.5557
5.	Cermin Diatonis Mayor	0.8026	0.6951	0.6527	0.7168
6.	Cermin [12]	0.1646	0.1747	0.1882	0.1758

Tabel 3 menunjukan modifikasi skema spiral dan cermin menghasilkan uji keacakan yang lebih baik dibandingkan dengan skema aslinya. Namun hasil uji keacakan pada modifikasi skema papan catur memperoleh nilai rata-rata 0.5877, tidak melampaui skema aslinya yang memperoleh nilai rata-rata 0.8348.

3.6 Perbandingan Uji Korelasi

Uji korelasi dilakukan untuk mengetahui tingkatan hubungan antara plaintext (x) dan ciphertext (y) dari algoritma yang telah dirancang. Dalam konteks kriptografi, nilai korelasi korelasi yang baik adalah r yang mendekati angka 0 [18]. Hasil perbandingan uji korelasi penelitian terdahulu terhadap modifikasi skema pengambilan diatonis mayor tertera pada tabel 4.

Tabel 4. Hasil uji korelasi

No.	Skema Pemasukan	Mean
1.	Modifikasi papan catur	0.2625
2.	Papan Catur [10]	0.3002
3.	Modifikasi spiral	0.3329
4.	Spiral [11]	0.3321
5.	Modifikasi cermin	0.2794
6.	Cermin [12]	0.5994

Plainteks yang digunakan pada masing-masing modifikasi skema adalah plainteks yang berbeda, menyesuaikan plainteks yang digunakan pada penelitian terdahulu. Pada skema pengambilan papan catur diatonis mayor menggunakan plainteks "gluttony", "deeeeeee" serta "$uR4b4Y4" sebagaimana yang digunakan pada uji korelasi penelitian [10]. Kemudian, pada skema spiral diatonis mayor menggunakan plainteks "magelang", "xxxxxxxy" serta "$Em4r@n9". Sedangkan pada skema cermin diatonis mayor menggunakan plainteks "bom atom", "ooooooop" serta "fT1 Uk$w".

4. Simpulan

Penelitian ini berhasil memodifikasi skema papan catur, skema spiral dan skema cermin dengan menerapkan aturan urutan indeks skema asli dan aturan kotak skema diatonis mayor. Hasil statistik menunjukan bahwa dua dari tiga modifikasi yang dilakukan pada skema pemasukan papan catur, spiral dan cermin

terbukti menghasilkan nilai keacakan yang lebih optimal. Namun pada modifikasi skema papan catur diatonis mayor tidak dapat menghasilkan nilai keacakan yang lebih optimal dibandingkan skema pemasukan papan catur. Hal ini ditunjukan pada skema papan catur menghasilkan rata-rata nilai keacakan sebesar 0.8348. Sedangkan pada modifikasi skema pemasukan tersebut hanya mampu menghasilkan rata-rata nilai keacakan sebesar 0.5877. Secara keseluruhan, skema pemasukan cermin mayor diatonis lebih optimal dalam menyamarkan plainteks dengan memperoleh nilai korelasi dibandingkan dengan skema cermin biasa. Penyamaran plainteks paling optimal dihasilkan pada modifikasi skema papan catur dengan nilai korelasi sebesar 0.2625, sedangkan skema papan catur hanya memperoleh nilai korelasi sebesar 0.3002.

Temuan penelitian ini memiliki beberapa implikasi penting bagi pengembangan algoritma *square transposition* dalam merancang skema pemasukkan atau skema pengambilan. Pertama, jika hasil perbandingan menunjukan bahwa integrasi tangga nada diatonis mayor memiliki karakteristik keacakan yang lebih baik, maka pendekatan tersebut dapat mengindikasikan bahwa konsep dari teori musik dapat menjadi sumber inspirasi yang valid dan efektif untuk merancang pola permutasi yang kompleks dan sulit diprediksi. Hal ini membuka perspektif baru selain menggunakan pendekatan geometris atau visual umum yang digunakan dalam merancang skema transposisi.

Meskipun demikian, penelitian ini hanya berfokus pada perancangan dan analisis algoritma *square transposition* dengan integrasi tangga nada diatonis mayor berukuran 8×8 (64-bit). Transposisi yang dilakukan pada tingkatan ini merupakan operasi tunggal, yaitu hanya mengacak posisi bit. Untuk mencapai tingkat keamanan yang lebih tinggi, diperlukan metode kriptografi yang lebih kompleks, umumnya melibatkan kombinasi berbagai operasi seperti subtitusi, permutasi dan operasi lainnya yang dilakukan dengan beberapa putaran.

Berdasarkan temuan awal dan keterbatasan yang diidentifikasi, algoritma *square transposition* dapat dikembangkan lebih lanjut. Misalnya, merancang pola-pola baru yang lebih kompleks dalam mengatur indeks pada skema pemasukkan dan skema pengambilan, serta penting untuk dilakukan studi dengan penggunaan ukuran kotak skema yang berbeda. Selain itu, metode ini dapat diintegrasikan atau memodifikasi pada algoritma yang telah ada, seperti mengganti atau menambah komponen proses enkripsi pada AES, DES atau algoritma lainnya.

Pustaka

[1] M. Tarawneh, "Cryptography: Recent Advances and Research Perspectives," *IntechOpen*, 2023.

[2] Khairani and M. Z. Siambaton, "Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker," *Sudo Jurnal Teknik Informatika*, vol. 2, no. 4, pp. 176–187, 2023.

[3] M. Hidayat, M. Tahir, and A. Sukriyadi, "PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA," *Jurnal Ilmiah Multidisiplin*, vol. 2, pp. 35–41, 2023.

[4] J. Dagadu, A. Armah, E. O. Aboagye, and S. A. Mansuru, "Rubik's Cube Enhanced Columnar Transposition Cipher," *Journal of Computer Sciences and Applications*, vol. 12, pp. 31–37, 2024.

[5] B. Thakkar, "A Comprehensive Study of Substitution and Transposition Techniques in Cryptographic Systems," *International Journal of Computer Science Trends and Technology*, vol. 13, pp. 15–19, 2025.

[6] A. Armah, S. Asare, and A.-M. Eric, "Enhancing Security in Modern Transposition Ciphers Through Algorithmic Innovations and Advanced Cryptanalysis," *Indonesian Journal of Computer Science*, vol. 13, no. 3, pp. 4391–4412, 2024.

[7] M. A. I. Pakereng and A. D. Wowor, "Square transposition: an approach to the transposition process in block cipher," *Bulletin of Electrical Engineering and Informatics*, vol. 10, pp. 3385–3392, 2021.

[8] J. Daemen and V. Rijmen, "The Design of Rijndael: The Advanced Encryption Standard (AES)," *Springer Berlin, Heidelberg*, 2020.

[9] A. Biryukov and C. D. Cannière, "Data Encryption Standard (DES)," *Springer, Cham*, 2025.

[10] W. R. Umar and A. D. Wowor, "Perancangan Algoritma Square Transposisi Dengan Skema Papan Catur," *Skripsi S-1 Teknik Informatika, FTI UKSW*, 2024.

[11] H. Patiung and A. D. Wowor, "Perancangan Algoritma Square Transposisi Dengan Skema Spiral," *INOVTEK Polbeng - Seri Informatika*, vol. 9, no. 2, pp. 878–889, 2024.

[12] J. P. A. Wawoh and A. D. Wowor, "Implementasi Pola Pembiasan Cermin dalam Merancang Algoritma Square Transposisi," *Skripsi S-1 Teknik Informatika, FTI UKSW*, 2024.

[13] K. A. Lestari, N. Kusumastuti, and F. Fran, "Penerapan Fungsi Transposisi Modulo Terhadap Perpindahan Nada Dasar Pada Tangga Nada Diatonis Mayor," *Bimaster*, vol. 12, no. 4, pp. 309–318, 2023.

[14] S. A. Priatna, "Peran Pemanasan Menggunakan Teknik Scale Mayor Dan Minor terhadap Pembelajaran Instrumen Piano bagi Anak-Anak," *Tamumatra: Jurnal Seni Pertunjukan*, vol. 7, no. 1, pp. 39–51, 2024.

[15] Y. Wajongkere, J. Titaley, and Y. A. Langgi, "Fungsi Transposisi Modulo dan Penerapannya Pada Pencarian Susunan Tangga Nada dan Tingkatan Akor," *d'Cartesian*, vol. 8, no. 1, pp. 11–17, 2019.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *National Institute of Standards and Technology*, 2010.

[17] A. Ramadhani and A. D. Wowor, "Modifkasi LFSR Dengan Skema A5/1 Dengan Variasi Fungsi XOR Pada Fungsi Umpan Balik," *JIKO (Jurnal Informatika dan Komputer)*, vol. 8, no. 1, pp. 161–173, 2024.

[18] J. T. K. Pallangan, "Identifikasi Nilai Keacakan berdasarkan Reposisi Fungsi XOR pada Blok Kedua LFSR A5/1," *Journal of Information System Research (JOSH)*, vol. 6, no. 1, pp. 679,687, 2024.

[19] R. M. Nafurbenan and A. D. Wowor, "Perancangan Enam Bagan Fungsi XOR sebagai Umpan Balik dalam Pembangkit Bilangan Acak LFSR dengan Skema A5/1," *Skripsi S-1 Teknik Informatika, FTI UKSW)*, 2022.

[20] T. S. Nahading and A. D. Wowor, "Desain Pembangkit Kunci LFSR dengan Skema A5/1 Menggunakan empat Blok Bit Fungsi XOR," *KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)*, vol. 4, no. 2, pp. 409–419, 2023.

[21] S. Angelina and A. D. Wowor, "Optimasi Pembangkit Bilangan Acak Dengan Fungsi Polinomial dan Kombinasi Metode Iterasi," *JIKO (Jurnal Informatika dan Komputer)*, vol. 8, no. 2, p. 367–379, 2025.