MODIFIKASI *RAIL FENCE TRANSPOSITION CIPHER* DENGAN *CHESS BOARD PATTERN*

SKRIPSI

OLEH
MUHAMMAD DENDY ARIFANDA
NIM. 14610008

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

MODIFIKASI *RAIL FENCE TRANSPOSITION CIPHER* DENGAN *CESS BOARD PATTERN*

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan
dalam Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
MUHAMMAD DENDY ARIFANDA
NIM. 14610008

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2021

MODIFIKASI *RAIL FENCE TRANSPOSITION CIPHER* DENGAN *CHESS BOARD PATTERN*

SKRIPSI

Oleh

MUHAMMAD DENDY ARIFANDA

NIM. 14610008

Telah Diperiksa dan Disetujui untuk Diuji

Tanggal 29 Mei 2021

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M.Si	Mohammad Nafie Jauhari, M.Si
NIDT. 19900511 20160801 1 057	NIDT. 19870218 20160801 1 056

Mengetahui,

Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si.
NIP. 19650414 200312 1 001

MODIFIKASI *RAIL FENCE TRANSPOSITION CIPHER* DENGAN *CHESS BOARD PATTERN*

SKRIPSI

Oleh

MUHAMMAD DENDY ARIFANDA

NIM. 14610096

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 28 Mei 2021

Penguji Utama	: Juhari, M.Si	.....
Ketua Penguji	: Evawati Alisah, M.Pd	.....
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	: Mohammad Nafie Jauhari, M.Si	.....

Mengetahui,

Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si.
NIP. 19650414 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Dendy Arifanda

NIM : 14610008

Program Studi : Matematika

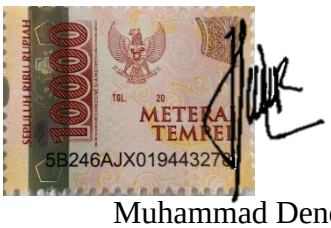
Fakultas : Sains dan Teknologi

Judul Skripsi : *Modifikasi Rail Fence Transposition Cipher* Dengan *Chess Board Pattern*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 6 Juni 2021

Yang membuat pernyataan,



Muhammad Dendy Arifanda

NIM.14610008

MOTTO

“Kamu mungkin tidak bisa kembali mengawali cerita, tapi kamu bisa memulai lagi untuk memperbaiki cerita”

~ Emha Ainun Nadjib ~

PERSEMBAHAN

Skirpsi ini penulis persembahkan untuk:

Ayahanda H. Sonlaili dan Ibunda Hj. Aminatus Sholihah tercinta, yang senantiasa dengan ikhlas mendoakan, memberikan nasehat, semangat, dan kasih saying yang tak ternilai kepada penulis. Istri tercinta Devi Nindy Purnama Sari yang senantiasa memberikan motivasi kepada penulis. Adik Muhammad Akbar Siregar dan Bilqis Fitri Nur Humairo' yang selalu memberikan dukungan kepada penulis.

KATA PENGANTAR

Assalamua'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt atas rahmat, taufik serta hidayah-Nya. Sehingga penulis mampu menyelesaikan penyusunan skripsi ini sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu penulis ucapan terimakasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya sampaikan terutama kepada:

1. Prof. Dr. H. Abd. Haris, M.Ag, selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si, Selaku Ketua Program Studi Matematika, Fakultas Sains Dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M.Si, sebagai pembimbing satu skripsi atas arahan, nasihat, dan ilmu yang diberikan untuk penulis.
5. M. Nafie Jauhari, M.Si, sebagai pembimbing dua skripsi atas saran dan arahan untuk penulis.
6. Juhari, M.Si, sebagai penguji utama skripsi atas saran dan kritik untuk penulis.

7. Evawati Alisah, M.Pd, sebagai ketua penguji skripsi atas kritik, saran dan dukungan untuk penulis.
8. Segenap sivitas akademika Program Studi Matematika, Fakultas Sains dan teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, terutama seluruh Dosen terimakasih atas segala ilmu dan bimbingannya.
9. Bapak H. Sonlaili dan Ibu Hj. Aminatus Sholihah yang selalu memberikan do'a, semangat serta motivasi kepada penulis sampai saat ini.
10. Sahabat-sahabat terbaik penulis yang selalu menemani, membantu, dan memberikan dukungan sehingga penulis dapat menyelesaikan skripsi ini.
11. Seluruh teman-teman di program studi matematika angkatan 2014 (MATH EIGEN) khususnya matematika-A, Teman-teman Pejuang Kripto, teman KBMB angkatan 2014, Terimakasih atas segala pengalaman berharga, kerja sama dan kebersamaan atas kenang-kenangan indah yang dirajut bersama dalam menggapai impian.

Semoga Allah SWT melimpahkan rahmat dan karunia-Nya kepada kita semua. Akhirnya penulis berharap semoga dengan rahmat dan izin-Nya mudah-mudahan skripsi ini bermanfaat bagi penulis dan bagi pembaca. *Amiin*

Wassalamualaikum Warahmatullahi Wabarakatuh

Malang, 3 Mei 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

ABSTRAK

Arifanda, Muhammad Dendy. 2021. **Modifikasi *Rail Fence Transposition Cipher* dengan *Chess Board Pattern***. Skripsi. Progam Studi Matematika Fakultas Sains Dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) M. Nafie Jauhari, M.Si.

Kata Kunci : Enkripsi, Dekripsi , Rail Fence Cipher, Chess Board Pattern

Algoritma *Rail Fence* merupakan algortima kriptografi kunci simetri yang menggunakan metode transformasi. Algoritma *Rail Fence* sering pula dikenal dengan algortima zig-zag, karena karakter pada pesan akan disusun ulang dengan cara membuat lintasan zig-zag. Enkripsi merupakan proses menyandikan pesan teks menjadi pesan tak terbaca, pesan asli tersebut plaintext (teks biasa) yang dirubah menjadi kode-kode yang sulit untuk dimengerti. Sedangkan dekripsi merupakan proses pengembalian pesan yang dienkripsikan ke bentuk asalnya.

Pada penelitian ini, peneliti memodifikasi Algoritma *Rail Fence* dengan menggunakan *Chess Board Patern*. Enkripsi dan dekripsi dengan *Chess Board Pattern* dilakukan dengan mengikuti pola papan catur berwarna hitam putih. Penelitian ini menggunakan kunci 2, 3, 4, 5, dan 6. Dari kelima kunci pada *key* 2 yang di modifikasi menggunakan *Chess Board Pattern* hasilnya tetap sama apabila di enkripsikan menggunakan *Rail Fence*, akan tetapi pada *key* 3, 4, 5, 6 yang sudah di modifikasi menggunakan chess board pattern memiliki hasil yang berbeda apabila dibandingkan dengan hasil enkripsi menggunakan *Rail Fence* biasa. Modifikasi *Rail Fence* dengan *Chess Board Pattern* ini berlaku apabila (*key*) > 2 agar memiliki hasil yang lebih rumit. Kombinasi algoritma *Rail Fence* dengan *Chess Board Pattern* menghasilkan pola enkripsi dan dekripsi yang beragam, sehingga proses enkripsi dan dekripsi menjadi lebih rumit. Hal ini dapat meningkatkan keamanan pesan rahasia dari pihak yang terlibat.

ABSTRACT

Arifanda, Muhammad Dendy. 2021. **On The Modification Of Rail Fence Transposition Cipher With Chess Board Pattern.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Supervisor: (I) Muhammad Khudzaifah, M.Sc. (II) M. Nafie Jauhari, M.Sc.

Keywords: Encryption, Decryption, Rail Fence Cipher, Chess Board Pattern

The Algorithm Rail Fence is often known as the zig-zag algorithm, because the characters in the message will be rearranged using a zig-zag path. An Encryption is the process of encoding a text message into an unreadable message, the original message is plaintext which is converted into codes that are difficult to understand. While decryption is a process of turring encrypted message to its original form.

In this study, the researcher modified the Rail Fence Algorithm by using the Chess Board Pattern. Encryption and decryption with the Chess Board Pattern is done by following the black and white chessboard pattern. This study uses 2, 3, 4, 5, and 6 keys. Among the five keys in key 2 which are modified using the Chess Board Pattern the results remain the same when encrypted using Rail Fence, but on keys 3, 4, 5, 6 which has been modified using the chess board pattern has different results when compared to the results of encryption using Rail Fence ordinary. The Modification of Rail Fence with Chess Board Pattern is valid if (key) > 2 to have more complicated results. The combination of the Rail Fence algoritm with the Chess Board Pattern produces a variety of encryption and decryption patterns, so that the encryption and decryption process becomes more complicated. This can increase the security of confidential messages from the parties involved.

ملخص

أريفا ندا ، محمد دندي. ٢٠٢١. **تعديل شفرة نقل سياج السكك الحديدية مع نمط لوحة الشطرنج** أطروحة.
برنامج دراسة الرياضيات ، كلية العلوم والتكنولوجيا ، جامعة الولاية الإسلامية مولانا مالكإبراهيم مالانج. المشرف: (١)محمد خديفة، ماجستير.(٢)محمد نافع جوهري ، ماجستير

الكلمات الرئيسية : التشفير ، فك التشفير ، تشفير سياج السكك الحديدية ، نمط لوح الشطرنج

تطور التكنولوجيا ينمو حاليا بسرعة. في بعض الأحيان تكون هذه البيانات سرية ، مثل البيانات التنظيمية
وبيانات الحالة والبيانات الشخصية. يجب الحفاظ على هذه السرية حتى لا يسيء أحد استخدام البيانات. إن أمان الرسالةهيتشفير تستخدم طريقة تحويل مفتاح *Rail Fence* السرية هو الهدف الرئيسي في تطوير التشفير. خوارزميةخوارزميةلأنه سيتم إعادة ترتيب الأحرف في ، zig-zag غالباً ما تعُرفأيضًا باسم خوارزمية *Rail Fence* متماثل.خوارزميةالرسالة عن طريق إنشاء مسار متعرج. التشفير هو عملية تشفير رسالة نصية في رسالة غير قابلة للقراءة ، والرسالةالأصلية عبارة عن نص عادي (نص عادي) يتم تحويله إلى أكواد يصعب فهمها. بينما فك التشفير عبارة عن رسالة تمإرجاعها إلى شكلها الأصلي

في هذه الدراسة ، قام الباحث بتعديل خوارزمية سياج السكك الحديدية باستخدام نمط رقعة الشطرنج. يتم التشفيروفك التشفير باستخدام نموذج رقعة الشطرنج باتباع نمط رقعة الشطرنج بالأبيض والأسود. تستخدم هذه الدراسة المفاتيح ٢و ٣ و ٤ و ٥ و ٦. من المفاتيح الخمسة في المفتاح ٢ والتي تم تعديلها باستخدام نموذج لوحة الشطرنج ، تظل النتائج كماهي عند تشفيرها باستخدام سياج السكك الحديدية، ولكن على المفاتيح٣ و ٤ و ٥ ، ٦ الذي تم تعديله باستخدام نمط رقعةالشطرنج له نتائج مختلفة عند مقارنته بنتائج التشفير باستخدام سياج السكك الحديدية العادي. تعديل سياج السكك الحديديةمع نمط الشطرنج صحيح إذا(مفتاح)<2 للحصول على نتائج أكثر تعقيدا. مزيج من الخوارزمية سياج السكك الحديدية معنمط الشطرنج تنتج مجموعة متنوعة من الأنماط التشفير وفك التشفير، بحيث تصبح عملية التشفير وفك التشفير أكثر.تعقيدا. هذا يمكن أن يزيد من أمن الرسائل السرية من الأطراف المعنية

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini sudah berkembang semakin pesat. Dengan berkembangnya teknologi informasi ini, pertukaran data menjadi suatu permasalahan. Hampir setiap hari pertukaran data terjadi, data ini bervariasi besarnya maupun jenisnya. Adakalanya data-data ini bersifat rahasia seperti data organisasi, data negara, maupun data pribadi.

Keamanan merupakan hal yang sangat penting bagi setiap individu maupun kelompok. Baik keamanan dari hal yang berupa kejahatan fisik, hingga kejahatan dunia maya. Kerahasiaan ini perlu di jaga agar tidak ada orang yang menyalahgunkan data-data tersebut. Maka informasi hanya boleh disampaikan kepada yang berhak menerimanya saja, seperti firman Allah SWT berikut:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ

***Artinya**:*

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui. (QS.Al-Anfal /8:27).

Dalam surah Al-Anfal ayat 27 tersirat bahwa “janganlah kamu mengkhianati amanat-amanat” agama Islam memerintahkan bahwa amanat apapun merupakan hal penting yang perlu dijaga. Maka agar terhindar dari keburukan media sosial perlu adanya solusi agar amanat-manat tersebut sampai kepada pihak yang dituju.

Kriptografi merupakan suatu ilmu menyembunyikan informasi. Kriptografi telah digunakan selama bertahun-tahun dengan tujuan untuk membuat informasi

penting hanya terbaca untuk penerima informasi (Zaru & Khan, 2018). Sampai saat ini sudah ada berbagai macam algoritma kriptogafi namun secara keseluruhan algoritma kriptografi dibagi menjadi dua yaitu klasik dan modern.

Kriptografi terdapat metode yang cukup penting, salah satunya adalah enkripsi(*encryption*). Enkripsi adalah proses mengubah pesan asli (*plaintext*) ke bentuk kode-kode yang tidak dapat dibaca (*ciphertext*). Sedangkan proses untuk mengembalikan ciphertext menjadi plaintext disebut dekripsi(*decryption*) (Ariyus, 2008).

Metode enkripsi Rail Fence merupakan satu bentuk *cipher* transposisi sederhana yang diinspirasi dari model *Polybius square*. *Polybius square* adalah menyusun huruf sebagai matriks 5x5 dang mengkodekan huruf A sebagai 1-1, uruf B sebagai 1-2 dan seterusnya. Setiap karaker pada *Polybius square* diganti dengan indeks *cell* matriks tanpa menggunakan kunci khusus dan hanya merubah posisi segingga teks tidak berbeda. Berbeda dengan *Polybius square* motode Rail Fence menyusun teks secara zig-zag yang model matriksnya diketahui oleh pengirim dan penerima pesan (Siahan, 2016).

Berdasarkan penelitian yang dilakukan oleh (Jayadilaga, 2017), dalam penelitian yang berjudul “Kriptografi Hybrid Algoritma Rail Fence Dan Elgamal Dalam Pengamanan Data Berbasis Teks”, algoritma Rail Fence memiliki kelebihan proses enkripsi dan dekripsi. Akan tetapi Algoritma Rail Fence memiliki kelemahan mudah untuk dipecahkan, karena semua karakter *plaintext* masih ada dan hanya mengalami perubahan posisi (Jayadilaha, 2017). Serta dalam penelitian Nurul Khairina pada tahun 2019 melakukan modifikasi algoritma myzkowski tranasposition cipher dengan menggunakan chess board pattern. Enkripsi dan

deskripsi dengan chess board pattern dilakukan dengan mengikuti pola papan catur berwarna hitam dan putih. Kombinasi algoritma myszkowski dengan *Chess Boar Pattern* menghasilkan enkripsi dan dekripsi yang beragam, hal ini dapat me ningkatkan keamanan pesan rahasia dari pihak yang terlibat (Khairina, 2019).

Algoritma Rail Fence memiliki kelebihan dan kekurangan, dimana kekurangan dari algoritma ini mudah untuk dipecahkan, maka peneliti akan memodifikasi Rail Fence dengan menggunakan Chess Board Pattern. Modifikasi ini bertujuan untuk memberikan penyandian baru, sehingga ciphertext yang dihasilkan akan lebih sulit untuk di pecahkan. Mencermati hal yang tela diuraikan di atas , maka penulis melakukan penelitian dengan judul " Modifikasi *Rail Fence Transposition Cipher* dengan *Chess Board Pattern*".

1.2 Rumusan Masalah

Merujuk pada latar belakang tersebut peneliti membuat rumusan masalah sebagai berikut:

1. Bagaimana proses enkripsi Algoritma Rail Fence Transposition dengan modifikasi menggunakan Chess Board Pattern?
2. Bagaimana proses dekripsi Algorima Rail Fence Transposition dengan modifikasi menggunakan Chess Board Pattern?

1.3 Tujuan Penelitian

Berdasarkan rumusan maslah di atas maka tujuan dari penelitian ini adalah:

1. Mengetahui proses enkripsi Algorima Rail Fence Transposition dengan modifikasi menggunakan Chess Board Pattern.
2. Mengetahui proses dekripsi Algorima Rail Fence Transposition dengan modifikasi menggunakan Chess Board Pattern.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan mampu memberikan bagi pembaca dan peneliti khususnya, selain itu juga diharapkan:

1. Mampu membantu pengamanan data.
2. Sebagai sarana pengembangan keilmuan dibidang matematika terapan.
3. Sebagai bahan referensi dalam pengembangan penelitian lebih lanjut.

1.5 Metode Penelitian

Penulisan penelitian ini dilakukan dengan studi literatur. Penulisan dimulai dengan mempelajari jurnal-jurnal, tugas akhir, artikel dan buku-buku tentang enkripsi serta dekripsi pada pesan teks beserta algoritma-algoritmanya. Adapun langkah-langkah penyelesaian penelitian ini, sebagai berikut:

1. Menyusun enkripsi Algoritma Rail Fence dengan memodifikasi menggunakan Chess Board Pattern.
   a. Menentukan 16 karakter huruf yang akan digunakan sebagai *plaintext*
   b. Menentukan berapa angka kunci dan jumlah baris sesuai dengan jumlah karakter plainteks
   c. Memasukkan plaintext pada baris dan kolom yang telah di sediakan dengan diagonal dari atas ke bawah dengan mengikuti pola rail fence
   d. Mengenkripsikan pesan dengan pola Algoritma rail fence pada kotak yang berwarna putih pada chess board pattern
2. Menyusun dekripsi Algoritma Rail Fence dengan dengan memodifikasi menggunakan Chess Boar Pattern
   a. Mendeskripsikan hasil dari enkripsi menggunakan chess board pattern

b. Menyusun dan membagi karakter entri ciphertext menjadi 3, 4, 5, dan 6 bagian secara berbaris kebawah
c. Mendekripsikan dengan menggunakan pola Rail Fence

1.6 Sistematika Penulisan

Adapun sistematika penulisan yang digunakan penulis terdiri dari empat bab, yang masing-masing terdapat subbab seperti berikut:

Bab I Pendahuluan

Bab ini meliputi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini berisi tentang definisi maupun teorema-teorema yang mendukung topik yaitu Pesan Teks, Algoritma kriptografi, Algorima kriptografi klasik, Algoritma Kriptografi modern, Enkripsi, Dekripsi, Algoritma Rail Fence Transposition Ciphter, serta Chess Board Pattern.

Bab III Pembahasan

Bagian pembahasan ini akan menjelaskan dan menguraikan secara keseluruhan langkah-langkah Enkripsi dan Deskripsi pada Algoritma Rail Fence Transposition Ciphter yang kemudian di modifikasi dengan Chess Board Pattern.

Bab IV Penutup

Bab ini berisi kesimpulan dari pembahasan yang sesuai dengan hasil penelitian, yang selanjutnya dapat digunakan sebagai saran bagi pembaca dan peneliti selanjutnya.

BAB II
KAJIAN PUSTAKA

2.1 Kriptografi

2.1.1 Definisi Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani "*cryptos*" yang berarti rahasia, dan "*graphein*" yang berarti tulisan. Oleh sebab itu kriptografi dapat diartikan sebagai tulisan rahasia. Terdapat beberapa definisi kriptografi dalam berbagai sumber. Deinisi lain dari kriptografi yaitu ilmu yang mempelajari metode-metode matematika yang berhubungan dengan aspek keamanan informasi seperti integritas, kerahasiaan serta otentikasi data (Nurdin, 2017).

Dengan demikian, kriptografi adalah suatu ilmu sekaligus seni yang memiliki tujuan untuk menajaga keamanan sebuah pesan (*cryptography is the art and science of keeping message secure*). Secara umum kriptografi adalah teknik pengamanan informasi dimana informasi diubah dengan kunci tertentu melalui enkripsi dan menjadikan informasi ke dalam suatu bentuk informasi baru yang tidak bisa di baca oleh orang yang tidak berhak menerima pesan tersebut, dan informasi tersebut hanya dapat diubah kembali menjadi informasi semula oleh orang yang berhak menerimanya melalui proses deskripsi (Nurdin, 2017).

2.1.2 Manfaat Kriptografi

Kriptografi memiliki beberapa aspek dalam tujuan untuk memberikan layanan keamanan. Aspek-aspek tersebut adalah sebagai berikut:

a. Kerahasiaan (*confidentiality*), yaitu layanan yang digunakan untuk menajaga isi pesan dari siapapun yang berhak untuk membacanya.

b. Otentikasi (*authentication*), adalah layanan yang digunakan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*). “Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?”.

c. Integritas data (*data integrity*), merupakan layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. “apakah pesan yang diterima masih asli atau tidak mengalami perubahan (*modifikasi*)?”.

d. Nirpenyangkalan (*non-repudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.1.3 Kompenen Kriptografi

Pada dasarnya komponen kriptografi terdiri dari beberapa komponen, antara lain:

1. Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli tersebut *plaintext* (teks biasa), yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode. Saama halnya dengan tidak mengerti sebuah kata maka dapat di lihat didalam kamus atau daftar istilah. Untuk mengubah teks biasa ke dalam bentuk teks kode dapat kita gunakan algoritma yang mengkodekan data yang kita inginkan.

2. *Dekripsi* merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsikan dikembalikan ke bentuk asalnya. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. *Kunci* adalah yang dipakai untuk melakukan enkripsi dan deksipsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia(*private key*) dank unci umum (*public key*).
4. *Ciphertext* merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).
5. Plaintext sering disebut dengan cleartext. Teks asli atau teks biasa ini merupakan pesan yang di tulis atau di ketik yang memiliki makna. Teks asli ini di proses menggunakan algoritma kriptografi untuk menjadi *ciphertext* (teks kode).
6. Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*,dsb).
7. *Cryptanalysis* bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks kode berasil diubah menjadi teks asli tanpa menggunakan kunci yang sah, proses tersebut dinamakan *breaking kode*.

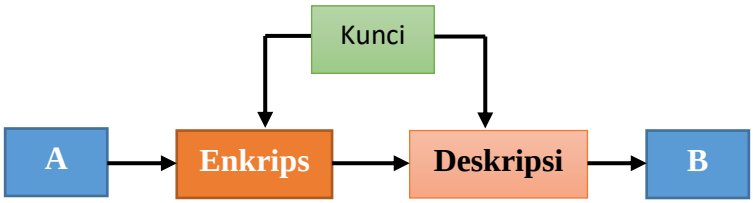
2.2 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Algoritma kriptografi ini bekerja dalam kombinasi dengan menggunakan kunci (key) seperti kata, nomor atau frase tertentu.

2.2.1 Algoritma Simetri

Algoritma ini juga disebut dengan algoritma klasik, karena memakai kunci yang sama untuk melakukan enkripsi dan deskripsi. Keamanan dari pesan yang menggunakan algortima ini tergantung pada kunci, jika kunci tersebut diketahui oleh orang lain maka orang tersebut tentunya bisa melakukan enkripsi dan deskrpsi terhadap pesan tersebut. Algoritma yang memakai kunci simetri diantaranya adalah Data Encryption Standart (DES), International Data Encryption Algorithm (IDEA) Advanced Encryption (AES), One Time Pad (OTP), dan lain sebagainya. Secara sederhana proses pengiriman pesan dengan algoritma sistematis dapat digambarkan sebagai berikut:



Gambar 2.1 Algoritma Simetris

Kelebihan kriptografi simetris adalah (Kamil, 2016) :

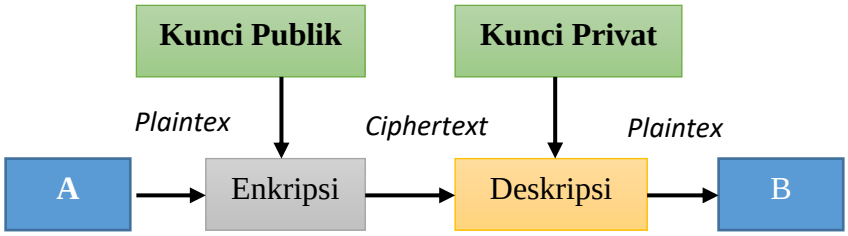
a. Proses enkripsi atau deskripsi kriptografi simetris membutuhkan waktu yang singkat.
b. Ukuran kunci simetris relative pendek.
c. Otentikasi pengiriman pesan langsung dari *ciphertext* yang diterima, karena kunci hanya diketahui oleh penerima dan pengirim saja.

Kekurangan kriptografi simetris adalah (Kamil, 2016):

a. Kunci simetris harus dikirim melalui saluran komunikasi ang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.
b. Kunci harus sering diubah, setiap kali melaksanakan komunikasi. Apabila kunci tersebut hilang atau lupa, maka pesan tersebut tidak dapat dibuka.

2.2.2 Algoritma Asimetri

Berbeda dengan kriptografi kunci simetris, kriptografi kunci public memiliki dua buah kunci yang berbeda pada proses enkripsi dan deskripsi. Kunci yang digunakan sering di sebut public Key dan deskripsi atau sering disebut Private key menggunakan kunci yang berbeda. Entitas pengirim akan mengenkripsikan dengan menggunakan kunci public, sedangan entitas penerima mendeskripsi menggunakan kunci Privat. Skema dari kriptografi dapat di lihat pada gambar:



Gambar 2.2 Algoritma Asimetri

Kelebihan kriptografi asimetris adalah (Kamil, 2016):

a. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomuniksi. Tidak ada kebutuhan mengirim kunci private sebagaimana kunci simetri.

b. Pasangan kunci privat dan kunci publik tidak perlu diubah dalam jangka waktu yang sangat lama.
c. Dapat digunakan dalam pengaman pengiriman kunci simetris.

Kelemahan kriptografi asimetrus adalah (Kamil, 2016):

a. Proses enkripsi dan deskripsi umumnya lebih lambat dari algoritma simetri, karena menggunakan bilangan yang besar.
b. Ukuran *ciphertext* lebih besar dari *plaintext*.
c. Ukuran kunci relative lebih besar dari pada ukuran kunci simetris.

2.3 Transposisi

Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati. Transposisi sering dikombinasikan dengan teknik lain untuk memperkuat keamanan suatu data (Supriyanto, Ardhianto, 2008). Terdapat beberapa algoritma dalam metode penyandian transposisi yaitu :

1. Penyandian transposisi Rail Fence cipher
2. Penyandian transposisi route
3. Penyandian transposisi kolom
4. Penyandian transposisi ganda

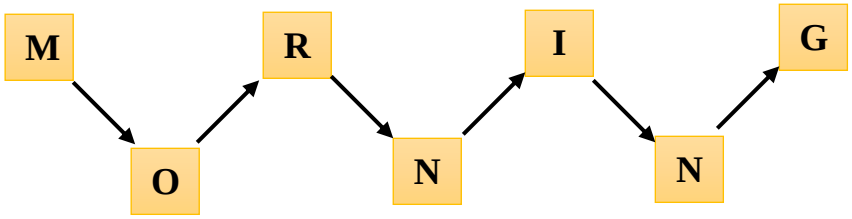
2.4 Algoritma Rail Fence Cipher

Algoritma *rail fence* merupakan algoritma kriptografi kunci simetri yang menggunakan metode transposisi. Cara kerja dari metode transposisi yaitu dengan menyusun ulang posisi masing-masing karakter pada pesan atau *plaintext* sehingga

didapatkan suatu enkripsi yang berbeda dari pesan aslinya. Algoritma rail fance sering pula dikenal dengan algoritma zig-zag, karena pada algoritma rail fence karakter pada pesan akan di susun ulang dengan cara membuat lintasan zig-zag. Kunci dari metode ini adalah seberapa banyak baris yang digunakan untuk melakukan proses enkripsi dan deskripsi. Baris yang digunakan harus lebih dari satu baris.

Langkah-langkah yang perlu dilakukan untuk mengenkripsi pesan dalam algoritma *rail fence* (Saini, 2015) adalah sebagai berikut :

a. Misalkan pesan yang akan dienkripsikan adalah MORNING dengan menggunakan kunci dua baris.
b. Pesan atau *plaintext* ditulis secara berururtan dengan bentuk diagonal.



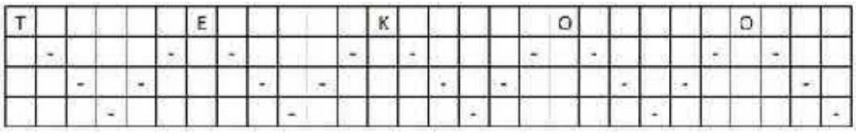
Gambar 2.3 Contoh Algoritma *Rail Fence*

c. Untuk mendapatkan hasil enkripsi, karakter ditulis secara berurutan dari kiri ke kanan dimulai dari baris yang paling atas. Sehingga diperoleh *ciphertext* yaitu MRIGONN.

Langkah-langkah dalam deskripsi ciphertext dari algoritma rail fence (Clark, n.d) adalah sebagai berikut:

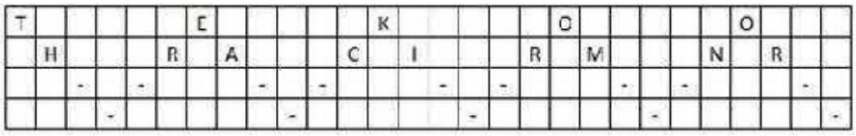
a. Misalkan pesan yang akan dienkripsi adalah TEKOOHRACIRMN-REATANFTETYTGHH dengan jumlah 4 baris (kunci) dan panjang 28 kolom (banyak karakter).

b. Letakkan “T” pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “E”. Lanjutkan hingga baris pertama mendapatkan pola seperti Gambar 2.4

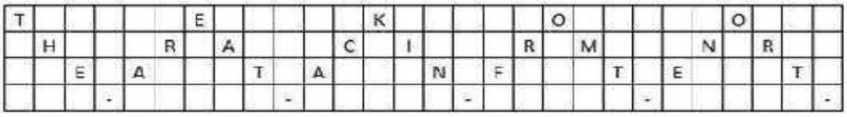


Gambar 2.4 Tahap Pertama Proses Deskripsi

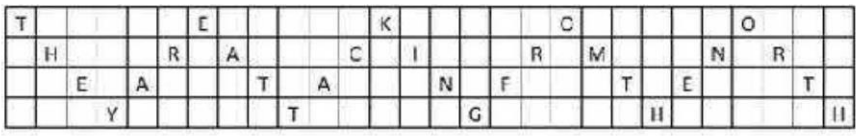
c. Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar 2.7



Gambar 2.5 Tahap Kedua Proses Deskripsi



Gambar 2.6 Tahap Ketiga Proses Deskripsi



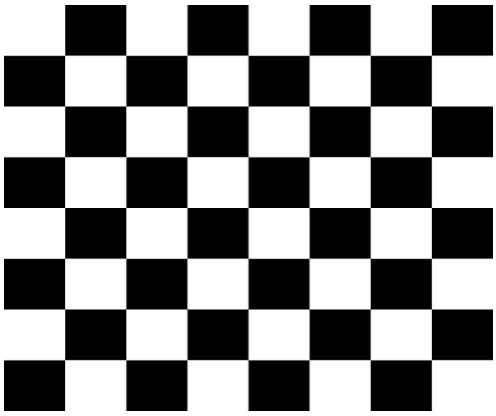
Gambar 2.7 Tahap Keempat Proses Deskripsi

d. Dari Gambar 2.7. didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu “THEY ARE ATTACKING FROM THE NORTH”.

2.5 Chess Board Pattern

Proses enkripssi kriptografi membutuhkan pola penyisipan yang sangat unik untuk mengamankan data dari pihak yang terkait. *Chess Board Pattern* memiliki pola seperti papan catur, dimana terdapat kolom berwarna hitam dan kolom berwarna putih yang saling berselang seling.

Teknik menyisipkan pesana pada pixel citra sangat menetukan hasil *stego-image*, model *chess board pattern* adalah teknik penyisipkan hasil modifikasi. Pesan akan disisipakn setiap kelang 1 pixel (Khairina, 2018). Adapun gambaran dari *Chess Board Pattern* adalah sebagai berikut:



Gambar 2.8 Chess Board Patter

2.6 Pesan

Pesan adalah serangkaian isyarat/symbol yang diciptakan oleh seseorang untuk maksud tertentu dengan harapan bahwa penyampaian isyarat/simbol itu akan berhasil dalam menimbulkan sesuatu. (Hafied, 2004: 14). Komunikasi dalam kehidupan manusia terasa sangat penting, karena dengan komunikasi dapat menjembatani segala bentuk ide yang akan disampaikan seseorang. Dalam setiap melakukan komunikasi unsur penting diantaranya adalah pesan, karena pesan disampaikan melalui media yang tepat, bahasa yang di mengerti, kata-kata yang

sederhana dan sesuai dengan maksud, serta tujuan pesan itu akan disampaikan dan mudah dicerna oleh komunikan.Adapun pesan itu menurut Onong Effendy, menyatakan bahwa pesan adalah : “suatu komponen dalam proses komunikasi berupa paduan dari pikiran dan perasaan seseorang dengan menggunakan lambang, bahasa/lambang-lambang lainnya disampaikan kepada orang lain”. (Effendy, 1989:224).

2.6.1 Keamanan Pesan

Pertukaran informasi terjadi setiap detik di internet sehingga banyak terjadi pencurian informasi oleh pihak-pihak tertentu yang tidak bertanggungjawab. Agar data yang dikirimkan aman dari pihak-pihak ini maka data dapat disembunyikan dengan menggunakan kriptografi dengan Algoritma Transposition Cipher. Algoritma kriptografi disebut juga cipher,

yaitu suatu aturan untuk enkripsi dan dekripsi, atau fungsi matematika untuk proses enkripsi. dan dekripsi. Keamanan data diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan cipherteks menjadi plainteks tanpa kunci. Makin banyak kerja dan waktu yang dibutuhkan, makin kuat algoritma kriptografi tersebut. (Nurdin,2017)

Adapun beberapa hal yang perlu diperhatikan dari keamanan informasi menurut Whitman dan Mattord (2011) sebagai berikut :

a. Physical Security yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

b. Personal Security yang overlap dengan „phisycal security' dalam melindungi orang-orang dalam organisasi
c. Operation Security yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
d. Communications Security yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
e. Network Security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen diatas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi, termasuk system dan perangkat yang digunakan, menyimpan, dan mengirimkannya. Keamanan terhadap pesan/informasi adalah hal yang sangat penting, bisa dibayangkan apabila informasi yang menjadi rahasia penting dapat bocor dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, kriptografi yang merupakan salah satu teknik pengamanan pesan diharapkan dapat tetap menjaga kerahasiaan isi dari informasi dan memberikan keyakinan pada penerima pesan bahwa informasi tersebut memang berasal dari pengirim yang tepat begitu pula sebaliknya pengirim yakin bahwa penerima informasi adalah pihak yang tepat.(Yuliana;2014).

BAB III
PEMBAHASAN

3.1 Proses Enkripsi Modifikasi Rail Fence Dengan Chess Board Pattern

Proses enkripsi dilakukan dengan menuliskan plaintext secara vertical 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 terserdiri terhadap *chess board pattern*. Pada bagian ini akan dilakukan proses enkripsi dan deskripsi. Berikut ini proses enkripsi dengan pola *Chess Board Pattern* dengan *plaintext* " **BLITAR KOTA PATRIA** " dengan kunci (*key*) 2, 3, 4, 5, 6 dan offset - 0.

a. Variasi 1

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 2

Offset = 0

- Enkripsi Rail Fence

B		**I**		**A**		**K**		**T**		**P**		**T**		**I**	
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BIAKTPTI LTROAARAA**"

- Modifikasi Enkripsi Rail Fence dengan Chess Board Pattern

B		**I**		**A**		**K**		**T**		**P**		**T**		**I**	
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**

Dengan dibaca secara horizontal maka akan di dapat:

Baris 1 = BIAKTPTI

Baris 2 = LTROAARAA

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BIAKTPTI LTROAARAA**"

b. Variasi 2

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 3

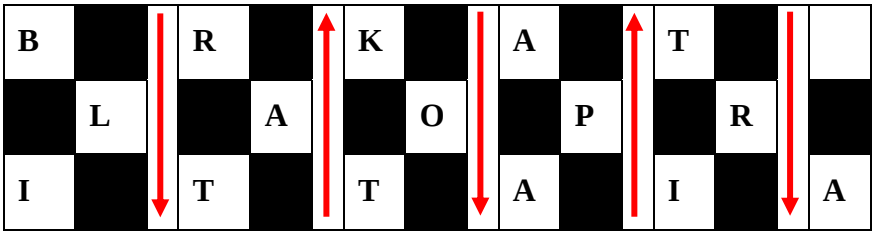
Offset = 0

- Enkripsi Rail Fence

B				**A**				**T**				**T**			
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**
		I				**K**				**P**				**I**	

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BATT LTROAARA IKPI**"

- Modifikasi Enkripsi Rail Fence dengan Chess Board Pattern



B		**R**		**K**		**A**		**T**	
	L		**A**		**O**		**P**		**R**	
I		**T**		**T**		**A**		**I**		**A**

Dengan dibaca secara horizontal maka akan di dapat:

Baris 1 = BRKAT

Baris 2 = LAOPR

Baris 3 = ITTAIA

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BRKAT LAOPR ITTAIA**"

c. Variasi 3

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 4

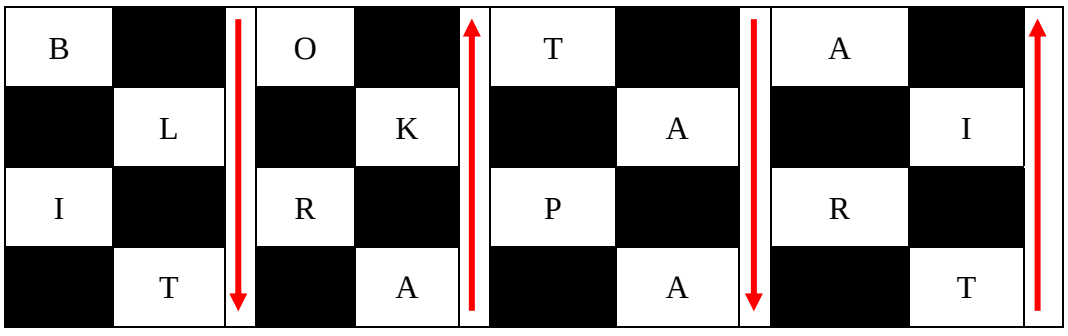
Offset = 0

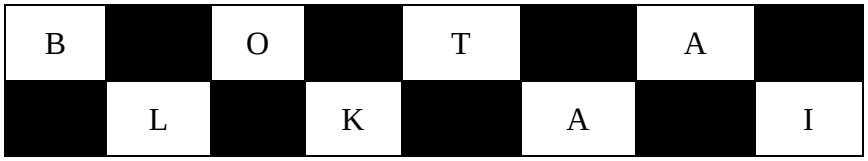
- Enkripsi Rail Fence

B						K						T			
	L				R		O				A		R		
		I		A				T		P				I	
			T						A						A

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BKT LROAR IATPI TAA**"

- Modifikasi Enkripsi Rail Fence dengan Chess Board Pattern





I		R		P		R	
	T		A		A		T

Dengan dibaca secara horizontal maka akan di dapat:

Baris 1 = BOTA

Baris 2 = LKAI

Baris 3 = IRPR

Baris 4 = TAAT

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BOTA LKAI IRPR TAAT**"

d. Variasi 4

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 5

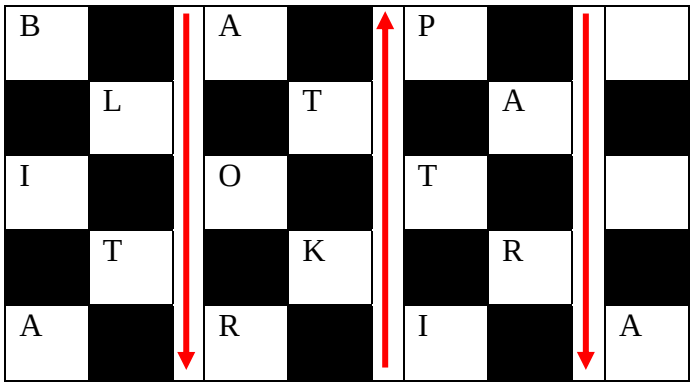
Offset = 0

- Enkripsi Rail Fence

B								T							
	L						O		A						A
		I				K				P				I	
			T		R						A		R		
				A								T			

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BT LOAA IKPI TRAR AT"**

- Modifikasi Enkripsi Rail Fence dengan Chess Board Pattern



B		A		P		
	L		T		A	
I		O		T		
	T		K		R	
A		R		I		A

Dengan dibaca secara horizontal maka akan di dapat:

Baris 1 = BAP

Baris 2 = LTA

Baris 3 = IOT

Baris 4 = TKR

Baris 5 = ARIA

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BAP LTA IOT TKR ARIA"**

e. **Variasi 5**

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 6

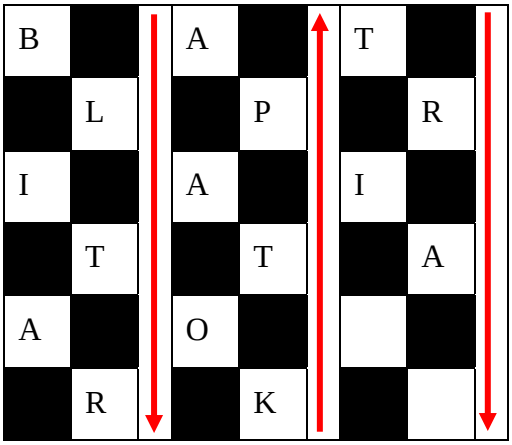
Offset = 0

- Enkripsi Rail Fence

B										P					
	L								A		A				
		I						T				T			
			T				O						R		
				A		K								I	
					R										A

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BP LAA ITT TOR AKI RA"**

- Modifikasi Enkripsi Rail Fence dengan Chess Board Pattern



B		A		T	
	L		P		R
I		A		I	
	T		T		A
A		O			
	R		K		

Dengan dibaca secara horizontal maka akan di dapat:

Baris 1 = BAT

Baris 2 = LPR

Baris 3 = IAI

Baris 4 = TTA

Baris 5 = AO

Baris 6 = RK

Maka *Ciphertext* dari " **BLITAR KOTA PATRIA**" adalah " **BAT LPR IAI TTA AO RK"**

Dari 5 variasi di atas di kelompokkan menjadi 1 tabel agar lebih mudah dalam memahami hasil yang di dapat dari enkripsi *Rail Fence* dan modifikasi enkripsi *Rail Fence* dengan *Chess Board Pattern* :

Plaintext = BLITARKOTAPATRIA

Kunci (*key*) = 2, 3, 4, 5, dan 6

Offset = 0

Kunci (key)	Ciphertext	Ciphertext Tanpa Modifikasi
2	**BIAKTPTI LTROAARAA**	**BIAKTPTI LTROAARAA**
3	**BRKAT LAOPR ITTAIA**	**BATT LTROAARA IKPI**
4	**BOTA LKAI IRPR TAAT**	**BKT LROAR IATPI TAA**
5	**BAP LTA IOT TKR ARIA**	**BT LOAA IKPI TRAR AT**
6	**BAT LPR IAI TTA AO RK**	**BP LAA ITT TOR AKI RA**

3.2 Proses Dekripsi Modifikasi Rail Fence Dengan Chess Board Pattern

a. Variasi 1

- Dekripsi Rail Fence

Ciphtertext = **BIAKTPTI LTROAARAA**

Kunci (*key*) = 2

Offset = 0

Langkah pertama:

Letakkan “B” pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “I”. Lanjutkan hingga baris pertama mendapatkan pola seperti gambar:

B		**I**		**A**		**K**		**T**		**P**		**T**		**I**	
	-		-		-		-		-		-		-		-

Langkah kedua:

Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar:

B		**I**		**A**		**K**		**T**		**P**		**T**		**I**	
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**

Dari gambar didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu **“BLITAR KOTA PATRIA”**.

- Dekripsi Modifikasi Rail Fence dengan Chess Board Pattern

Proses deskripsi *ciphtertext* akan dituliskan pada kotak berwarna putih, penulisan *ciphtertext* dilakukan secara *horizontal* dan dibaca secara *vertical* sehingga deskripsi menjadi :

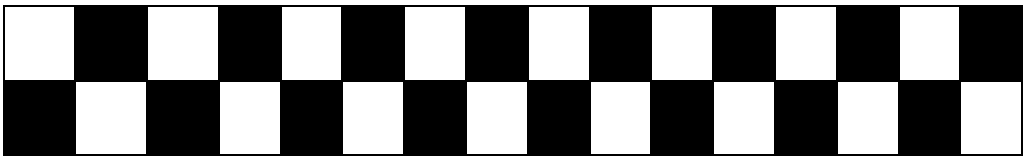
Ciphtertext = **BIAKTPTI LTROAARAA**

Kunci (*key*) = 2

Offset = 0

Langkah pertama :

Gambar baris / urutan sesuai dengan jumlah karakter dan *key*-nya.



Langkah kedua :

Hitung jumlah karakter pada masing-masing baris.

Baris 1 = 8

Baris 2 = 8

Langkah ketiga :

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada ciphertext sesuai urutannya, sehingga dapat ditentukan menjadi :

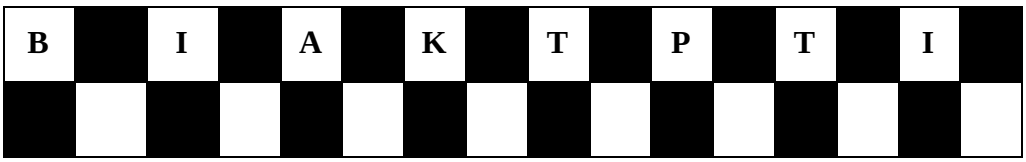
Baris 1 = **BIAKTPTI**

Baris 2 = **LTROAARAA**

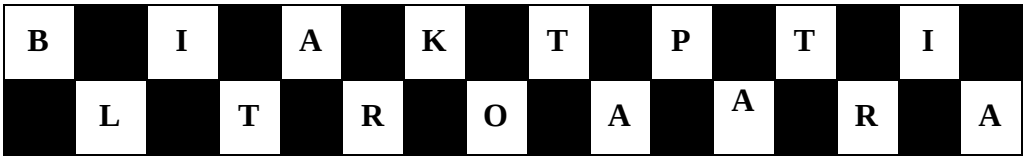
Langkah keempat:

Gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

Baris 1 = BIAKTPTI



Baris 2 = LTROAARA



Maka *Plaintext* dari "**BIAKTPTI LTROAARAA**" adalah " **BLITAR KOTA PATRIA"**

b. Variasi 2

- Dekripsi Rail Fence

Ciphtertext = **BATT LTROAARA IKPI**

Kunci (*key*) = 3

Offset = 0

Langkah pertama:

Letakkan “B” pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “A”. Lanjutkan hingga baris pertama mendapatkan pola seperti gambar:

B				**A**				**T**				**T**			
	-		-		-		-		-		-		-		-
		-				-				-				-	

Langkah kedua:

Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar:

B				**A**				**T**				**T**			
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**
		-				-				-				-	

B				**A**				**T**				**T**			
	L		**T**		**R**		**O**		**A**		**A**		**R**		**A**
		I				**K**				**P**				**I**	

Dari gambar didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu **“BLITAR KOTA PATRIA”**.

- Dekripsi Modifikasi Rail Fence dengan Chess Board Pattern

Proses deskripsi *ciphtertext* akan dituliskan pada kotak berwarna putih, penulisan *ciphtertext* dilakukan secara *horizontal* dan dibaca secara *vertical* sehingga deskripsi menjadi :

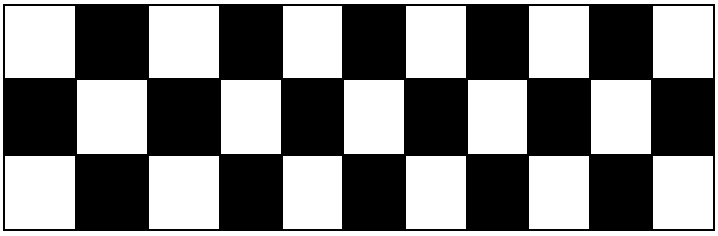
Ciphtertext = **BRKAT LAOPR ITTAIA**

Kunci (*key*) = 3

Offset = 0

Langkah pertama :

Gambar baris / urutan sesuai dengan jumlah karakter dan *key*-nya.



Langkah kedua :

Hitung jumlah karakter pada masing-masing baris.

Baris 1 = 5

Baris 2 = 5

Baris 3 = 6

Langkah ketiga :

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada ciphertext sesuai urutannya, sehingga dapat ditentukan menjadi :

Baris 1 = **BRKAT**

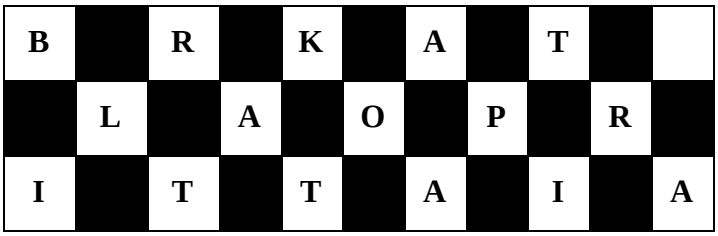
Baris 2 = **LAOPR**

Baris 3 = **ITTAIA**

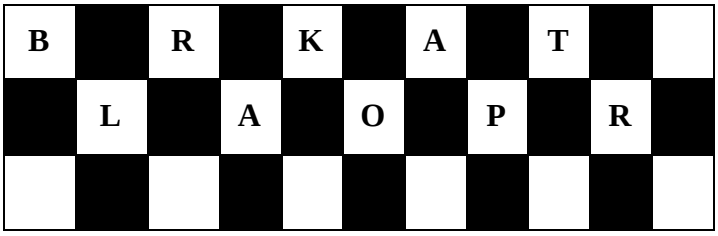
Langkah keempat:

Gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

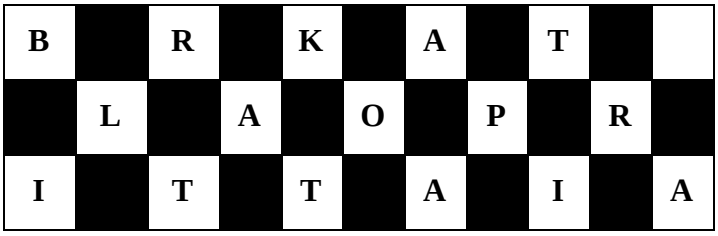
Baris 1 = BRKAT

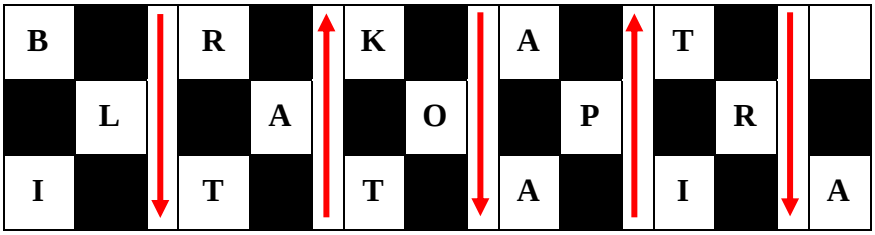


Baris 2 = LAOPR



Baris 3 = ITTAIA





Maka *Plaintext* dari "**BRKAT LAOPR ITTAIA**" adalah " **BLITAR KOTA PATRIA"**

c. Variasi 3

- Dekripsi Rail Fence

Ciphtertext = **BKT LROAR IATPI TAA**

Kunci (*key*) = 4

Offset = 0

Langkah pertama:

Letakkan “B” pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “K”. Lanjutkan hingga baris pertama mendapatkan pola seperti gambar:

B						K						T			
	-				-		-				-		-		
		-		-				-		-				-	
			-						-						-

Langkah kedua:

Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar:

B						K						T			
	L				R		O				A		R		
		-		-				-		-				-	
			-						-						-

B						K						T			
	L				R		O				A		R		
		I		A				T		P				I	
			-						-						-

B						K						T			
	L				R		O				A		R		
		I		A				T		P				I	
			T						A						A

Dari gambar didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu **“BLITAR KOTA PATRIA”**.

- Dekripsi Modifikasi Rail Fence dengan Chess Board Pattern

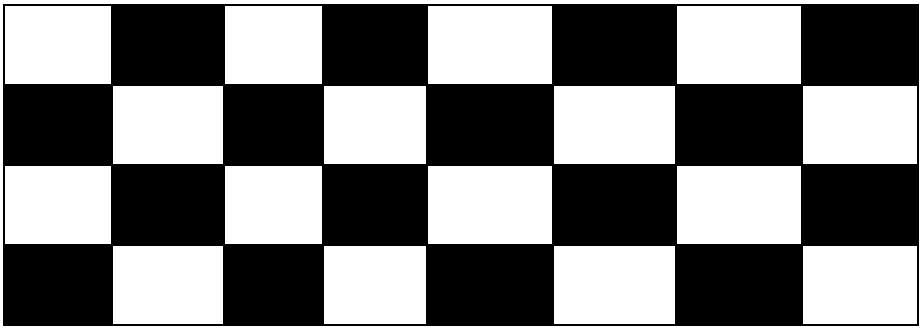
Ciphtertext = **BOTALKAIIRPRTAAT**

Kunci (*key*) = 4

Offset = 0

Langkah pertama :

Gambar baris / urutan sesuai dengan jumlah karakter dan *key*-nya.



Gambar 3.4 Pola Chess Board Pattern

Langkah kedua :

Hitung jumlah karakter pada masing-masing baris.

Baris 1 = 4

Baris 2 = 4

Baris 3 = 4

Baris 4 = 4

Langkah ketiga :

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada ciphertext sesuai urutannya, sehingga dapat ditentukan menjadi :

Baris 1 = **BOTA**

Baris 2 = **LKAI**

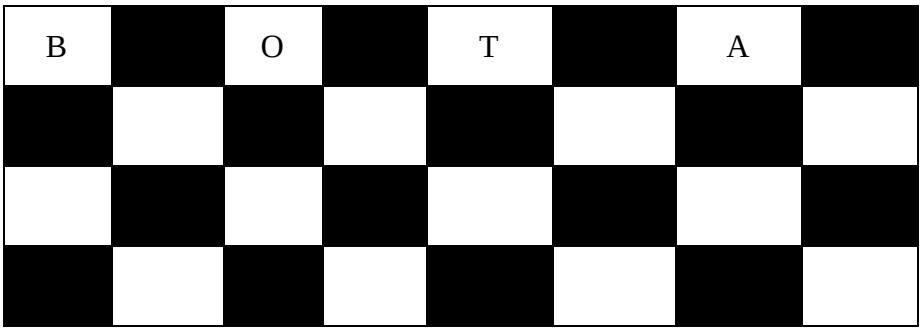
Baris 3 = **IRPR**

Baris 4 = **TAAT**

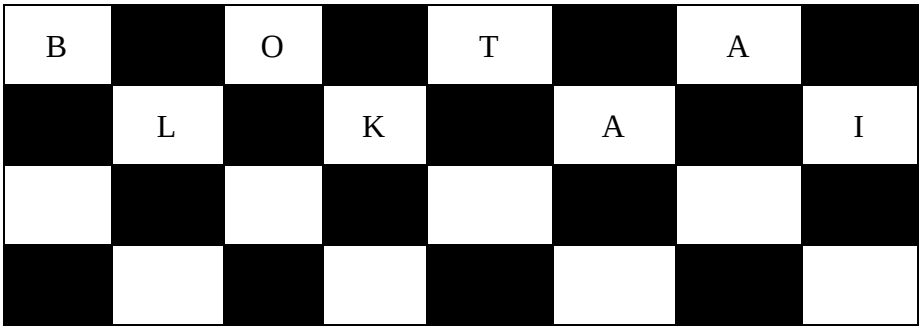
Langkah keempat:

Gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

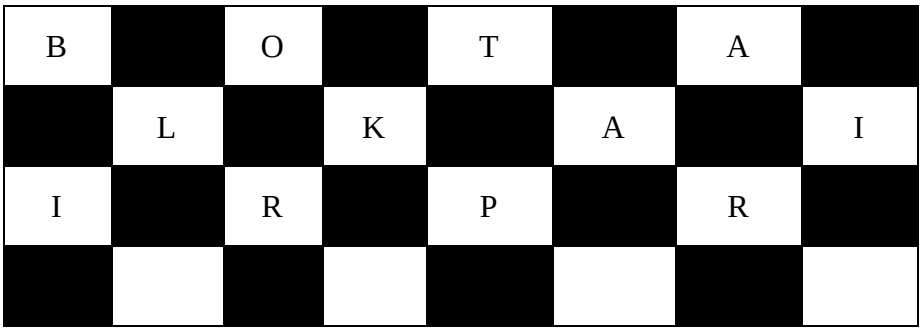
Baris 1 = BOTA



Baris 2 = LKAI

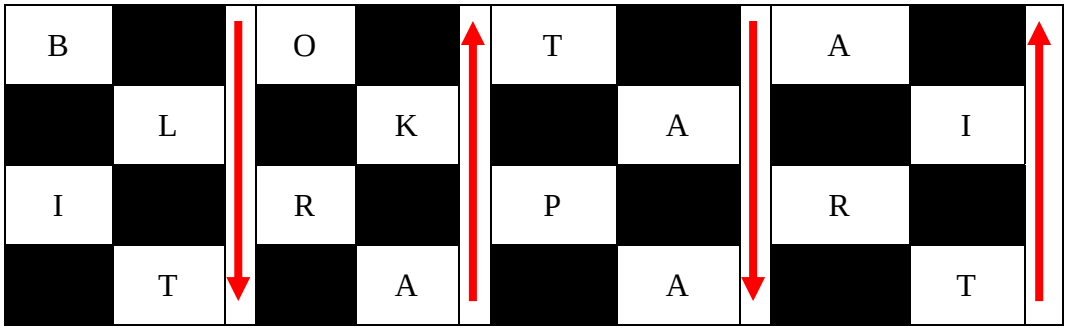


Baris 3 = IRPR



Baris 4 = TAAT

B		O		T		A	
	L		K		A		I
I		R		P		R	
	T		A		A		T



Maka *Plaintext* dari "**BOTA LKAI IRPR TAAT**" adalah " **BLITAR KOTA PATRIA"**

d. Variasi 4

➢ Dekripsi Rail Fence

Ciphtertext = **BT LOAA IKPI TRAR AT**

Kunci (*key*) = 5

Offset = 0

Langkah pertama:

Letakkan "B" pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter "T". Lanjutkan hingga baris pertama mendapatkan pola seperti gambar:

B								T							

	-						-		-						-
		-				-				-				-	
			-		-						-		-		
				-								-			

Langkah kedua:

Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar:

B								T							
	L						O		A						A
		-				-				-				-	
			-		-						-		-		
				-								-			

B								T							
	L						O		A						A
		I				K				P				I	
			T		R						A		R		
				-								-			

B								T							
	L						O		A						A
		I				K				P				I	
			T		R						A		R		
				A								T			

Dari gambar didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu **"BLITAR KOTA PATRIA"**.

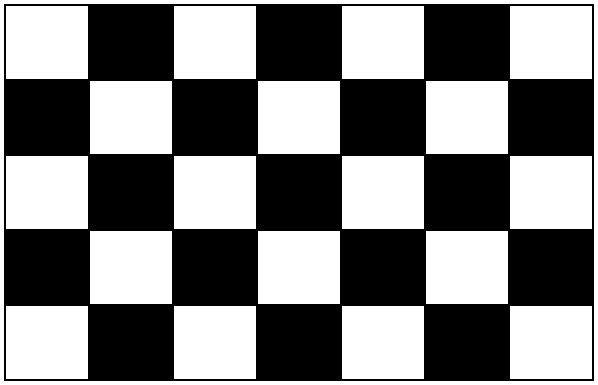
- Dekripsi Modifikasi Rail Fence dengan Chess Board Pattern

Ciphtertext = **BAP LTA IOT TKR ARIA**

Kunci (*key*) = 5

Offset = 0

Langkah pertama :



Langkah kedua :

Hitung jumlah karakter pada masing-masing baris.

Baris 1 = 3

Baris 2 = 3

Baris 3 = 3

Baris 4 = 3

Baris 5 = 4

Langkah ketiga :

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada ciphertext sesuai urutannya, sehingga dapat ditentukan menjadi :

Baris 1 = **BAP**

Baris 2 = **LTA**

Baris 3 = **IOT**

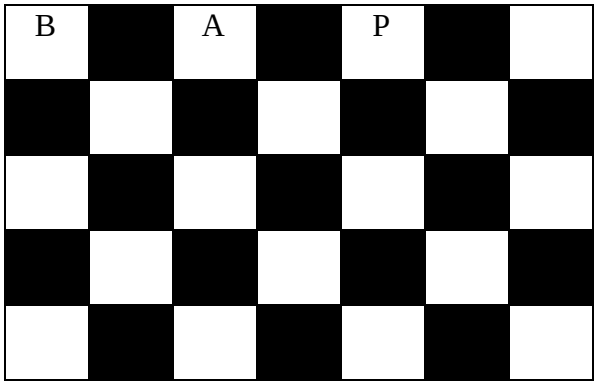
Baris 4 = **TKR**

Baris 5 = **ARIA**

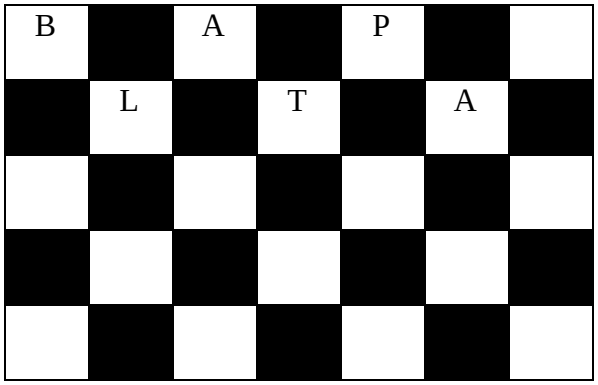
Langkah keempat:

Gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

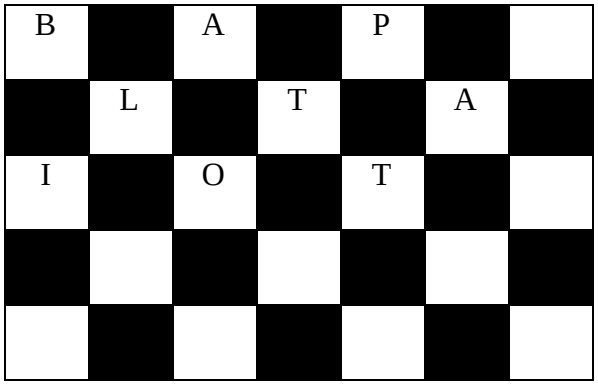
Baris 1 = BAP



Baris 2 = LTA



Baris 3 = IOT

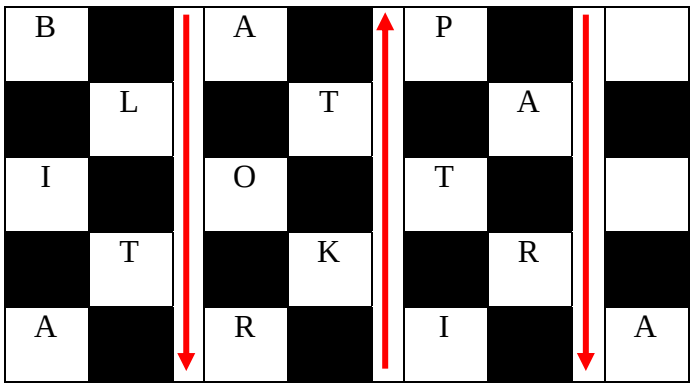


Baris 4 = TKR

B		A		P		
	L		T		A	
I		O		T		
	T		K		R	

Baris 5 = ARIA

B		A		P		
	L		T		A	
I		O		T		
	T		K		R	
A		R		I		A



Maka *Plaintext* dari "**BAP LTA IOT TKR ARIA**" adalah " **BLITAR KOTA PATRIA"**

e. Variasi 5

- Dekripsi Rail Fence

Ciphtertext = **BP LAA ITT TOR AKI RA**

Kunci (*key*) = 6

Offset = 0

Langkah pertama:

Letakkan “B” pada kolom pertama. Kemudian beri tanda garis pada kotak selanjutnya di bawahnya secara diagonal sampai kembali pada baris teratas, dan letakkan karakter “P”. Lanjutkan hingga baris pertama mendapatkan pola seperti gambar:

B										P					
	-								-		-				
		-						-				-			
			-				-						-		
				-		-								-	
					-										-

Langkah kedua:

Lanjutkan cara ini baris demi baris, dan akan diperoleh hasil seperti gambar:

B										P					
	L								A		A				
		-						-				-			
			-				-						-		
				-		-								-	
					-										-

B										P					
	L								A		A				
		I						T				T			
			-				-						-		
				-		-								-	
					-										-

B										P					
	L								A		A				
		I						T				T			
			T				O						R		
				-		-								-	
					-										-

B										P					
	L								A		A				
		I						T				T			
			T				O						R		
				A		K								I	
					-										-

B										P					
	L								A		A				
		I						T				T			
			T				O						R		
				A		K								I	
					R										A

Dari gambar didapatkan sebuah pesan yang dapat dibaca secara diagonal yaitu **"BLITAR KOTA PATRIA"**.

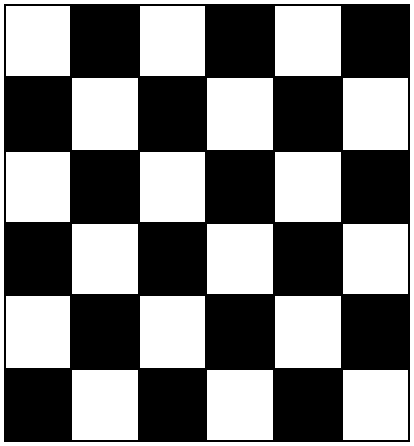
- Dekripsi Modifikasi Rail Fence dengan Chess Board Pattern

  Ciphtertext = **BAT LPR IAI TTA AO RK**

  Kunci (*key*) = 6

  Offset = 0

Langkah pertama :



Langkah kedua :

Hitung jumlah karakter pada masing-masing baris.

Baris 1 = 3

Baris 2 = 3

Baris 3 = 3

Baris 4 = 3

Baris 5 = 2

Baris 6 = 2

Langkah ketiga :

Sesuaikan jumlah karakter pada masing-masing baris dengan karakter pada ciphertext sesuai urutannya, sehingga dapat ditentukan menjadi :

Baris 1 = **BAT**

Baris 2 = **LPR**

Baris 3 = **IAI**

Baris 4 = **TTA**

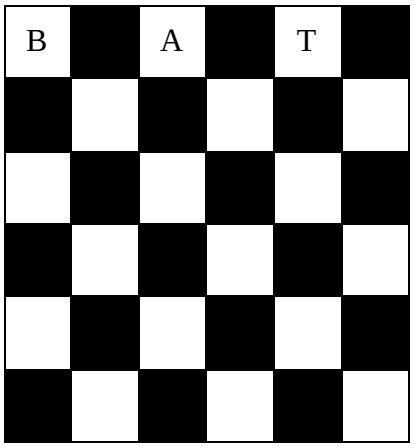
Baris 5 = **AO**

Baris 6 = **RK**

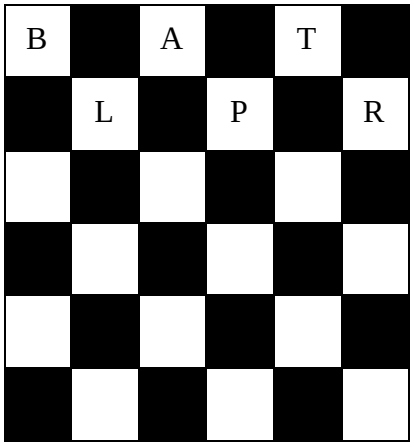
Langkah keempat:

Gambarkan kembali baris yang sudah ditentukan sesuai karakter pada masing-masing baris.

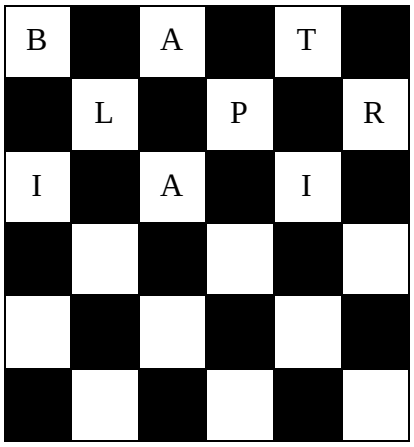
Baris 1 = BAT



Baris 2 = LPR



Baris 3 = IAI



Baris 4 = TTA

B		A		T	
	L		P		R
I		A		I	
	T		T		A

Baris 5 = AO

B		A		T	
	L		P		R
I		A		I	
	T		T		A
A		O			

Baris 6 = RK

B		A		T	
	L		P		R
I		A		I	
	T		T		A
A		O			
	R		K		

Maka *Plaintext* dari "**BAT LPR IAI TTA AO RK**" adalah " **BLITAR KOTA PATRIA"**

3.3 Kajian Keagamaan

Penyandian data atau pesan yang biasanya disebut dengan proses enkripsi bertujuan untuk melindungi pesan dari pihak yang tidak mempunyai hak untuk mengetahui isi pesan maupun data tersebut. Kerahasiaan suatu pesan tentunya memiliki alasan dan tujuan tertentu guna untuk pihak seseorang yang dituju. Adapun salah satu tujuannya untuk melindungi privasi seseorang yang bisa jadi tidak baik untuk diketahui pihak lain ataupun masyarakat luas. Selain untuk menjaga privasi orang lain, mengenkripsikan pesan juga bertujuan untuk menjaga amanat. Pada Al-Quran surat Al-Anfal ayat 27 berikut ini telah disampaikan larangan dalam mengkhianati amanat yang sudah di berikan.

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ

***Artinya**:*

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui. (QS.Al-Anfal /8:27).

Al-Quran surat Al-Anfal aat 27 ini menerangkan bahwa suatu amanat dalam konteks masa kini yaitu suatu informasi yang sudah diamanatkan kepada kita, maka kita harus bisa menjaga amanat tersebut supaya tidak dapat di sadap, atau disalah gunakan oleh pihak yang tidak berkepentingan. Oleh sebab itu kita melakukan ikhtiar untuk mengamankan pesan dengan cara pengamanan pesan menggunakan teknik pengenkripsian pesan.

Adapun ayat Al-Quran yang juga mendukung amanat yang dikandung dalam Al-Quran surat Al-Anfal ini yaitu Al-Quran surat An-Nisa ayat 58 yang berbunyi:

إِنَّ اللّهَ يَأْمُرُكُمْ أَن تُؤدُّواْ الأَمَانَاتِ إِلَى أَهْلِهَا وَإِذَا حَكَمْتُم بَيْنَ النَّاسِ أَن تَحْكُمُواْ بِالْعَدْلِ إِنَّ اللّهَ نِعِمَّا يَعِظُكُم بِهِ إِنَّ اللّهَ كَانَ سَمِيعًا بَصِيرًا

Artinya :

Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hokum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat (QS. An-Nisa 4/58).

Amanat memiliki arti dipercaya atau terpecaya, amanat berkaitan tentang menjaga kepercayaan orang lain atas sesuatu yang telah di titipkan oleh pemberi amanah. Hal ini amanat dapat diartikan berupa benda, perkataan, perbuatan, maupun pesan. Kedua ayat tersebut mempunyai pesan bahwa amanat-amanat yang telahh diberikan haruslah disampaikan kepada yang berhak menerima. Mereka yang bisa menjaga amanat adalah termasuk orang-orang yang beriman.

BAB IV
PENUTUP

4.1 Kesimpulan

Dari Analisa dan pembahasan dapat diambil beberapa kesimpulan sebagai berikut :

1. Modifikasi Algoritma Rail Fence dengan Chess Board Pattern dapat membentuk berbagai variasi proses enkripsi, sehingga secata tidak langsung meningkatkan kerumitan proses enkripsi. Kunci yang digunakan dalam proses enkripsi harus sama dengan kunci yang sudah di tentukan oleh orang yang mengirim pesan. Dalam penelitian ini menggunakan kunci 2, 3, 4, 5, dan 6. Dari kelima kunci tersebut pada *key* 2 yang di modifikasi menggunakan chess board pattern hasilnya tetap sama apabila di enkripsikan menggunakan rail fence, akan tetapi pada *key* 3, 4, 5, 6 yang sudah di modifikasi menggunakan chess boar pattern memiliki hasil yang berbeda apabila dibandingkan dengan hasil enkripsi menggunakan rail fence. Modifikasi Rail Fence dengan Chess Board Pattern ini berlaku apabila kunci (*key*) > 2 agar memiliki hasil yang lebih rumit. Enkripsi menggunakan chess board pattern ini memiliki keunikan tersendiri karena proses pengenkripsian dilakukan secara vertical dengan mengisi kota berwarna putih dan mengabaikan kotak berwarna hitam dengan menggunakan pattern Rail Fence dalam proses enkripsi.
2. Proses deskripsi *ciphtertext* akan dituliskan pada kotak berwarna putih dan mengabaikan kotak yang berwarna hitam, penulisan *ciphtertext* dilakukan secara *horizontal* dan dibaca secara *vertical*. Dari kunci 2, 3, 4, 5, dan 6 pola

penggambaran baris berbeda-beda sesuai dengan jumlah kunci yang telah di tentukan oleh pengirim pesan.

4.2 Saran

Pada penelitian ini membahas mengenai Rail Fence yang dimodifikasi menggunakan Chess Board Pattern. Untuk pengembangan penelitian selanjutnya disarankan untuk memodifikasi algoritma cipher transposition yang lain seperti *Route Cipher* dan *Columnar Transposition*. Selain itu disarankan modifikasi Algoritma Rail Fence Transposition Cipher dengan Chess Board Pattern ini kedepannya dapat dikombinasikan dengan salah satu bilangan acak.

DAFTAR PUSTAKA

Cangara, Hafied. 2004. *Pengantar Ilmu Komunikasi*. Jakarta : Kencana Prenada Media Group.

Effendy, Onong Uchjana. 1989. *KAMUS KOMUNIKASI*. Bandung : PT. Mandar Maju. J.Jiao, C. Huang, H.Lin, & G.Zhang, "*A Chinese Chessboard Calibration Method in Chess-Playing Robot by Machine Vision Sensing*", IOP Conf.Series: Journal of Phyisics : 1026, 2018.

Kamil, F. (2016). *Implementasi Kriptografi dengan Menggunakan Algoritma Advanced Encryption Standart (AES 256) dan Lempel Ziv Welch (LZW)*. Tanggerang: STMIK Raharja.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika Bandung.

Munir, Rinaldi. 2019. *Kriptografi*. Bandung: Informatika Bandung.

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

Nishika dan R.K. Yadav, "A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment". International Journal of Computer Science and Mobile Computing Vol. 2(6), pp. 53-59.

Saini, B., 2015. *Modifed Caeser Chipher and Rail Fence Technique to Enhance Security*. International Journal of Trend in Reseacrh and Development, 2(5), pp. 348-350.

Whitman, M.E., & Mattord, H.J, Management of Information Security, Third Edition, Boston: Course Technology, 2010

RIWAYAT HIDUP

Muhammad Dendy Arifanda lahir di Kabupaten Tulungagung pada 28 September 1995. Memiliki nama panggilan Dendy . Bertempat tinggal di Dsn. Jatirejo Ds. Tenggur Kec. Rejotangan Kab. Tulungagung. Merupakan anak pertama dari Bapak H. Sonlaili dan Ibu Hj. Aminatus Sholihah.

Pendidikan yang pernah ditempuh yaitu TK Tarbiyatul Islamiyah. Kemudian melanjutkan sekolahnya di MI Manba'ul Ulum dan lulus pada tahun 2008. Menempuh pendidikan MtsN 1 Blitar lulus pada tahun 2011. Melanjutkan pendidikan MAN 2 Tulungagung pada tahun 2014. Tahun 2014 melanjutkan studi ke jenjang pendidikan strata 1 di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil jurusan Matematika Fakultas Sains dan Teknologi.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAUALANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax.(0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Muhammad Dendy Arifanda
NIM : 14610008
Fakultas/Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Modifikasi *Rail Fence Transposition Cipher* dengan *Chess Board Pattern*
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1	17 November 2020	Konsultasi BAB I & II	1.
2	19 November 2020	Revisi BAB I & II	2.
3	23 November 2020	ACC BAB I & II	3.
4	23 Februari 2021	Konsultasi BAB I, II & III	4.
5	26 Februari 2021	Revisi BAB I, II & III	5.
6	8 Maret 2021	ACC BAB I, II & III	6.
7	22 April 2021	Konsultasi BAB IV	7.
8	28 April 2021	Revisi BAB IV	8.
9	4 Mei 2021	Revisi BAB I, II & III	9.
10	6 Mei 2021	ACC BAB I, II & III	10.
11	6 Mei 2021	ACC BAB IV	11.
12	14 Juni 2021	Konsultasi Keagamaan	12.
13	16 Juni 2021	ACC Keagamaan	13.
14	18 Juni 2021	ACC Keseluruhan	14.

Malang, 21 Juni 2021
Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001