Analisa Algoritma *Ciphers Transposition*: *Study Literature*

Juwita Artanti Kusumaningtyas
Institut Agama Islam Negeri (IAIN) Salatiga
mee.juwita@gmail.com

Abstrak

Abstract - ***Technological developments allow the sending and storage of data can be done quickly, easily, practically, and safely. One security used uses cryptographic techniques. Cryptography is a technique of converting original text (plaintext) into secret text (ciphertext) using cryptographic algorithms (ciphers) or what is called the encryption process. The decryption process is the process of converting data encoded into original data. One of the cryptographic algorithms is the Cipher Transposition Algorithm. The analysis aims to determine the characteristics and application of the Transposition Cipher. The method used in this study by means of Study Literature, analyzes previous research from journals related to the Transposition Cipher Algorithm. The results are in the form of a view using the study literature method and knowing the characteristics and application of the Cipher Transposition algorithm and analyzing trends in previous studies.***

Kata Kunci : ***Cryptography, Algorithms, Cipher Transposition, Study literature***

I. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) dibilang cukup pesat, dengan segala fasilitas dari inovasi-inovasi yang terus mengalami perkembangan dari waktu ke waktu. Hal ini juga berpengaruh terhadap kebutuhan manusia yang semakin bergantung terhadap penggunaan teknologi. Dimulai digunakan untuk hiburan, pekerjaan, dan melancarkan komunikasi. Salah satu alat teknologi yang sering digunakan adalah komputer. Penggunaan komputer sendiri terus mengalami perkembangan, tidak hanya dari segi perangkat keras tetapi juga perangkat lunak.

Kemajuan teknologi juga diikuti dengan perkembangan informasi. Hal ini dibantu dengan penggunaan internet yang semakin menjamur di kalangan masyarakat luas. Akibatnya pengiriman dan penyimpanan data bisa dilakukan dengan cepat, mudah, dan praktis. Proses penyimpanan data dan informasi yang dihadapi selanjutnya yaitu dari segi keutuhan dan keamanan. Karena sekarang ini banyak orang yang tidak bertanggung jawab untuk melakukan sabotase terhadap data yang dikirimkan melalui jaringan.

Penggunaan kriptografi digunakan untuk mencegah adanya penyadapan data pada pengiriman dengan cara penyandian data. Penyandian data dengan cara mengubah teks asli (*plaintext*) menjadi teks yang tersandi (*ciphertext*) yang tidak mempunyai makna dan tidak dapat dibaca. Metode yang digunakan dengan menggunakan enkripsi untuk penyandian dan dekripsi untuk membuka penyandian tersebut. Proses enkripsi merubah data asli (*plaintext*) menjadi teks sandi (*ciphertext*). Sedangkan proses dekripsi merubah data tersandikan (*ciphertext*) menjadi data asli (*plaintext*) ketika data diterima.

Pada proses enkripsi dan dekripsi memerlukan algoritma, yang disebut algoritma kriptografi (*cipher*). Algoritma kriptografi sangat beragam, tujuannya membuat serumit mungkin pesan yang dikirim sehingga data didalamnya aman kemudian hanya orang yang berhak saja yang dapat menggunakan data tersebut.

Algoritma kriptografi klasik terdapat dua jenis, yaitu Cipher Substitusi (*Substitution Ciphers*) dan Cipher Transposisi (*Transposition Ciphers*). Algoritma yang dianalisa pada jurnal ini merupakan Cipher Transposisi. Cipher Transposisi merupakan algoritma yang plaintext tetap sama, tatapi urutannya yang berubah.

Permasalahan yang timbul, kurangnya pengetahuan pengguna, mengenai karakteristik dan penerapan dari *Cipher Transposition*. Metode yang digunakan dengan *study literature*, melihat dari penelitian-penelitian dari beberapa jurnal mengenai Cipher Transposisi dan memberikan kesimpulan mengenai kegunaan algoritma tersebut.

Hasil dari jurnal yang berjudul "Analisa Algoritma *Cipher Transposition*: *Study Literature*" diharapkan bisa memberikan pandangan dengan menggunakan metode *study literature* dan mengetahui karakteristik dan penerapan algoritma *Cipher Transposition*.

II. METODE

Metode yang berkaitan dengan analisa ini *Study literature* atau tinjauan pustaka merupakan peninjauan kembali pustaka-pustaka yang berkaitan. Oleh karena itu tinjauan pustaka berfungsi sebagai peninjauan kembali pustaka (laporan penelitian, dan sebagainya) tentang masalah yang berkaitan-tidak selalu harus tepat identik dengan bidang permasalahan yang dihadapi-tetapi termasuk pula yang sering dan berkaitan.

Analisa *Study literature* ini melakukan analisa dari setiap jurnal dari penelitian terdahulu yang berkaitan dengan Algoritma *Cipher Transposition.* Hasil dari analisa tersebut, dilakukan pembahasan untuk lebih mengetahui karakteristik dan penerapan *Cipher Transposition.* Setelah melakukan pembahasan, analisa ini diakhiri dengan kesimpulan mengenai algoritma *Cipher Transposition.*

III. HASIL DAN PEMBAHASAN

A. Penelitian Terdahulu

Penelitian terdahulu pertama, oleh Endro Aryanto dkk, membahas mengenai implementasi algoritma Sosemanuk dan algoritma Dicing dan mencari perbedaan dari keduanya. Algoritma Sosemanuk dan algoritma Dicing merupakan algoritma *stream cipher* memiliki panjang kunci 128 sampai 256 bit. Kedua algoritma *stream cipher* menggunakan kombinasi LFSR (*Linear Feedback Shift Register*) dan FSM (*Finite State Machine*) sebagai pembangkit kuncinya. Parameter yang digunakan dalam perbandingan algoritma Sosemanuk dan algoritma Dicing yaitu Avalanche Effect (AE), lama waktu proses, dan memori. Hasilnya Algoritma Sosemanuk lebih besar dari algoritma Dicing, sehingga algoritma Sosemanuk lebih handal daripada algoritma Dicing. Proses algoritma Sosemanuk 4,77%, sehingga waktu yang diperlukan lebih lama dan memori yang digunakan lebih besar dari Dicing.

Penelitian terdahulu kedua, dengan judul "Perbandingan Kriptografi Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher" ditulis oleh Achmad Syafa'at, membahas mengenai membandingkan algoritma Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher dari analisa penelitian terdahulu yang didapatkan penulis dari internet, jurnal, buku, maupun artikel yang sesuai dengan bahasan materi. Manfaat yang didapatkan dari pembahasan algoritma kriptografi klasik adalah memberikan konsep dasar tentang kriptografi, dimana mempelajari krintografi klasik merupakan dasar untuk memahami algoritma kriptografi modern. Hasil yang diperoleh dari jurnal ini adalah mengetahui kelemahan-kelemahan algoritma klasik. *Caesar Cipher*, metode ini mudah dipecahkan dengan metode *exhaustive key* search karena jumlah kuncinya sangat sedikit yaitu hanya ada 26 kunci abjad. Penggunaan Cipher Substitusi Homofonik lebih sulit dipecahkan daripada *Caesar Cipher*, tetapi ketika menggunakan metode *known plaintext attack*, cipher ini dapat mudah diuraikan menjadi plainteks, tetapi jika menggunakan *ciphertext only attack* akan lebih sulit. Poligram di dalam *playfair cipher* tidak cukup besar dan berupa dua huruf saja, sehingga hal ini menyebabkan tidak aman untuk digunakan. Penggunaan metoda analisis frekuensi akan membuat *flaypair cipher* relatif sulit dipecahkan, tetapi ketika menggunakan tabel frekuensi kemunculan pasangan huruf akan mudah dipecahkan.

Penelitian terdahulu ketiga, oleh Maureen Linda Caroline, membahas mengenai penggunaan *Vigènere Cipher*, metode enkripsi abjad-majemuk manual. Pada dasarnya, *Vigènere Cipher* menggunakan bujur sangkar *Vigènere Cipher* untuk melakukan enkripsi. Setiap baris pada bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Bedanya pada *Vigènere Cipher* setiap huruf pada plainteks dienkripsi menggunakan kunci yang berbeda. Metode yang dilakukan selanjutnya yaitu menggunakan Kasiski, metode ini membantu untuk menemukan panjang kunci *Vigènere Cipher*. Metode ini memanfaatkan keuntungan bahwa Bahasa Inggris tidak banyak mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau *triple* huruf, seperti TH, THE, dsb. Perulangan kelompok ini ada kemungkinan menghasilkan kriptogram yang berulang. Langkah-langkah metode Kasiski dengan menemukan semua kriptogram yang berulang didalam cipherteks, kemudian hitung jarak antara kriptogram yang berulang, hitung semua factor (pembagi) dari jarak tersebut, kemudian tentukan irisan dari himpunan factor pembagi tersebut. Nilai yang muncul didalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut adalah panjang kunci. Hasilnya diketahui keunggulan keunggulan *Triple Transposition Vigènere Cipher*, yaitu proses enkripsi/dekripsi yang sederhana karena diperlukan 3 kunci transposisi dan 3 kunci substitusi yang berbeda, relative fleksibel dan mudah untuk dilakukan manual ataupun dengan bantuan program komputer, kekuatan enkripsinya sekuat *One-Time Pad* yaitu kunci yang digunkaan sesuai syarat untuk *unbreakable cipher* dan untuk kelemahannya *Triple Transposition Vigènere Cipher* yaitu untuk ukuran plainteks yang besar sulit untuk mendapatkan tiga buah kunci yang cukup pendek, dan masih adanya kemungkinan terjadinya pengulangan kriptogram baik itu pasangan huruf atau triple huruf atau lebih dari itu sama pada plainteks yang terpisah sejauh kelipatan dari panjang kunci baru K.

B. Hasil Study Literature

Tabel 1 Hasil *Study Literature*

Penulis	Tahun	Algoritma	Metode	Tujuan	Konstribusi
Morteza Heydari, Mahdieh Nadi Senejani	2014	*Cipher Transposition & Cuckoo Search*	- Menggunakan Cuckoo Search Algorithm (CSA) dengan *cryptanalysis* menggunakan *cipher transposition*	menganalisis keamanan informasi dengan peningkatan kecepatan proses enkripsi dan dekripsi.	- Penggunaan *cipher transposition* dengan *cuckoo Search* sangat efektif digunakan pada *cipher transposition* bahkan *key* panjang sampai 30 masih dapat dipecahkan
Sombir Singh, Sunil K. Maakar, Dr. Sudesh Kumar	2013	*Cipher Transposition*	Menambahkan teknik Transposisi sebelum menggunakan proses algoritma DES (*Data Enchryption System*)	Untuk meningkatkan keamanan algoritma DES menggunakan teknik Transposisi untuk menghindari serangan dari *brute force.*	Mengubah *plain text* menjadi *cipher text*: - *Plain text* diterapkan teknik Transposisi berdasarkan jumalah kolom. - *Cipher text* dari hasil transposisi kemudian dilakukan lagi *cipher text* dengan menggunakan DES untuk menjadi *cipher text* baru.
Mr. Vinod Saroha, Suman Mor, Anurag Dagar	2012	*Cipher Transposition*	Menggunakan dua teknik yaitu teknik transposisi dan teknik *Caesar cipher*	Mengkombinasikan dua teknik antara substitusi dan transposisi untuk menghindari serangan dari *brute force.*	Mengubah *plain text* menjadi *cipher text*: - *Plain text* di enkripsi terlebih dahulu dengan menggunakan *Caesar cipher.* - Hasil *Cipher text* tersebut di enkripsi lagi dengan menggunakan teknik transposisi.
A.S. Al-Khalid, S.S. Omran, Dalal A. Hammood	2013	*Cipher Transposition & Genetic Algorithm*	Menggunakan metode untuk menemukan panjang *key.* Fokusnya menggunakan bi- dan tri- agram.	Mencari solusi optimal *key,* (bigram, trigram)	Jurnal ini memperlihatkan perbandingan *cipher transposition* untuk melihat mana yang lebih aman.
Gaurav Shrisvastava, Ravindra Sharma, Manorama Chouhan	2013	*Cipher Transposition*	Memodifikasi teknik *Caesar Cipher* dengan melakukan dua kali teknik Transposisi	Membuktikan bahwa metode *Caesar Cipher* lebih aman dan efisien.	Melakukan enkripsi dengan *Caesar Cipher,* kemudian hasilnya dilakukan tenik transposisi. Hasil dari teknik transposisi tersebut, di lakukan lagi teknik transposisi. Sehingga penggunaan teknik transposisi sebanyak dua kali. Kesimpulan: *Caesar Cipher* terlalu sederhana dan kemungkinan besar terjadi *brute force.* Sehingga dimodifikasi dengan teknik Transposisi supaya lebih komplek. Dari 2 kombinasi

					ini membuat lebih aman dan kuat.
Omar Alkathiry, Ahmad Al-Mogren	2014	*Cipher Transposition*	Menggunakan algoritma genetik untuk memecahkan *Cipher Transposition*	Memecahkan *Cipher Transposition* dan memberi saran dari optimal *key* dalam enkripsi yang paling baik.	Dengan menggunakan algoritma genetik terdapat 50% *key* dapat dipecahkan. *Key* didukung oleh operasi *Novel Cross Over* dimana pencarian *skiming* yang dihasilkan jauh lebih cepat. Untuk kedepannya, algoritma genetik dapat dikembangkan lebih untuk *key* yang lebih panjang.
Morteza Heydari, Gholamreza L. Shabgahi, Mohammad M. Heydari	2013	*Cipher Transposition*	Pendekatan menggunakan *cryptanalysis* dari *cipher transposition* menggunakan GA (*genetic algorithm*) ditingkatkan dengan *fitness function.* Penggunaan *fitness function* dievaluasi berdasarkan bigram dan trigram.	Melakukan *cryptanalysis* menggunakan *cipher Transposition* dengan *key* yang panjang untuk menengkatkan *genetic algorithm*	Menunjukkan algoritma yang diusulkan sangat efektif digunakan untuk *cryptanalysis* menggunakan *cipher transposition* dengan panjang *key* hingga 25. Algoritma ini memiliki kecepatan konvergensi yang tinggi dan dapat meminimalkan *error*. ➔ Mutasi diambil secara acak 7% dari generasi baru. ➔ 0,0 (unigram), 0,7 (bigram), 0,3 (trigram). ➔ *Fitness function* adalah teknik yang kuat untuk menyerang *cipher transposition.*
R. Toemeh, S. Arumugam	2007	*Cipher Transposition*	Genetik algoritma: Mutasi 2 posisi, Mendiskripsikan *key* kemudian mengukur hasil fungsi setiap *key* dan *key* pendek. *Fitness function* :bigram dan trigram	Mengetahui penggunaan algoritma genetika dalam *cryptanalysis* transposisi cipher.	Pemulihan *key* 1000 huruf di *ciphertext* adalah 13,25 dari panjang *key* 15. Sehingga perbaikan *key* untuk panjang *key* 15 adalah 13%. Waktu untuk memecahkan/menggagalkan *key* lebih sedikit daripada saat serangan *Brute Force*, karena jumlah *key* untuk cipher transposisi itu N adalah N! (faktorial)
Anupama Mishra	2013	*Cipher Transposition & Caesar Cipher*	Menyajikan perspektif mengenai kombinasi teknik substitusi dan transposisi	Membuat *Caesar cipher* yang lebih baik.	- Untuk membuat lebih aman, menggunakan teknik transposisi, enkripsi dengan *key* yang sama pada setiap tingkat dan enkripsi dengan *key* yang berbeda pada setiap tingkat. - Menggunakan dua metode (substitusi dan transposisi) lebih aman. - Metode substitusi hanya mengganti

						huruf dengan metode *letter* dan transposisi mengubah posisi karakter.
Shishir Shukla, Prabhat Kumar Verma	2014	*Affine Substition Cipher & Transpositio n Cipher*	Mengkonversikan dua teknik (transposisi dan substitusi)	Mengetahui implementasi teknik *Affine Cipher Substitution* dan *Transposition Cipher*.	-	Ketika menerapkan *Affine Cipher Substitution* saja, *ciphertext* tidak aman.
					-	Ketika menggabungkan kedua teknik ini dapat memberikan keamanan jauh lebih aman daripada maisng-masing dari teknik ini berdiri sendiri.
Gaurav Shrivastava, Manoj Chouhan, Manoj Dhawan	2013	*Transpositio n Cipher & Playfair Cipher*	Menggunakan matrik 8x8 *playfair cipher* dan menggunakna *simple columnar transposition technique* .	Memodifikasi *playfair cipher* (8x8)	-	Dengan menggunakan matrik 8x8, dapat memperpanjang angka dan symbol untuk berbagai penggunaan.
Poonam Garg	2009	*Transpositio n cipher*	*Cryptanalysis* berdasarkan algoritma genetika, tabu search & simulasi annealing dan *cryptography*	Melakukan dua komplementer (kriptografi dan kriptanalisis)untuk memecahkan cipher transposisi	-	Dalam teknik eksperimen yang menggunakan 100 kali percobaan per data dengan bahasa C.
					-	10 kali percobaan ada 10 kegagalan.
					-	Hasil yang terbaik untuk setiap pesan itu rata-rata menghasilkan pola data yang dieksperimenkan.
					-	Dalam jurnal ini masing-masing dibandingkan dengan tiga teknik yang berbasis dua criteria.
					-	Kriteria pertama, dibuat ciphertext yang disediakan untuk menyerang.
					-	Menunjukkan rata-rata *key* dengan benar untuk ukuran transposisi 15.
Okike Benjamin, E.J.D Garba	2015	*Transpositio n Cipher*	*Teknik Okike*	Mengenalkan metode *Okike's Merged*	-	Membagi 2 plaintext,
					-	Satu dienkripsi dengan *columnar transposition*, yang satunya dienkripsi menggunakan *irregular*.
					-	Setelah itu hasil cypertext keduanya

						digabungkan menggunakan metode *Okike's Merged.*
Reyhan Yuanza Pohan	2007	*Cipher Transpositio n*	*chipper transposition*	Membandingkan berbagai macam *chipper transposition*	-	Semua algoritma cipher transposisi mempunyai kelemahan yaitu serumit apapun melakukan transposisi atau permutasi pada karakter-karakter dalam plainteks, kita hanya melakukan mengacak urutan dari plainteks tidak mengubahnya. Sehingga memecahkan *cipher* transposisi tidak sulit.
					-	Algoritma baru melakukan urutan penulisan plainteks menjadi cipherteks menggunakan *rail fence cipher* dalam kolom-kolom seperti pada *columnar transposition* dengan tambahan kunci seperti *route cipher*.
Jawad Ahmad Dar	2014	*Columnar Transpositio n Cipher*	Mengkombinasikan dari 3 algoritma (*simple columnar transposition, Caesar cipher, rail fence*)	Meningkatkan keamanan data *Columnar Transposition Cipher* dari *Caesar Cipher* dan *Rail Fence Cipher*.	-	Plaintext dilakukan substitusi dengan menggunakan Caesar cipher. Setelah itu dilakukan columnar transposisi yang sekaligus dikombinasikan dengan rail fence untuk menghasilkan algoritma baru.
Massoud Sokouti, Babak Sokouti, Saeid Pashazadeh	2009	*Transpositio n cipher*	Memodifikasi cara penerapan *tranposition*	Membuat jenis dari transposisi baru.	-	Membagi plaintext ke dalam jenis 64 bit, 128 bit, dan 256 bit.
					-	Kemudian menambahkan 8 bit untuk setiap plaintext, terdiri dari 7 *key* dan 1 random bit.
Quist, Aphetsi Kester	2013	*Columnar Transposisi Cipher*	Menggabungkan Vigenere Cipher dan Columnar Transposisi Cipher	Membuat modifikasi transposisi yang baru	-	Melakukan columner transposisi terlebih dahulu.

					- Cyphertext dari hasil columner transposisi dienkripsi lagi dengan menggunakan vigenere cipher.
Matthew D. Russell, John A. Clark, Susan Stepney	2003	*Cipher Transposition*	Memecahkan *cipher transposition* dengan *Ants*	Membuat *Ants* untuk memecahkan *Transposition Ciphers*	- Menggunakan dua herostik, yang pertama mengenali plaintext menggunakan *dictionary, Dict* dan mengindikasikan keterkaitan kolom dengan bigram, *Adj* - *ACO (Ant Colony Optimisation)* yang digunakan untuk memecahkan *irregular* dan *columner transposition* bahkan sampai *double columner transposition*
Dharmendra Kumar Gupta, Sumit Kumar Srivastava, Vedpal Singh	2012	*Cipher Transposition (Columnar) & Caesar Cipher*	Menggunakan *Columnar Transposition* digabungkan dengan *Caesar Cipher*.	Membentuk suatu metode baru : hybrid antara *columnar transposition & Caesar cipher*	- Plaintext disubstitusikan menggunakan *Caesar cipher* kemudian diterapkan *columnar transposition* - Proses tersebut diulang sebanyak digit dari *key Caesar Cipher*.
Randhir Kumar	2014	*Cipher Transposition & Caesar Cipher*	Metode *cipher Substitution* dan *cipher Transposition* untuk mengkodekan	Mengkodekan memo dengan mengkombinasikan dua algoritma	- Mengkombinasikan dua algoritma (*cipher substitution & transposition*) yaitu hybrid.
Rumalingam Sugumar, Tamilenthi. S, Gurunathan.M	2012	*Transposition Cipher & Caesar Cipher*	Mengkombinasikan Algoritma *Caesar Cipher* dan *Cipher Transposition.*	Melakukan penggabungan *Algoritma Caesar Cipher* & *Cipher Transposition* untuk mngamankan data	- Mengkombinasikan *Cipher Transposition* dan *Cipher Caesar.* - Mengubah plainteks berdasarkan besar *bytes*,dengan *Caesar cipher* dahulu, kemudian menggunakan *cipher transposition.*
Mu. Annalakshmi, A. Padmapriya	2013	*Cipher Transposition*	Mengkombinasikan *Rail fence cipher* dan *columnar transposition*	Mengkombinasikan kedua algoritma supaya lebih aman.	- Mengubah posisi dengan cara *columnar transposition*, kemudian mengubah lagi

					-	dengan *rail fence cipher*. Algoritma ini diberi nama zigzag.
BhowmickA, Geetha, M	2015	*Transpositio n Cipher*	*Cipher Substitution & Cipher Transposition*	Mengkombinasikan antara *cipher substitution I* dan *cipher transposition*	-	Meningkatkan algoritma *columnar transposition* dan *myszkowski transposition*.
Anirban Bhowmick, Anand Vardhan Lal, Nitish Ranjan	2015	*Myszkowski Transpositio n*	Mengkombinasikan *Myszkowski Transposition* dengan *Playfair Cipher*	Meningkatkan keamanan dari algoritma klasik.	-	Menggabungkan *Playfair cipher* dengan matrix 6x6 dan digabungkan dengan *double myszkowski.*

IV. PEMBAHASAN

A. Algoritma *Cipher Transposition*

Cipher Transposition dapat disebut juga sebagai *cipher* permutasi karena sebenarnya metode *cipher transposition* ini memutasikan karakter-karakter plainteks, yaitu dengan menyusun ulang urutan karakter dalam pesan. Metode *Cipher Transposition* dimana posisi plainteks (karakter atau kode khusus) dirubah, sehingga hasilnya menjadi ciperteks dengan urutan yang berubah atau berbeda. Sehingga *Cipher Transposition* merupakan metode yang digunakan untuk mengubah plainteks menjadi ciperteks dengan mengubah urutannya.

Menurut jenisnya, *Cipher Transposition* terdiri dari :

1) Rail Fence Cipher

Rail Fence cipher merupakan salah satu aloritma yang lemah untuk dilakukan Cryptanalyze. Hanya menemukan k*ey* untuk memecahkan, maka sudah dapat memecahkan dan menemukan plainteksnya. Contohnya jika ada dua baris, maka 1, 3, 5 pesan dalam baris tersebut adalah 2, 4, 6 dan seterusnya. *Rail Fence cipher* menjadikan plainteks ditulis ke bawah secara berturut-turut seperti rel dari rel yang telah ditentukan, kemudian bergerak naik. Ciperteksnya dengan membaca berdasarkan baris.

Sehingga *Rail Fence cipher* adalah mengubah susunan dari plainteks menjadi turun kebawah secara ‘zig-zag’ dengan panjang turun kebawah (*key*) ditentukan sebelum naik lagi keatas dengan ‘zig-zag’. Cipherteks yang digunakan yaitu dengan membaca susunan tersebut secara horizontal. *Rail Fence cipher* pernah digunakan selama Perang Saudara Amerika, ketika digunakan untuk penyembunyian pesan militer Union maupun mata-mata Konfederasi.

Contoh : k= 3 *offset = 0*
Plainteks : SATYA WACANA

S……A…….A……
..A..Y…W..C...N….
…T…....A…....A...

Ciperteks : SAAA YWCNT AA

Biasanya penulisannya dengan menggunakan panjang blok, seperti contoh diatas menggunakan panjang blok 5. Bila panjang karakter tidah habis dibagi dengan blok yang ditentukan, biasanya ada penambahan karakter secara *dummy* saat pengenkripsian.

Kelebihan dari *Rail Fence cipher* adalah pada penulisan plainteks menjadi cipherteks yang dilakukan ‘zig-zag’ sehingga menambah kerumitan proses enkripsi maupun dekripsi. Kekurangan dari *Rail Fence cipher* adalah tidak mengubah karakter kedalam karakter lain, hanya mengubah posisi plainteks, sehingga kemungkinan pesan dapat dipecahkan.

2) Route Cipher

Route Cipher adalah plainteks yang pertama ditulis kemudian dibaca menurut *key* yang sudah ditentukan. Pembacaan ciperteks dilakukan dalam pola yang diberikan pada kunci. *Route Cipher* ini diperkenalkan oleh Kolonel Parker Hitt untuk Militer Ciphers, untuk tentara dan warga sipil pada tahun 1916.

Contoh : k = 4, spiral ke dalam arah jarum jam kanan atas.

Plainteks : SATYA WACANA

S Y A N
A A C A
T W A X

Ciperteks : NAX AWT ASY ACA

Kelebihan *Route Cipher* bisa dikatakan mempunyai proses enkripsi rumit. Hal ini dikarenakan *key* yang lebih membuat proses enkripsi dan dekripsi menjadi fleksibel. Kekurangannya yaitu justru pada panjang *key* yang digunakan. Jika pemilihan rute *key* tidak tepat, akan meninggalka potongan plainteks, sehingga dapat memberikan petunjuk pemecahan pesan.

3) Columnar Transposition

Columnar Transposition merupakan enkripsi yang termasuk mudah untuk terdeteksi oleh kriptanalis dengan melihat jumlah frekuensinya. *Columnar Transposition* sendiri merupakan pesan yang ditulis dalam suatu deret yang

kemudian dikolomkan. Cara membacanya dari kolom per kolom sesuai kolom yang terpilih. Dalam perang dunia I, Jerman menggunakan *Columnar Transposition* yang disebut ubchi.

Contoh : kata KUCING mempunyai panjang 6 (panjang baris adalah 6), didefinisikan menurut urutan alphabet dari kata kunci. Dengan menggunakan KUCING menjadi [4 6 1 3 5 2].

Plainteks : KULIAH KAMPUS SATYA WACANA

Enkripsi *Columnar Transposition* dengan *key* KUCING [4 6 1 3 5 2]

4	6	1	3	5	2
K	U	L	I	A	H
K	A	M	P	U	S
S	A	T	Y	A	W
A	C	A	N	A	X
Q	T	Y	V	R	D

Ciperteks : LMTAY HSWXD IPYNV KKSAQ AUAAR UAACT

Pada *Columnar Transposition* secara umum, semua kolom yang kosong diisi dengan *dummy* seperti pada contoh [X Q T Y V R D], namun ada juga yang membiarkan kosong. Jika membiarkan kosong maka Ciperteks menjadi: LMTAH SWIPY NKKSA AUAAU AAC.

Kelebihan *Columnar Transposition* adalah biasanya algoitma ini digunakan untuk menambah kekuatan dan kerumitan *cipher* lain. Sehingga banyak yang dimodifikasikan dengan *Columnar Transposition.* Kekurangannya algoritma ini paling standar, sangat matematis sehingga proses enkripsi dan dekripsi tidak begitu rumit.

4) Myszkowski Transposition

Myszkowski Transposition untuk kedepannya ditulis dalam matriks secara *row-wise manner*. Enkripsi ini merupakan variasi dari *columnar transposition*. *Myszkowski Transposition* merupakan algoritma yang mirip dengan *columnar transposition*, hanya saja algoritma ini menggunakan *key* dari karakter berulang.

Contoh :

Key LAPTOP mempunyai urutan [2 1 4 6 3 5]. Kolom plainteks dengan nomor urutan angka yang unik dibaca kebawah, sedangkan yang sama dibaca dari kiri ke kanan.

Plainteks : AKU KULIAH DI SATYA WACANA *key* = [2 1 4 5 3 4]

2	1	4	5	3	4
A	K	U	K	U	L
I	A	H	D	I	S
A	T	Y	A	W	A
C	A	N	A	S	A
L	A	T	I	G	A

Ciperteks: KATAA AIACL UIWSG ULHSY ANATA KDAAI

Kelebihannya adalah dari keseluruhan *Transposition Cipher*, algoritma ini yang memiliki tingkat kerumitan tinggi dengan kunci yang sederhana, dan memiliki pembacaan ciperteks dua arah. Kelemahannya masih bisa dibaca kriptanalis karena tidak mengganti karakter dari pesan.

B. Analisa Trend Cipher Transposition

Melihat hasil Studi Literatur yang telah dilakukan dari 24 jurnal, dapat melakukan analisa trend para peneliti mengenai algoritma. Analisa trend *cipher transposition* dibedakan menjadi dua, yaitu dilihat berdasarkan tahun penelitian.

Berdasarkan 24 jurnal yang dianalisa, maka dibagi menjadi tiga kelompok trend penelitian yang dilakukan oleh penelti terdahulu terhadap algoritma *transposition*. Kelompok tersebut yaitu : 1) Jurnal < 2010 2) Jurnal 2010-2014 3) Jurnal 2015.

Tabel 2 Analisa Trend Berdasarkan Tahun < 2010

Tahun Jurnal	Trend Penelitian *Cipher Transposition*
2003	Penelitian pada jurnal tahun 2012 terdapat tiga jurnal, yaitu Matthew D. Russell,dkk, yang membahas mengenai *Ants* untuk memecahkan *transposition* bahkan *double transposition*.
2007	Penelitian pada jurnal tahun 2012 terdapat tiga jurnal, yaitu R. Toemeh, S. Arumugam, dan Reyhan Yuanza Pohan, keduanya melakukan penelitian terhadap *transposition* dengan beda cara. Ada yang menggabungkan *transposition* dengan genetic, ada yang melakukan perbandingan di algoritma *transposition*.
2009	Penelitian pada jurnal tahun 2012 terdapat tiga jurnal, yaitu Poonam Garg dan *massoud*., keduanya pembahasannya juga berbeda jauh, yaitu penggabungan *transposition* dengan *genetic* dan jurlah satunya membahas perbandingan dalam jenis *transposition.*

Berdasarkan jurnal pada tahun< 2010, yang mulai trend dilakukan yaitu menghubungan *transposition* dengan allgoritma genetic. Algoritma genetik sendiri seperti sistem pencarian dalam suatu komputerisasi.

Tabel 3 Analisa Trend Berdasarkan Tahun 2010-2014

Tahun Jurnal	Trend Penelitian *Cipher Transposition*
2012	Penelitian pada jurnal tahun 2012 terdapat tiga jurnal, yaitu Mr. Vinod Saroha,dkk, Dharmendra Kumar Gupta,dkk, dan Rumalingam Sugumar, dkk, ketiga jurnal ini semua membahas mengenai penggabungan *transposition* dan *Caesar cipher*. Jurnal-jurnal ini beralasan, karena lemahnya keamanan dari algoritma *Caesar cipher*, maka diperlukan modifikasi. Kemudian untuk *transposition*, karena algoritma ini lebih fleksibel untuk dihubungkan dengan algoritma lain.

2013	Penelitian pada jurnal 2013 terdapat delapan jurnal, yaitu Sombir Singh, dkk, A.S. Al-Khalid, dkk, Gaurav Shrisvastava, dkk, Morteza Heydari, dkk, Anupama Mishra, Gaurav Shrivastava, dkk, Quist, dkk, Mu. Annalakshmi, dkk, kedelapan jurnal ini semua membahas mengenai kombinasi algoritma *transposition* dengan algoritma lain. Melihat data dari delapan jurnal ini, dapat dikategorikan: - pada tahun 2013 ada yang mulai mencoba mengkombinasikan dengan algoritma *playfair*, algoritma *vigenere*, DES, genetik. Alasannya, rata-rata mereka menganggap ketiga algoritma ini cocok untuk *transposition* karena memberikan kerumitan pada plainteks. - Ada dua yang masih mengikuti trend 2012 dengan menggabungkan dengan *Caesar cipher*. Namun ada satu jurnal milik Gaurav Shrisvastava, dkk menggunakan *double transposition.* - Satu jurnal lagi lebih memilih mengkombinasikan dua algoritma dalam *transposition*, yaitu *columnar transposition* dan *rail fence* supaya lebih mengunggulkan *transposition* itu sendiri.
2014	Penelitian pada jurnal 2014 terdapat lima jurnal, yaitu Morteza Heydari, dkk, Omar Alkathiry, dkk, Shishir Shukla,dkk, Jawad Ahmad Dar, Randhir Kumar, kelima jurnal ini: - dua diantaranya masih mengkombinasikan *transposition* dengan *Caesar cipher*. Adapula yang menggabungkan *Caesar cipher* dengan dua algoritma *transposition* sekaligus, yaitu *columnar* dan *rail fance.* - Tiga diantaranya ada yang mencoba mengkombinasikan dengan *cuckoo search*, genetic, dan *affine substitution.*

Berdasarkan Tahun 2010-2014 maka trend yang saat itu dilakukan penelitian terhadap *transposition* yaitu mengkombinasikan *transposition* dengan algoritma *Caesar cipher*, terutama jenis algoritma *columnar transposition.* Pemilihan *columnar transposition* dikarenakan, algoritma ini tergolong yang mudah dipecahkan, sehingga perlu adanya modifikasi dan tidak diimplementasikan sendiri.

Tabel 4 Analisa Trend Berdasarkan Tahun 2015

Tahun Jurnal	Trend Penelitian *Cipher Transposition*
2015	Penelitian pada jurnal 2013 terdapat delapan jurnal, yaitu Okike Benjamin,dkk, BhowmickA,dkk, Anirban Bhowmick,dll. ketiga jurnal ini semua membahas mengenai kombinasi algoritma *transposition* dengan algoritma lain. - dua diantaranya membahas algoritma *myszkowski* yang penelitian pada tahun sebelum-sebelumnya jarang untuk disinggung. Satunya dikombinasikan dengan *playfair*, kemudian jurnal yang satunya dikombinasikan dengan *columnar transposition* dengan *substitution.* - Satu diantaranya penelitian masih menghubungkan *columnar* dengan *irregular.*

Berdasarkan Tahun 2018 maka trend yang dilakukan terhadap penelitian *transposition* yaitu penelitian mulai meneliti algoritma *myszkowski*, walaupun dalam algoritma *transposition* ini merupakan algoritma yang aman, namun masih perlu adanya modifikasi karena hanya memperumit langkah-langkah pemecahan pesan.

IV. REKOMENDASI

Rekomendasi yang diberikan untuk kedepannya, berupa usulan yaitu memanfaatkan algoritma *transposition* yang ada, dengan menggabungkan ketiga algoritma *transposition.* Sehingga dapat memberikan perbaikan algoritma *cipher transposition* dengan menggabungkan kelebihan yang dimiliki dari masing-masing algoritma *transposition.* Kemudia digabungkan dengan algoritma *Caesar cipher*, karena algoritma ini lebih mudah diterapkan dan fleksibel dari langkah kerjanya.

Algoritma ini mengubah dari plainteks menjadi cipherteks menggunakan langkah-langkah *rail fence cipher*, namun menggunakan kolom-kolom seperti *columnar transposition* dengan tambahan kunci seperti pada *route cipher* dan *myszkowski transposition.* Untuk lebih jelasnya, langkah-langkahnya sebagai berikut:

Plainteks : THIS IS MY JOURNAL ABOUT CIPHERS TRANSPOSITION

Enkripsi dilakukan dengan kunci JOURNALS [2 5 8 6 4 1 3 7], *offset* = 0, ganjil bawah-atas, genap kiri-kanan

2	5	8	6	4	1	3	7
T	H	I	S	I	S	M	Y
A	I	A	N	H	U	C	J
H	C	U	T	C	I	P	H
S	N	A	H	T	S	H	E
H	C	S	I	T	I	C	N

Maka Cipherteksnya adalah :

ISIUS ORPOM ONOLH NEHJY TISIA ANRBU TCSAR TPSIT

Kemudian digabungkan lagi dengan menggunakan algoritma *Caesar cipher* dengan panjang kunci pergeseran alphabet dengan k=4, sehingga menjadi :

Ciperteks : MWMYW SVTSQ SRSPL RILNC XMWME ESVFY XGWEV XTWMX

Proses enkripsi dimulai dengan menghitung jumlah panjang *key* (k) dalam hal ini JOURNALS yaitu 8 seperti *rail fence cipher*, kemudian membuat 8 kolom yang dibuat nomor urutan sesuai abjad seperti *columnar transposition.* Urutan penulisannya dilakukan seperti *rail fence* secara horizontal, karena nilai *offset*=0, maka dimulai dari kolom pertama. Setelah kolom terisi, pembacaan cipherteks dilakukan sesuai dengan pembacaan *route cipher* dengan cara mirip *myszkowski transposition*, dalam hal ini ganjil bawah-atas genap kiri-kanan. Hal ini menunjukkan jika nomor kolom ganjil, maka dibaca dari bawah ke atas, kalau genap maka membacanya dari kiri ke kanan. Setelah itu digabungkan dengan algoritma *Caesar Cipher* dengan k=4.

Selain itu untuk kedepannya, pengembangan algoritma *myszkowski transposition* bisa lebih ditingkatkan, karena walaupun tergolong tingkat keamanan *myszkowski transposition* lebih tinggi dibandingkan dengan algoritma *transposition* lainnya, lebih baik jika terus dilakukan pengembangan. Hal ini bisa dilakukan dengan penggabungkan dengan sesama algoritma *transposition* ataupun dengan algoritma *substitution* yang lebih fleksibel dan cocok.

Selanjutnya, dari banyak penelitian belum ada yang membandingkan suatu metode pengembangan yang para peneliti terdahulu lakukan dengan panjang kunci yang berbeda untuk menilai tingkat keamanan pengembangan metode *transposition* yang telah para peneliti lakukan.

V. KESIMPULAN

Cipher Transposition merupakan salah satu algoritma kriptografi yang melakukan pengacakan pada urutan atau posisi semula dari plainteks. *Cipher Transposition* memiliki macam-macam algoritma yang memiliki kelebihan, kekurangan dan cara kerjanya masing-masing, yaitu : *rail fence cipher*, *columnar transposition*, *route cipher*, dan *myszkowski transposition.*

Jumlah 24 jurnal dari studi literature ini, dapat diambil benang merah bahwa secara keseluruhan algoritma *transposition* sudah menjadi algoritma yang tidak aman, karena banyak penelitian yang mengungkapkan dengan beberapa algoritma, dapat melakukan *crack* algoritma *transposition* ini, oleh sebab itu beberapa penelitian yang lain membahas untuk mengembangkan algoritma *transposition* menjadi algoritma baru, baik penggabungan dengan algoritma lain atau mengubah cara *transposition* itu sendiri.

Columner transposition sering dibahas (populer), dikarenakan lebih lemah dibanding jenis *transposition* yang lain, karena tingkat kerumitannya rendah. Sehingga teknik ini lebih fleksibel untuk dikombinasikan dengan algoritma yang lain untuk meningkatkan keamanan. Algoritma lain seperti *rail fence cipher* mempunyai kelebihan saat penulisan menjadi cipherteks, *route cipher* mempunyai kelebihan penentuan kunci yang paling kuat, dan *myszkowski transposition* mempunyai kelebihan sebagai algoritma pengembangan yang baik diantara algoritma *transposition* lainnya.

Kekurangan dari keempat algoritma *transposition* yaitu frekuensi kemunculan cipherteks yang sama dengan plainteks. Sehingga untuk menghasilkan algoritma yang lebih aman, sebaiknya algoritma *transposition* dikolaborasikan dengan algoritma *substitution* atau dengan merancang algoritma baru. seperti contohnya dalam usulah pada rekomendasi yang menggabungkan keempat algoritma *transposition* dengan algoritma *Caesar cipher.*

Berdasarkan 24 jurnal yang dianalisa, menunjukkan bahwa *transposition cipher* lebih banyak dimodifikasi dengan algoritma *Caesar cipher,* karena selain menambah tingkat kerumitan mengubah plainteks, keduanya lebih fleksibel untuk diterapkan. Kedepannya, yang lebih banyak dilakukan penelitian, perkembangan salah satu algoritma *transposition* adalah algoritmas *myszkowski*.

DAFTAR PUSTAKA

[1] Hidayat, S.M. (n.d). Studi Literatur. UMB: Pusat Pengembangan Bahan Ajar

[2] Ariyanto, Endro, dkk. 2008. Analisa Implementasi Algoritma Stream Cipher Sosemanuk Dan Dicing Dalam Proses Enkripsi Data, Institut Teknologi Telkom, Bandung

[3] Syafa'at, Achmad. 2009. Perbandingan Kriptografi Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher, Universitas Langlang Buana, Bandung Caroline, L. Maureen. 2012. Metode Enkripsi Baru : Triple Transposition Vigènere Cipher, Institut Teknologi Bandung, Bandung

[4] Heydar, M., Senejani, M.N. 2014. Automated Cryptanalysis of TransporsitionCiphers Using Cuckoo Search Algorithm. International Journal of Computer Science and Mobile Computing. Vol.3. Issue 1. Pp 140-149

[5] Singh, S., Maakar, S.K., Kumar, S. 2013. Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques. International Journal of Advanced Research in Computer Science and Software Engineering. Vo. 3. Issue 6. Pp 464-471

[6] Saroha, V., Mor, S., Dagar, A. 2012. Enhancing Security of Caesar Cipher by Double Columnar Transposition Method. Vol. 2. Issue 10. Pp 86-88

[7] Al-Khalid, A.S., Omran, S.S., Hammood, D.A. 2013. Using Genetic Algorithms To Break A Simple Transposition Cipher. The 6th International Conference on Information Technology (ICIT)

[8] Shrivastava, G., Sharma, R., Chrouhan, M. 2013. Using Letters Frequency Analysis in Caesar Cipher With Double Columnar Transposition Technique. International Journal Of Engineering Sciences & Research Technology

[9] Alkathiry, O., Al-Morgen, A. 2014. A Powerful Genetic Algorithm to Crack a Transposition Cipher. International Journal of Future Computer and Communication. Vol 3. No 6. Pp 395-399

[10] Heydar, M., Shabgahi, G.L., Heydari, M.M. 2013. Cryptanalysis of Transposition Cipher with Long Key

Lengths Using an Improved Genetic Algorithm. World Applied Sciences Journal
[11] Toemeh, R., Arumugam, S. 2007. Breaking Transposition Cipher with Genetic Algorithm. Electronics And Electrical Engineering
[12] Mishra, A. 2013. Enhancing Security Of Caesar Cipher Using Different Methods. International Journal of Research in Engineering and Technology. Vol 02. Issue 09. Pp 327-332
[13] Shukla, S., Verma, P.K. 2014. Implementation of Affine Substitution Cipher With Keyed Transposition Cipher for Enhancing Data Security. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 4. Issue 1
[14] Shrivastava, G., Sharma, R., Chouhan, M. 2013. Using Letters Frequency Analysis in Caesar Cipher With Double Columnar Transposition Technique. International Journal Of Engineering Sciences & Research Technology
[15] Garg, P. 2009. Genetic Algorithms, Tabu Search And Simulated Anneling : A Comparison Between Three Approaches For The Cryptanalysis Of Transposition Cipher. Journal of Theoretical and Applied Information Technology
[16] Benjamin, O., Garba, E.J.D. 2015. Development of Okike's Merged Irregular Transposition Cipher and Its Level Error. British Journal of Mathematics & Computer Science
[17] Pohan, R.Y. 2007. Studi dan Perbadingan Berbagai Macam Algoritma Cipher Transposisi. Teknik Informatika : ITB
[18] Bhowmick, A., Geetha, M. 2015. Enhancing Resistance of Hill Cipher Using Columnar and Myszkowski Transposition, International Journal of Computer Sciences and Engineering. Vol. 03.Issue 02. Pp 20-27
[19] Bhowmick, A., Lal, A.V., Ranjan, Nitish. 2015. International Journal Engineenering Research & Technology(IJERT). VOl 4. Issue 07. Pp 1001-1014.
[20] Dar, J.A. 2014. Enhancing The Data Security Of Simple Columnar Transposition Cipher By Caesar Cipher And Rail Fence Cipher Technique.
[21] Sokouti, M., Sokouti, B., Pashazadeh, S. 2009. An Approach in Improving Transposition Cipher System. Indian Journal of Science and Technology
[22] Quist., Kester, A. 2013. A Hybrid Cryptosystem Based On Vigenere Cipher And Columnar Transposition Cipher. International Journal Of Advanced Technology & Engineering Research (IJATER)
[23] Russell, M.D., Clark, J.A., Steoney, S. [n.d]. Making the Most of Two Heuristics: Breaking Transposition Cipher with Ants.
[24] Gupta, D.K., Srivastava, S.K., Singh, V. 2012. New Concept Of Symmetric Encryption Algorithm A Hybrid Approach Of Caesar Cipher And Columnar Transportation In Multi Stages. Journal of Global Research in Computer Science. Vol 3. Issue 1. January
[25] Kumar, R. 2014. Integration Of Caesar Cipher with Redefence cipher Enhancing Data Security.International Journal for Scientific Research & Development. Vol 2. Issue 05
[26] Sugumar, R., S, Tamulahenthi., Gurnathan, M. 2012. Review of Effective Data Encrystion and Decryption Technique
[27] Annalakshmi, Mu. Padmapriya, A. 2012. Zigzag Ciphers : A Novel Transposition Method. International Conference on Computing and Information.
[28] Christensen, C. 2006. Transposition Ciphers.http://www.nku.edu/, diakses pada 31 Agustus 2018