# Implementasi XOR Guna Peningkatan Enkripsi Teks Menggunakan Rotasi Multi Kubus

*XOR Implementation to Improve Text Encryption Using Multi Cube Rotation*

Rihartanto[1], Didi Susilo Budi Utomo[2], AnsarRizal[3]
[1,2,3]Jurusan Teknologi Informasi, Politeknik Negeri Samarinda
E-mail: [1]rihart.c@gmail.com, [2]dsbudiutomo10@gmail.com, [3]ansardeuy@gmail.com

**Abstrak**

Meluasnya penggunaan internet semakin memudahkan seseorang untuk mendapatkan informasi. Kemudahan akses ini membuka peluang perilaku illegal dalam memperoleh dan atau penyebaran informasi. Karenanya pengamanan informasi menjadi faktor krusial saat ini. Dalam penelitian ini operasi XOR menggunakan bilangan acak digunakan untuk meningkatkan hasil enkripsi teks menggunakan rotasi multi kubus. Hasil pengujian menunjukkan terjadi peningkatan yang signifikan. Nilai korelasi meningkat sebesar 82%, Nilai MAE meningkat sebesar 77% dan nilai AE meningkat sebesar 44%. Peningkatan ini menunjukkan penggunaan XOR pada rotasi multi kubus mampu memenuhi kriteria difusi dan konfusi sebagai karakteristik kriptografi yang baik.

**Kata kunci**: rotasi kubus, multi kubus, XOR

***Abstract***

*The widespread use of the internet makes it easier for people to get information. This ease of access opens up opportunities for illegal behavior in obtaining and/or disseminating information. Therefore, information security is a crucial factor today. In this research, the XOR operation using random numbers improves text encryption results using multi-cube rotation. The test results show that there has been a significant increase. The correlation value increased by 82%, the MAE value increased by 77%, and the AE value increased by 44%. This improvement shows that the use of XOR in the multi-cube rotation can fulfill the diffusion and confusion criteria as characteristics of good cryptographic techniques.*

***Keywords****: cube rotation, multi-cube, XOR*

## 1. PENDAHULUAN

Informasi merupakan komoditas penting yang perlu dilindungi. Bukan hanya kontennya, saluran atau media yang digunakan untuk menyebarkan informasi juga perlu mendapat pengamanan. Meluasnya penggunaan internet semakin memudahkan seseorang atau pihak tertentu untuk mendapatkan informasi. Kemudahan akses ini membuka peluang penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab dalam melakukan tindakan ilegal seperti peretasan data sensitif atau penyebaran informasi hoax.

Keamanan informasi merupakan aspek penting yang memerlukan perhatian serius. Salah satunya adalah dengan memanfaatkan teknik kriptografi. Kriptografi adalah suatu seni atau ilmu yang digunakan untuk mengamankan atau melindungi data dan informasi[1][2]. Tujuannya tentu saja untuk mengamankan informasi dari pengguna yang tidak berwenang, dalam konteks hanya mereka yang mempunyai izin yang sesuai yang dapat mengakses isi suatu informasi. Proses kriptografi terbagi menjadi dua bagian, yaitu proses enkripsi dan dekripsi. Kedua proses tersebut biasanya memerlukan kata kunci, dimana kata kunci tersebut bisa simetris atau asimetris [3] tergantung pada teknik kriptografi yang digunakan.

Merujuk pada pendapat Claude Shannon, ahli teori informasi dalam laporan rahasianya tahun 1945, ada dua sifat penting dalam algoritma enkripsi yang kuat [4]–[6], yaitu konfusi dan

difusi. Konfusi adalah operasi enkripsi di mana hubungan antara kunci dan teks tersandi dikaburkan. Sementara difusi adalah operasi enkripsi di mana pengaruh satu simbol teks biasa tersebar ke banyak simbol teks tersandi dengan tujuan menyembunyikan properti statistik teks biasa. Sederhananya, konfusi mengakibatkan perubahan bentuk, sementara difusi mengakibatkan perpindahan posisi.

Transposisi adalah teknik yang memenuhi sifat difusi. Pada transposisi suatu unsur mengalami perpindahan dari posisi awal ke posisi lain. Tidak ada perubahan pada data, namun perpindahan tersebut dapat menghasilkan urutan data yang berbeda dari aslinya. Ada beberapa teknik transposisi yang banyak digunakan dalam enkripsi data, antara lain transposisi zigzag [11], transposisi kolumnar [7]–[9] dan transposisi ganda [10].Teknik ini dapat digunakan baik untuk enkripsi teks[7], [8], [12], citra[13] atau audio[14].

Dalam ruang tiga dimensi, transposisi dilakukan dengan menggunakan bentuk kubus [15], [16] meniru prinsip permainan Rubik[17]–[19]. Dalam implementasinya terdapat dua cara untuk menempatkan data ke dalam kubus, yang pertama pada sisi luar kubus seperti pada permainan Rubik [15], [16], [20] dan yang kedua dengan menganggap kubus sebagai array 3D [21] sehingga mampu menampung data dalam jumlah yang lebih banyak. Dalam banyak penelitian, rotasi kubus digunakan untuk mengenkripsi citra, sehingga data yang dienkripsi merupakan nilai intensitas piksel yang berada pada ruang nilai 0 hingga 225. Untuk meningkatkan hasil enkripsi pada citra, ada yang mengombinasikan rotasi kubus ini menggunakan transformasi Fourier, metoda sebaran logistic dan chaotic map.

Berbeda dengan penelitian-penelitian tersebut, pada penelitian ini data yang dienkripsi berupa karakter teks yang berada pada rentang nilai ASCII 0 hingga 127. Transposisi yang dilakukan berupa rotasi kubus menggunakan sejumlah kubus yang memiliki beragam ukuran. Setiap elemen kubus diisi dengan satu karakter. Rotasi kubus mengikuti sumbu X, Y, dan Z. Untuk memenuhi kriteria konfusi, dilakukan operasi XOR agar data hasil enkripsinya berada pada rentang nilai ASCII 0 hingga 255. Tujuan dari penelitian ini adalah untuk menghasilkan hasil enkripsi yang memenuhi dua sifat kriptografi yaitu difusi dan konfusi.

## 2. METODE PENELITIAN

Secara garis besar, metode yang digunakan di sini dapat dibedakan menjadi tiga bagian. Yaitu rotasi kubus untuk melakukan transposisi, operasi XOR untuk meningkatkan hasil transposisi, dan penentuan ukuran-ukuran kubus yang digunakan dalam rotasi serta penentuan nilai awal untuk operasi xor pada setiap hasil rotasi kubus.

### *2.1 Rotasi Kubus*

Rotasi kubus mirip dengan rotasi bujursangkar. Perbedaannya rotasi kubus bekerja dalam ruang tiga dimensi sementara rotasi bujursangkar bekerja dalam ruang dua dimensi[23]. Rotasi dapat dilakukan searah dengan jarum jam (clock wise—CW) atau berlawanan arah dengan jarum jam (counter clock wise—CCW). Jarak putar dalam satu rotasi adalah perpindahan sejauh 90 derajat dengan titik tengah kubus sebagai pusat rotasi.

Pada kubus, rotasi dapat dilakukan pada satu sumbu, dua sumbu atau tiga sumbu. Arah rotasi kubus pada setiap sumbu diilustrasikan pada Gambar 1. Secara matematis, perpindahan elemen array dalam rotasi kubus mengikuti persamaan (1), (2), (3), (4), (5) dan (6)[22]. xCW dan xCCW adalah rotasi pada sumbu x, yCW dan yCCW adalah rotasi pada sumbu y, serta zCW dan zCCW adakah rotasi pada sumbu z.

$$xCW[i,j,k] = X[n-j-1,i,k] \quad (1)$$

$$xCCW[i,j,k] = X[j,n-i-1,k] \quad (2)$$

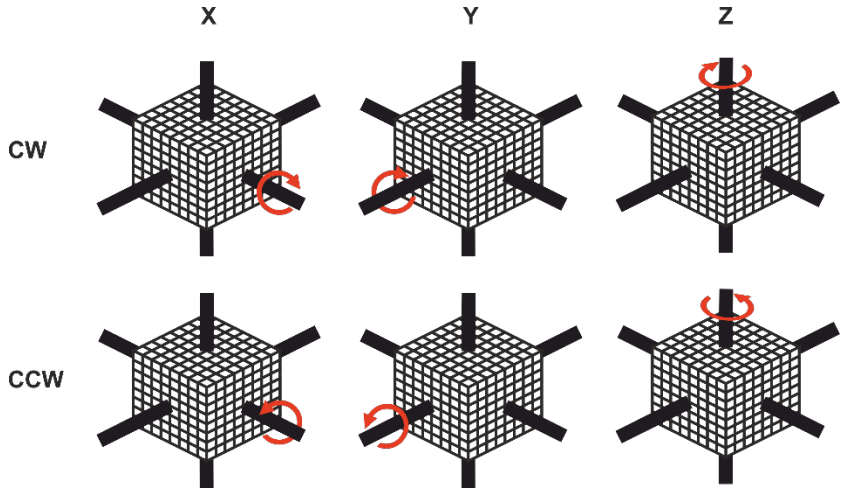
$$yCW[i,j,k] = X[n-k-1,j,i] \quad (3)$$

$$yCCW[i,j,k] = X[k,j,n-i-1] \quad (4)$$

$$zCW[i,j,k] = X[i,n-k-1,j] \quad (5)$$

$$zCCW[i,j,k] = X[i,k,n-j-1] \quad (6)$$

Jika rotasi dilakukan pada sumbu yang sama, dua kali rotasi CW akan memberikan hasil yang sama dengan dua kali rotasi CCW. Sementara empat kali rotasi pada arah yang sama akan memberikan hasil yang sama dengan sebelum dilakukan rotasi. Demikian pula, satu rotasi CW memberikan hasil yang sama dengan tiga kali rotasi CCW dan satu rotasi CCW memberikan hasil yang sama dengan tiga kali rotasi CW. Dari sudut pandang ini, untuk tujuan meminimalkan jumlah perpindahan data dalam array, hanya ada 3 rotasi yang memberikan hasil yang berbeda yaitu CW, CCW dan 2CW atau 2CCW.




Gambar 1 Ilustrasi arah rotasi kubus pada setiap sumbu

Perpindahan elemen sejauh 2CW atau 2CCW pada sumbu x, y dan z mengikuti persamaan (7), (8) dan (9). Ketiga formula ini digunakan sebagai alternatif untuk meminimalkan jumlah perpindahan elemen dalam array pada saat rotasi. Karena perpindahan sejauh 180 derajat juga dapat dihasilkan dari dua kali rotasi CW atau dua kali rotasi CCW sesuai dengan sumbu kubus yang diberikan.

$$x2CW[i,j,k] = X[n-i-1,n-j-1,k] \quad (7)$$

$$y2CW[i,j,k] = X[n-i-1,j,n-k-1] \quad (8)$$

$$z2CW[i,j,k] = X[i,n-j-1,n-k-1] \quad (9)$$

*2.2 Operasi XOR dengan Bilangan Acak*

Data teks berada pada domain ASCII standar yang memilik nilai ASCII antara 0 sampai dengan 127. Data teks yang dimaksud di sini adalah karakter berupa angka, huruf dan simbol serta beberapa karakter kontrol seperti tab dan enter. Operasi XOR digunakan untuk mengubah domain dari teks tersebut agar nilainya berada pada rentang nilai ASCII 0 hingga 255, yang berarti meningkatkan variasi dari hasil enkripsi.

Dalam penelitian ini operasi XOR dilakukkan dengan memanfaatkan bilangan acak yang dibangkitkan menggunakan Pseudo Random Number Generator (PRNG). Hasil enkripsi adalah data yang dihasilkan dari operasi XOR antara teks asli dengan bilangan random. Sedangkan hasil dekripsi adalah hasil operasi XOR antara teks hasil enkripsi dengan bilangan random.

Misalkan isi pesan yang akan dienkripsi adalah “Hujan”, artinya dibutuhkan lima buah angka untuk melakukan operasi XOR yang bernilai antara 0 sampai 255. Misalkan nilai acak yang diperoleh dari PRNG untuk karakter pertama adalah 253 maka empat bilangan lainnya adalah penambahan nilai 1 dari bilangan tersebut kemudian melakukan operasi modulus 256 untuk mempertahankan nilainya berada pada rentang 0 hingga 255. Ilustrasi operasi enkripsi dan dekripsi ditunjukkan pada Gambar 2. Hasil enkripsi diperoleh dari operasi XOR antara pesan dengan bilangan acak, sementara hasil dekripsi diperoleh dari operasi XOR antara hasil enkripsi dengan bilangan acak.

| **Proses Enkripsi** | | | | | |
|---|---|---|---|---|---|
| Pesan | H | u | j | a | n |
| ASCII | 72 | 117 | 106 | 97 | 110 |
| Angka acak | 253 | 254 | 255 | 0 | 1 |
| Pesan | 01001000 | 01110101 | 01101010 | 01100001 | 01101110 |
| Angka acak | 11111101 | 11111110 | 11111111 | 00000000 | 00000001 |
| XOR | 10110101 | 10001011 | 10010101 | 01100001 | 01101101 |
| ASCII | 181 | 139 | 149 | 97 | 109 |
| Hasil enkripsi | µ | ‹ | • | a | m |

| **Proses Dekripsi** | | | | | |
|---|---|---|---|---|---|
| Hasil enkripsi | µ | ‹ | • | a | m |
| ASCII | 181 | 139 | 149 | 97 | 109 |
| Angka acak | 253 | 254 | 255 | 0 | 1 |
| Pesan | 10110101 | 10001011 | 10010101 | 01100001 | 01101101 |
| Angka acak | 11111101 | 11111110 | 11111111 | 00000000 | 00000001 |
| XOR | 01001000 | 01110101 | 01101010 | 01100001 | 01101110 |
| ASCII | 72 | 117 | 106 | 97 | 110 |
| Hasil dekripsi | H | u | j | a | n |

Gambar 2. Ilustrasi enkripsi dan dekripsi dengan operasi XOR

PRNG digunakan untuk mendapatkan bilangan acak pertama. PRNG diaktifkan menggunakan nilai *seed* (bibit) tertentu yang diperoleh dari kunci enkripsi yang dimasukkan. *Seed* dihitung dengan cara menjumlahkan nilai ASCII setiap karakter kunci yang dikalikan pangkat dua posisinya masing-masing. Misalkan kunci yang diberikan adalah “ab12”. Nilai ASCII untuk setiap karakater dalam kunci tersebut berturut-turut adalah 97, 98, 49 dan 50. Maka nilai seed yang diperoleh dari kunci tersebut adalah ((97× (1^2)) + (98× (2^2)) + (49× (3^2)) + (50× (4^2))) yaitu 1730. Cara menentukan *seed* seperti ini bertujuan agar diperoleh nilai yang berbeda jika kunci yang diberikan memiliki karakter yang sama namun memiliki urutan yang berbeda. Sehingga “12ab” akan menghasilkan nilai 2690 dan “a1b2” menghasilkan nilai 1975.

Operasi XOR untuk peningkatan hasil enkripsi transposisi ditunjukkan pada Algortima 1. Sebagai input adalah teks asli (pada proses enkripsi) atau hasil enkripsi (pada proses dekripsi) dan angka acak. Operasi XOR dilakukan terhadap nilai ASCII dari setiap karakter dengan angka acak yang dikirim untuk karakter pertama. Untuk karakter berikutnya, angka acak ini ditambahkan dengan satu, namun tetap dijaga agar nilanya tetap berada pada rentang 0 sampai 255 menggunakan operasi modulus.

### *2.3 Multi Kubus*

Multi kubus yang dimaksud disini adalah penggunaan lebih dari satu kubus dengan ukuran yang sama dan atau berbeda pada operasi transposisi karakter. Ukuran kubus dipilih secara acak berdasarkan jumlah karakter yang tersedia, dengan asumsi bahwa setiap kubus harus terisi penuh. Jika sisi kubus bernilai 2 maka jumlah karakter yang dapat di tampung adalah 8 yang diperoleh

dari perkalian 2×2×2, jika sisi bernilai 3 maka kapasitasnya adalah 27 yang diperoleh dari perkalian 3×3×3 dan seterusnya. Ukuran sisi kubus berada pada rentang 1 hingga ukuran maksimal yang dipilih atau ukuran maksimal yang memungkinkan. Karena setiap kubus harus terisi penuh, maka ada kemungkinan terjadi penambahan karakter tertentu (padding) jika jumlah karakter yang tersedia kurang dari kapasitas tampung kubus.

Algoritma penentuan ukuran multi kubus dan penentuan angka acak untuk operasi XOR ditunjukkan pada Algortima 2. Misalkan teks yang akan dienkripsi terdiri dari 146 karakter, sementara ukuran sisi kubus maksimal yang diinginkan adalah 6 dan seed untuk bilangan random adalah 5250, maka akan diperoleh ukuran kubus berturut-turut [5,2,2,2] dan angka random untuk memulai operasi xor pada setiap kubus adalah [74, 97, 249, 168]. PRNG yang digunakan adalah randint pada pemrograman python. Pada contoh ini, ukuran 6 sebagai sisi kubus tidak dapat digunakan karena jumlah karakter yang tersedia tidak mencukupi. Karena itu dipilih ukuran lain yang lebih kecil antara 2 sampai 5 secara acak.

**Algoritma 1:** Operasi XOR

**Input**: plainteks, angka_random
**Output**: cipherteks

```
1.  Function xorTeks(plainteks, nrand)
2.  cipherteks ←""
3.  for karakter dalam plainteks
4.     nchr  ← ASC( karakter )
5.     cchr ← CHAR(nchr ⊕ nrand)
6.     cipherteks ← cipherteks + cchr
7.     nrand ← (nrand+1) % 256
8.  end for
9.  return cipherteks
```

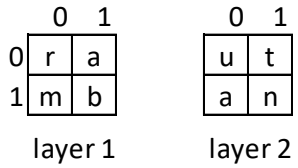
**Algoritma 2:** Penentuan ukuran kubus dan angka acak

**Input**: panjang teks, ukuran kubus maksimal, nilai seed
**Output**: list_ukuran_kubus, list_angka_random

```
1.  Function ukuranKubus(pjTeks, ukMaks, nSeed)
2.     listKubus ← [ ]
3.     listRandom ← [ ]
4.     ukKubus = 0
5.     aktifkan seed bilangan random
6.
7.     #tentukan ukuran kubus memungkinkan sesuai
8.     #jumlah karakter yang masih tersisa
9.     while pjTeks > 0
10.       while pjTeks >= ukMaks**3 and ukMaks >=2
11.          ukKubus = randint(2, ukMaks)
12.          tambahkan ukKubus ke listKubus
13.          pjTeks ← pjTeks – (ukKubus ^ 3)
14.
15.       ukMaks ← ukMaks -1
16.       if pjTeks>1 and pjTeks< 8
17.          tambahkan ukKubus=2 ke listKubus
18.          pjTeks ← 0
19.       else if pjTeks==1
20.          tambahkan ukKubus=1 ke listKubus
21.          pjTeks ← 0
22.
23.    #ambil nilai int 8bit utk xor pada setiap kubus
24.    for i=0 sampai i< length(listKubus)
25.       tambahkan randint(0,255) ke listRandom
26.
27.    return listKubus, listRandom
```

Dari ukuran sisi kubus yang diperoleh, kubus pertama diisi dengan 125 karakter, kubus kedua hingga ke empat masing-masing diisi dengan 8 karakter. Jika dijumlahkan seluruhnya terdiri dari 149 karakter. Hal ini menujukkan bahwa pada kubus terakhir terjadi penambahan sebanyak 3 karakter. Kondisi ini terjadi ketika jumlah karakter yang tersedia lebih dari satu dan kurang dari 8.

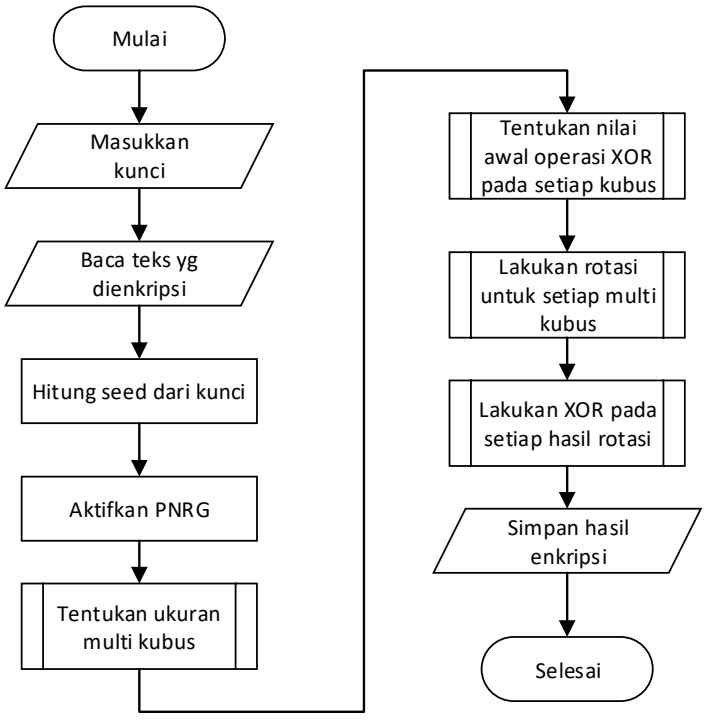
Pengisian karakter ke dalam kubus dilakukan dalam urutan baris, kolom dan layer. Misalkan kubus berukuran 2×2×2 akan diisi dengan teks “rambutan”. Jika indeks dimulai dari 0 sementara urutan koordinat elemen ditulis dalam urutan [baris, kolom, layer] maka pengisian dimulai dari posisi [0,0,0] , [0,1,0], [1,0,0], [1,1,0] hingga [1,1,1]. Cara yang sama digunakan untuk pembacaan karakter dari kubus setelah dilakukan rotasi. Ilustrasi pengisian teks tersebut di dalam kubus ditunjukkan pada Gambar 3.




Gambar 3. Ilustrasi penempatan teks “rambutan” di dalam kubus 2×2×2

## 3. HASIL DAN PEMBAHASAN

Tahapan proses enkripsi yang mengimplementasikan operasi XOR untuk peningkatan enkripsi mengunakan multi kubus ditunjukkan pada Gambar 4. Dimulai dengan memasukkan kata kunci serta membaca teks yang akan dienkripsi. Nilai seed yang digunakan untuk pembangkit bilangan random menggunakan PRNG dihitung dari nilai kunci yang dimasukkan. Selanjutnya menentukan ukuran-ukuran kubus yang digunakan dihitung berdasarkan jumlah karakter yang dari teks yang akan dienkripsi. Untuk setiap kubus juga ditentukan bilangan awal yang akan digunakan untuk melakukan operasi XOR. Proses enkripsi dilakukan per blok karakter, dimana ukuran blok disesuaikan dengan ukuran kubus. Pada blok terakhir, jika jumlah karakter lebih kecil dari kapasitas kubus maka dilakukan penambahan karakter (padding) menggunakan karakter NULL. Rotasi dilakukan menurut arah yang ditentukan untuk memperoleh hasil transposisi. Operasi XOR dilakukan pada hasil transposisi ini untuk mendapatkan teks hasil enkripsi.




Gambar 4. Tahapan proses enkripsi teks dengan XOR pada rotasi multi kunus

Teks yang digunakan sebagai bahan uji ditunjukkan pada Tabel 1 yang terdiri teks dalam bentuk kalimat biasa dan teks yang berisi frasa berulang. Keduanya memiliki jumlah karakter yang hampir sama dengan karakteristik yang berbeda. Rotasi kubus dilakukan pada setiap sumbu masing-masing satu kali. Rotasi yang dilakukan dapat CW (90° searah jarum jam), CCW (90° berlawanan arah jarum jam) atau 2CW (180°). Untuk tujuan pengujian, rotasi multi kubus

berturut-turut dilakukan pada sumbu X, Y dan Z, dan rotasi yang dilakukan pada setiap sumbu adalah salah satu dari CW, CCW dan 2CW, sehingga terdapat 27 kombinasi rotasi. Sebagai pembangkit random digunakan nilai 5250, sehingga untuk teks pertama diperoleh urutan kubus [5, 2, 2, 2] dan urutan angka acak untuk operasi setiap kubus [74, 97, 249, 168]. Sementara untuk teks kedua diperoleh urutan kubus [5, 2, 2, 2, 1] dan urutan angka acak untuk operasi setiap kubusnya adalah [97, 249, 168, 48, 156].

Tabel 1 Teks untuk pengujian

| No. | Teks pesan | Jumlah karakter |
|---|---|---|
| 1 | Diperlukan sumber daya manusia yang unggul, berkualitas, dan memiliki karakter yang bernilai dan berintegritas untuk mencapai Indonesia Emas 2045. | 146 |
| 2 | Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya Indonesia Raya. | 150 |

Proses Ekripsi teks dibedakan menjadi dua. Enkripsi dengan rotasi multi kubus saja dan enkripsi menggunakan rotasi multi kubus yang ditingkatkan dengan operasi XOR. Penggunaan multi kubus dengan ukuran yang berbeda bertujuan untuk menghilangkan pola pengambilan jumlah karakter dari pesan asli yang dienkripsi. Juga untuk meminimalkan jumlah karakter tambahan yang digunakan untuk melengkapi isi kubus jika jumlah karakter pada kubus terakhir tidak mencukupi.

Hasil rotasi kubus merupakan perpindahan posisi karakter dari posisi awal ke posisi yang baru. Posisi karakter yang baru bisa jadi berada sebelum, sesudah atau sama dengan posisi awalnya. Semakin besar ukuran kubus, biasanya semakin jauh perpindahan karakter dari posisi awalnya. Contoh hasil enkripsi menggunakan rotasi multi kubus ditunjukkan pada Tabel 2. Rotasi pertama ke arah CW pada semua sumbu dan rotasi kedua ke arah CCW pada semua sumbu.

Tabel 2 Contoh hasil enkripsi menggunakan multi kubus

| Rotasi | Hasil enkripsi teks1 | Hasil enkripsi teks2 |
|---|---|---|
| xcw, ycw, zcw | repiDaisunsatily retgetninakulgnay nad ,b gnasatirbmus ggnu imem linreutnu ad reb ,lu ikilad ianem kam ayaukrekarakreb niapacI nodnseaiamE s02.54 | nodnI ayaR aisenodnI ayaR aisenodnI ayaR aisenodnI ayaR aisenodnI ayaR aisenodnI ayaR aisenodnI ayaR aisenodnIseR aiya aodnIenisaR aay. |
| xccw, yccw, zccw | integter ylitasnusiaDiperritasang b, dan yanglukan untuernil memi ungg sumbk menai daliki ul, ber dacapain berkarakerkuaya maon Iesndmaias E.2045 | Raya Indonesia Raya IndonIndonesia Raya Indonesia esia Raya Indonesia Raya Raya Indonesia Raya IndonIndonesia Raya Indonesia Resayiadoa neInRasiyaa . |

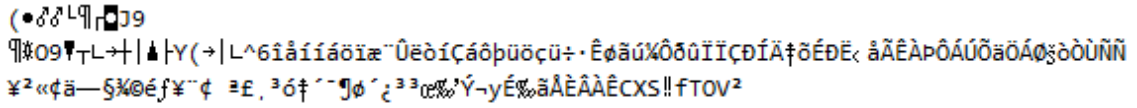
Hasil rotasi pada Tabel 2 berisi karakter-karakter yang sama dari teks1 dan teks2, namun dalam urutan karakter yang berbeda-beda sehingga relatif tidak memiliki arti. Namun demikian, terutama pada hasil enkripsi teks2 yang merupakan frasa berulang, masih telihat pola atau urutan karakter yang memiliki arti yang relatif mudah diduga. Dari dua contoh ini saja dapat diasumsikan bahwa transposisi menggunakan rotasi multi kubus masih belum memberikan hasil enkripsi yang baik. Hasil pengujian enkripsi teks menggunakan rotasi multi kubus ditunjukkan pada Tabel 3.

Hasil pengujian menujukkan bahwa ada sejumlah kombinasi yang memberikan hasil sama. Diantaranya adalah rotasi dengan urutan [xcw, ycw, zcw] memberikan hasil yang sama dengan [xccw, ycw, zccw]. Rotasi dengan urutan [xcw, yccw, zcw] memberikan hasil yang sama dengan [xccw, yccw, zccw] dan [x2cw, yccw, z2cw]. Bahkan, rotasi 180° atau 2CW pada setiap sumbu akan berikan hasil yang persis sama dengan teks aslinya. Rata-rata nilai korelasi sebesar 0.288 menunjukkan masih adanya hubungan pesan asli dengan hasil ekripsinya. Demikian pula nilai AE yang menunjukkan bahwa jumlah bit yang berubah relatif sedikit yaitu pada kisaran 28%. Artinya, enkripsi teks menggunakan rotasi multi kubus bukanlah pilihan yang baik untuk tujuan pengamanan data atau informasi.

Tabel 3 Hasil Pengujian Enkripsi dengan Rotasi Multi Kubus

| Rotasi | Hasil enkripsi Teks1 | | | Hasil enkripsi Teks2 | | |
|---|---|---|---|---|---|---|
| | R | MAE | AE | r | MAE | AE |
| xcw, ycw, zcw | 0.175 | 25.906 | 0.305 | 0.128 | 25.307 | 0.260 |
| xcw, ycw, zccw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| xcw, ycw, z2cw | 0.283 | 22.349 | 0.282 | 0.076 | 24.067 | 0.300 |
| xcw, yccw, zcw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| xcw, yccw, zccw | 0.297 | 23.571 | 0.290 | 0.135 | 23.707 | 0.247 |
| xcw, yccw, z2cw | 0.306 | 22.416 | 0.287 | 0.250 | 21.053 | 0.275 |
| xcw, y2cw, zcw | 0.229 | 24.013 | 0.300 | 0.103 | 23.653 | 0.302 |
| xcw, y2cw, zccw | 0.366 | 20.631 | 0.275 | 0.030 | 22.707 | 0.270 |
| xcw, y2cw, z2cw | 0.220 | 24.336 | 0.302 | (0.051) | 27.293 | 0.328 |
| xccw, ycw, zcw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| xccw, ycw, zccw | 0.175 | 25.906 | 0.305 | 0.128 | 25.307 | 0.260 |
| xccw, ycw, z2cw | 0.229 | 24.013 | 0.300 | 0.103 | 23.653 | 0.302 |
| xccw, yccw, zcw | 0.297 | 23.571 | 0.290 | 0.135 | 23.707 | 0.247 |
| xccw, yccw, zccw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| xccw, yccw, z2cw | 0.366 | 20.631 | 0.275 | 0.030 | 22.707 | 0.270 |
| xccw, y2cw, zcw | 0.306 | 22.416 | 0.287 | 0.250 | 21.053 | 0.275 |
| xccw, y2cw, zccw | 0.283 | 22.349 | 0.282 | 0.076 | 24.067 | 0.300 |
| xccw, y2cw, z2cw | 0.220 | 24.336 | 0.302 | (0.051) | 27.293 | 0.328 |
| x2cw, ycw, zcw | 0.283 | 22.349 | 0.282 | 0.076 | 24.067 | 0.300 |
| x2cw, ycw, zccw | 0.229 | 24.013 | 0.300 | 0.103 | 23.653 | 0.302 |
| x2cw, ycw, z2cw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| x2cw, yccw, zcw | 0.366 | 20.631 | 0.275 | 0.030 | 22.707 | 0.270 |
| x2cw, yccw, zccw | 0.306 | 22.416 | 0.287 | 0.250 | 21.053 | 0.275 |
| x2cw, yccw, z2cw | 0.230 | 24.510 | 0.310 | 0.238 | 20.680 | 0.315 |
| x2cw, y2cw, zcw | 0.227 | 24.456 | 0.314 | (0.051) | 27.387 | 0.328 |
| x2cw, y2cw, zccw | 0.227 | 24.456 | 0.314 | (0.051) | 27.387 | 0.328 |
| x2cw, y2cw, z2cw | 1.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.000 |
| Rata-rata | 0.288 | 22.660 | 0.286 | 0.153 | 22.441 | 0.284 |

Karena kekurangan ini, diperlukan metoda, teknik atau pendekatan lain untuk meningkatkan hasil enkripsi. Untuk tujuan ini digukanan operasi XOR dengan memanfaatkan bilangan acak. Operasi XOR mengakibatkan perubahan bentuk pada setiap karakter. Teks yang semula berada pada rentang nilai ASCII 0 hingga 127, berubah menjadi berada pada rentang 0 hingga 255. Hasilnya adalah deretan karakter-karakter yang tidak terbaca dan sama sekali tidak memiliki arti. Gambar 5 adalah contoh hasil operasi XOR pada teks2 setelah dilakukan rotasi multi kubus dengan rotasi dengan urutan [x2cw, yccw, z2cw]. Hasil pengujian XOR untuk peningkatan hasil engkripsi dengan rotasi multi kubus ditunjukkan pada Tabel 4.



Gambar 5. Contoh hasil enkripsi menggunakan multi kubus dan XOR

Pada Tabel 4 terlihat bahwa koefesien korelasi seluruhnya sangat mendekati nilai 0 dengan rata-rata nilai korelasi -0.051, meningkat dari sebelumnya 0.288 pada teks1 dan untuk teks2 meningkat dari 0.153 menjadi 0.017. Nilai koefesien korelasi 0 atau sangat mendekai 0 berarti bahwa hasil enkripsi sama sekali tidak dipengaruhi oleh teks aslinya.

Tabel 4 Hasil Pengujian XOR pada Peningkatan Hasil Enkripsi dengan Rotasi Multi Kubus

| Rotasi | Hasil enkripsi Teks1 | | | Hasil enkripsi Teks2 | | |
|---|---|---|---|---|---|---|
| | r | MAE | AE | r | MAE | AE |
| xcw, ycw, zcw | (0.060) | 91.584 | 0.505 | 0.006 | 94.260 | 0.523 |

| | | | | | | |
|---|---|---|---|---|---|---|
| xcw, ycw, zccw | (0.027) | 92.013 | 0.502 | 0.063 | 93.393 | 0.525 |
| xcw, ycw, z2cw | (0.035) | 91.289 | 0.512 | (0.021) | 103.553 | 0.520 |
| xcw, yccw, zcw | (0.029) | 92.510 | 0.517 | 0.057 | 94.447 | 0.540 |
| xcw, yccw, zccw | (0.090) | 92.430 | 0.515 | (0.004) | 94.073 | 0.523 |
| xcw, yccw, z2cw | (0.057) | 93.074 | 0.522 | 0.014 | 89.913 | 0.530 |
| xcw, y2cw, zcw | (0.036) | 91.530 | 0.510 | 0.013 | 93.900 | 0.527 |
| xcw, y2cw, zccw | (0.048) | 93.732 | 0.522 | (0.024) | 94.167 | 0.538 |
| xcw, y2cw, z2cw | (0.062) | 93.839 | 0.513 | 0.001 | 93.140 | 0.532 |
| xccw, ycw, zcw | (0.027) | 92.013 | 0.502 | 0.063 | 93.393 | 0.525 |
| xccw, ycw, zccw | (0.060) | 91.584 | 0.505 | 0.006 | 94.260 | 0.523 |
| xccw, ycw, z2cw | (0.058) | 92.765 | 0.510 | (0.001) | 90.420 | 0.528 |
| xccw, yccw, zcw | (0.090) | 92.430 | 0.515 | (0.004) | 94.073 | 0.523 |
| xccw, yccw, zccw | (0.029) | 92.510 | 0.517 | 0.057 | 94.447 | 0.540 |
| xccw, yccw, z2cw | (0.069) | 93.987 | 0.507 | (0.005) | 102.793 | 0.528 |
| xccw, y2cw, zcw | (0.040) | 93.060 | 0.503 | 0.010 | 95.647 | 0.555 |
| xccw, y2cw, zccw | (0.054) | 91.517 | 0.510 | 0.028 | 95.900 | 0.542 |
| xccw, y2cw, z2cw | (0.062) | 92.067 | 0.510 | 0.030 | 95.140 | 0.527 |
| x2cw, ycw, zcw | (0.035) | 91.289 | 0.512 | (0.021) | 103.553 | 0.520 |
| x2cw, ycw, zccw | (0.058) | 92.765 | 0.510 | (0.001) | 90.420 | 0.528 |
| x2cw, ycw, z2cw | (0.027) | 92.013 | 0.502 | 0.063 | 93.393 | 0.525 |
| x2cw, yccw, zcw | (0.069) | 93.987 | 0.507 | (0.005) | 102.793 | 0.528 |
| x2cw, yccw, zccw | (0.057) | 93.074 | 0.522 | 0.014 | 89.913 | 0.530 |
| x2cw, yccw, z2cw | (0.029) | 92.510 | 0.517 | 0.057 | 94.447 | 0.540 |
| x2cw, y2cw, zcw | (0.049) | 92.282 | 0.513 | 0.041 | 103.153 | 0.517 |
| x2cw, y2cw, zccw | (0.080) | 92.483 | 0.532 | 0.019 | 89.140 | 0.545 |
| x2cw, y2cw, z2cw | (0.050) | 94.604 | 0.522 | 0.009 | 95.527 | 0.537 |
| Rata-rata | (0.051) | 92.553 | 0.512 | 0.017 | 95.158 | 0.530 |

Peningkatan juga terjadi pada nilai MAE dan AE. Nilai AE seluruhnya berada di atas 50% relevan dengan penelitian sebelumnya [24],[25], [26]. Nilai rata-ratanya adalah 51% untuk teks1 dan 53% untuk teks2. Peningkatan yang terjadi adalah sebesar 44% pada teks1 dan 46% pada teks2. Nilai AE menunjukkan seberapa banyak perubahan yang terjadi pada teks hasil enkripsi. Teknik enkripsi yang digunakan dikatakan baik jika jumlah bit yang berubah lebih dari 45% [27]. Sementara peningkatan pada nilai MAE menunjukkan bahwa sebaran posisi karakter menjadi semakin lebar, yang semula hanya sejauh 22 karakter dari posisi awal menjadi 95 karakter dari posisi awal ke arah sebelum atau sesudahnya. Peningkatan yang diperoleh sebesar 77%.

Hasil enkripsi menggunakan rotasi multi kubus berhasil ditingkatkan menggunakan operasi XOR sehingga memenuhi karakteristik teknik enkripsi yang baik yaitu difusi dan konfusi. Difusi mengakibatkan perubahan posisi karakter dan konfusi mengakibatkan perubahan karakter. Perubahan karakter pada posisi yang tersebar secara tidak merata tentu saja akan menambah tingkat kesulitan dalam upaya kriptanalis.

## 4. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa operasi XOR berhasil meningkatkan kinerja hasil enkripsi menggunakan rotasi multi kubus. Penggunaan multi kubus mengakibatkan ukuran blok karakter yang dienkripsi berubah secara tidak konsisten. Yang kemudian ditingkatkan dengan operasi XOR yang memperlebar perubahan hasil enkripsi dari rentang ASCII standar menjadi rentang ASCII extended. Penggunaan operasi XOR juga berhasil menghilangkan korelasi antara teks asal dengan hasil enkripsi, memperluas sebaran perubahan teks serta meningkatkan jumlah bit yang mengalami perubahan secara signifikan. Penelitian selanjutnya diarahkan pada upaya efesiensi penggunaan rotasi untuk mengurangi jumlah iterasi perpindahan data selama proses

enkripsi, terutama pada data yang berukuran relatif besar seperti citra dengan resolusi tinggi.

## UCAPAN TERIMA KASIH

Terimakasih penulis sampaikan atas dukungnya kepada P3M Politeknik Negeri Samarinda melalui DIPA Politeknik Negeri Samarinda Nomor SP DIPA-023.18.2.677612/2023.

## DAFTAR PUSTAKA

[1] S. A. Hannan and A. M. A. M. Asif, "Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption," *Int. J. Comput. Sci. Softw. Eng.*, vol. 6, no. 2, pp. 41–46, 2017.

[2] H. Delfs and H. Knenbl, *Introduction to Cryptography: Principles and Application*, Third Edit. Berlin: Springer-Verlag GmbH, 2015. doi: 10.1007/978-3-662-47974-2.

[3] R. Dixit and K. Ravindranath, "Encryption techniques & access control models for data security : A survey," *Int. J. Eng. Technol.*, vol. 7, no. 1.5, pp. 107–110, 2018, doi: 10.14419/ijet.v7i1.5.9130.

[4] B. Schneier, *Applied Crypthography*, 20th Anniv. Indianapolis: John Wiley & Sons, Inc, 2015.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Seventh Ed. Harlow: Pearson Education Limited, 2017.

[6] C. Paar and J. Pelzl, *Understanding Cryptography*. Berlin: Springer-Verlag, 2010. doi: 10.1007/978-3-642-04101-3.

[7] M. B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition," *Int. J. Comput. Appl.*, pp. 19–23, 2014.

[8] B. Bjorkman and R. Talbert, "Fixed Points of Columnar Transpositions," *J. Discret. Math. Sci. Cryptogr.*, vol. 18, no. 5, pp. 541–557, Sep. 2015, doi: 10.1080/09720529.2014.986910.

[9] S. Majumdar, A. Maiti, B. Bhattacharyya, and A. Nath, "A New Bit-level Columnar Transposition Encryption Algorithm," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 7, pp. 176–184, 2015, [Online]. Available: http://www.ijarcsms.com/July2015.htm

[10] N. Sinha and K. Bhamidipati, "Improving Security of Vigenère Cipher by Double Columnar Transposition," *Int. J. Comput. Appl.*, vol. 100, no. 14, pp. 6–10, 2014, doi: 10.5120/17591-8290.

[11] M. Annalakshmi and A. Padmapriya, "Zigzag Ciphers : A Novel Transposition Method," in *International Conference on Computing and information Technology (IC2IT-2013)*, 2013, pp. 8–12.

[12] O. P. Baghel, "Combination of Transposition and Alpha-Numeric Vigenere Table for Secure Communication," *J. Netw. Commun. Emerg. Technol.*, vol. 7, no. 4, pp. 15–17, 2017.

[13] A. Rizal, D. Susilo Budi Utomo, R. Rihartanto, and A. Susanto, "Encryption of RGB Image Using Hybrid Transposition," in *Advances in Social Science, Education and Humanities Research*, 2019, vol. 203, no. ICLICK 2018, pp. 57–61. doi: 10.2991/iclick-18.2019.13.

[14] A. Jawahir and H. Haviluddin, "An audio encryption using transposition method," *Int. J. Adv. Intell. Informatics*, vol. 1, no. 2, p. 98, Jul. 2015, doi: 10.26555/ijain.v1i2.24.

[15] X. Feng, X. Tian, and S. Xia, "A novel image encryption algorithm based on fractional Fourier transform and magic cube rotation," *Proc. - 4th Int. Congr. Image Signal Process. CISP 2011*, vol. 2, no. 5, pp. 1008–1011, 2011, doi: 10.1109/CISP.2011.6100319.

[16] X. Feng, X. Tian, and S. Xia, "An improved image scrambling algorithm based on magic cube rotation and chaotic sequences," *Proc. - 4th Int. Congr. Image Signal Process. CISP 2011*, vol. 2, pp. 1021–1024, 2011, doi: 10.1109/CISP.2011.6100274.

[17] L. Zhang, X. TiaN, and S. Xia, "Scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence," *Proc. - 2011 Int. Conf. Multimed. Signal Process. C. 2011*, vol. 1, pp. 312–315, 2011, doi: 10.1109/CMSP.2011.69.

[18] K. Loukhaoukha, J. Chouinard, and A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik ' s Cube Principle," *J. Electr. Comput. Eng.*, vol. 2012, 2012, doi: 10.1155/2012/173931.

[19] P. Praveenkumar *et al.*, "Rubik's Cube Blend with Logistic Map on RGB: A Way for Image Encryption," *Reasearch J. Inf. Technol.*, vol. 6, no. 3, pp. 207–215, 2557, doi: 10.3923/rjit.2014.207.215.

[20] F. Twum, J. B., and M.-D. William, "A Proposed Enhanced Transposition Cipher Algorithm based on Rubik's Cube Transformations," *Int. J. Comput. Appl.*, vol. 182, no. 35, pp. 18–26, 2019, doi: 10.5120/ijca2019918323.

[21] D. Rajavel and S. P. Shantharajah, "Cubical key generation and encryption algorithm based on hybrid cube's rotation," *Int. Conf. Pattern Recognition, Informatics Med. Eng. PRIME 2012*, pp. 183–187, 2012, doi: 10.1109/ICPRIME.2012.6208340.

[22] Rihartanto, D. S. B. Utomo, H. Februariyanti, A. Susanto, and W. Khafidhah, "Bit-based cube rotation for text encryption," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, pp. 709–717, 2023, doi: 10.11591/ijece.v13i1.pp709-717.

[23] R. Rihartanto, R. K. Ningsih, A. F. O. Gaffar, and D. S. B. Utomo, "Implementation of vigenere cipher 128 and square rotation in securing text messages," *J. Teknol. dan Sist. Komput.*, vol. 8, no. 3, pp. 201–209, 2020, doi: 10.14710/jtsiskom.2020.13476.

[24] H. V. Gamido, "Implementation of a bit permutation-based advanced encryption standard for securing text and image files," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, pp. 1596–1601, 2020, doi: 10.11591/ijeecs.v19.i3.pp1596-1601.

[25] S. D. Mohammed and T. M. Hasan, "Cryptosystems using an improving hiding technique based on latin square and magic square," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 510–520, 2020, doi: 10.11591/ijeecs.v20.i1.pp510-520.

[26] J. N. B. Salameh, "A new symmetric-key block ciphering algorithm," *Middle East J. Sci. Res.*, vol. 12, no. 5, pp. 662–673, 2012, doi: 10.5829/idosi.mejsr.2012.12.5.1685.

[27] H. Noura, L. Sleem, M. Noura, M. M. Mansour, A. Chehab, and R. Couturier, "A new efficient lightweight and secure image cipher scheme," *Multimed. Tools Appl.*, vol. 77, no. 12, pp. 15457–15484, 2018, doi: 10.1007/s11042-017-5124-9.