Prosiding Seminar Nasional Teknologi Informatika
Volume 2 Nomor 1
November 2019
ISBN : 978-602-50006-1-4

Modifikasi *Myszkowski Transposition Cipher* dengan *Chess Board Pattern*

Nurul Khairina
Universitas Medan Area
nurulkhairina27@email.com

Muhammad Khoiruddin Harahap
Politeknik Ganesha Medan
choir.harahap@yahoo.com

Abstrak

Keamanan sebuah pesan rahasia menjadi tujuan utama dalam pengembangan bidang ilmu kriptografi. Dalam ilmu komputer, matematika kerap kali digunakan dalam pembentukan algoritma kriptografi klasik maupun kriptografi modern. Algoritma *Myszkowski Transposition Cipher* merupakan salah satu algoritma kriptografi klasik dengan jenis algoritma transposisi yang menerapkan permutasi matematika. Pada penelitian ini, peneliti memodifikasi algoritma *Myszkowski Transposition Cipher* dengan *Chess Board Pattern*. Enkripsi dan dekripsi dengan *Chess Board Pattern* dilakukan dengan mengikuti pola papan catur berwarna hitam putih. Kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern* menghasilkan variasi pola enkripsi dan dekripsi yang beragam, sehingga proses enkripsi dan dekripsi menjadi lebih rumit. Hal ini juga dapat meningkatkan keamanan pesan rahasia dari pihak yang tidak terlibat.

Kata Kunci — *myszkowski transposition cipher; chess board pattern*

I. PENDAHULUAN

Kriptografi merupakan sebuah seni [1] dan bidang ilmu yang memiliki beberapa jenis algoritma yang sering digunakan untuk memberi keamanan pada pesan rahasia ataupun dokumen rahasia. Kriptografi yang terdiri dari algoritma *Myszkowski Transposition Cipher* merupakan salah satu algoritma transposisi yang unik dan menarik untuk dimodifikasi karena terdapat perbedaan cara pembacaan *ciphertext* saat bertemu dengan penomoran kunci yang sama. Dalam ilmu kriptografi, algoritma transposisi melakukan proses enkripsi dengan cra menerapkan permutasi pada *plaintext* untuk menghasilkan *ciphertext* [2] [3]. Algoritma ini juga sering dianggap sebagai algoritma permutasi [4] [5]. Berikut ini beberapa penelitian terdahulu yang terkait:

Penelitian Hardi [6] melakukan kombinasi algoritma *Myszkowski Transposition* dan *Modified Least Significant Bit* (MLSB). Hasil penelitian menunjukan bahwa algoritma *Myszkowski* dapat meningkatkan keamanan pesan rahasia, namun

ISBN : 978-602-50006-1-4

apabila diterapkan pada gambar berukuran besar, membutuhkan waktu proses yang cukup lama.

Penelitian Singh [7] melakukan pengembangan algoritma *playfair cipher* dengan kombinasi bilangan acak dan *vigenere cipher*. Kemudian juga terdapat peran algoritma *Myszkowski Transposition Cipher* dalam pengembangan algoritma *playfair cipher*. Hasil penelitian menunjukkan bahwa algoritma *playfair cipher* yang dikombinasikan dengan *vigenere cipher* lebih baik dari algoritma *playfair cipher* asli.

Penelitian Garvit [8] melakukan analisis dan mendesain algoritma sederhana yang berdasarkan dengan objek multi dimensi. Penelitian ini menghasilkan algoritma baru yang berasal dari analisis kelebihan dan kelemahan beberapa algoritma kriptografi transposisi.

Penelitian Bhowmic [9] melakukan kombinasi algoritma columnar dan *Myszkowski Transposition* untuk meningkatkan kekuatan algoritma Hill Cipher. Hasil penelitian menunjukkan bahwa modifikasi algoritma Hill Cipher memiliki keamanan yang lebih baik dari pada algoritma aslinya.

II. LANDASAN TEORI

A. Algoritma *Myszkowski Transposition Cipher*

Myszkowski Transposition Cipher merupakan salah satu jenis algoritma tranposisi cipher yang memiliki keunikan tersendiri. Pada proses enkripsi, *plaintext* ditulis secara horizontal dari kiri ke kanan, kemudian *ciphertext* dibaca secara vertikal sesuai dengan urutan kunci. Adapun algoritma *Myszkowski Transposition Cipher*, adalah sebagai berikut [10]:

1. Enkripsi :

Sebelum melakukan proses enkripsi, terlebih dahulu dilakukan pembentukan kunci. Beberapa huruf yang dibentuk secara manual ataupun acak dapat menambah variasi pembentukan kunci. Misalkan terdapat *plaintext* dan kunci sebagai berikut:

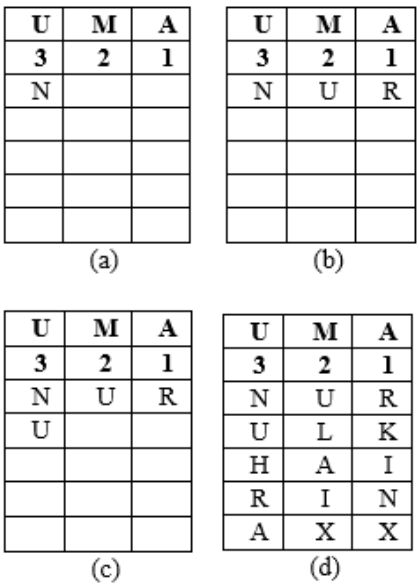
Plainteks : NURUL KHAIRINA
Kunci : UMA

Proses enkripsi dimulai dengan membentuk sejumlah baris dan kolom untuk menampung *plaintext*. Terdapat 13 huruf pada *plaintext* yang akan menjadi acuan dalam membentuk baris, dan 3 huruf pada kunci akan menjadi acuan untuk membentuk kolom. Sehingga jumlah kolom dan baris yang dibutuhkan adalah :

Kunci = 3 huruf => 3 kolom
Plaintext = 13 huruf => 13/3 = 4.3 => 5 baris

Kunci pada contoh diatas terdiri dari 3 huruf, sehingga dapat kita beri penomoran sesuai urutan abjad, yaitu U = 3; M = 2; A = 1.

Setelah membentuk baris dan kolom yang memungkinkan, *plaintext* dapat ditulis secara berurutan dan horizontal. Secara rinci dapat dilihat pada Gambar 1 :



Gambar 1. Proses Enkripsi (a), (b), (c), Hasil Enkripsi (d).

Pada Gambar 1, dua baris teratas merupakan kunci dan penomoran kunci yang digunakan dalam proses enkripsi, kemudian 2 huruf X terakhir merupakan *dummy* yang digunakan untuk memenuhi kotak kosong yang tidak terisi oleh *plaintext*.

Dari proses enkripsi tersebut, *ciphertext* dapat diperoleh dengan cara membaca huruf secara vertikal dari atas ke bawah sesuai dengan penomoran kunci.

Kunci	1	2	3
Ciphertext	RAKINX	ULAIX	NUHRA

Sehingga *Ciphertext* menjadi :

Ciphertext : RAKINX ULAIX NUHRA

ISBN : 978-602-50006-1-4

Keunikan algoritma *Myszkowski* terlihat apabila terdapat kunci yang memiliki huruf yang berulang. Pada kasus seperti ini, *ciphertext* akan dibaca secara horizontal. Misalkan :

Plainteks : NURUL KHAIRINA
Kunci : OKTOBER

Proses Enkripsi :

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
N	U	R	**U**	L	K	H
A	I	R	**I**	N	A	X

Gambar 2. Variasi Enkripsi

Ciphertext : LN KA UI **NU AI** HX RR

Dapat dilihat pada Gambar 2, terdapat dua huruf kunci yang sama yaitu huruf O, dengan penomoran kunci = 4. Pembacaan *ciphertext* tidak dilakukan secara vertikal, melainkan secara horizontal dan menghasilkan NU AI.

O	**O**
4	**4**
N	U
A	I

Gambar 3. Pembacaan *Ciphertext* Secara Horizontal terhadap Huruf Kunci yang Sama.

2. Dekripsi :

Proses dekripsi dapat dilakukan apabila pihak penerima pesan rahasia *(ciphertext)* mengetahui pola kunci dan ukuran baris dan kolom yang digunakan pihak pengirim pesan. Proses dekripsi dapat dilakukan dengan menuliskan *ciphertext* secara vertikal dari atas ke bawah secara berurutan sesuai dengan penomoran kunci. Pada penomoran kunci yang sama, *ciphertext* ditulis secara horizontal.

Ciphertext : LN KA UI NU AI HX RR
Kunci : OKTOBER

Proses Dekripsi :

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
				L		
				N		

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
				L	K	
				N	A	

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
	U			L	K	
	I			N	A	

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
N	U		**U**	L	K	
	I			N	A	

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
N	U		**U**	L	K	
A	I		**I**	N	A	

O	**K**	**T**	**O**	**B**	**E**	**R**
4	**3**	**6**	**4**	**1**	**2**	**5**
N	U	R	**U**	L	K	H
A	I	R	**I**	N	A	X

Gambar 4. Proses Dekripsi

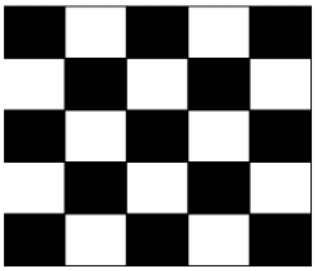
Dari gambar 4, *plaintext* dapat diperoleh dengan membaca huruf dari kolom paling kiri tanpa memperdulikan penomoran kunci, sehingga diperolehlah :

Plaintext : NURUL KHAIRINA

B. Chess Board Pattern

Proses enkripsi kriptografi membutuhkan pola penyisipan yang unik untuk mengamankan data dari pihak yang tidak terkait. *Chess Board Pattern* memiliki pola seperti papan catur, dimana terdapat kolom berwarna hitam dan putih yang saling berselang seling. Adapun gambaran *Chess Board Pattern* adalah sebagai berikut [11]:

ISBN : 978-602-50006-1-4



Gambar 5. *Chess Board Pattern*

III. METODOLOGI PENELITIAN

Pada penelitian kali ini, akan dilakukan modifikasi terhadap algoritma *Myszkowski Transposition Cipher*. Proses enkripsi dan dekripsi akan di lakukan dengan mengikuti pola papan catur *(Chess Board Pattern)*.

A. Enkripsi :

Enkripsi dilakukan dengan menuliskan *plaintext* pada pola papan catur yang berwarna putih, dan mengabaikan setiap kolom yang berwarna hitam. Namun ketentuan ini tidak bersifat baku, dimana adakalanya pihak pengirim pesan akan memiliki modifikasi tersendiri terhadap *chess board pattern*, sehingga proses enkripsi dapat memiliki beberapa variasi. Enkripsi pada pola papan catur ini memiliki baris dan kolom yang dapat ditentukan dari jumlah *plaintext* dan jumlah kunci.

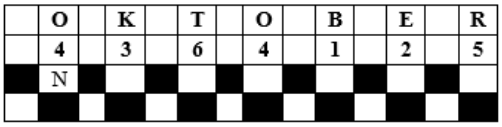
Jumlah baris : 2 x (jumlah *plaintext* / jumlah kunci), kemudian hasilnya dibulatkan keatas
Jumlah kolom : 2 x jumlah kunci

Pembacaan *ciphertext* akan dilakukan secara vertikal sesuai dengan penomoran kunci, kemudian akan dibaca secara horizontal apabila terdapat penomoran kunci yang sama.

B. Dekripsi :

Proses dekripsi dapat dilakukan dengan menuliskan *ciphertext* secara vertikal dari atas ke bawah secara berurutan sesuai dengan penomoran kunci dan pola papan catur yang digunakan saat enkripsi. Namun ketentuan tersebut dapat berubah apabila pihak pengirim pesan memiliki pola modifikasi sendiri dengan *Chess Board Pattern*, sehingga proses dekripsi akan tetap mengikuti pola yang telah disepakati.

Berikut ini gambaran enkripsi dengan *chess board pattern* beserta kunci dan penomoran kunci.



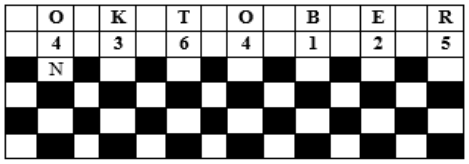
Gambar 6. *Chess Board Pattern* untuk Enkripsi Algoritma *Myszkowski*

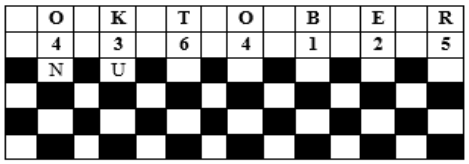
IV. HASIL DAN PEMBAHASAN

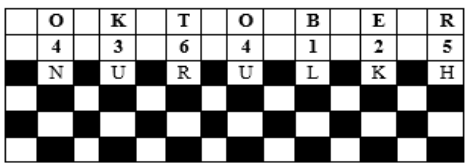
Dengan adanya kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern*, maka akan terdapat beberapa variasi terhadap proses enkripsi, pembacaan *ciphertext*, dan proses dekripsi yang memungkinkan. Pada bagian ini, akan dilakukan uji coba dengan 2 model proses enkripsi dan dekripsi. Berikut ini proses enkripsi dengan *plaintext* NURUL KHAIRINA dengan kunci OKTOBER.

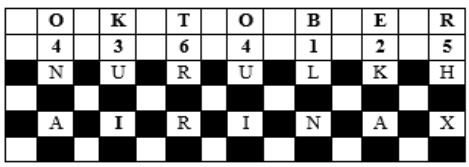
A. Enkripsi Variasi 1 :

Proses enkripsi dilakukan dengan pola *Chess Board*. *Plaintext* akan ditulis pada setiap kotak yang berwarna putih dan berkelang 1 baris. Pembacaan *ciphertext* akan dilakukan secara vertikal dari atas ke bawah sesuai dengan penomoran kunci. Apabila terdapat penomoran kunci yang sama, maka *ciphertext* akan dibaca secara horizontal. Secara rinci dapat dilihat pa









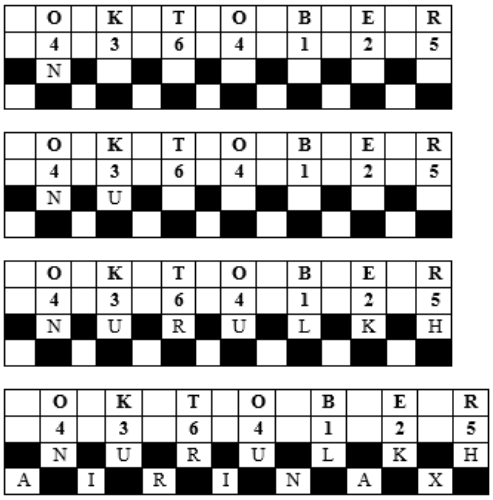
ISBN : 978-602-50006-1-4

Gambar 7. Proses Enkripsi dengan *Chess Board Pattern* Variasi 1

Sehingga diperoleh :
Ciphertext : LN KA UI NU AI HX RR

B. Enkripsi Variasi 2 :

Proses enkripsi dilakukan dengan pola *Chess Board. Plaintext* akan ditulis pada setiap kotak yang berwarna putih secara berurutan. *Ciphertext* dapat dibaca secara diagonal dari atas ke bawah sesuai penomoran kunci dan pola kotak berwarna putih. Apabila terdapat penomoran kunci yang sama, maka *ciphertext* dapat dibaca secara horizontal. Secara rinci dapat dilihat pada Gambar 8.

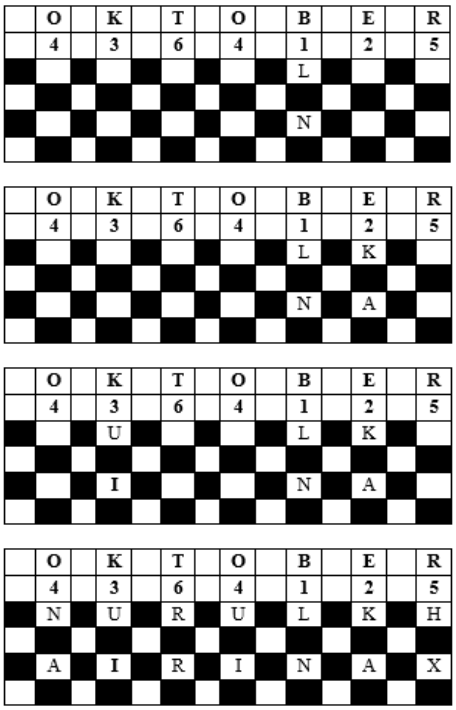


Gambar 8. Proses Enkripsi dengan *Chess Board Pattern* Variasi 2

Sehingga diperoleh :
Ciphertext : LN KA UI NU AI HX RR

C. Dekripsi Variasi 1 :

Proses dekripsi pada variasi 1 ini akan mengikuti pola enkripsi pada variasi 1. Pada proses dekripsi variasi 1, c*iphertext* akan dituliskan pada kotak berwarna putih dengan kelang 1 baris secara vertikal dan *plaintext* dibaca secara horizontal. Sehingga dekripsi menjadi :



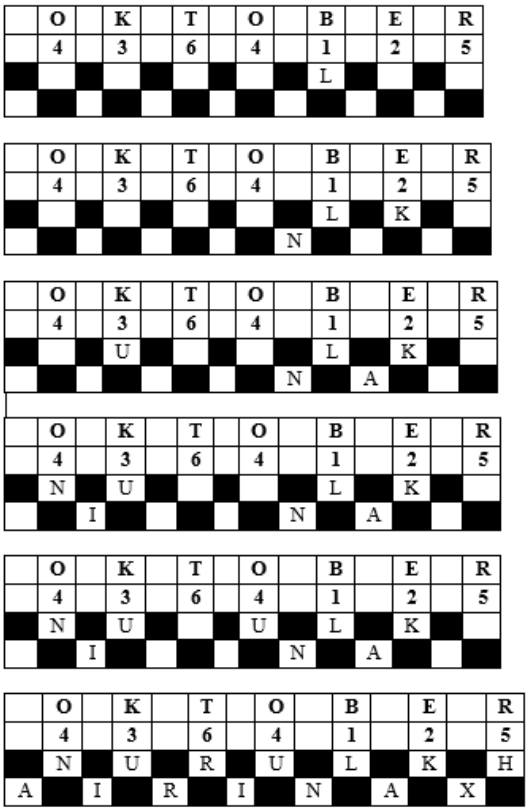
Gambar 9. Proses Dekripsi dengan *Chess Board Pattern*

Sehingga diperoleh *plaintext* :
Plaintext : NURULKHAIRINAX

D. Dekripsi Variasi 2 :

Proses dekripsi pada variasi 2 ini akan mengikuti pola enkripsi pada variasi 2. Pada proses dekripsi variasi 2, c*iphertext* akan dituliskan pada kotak berwarna putih secara diagonal dari atas ke bawah dan *plaintext* dibaca secara secara horizontal. Sehingga dekripsi menjadi :

ISBN : 978-602-50006-1-4



Gambar 10. Proses Dekripsi dengan *Chess Board Pattern*

Sehingga diperoleh *plaintext* :
Plaintext : NURULKHAIRINAX

V. KESIMPULAN

A. *Kesimpulan*

Adapun kesimpulan dari penelitian ini adalah sebagai berikut :

1. Kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern* dapat membentuk banyak pola proses enkripsi, sehingga secara tidak langsung dapat meningkatkan kerumitan proses enkripsi dan memberikan keamanan yang lebih baik terhadap pesan rahasia.
2. *Myszkowski Transposition Cipher* memiliki keunikan tersendiri, dimana *ciphertext* dibaca secara secara vertikal sesuai dengan penomoran kunci, dan dibaca secara horizontal apabila terdapat penomoran kunci yang sama.

B. Saran

Adapun saran untuk perkembangan penelitian ini adalah sebagai berikut :

1. Pola enkripsi yang diterapkan pada kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern*, kedepannya dapat diterapkan pada bidang ilmu steganografi.
2. Algoritma *Myszkowski* dengan *Chess Board Pattern* ini kedepannya dapat dikombinasikan dengan salah satu algoritma bilangan acak.

REFERENSI

[1] R. A. Indra and W. Pramusinto, "Aplikasi Email (Electronic Mail) Menggunakan Algoritma Advanced Encryption Standard(AES-128) dan Algoritma Rivest Cipher 4 (RC4) Berbasis Web," in *SKANIKA*, 2018, vol. 1, no. 2, pp. 704–710.

[2] A. Banerjee, M. Hasan, and H. Kafle, *Secure Cryptosystem Using Randomized Rail Fence Cipher for Mobile Devices Amit*. Springer International Publishing, 2019.

[3] A. Rizal, D. Susilo Budi Utomo, R. Rihartanto, and A. Susanto, "Encryption of RGB Image Using Hybrid Transposition," in *International Conference on Life, Innovation, Change, and Knowledge*, 2018, vol. 203, pp. 57–61.

[4] J. X. Chen, Z. L. Zhu, C. Fu, H. Yu, and Y. Zhang, "Reusing The Permutation Matrix Dynamically for Efficient Image Cryptographic Algorithm," *Signal Processing*, vol. 111, pp. 294–307, 2015.

[5] G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. Van Assche, and R. Van Keer, "Farfalle : Parallel Permutation-Based Cryptography," *IACR Trans. Symmetric Cryptol.*, vol. 2017, no. 4, pp. 1–38, 2017.

[6] S. M. Hardi, D. Rachmawati, F. Chairinnisa, I. Jaya, and J. T. Tarigan, "Combination of Myszkowski Transposition Algorithm and Modified Least Significant Bit (MLSB) Green Channel on PNG Image Security," *J. Phys. Conf. Ser.*, vol. 1235, no. 1, pp. 1–7, 2019.

[7] S. Singh and A. Dixit, "An Approach for Enhancing the Security of Playfair Cipher," *Imp. J. Interdiscip. Res.*, vol. 3, no. 6, pp. 434–438, 2017.

[8] G. Jindal, S. Baranwal, and S. Chaudhary, "Cryptography Using Multi-Dimensional Objects," in *International Conference on Advances in Engineering Science Management & Technology*, 2019, pp. 1–5.

[9] A. Bhowmick and M. Geetha, "Enhancing Resistance of Hill Cipher using Columnar

ISBN : 978-602-50006-1-4

and Myszkowski Transposition," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 2, pp. 20–25, 2015.

[10] J. A. Kusumaningtyas, "Analisa Algoritma Ciphers Transposition : Study Literature," *Multimatrix*, vol. I, no. 1, pp. 1–12, 2018.

[11] N. Khairina and M. K. Harahap, "Menjaga Kerahasiaan Data dengan Steganografi Kombinasi LSB-2 dengan LSB-3 Dan Chess Board Pattern," *SinkrOn*, vol. 3, no. 1, p. 286, 2018.