Terbit online pada laman web jurnal: **https://ejurnalunsam.id/index.php/jicom/**

JICOM
Jurnal Informatika dan Teknologi Komputer

Vol. 03 No. 01 (2022) 40 - 48 E-ISSN : 2774-7115 P-ISSN : 27752089

Implementasi Algoritma One Time Mengggunakan Algoritma Chiper Transposition Sebagai Pengamanan Rahasia Pesan

Lintang Purnama[1], Dadang Iskandar Mulyana[2], Yoni Maulana[3], Eka Okta Putri Sulaiman[4]
[1,2,3,4]Teknik Informatika, St .Ilmu Komputer Cipta Karya Informatika, Jakarta, Indonesia
Email: [1]lintangpurnama1@gmail.com, [2]mahvin2012@gmail.com, [3]yonymaulana@gmail.com,[4] iam.ekaokta@gmail.com
Email Penulis Korespondensi: yonymaulana@gmail.com

Abstract
Data security is a very important aspect in sending messages, especially for messages that are confidential. We can know this from daily activities, for example using the internet to send e-mails, social media, buying and selling online, and others. For that we need a code so that the message is still confidential, because the secret and security of data that is operated on a public network is vulnerable to attack by anything. cryptography is "secretwriting" (secret writing). There are definitions of cryptography that have been expressed in various literatures. The definition of cryptography used in obsolete books, namely before the 1980s, states that cryptography is the art and science used to claim the confidentiality of a message by using a method of encoding the message into a form that the person can no longer understand. other. At this time, it is mandatory for every manager and owner of an information system to think about how to protect the security of their information system in order to avoid various kinds of risks that could cause losses. In the transposition cipher technique, the letters in the plaintext and ciphertext remain the same, but the order is changed. In other words, this technique transposes a series of characters in a text. The One Time Pad (OTP) algorithm is a stream cipher that encrypts and decrypts one character at a time. The One Time Pad algorithm has the criteria that the length of the text is the same as the length of the key, otherwise the message character on the key will iterate over the message and the length of the message is the same as the length of the key. The One Time Pad algorithm is safe to use in encoding, because it has a different key in each encoding for the original message, this algorithm has a weakness in its description that sometimes the ciphertext cannot be returned intact. Cipher Transposition Algorithm can divide messages into blocks whose length corresponds to the length of the key, if the length of the message is shorter than the block length, then each remaining block will be filled by an example. The Transposition Cipher Algorithm applies the reader vertically to the decryption and horizontally to the encryption process.

Keywords*: Cryptography, Security, One Time Algorithm, Transposition Cipher Algorithm.*

Abstrak− Keamanan data merupakan aspek yang sangat penting dalam pengiriman pesan terutama untuk pesan yang bersifat rahasia. Hal tersebut dapat kita ketahui dari aktivitas sehari-hari contohnya penggunaan internet untuk mengirimkan e-mail, sosial media, jual beli secara online, dan lain-lain. Untuk itu diperlukan suatu kode agar pesan tersebut masih bersifat rahasia, karena rahasia dan keamanan data yang dioperasionalkan pada jaringan publik rentan terhadap serangan oleh apapun. kriptografi adalah " secretwriting " (*rahasia tulisan*). Terdapat definisi kriptografi yg sudah diungkapkan pada aneka macam literatur. Definisi kriptografi yg dipakai pada kitab - kitab yg telah usang yaitu sebelum tahun 1980-an, mengemukakan bahwa kriptografi adalah seni & ilmu yg dipakai buat mengklaim kerahasiaan sebuah pesan menggunakan memakai cara melakukan penyandian pesan tadi ke pada bentuk yg tidak bisa dipahami lagi maknanya sang orang lain. Pada saat ini membuat setiap pengelola & pemilik system informasi wajib & harus memikirkan bagaimana cara supaya bisa melindungi keamanan sistem keterangan yg dimilikinya supaya terhindar berbagai macam resiko yg mampu saja bisa mengakibatkan kerugian. Pada teknik cipher transposisi, huruf-huruf yang ada didalam plaintext dan ciphertext tetap sama, tetapi urutannya diubah. Dengan kata lain, Teknik ini

Diterima Redaksi : 06-02-2022 | Selesai Revisi : 04-04-2022 | Diterbitkan Online : 04-04-2022

melakukan transpose terhadap rangkaian karakter yang ada didalam suatu teks. Algoritma One Time Pad (OTP) merupakan stream cipher yg melakukan enkripsi & dekripsi satu karakter setiap kali. Algoritma One Time Pad memiliki kriteria panjang teks sama dengan panjang key jika tidak sama maka karakter pesan pada key akan melakukan iterasi pesan dan panjang pesan sama dengan panjang key. Algoritma One Time Pad aman dipakai dalam penyandian, karena memiliki key yang berbeda di setiap penyandiannya terhadap pesan asli, algoritma ini memiliki kelemahan pada dekrispsinya yang terkadang ciphertext tidak dapat kembali secara utuh. Algoritma Cipher Transposisi dapat membagi pesan ke dalam blok yang panjangnya sesuai dengan panjang key, jika panjang pesan lebih pendek panjang blok, maka setiap blok yang bersisa akan diisi oleh contoh. Algoritma Chiper Transposisi menerapkan pembaca secara vertikal pada dekripsi dan horizontal pada proses enkripsi.

Kata Kunci: Kriptografi,Keamanan,Algoritma One Time,Algoritma Transposition Chiper.

1. PENDAHULUAN

Kehidupan saat sangat butuh Teknologi Komputer terutama personal juga kelompok (organisasi). Kelompok (organisasi) tadi sangat membutuhkan adanya komputerisasi pada setiap kegiatannya. Setelah kita ketahui penggunaan komputerisasi barusan, maka harus di buatlah sebuah pengamanan bagi seluruh aset-asetnya, terutama untuk data-data & fakta-fakta yang krusial demi menjaga kerahasiaan data. Dari keamanan data tadi menyebabkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik supaya bisa mengamankan data menurut banyak sekali ancaman yang mungkin timbul. Ini adalah latar belakang berkembangnya sistem keamanan data yang berfungsi buat melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi. [1].

Keamanan sangat dibutuhkan karenabanyak data yang bersifat rahasia dan tidak bisa dirubah oleh pihak yang tidak berhak untuk merubahnya. Supaya bisa mengamankan file data yang di maksud maka bisa menggunakan kriptografi. Oleh karena itu, pengguna filedata membutuhkan bantuan untuk keamanan file data yang disimpannya [2].

Perkembangan teknologi informatika yang sangat cepat & pesat, membawa perubahan yang sangat besar disegala bidang. Salah satunya antara lain perekonomian. Perkembangan teknologi membangkitkan bidang bisnis menggunakan sangat cepat, setiap aktivitas bisnis bisa pada topang menggunakan adanya teknologi yang maju. Perkembangan teknologi membuahkan ketatnya persaingan pada global bisnis. Perkembangan teknologi informatika yang sangat cepat & pesat, membawa perubahan besardisegala bidang. Salah satu antara lain merupakan perekonomian. Perkembangan teknologi membangkitkan bidang bisnis menggunakan sangat cepat, setiap aktivitas bisnis bisa pada topang menggunakan adanya teknologi yang maju. Perkembangan teknologi membuahkan ketatnya persaingan pada global bisnis.[3]

Solusi buat keamanan citra digital berdasarkan agresi atau penyadapan merupakan menggunakan cara mengekripsinya. Enkripsi citra adalah teknik buat melindungi citra menggunakan cara menyandikan citra (plain-image) sebagai akibatnya tidak bisa dikenali lagi (chiper-image). Chaos dipilih lantaran ciri yaitu sensitivitas terhadap syarat awal, berkelakuan acak, & tidak mempunyai periode berulang. arnold cat map dipakai buat mengacak susunan pixel-pixel, sedangkan logistic map dipakai menjadi pembangkit keystream. Adapun pendekatan teknik selektif yaitu hanya mengenkripsi sebagian elemen pada pada citra tetapi efeknya holistik citra terenkripsi[4]

Keamanan data adalah aspek yang sangat penting dalam pengiriman pesan terutama untuk pesan yang bersifat rahasia. Hal tersebut dapat kita ketahui dari aktivitas sehari-hari contohnya penggunaan internet untuk mengirimkan e-mail, sosial media, jual beli secara online, dan lain-lain. Untuk itu diperlukan suatu kode agar pesan tersebut masih bersifat rahasia dan aman, karena keamanan data yang dioperasionalkan pada jaringan publik rentan terhadap serangan oleh siapapun. Layanan keamanan data diwujudkan dengan menggunakan mekanisme keamanan data. Mekanisme keamanan data pada implementasinya menggunakan teknik- teknik penyandian, yaitu kriptografi. penelitian[5]

Cara Untuk mampu menaikkan keamanan memakai kombinasi antara kriptografi & steganografi, dimana pesan rahasia harus dienkripsi terlebih dahulu, kemudian ciphertext disembunyikan pada media lain sehingga akibatnya pihak yg tidak berkepentingan tidak menyadari adanya pesan. Berdasarkan latar belakang masalah, proses pertukaran pesan memerlukan jaminan keamanan & kerahasiaan.[6]

Diperlukannya pengembangan teknik keamanan yg bisa menaruh perlindungan lebih baik dalam pesan rahasi, & menjaga kerahasiaan pesandengan menyembunyikannya kepada media lain(gambar) supaya eksistensi pesan misteri tidak diketahui. Tujuan yg ingin digapai adalah merancang sebuah pelaksanaan yg bisa mengenkripsi & mendekripsi pesan teks memakai prosedur pemecahan kriptografi AES & pula Merancang sebuah pelaksanaan yg bisa menyisipkan & mengekstrak cipherteks berupa blok-blok integer pada media berupa citra digital memakai algoritma LSB.[7]

2. METODE PENILITIAN

2.1 Keamanan

Pada saat ini membuat setiap pengelola & pemilik system informasi wajib & harus memikirkan bagaimana cara supaya bisa melindungi keamanan sistem keterangan yg dimilikinya supaya terhindar berbagai macam resiko yg mampu saja bisa mengakibatkan kerugian. Keamanan sistem berdasarkan Garfinkel yg dinyatakan oleh rahardjo mengutarakan bahwa keamanan personal komputer meliputi 3 aspek yg mencakup Confidentiality, Integrity & Availability.[8]

Masalah Keamanan merupakan salah satu aspek yang penting dari sebuah system informasi. Sayang sekali aspek masalah kemanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola system informasi.[9]

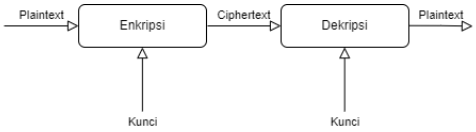
2.2 Kriptografi

Kriptografi ialah "secretwriting" (tulisan rahasia). Terdapat definisi kriptografi yg sudah diungkapkan pada aneka macam literatur. Definisi kriptografi yg dipakai pada kitab - kitab yg telah usang yaitu sebelum tahun 1980-an, mengemukakan bahwa kriptografi adalah seni & ilmu yg dipakai buat mengklaim kerahasiaan sebuah pesan menggunakan memakai cara melakukan penyandian pesan tadi ke pada bentuk yg tidak bisa dipahami lagi maknanya oleh orang lain. Pendapat yg diutarakan pada atas tentang kriptografi yg dipakai buat mengklaim keamanan pada sebuah komunikasi krusial misalnya komunikasi pada kalangan militer, diplomat, & mata-mata mungkin cocok dalam masa dulu. Tetapi dalam waktu ini kriptografi bukan hanya sebuah privasi, namun juga bertujuan buat data.[8]

Aspek Kriptografi Tujuan kriptografi adalah memberikan keamanan. Memberikan layanan keamanan kriptografi harus meliputi aspek-aspek :

1. Authority untuk menjaga informasi dari pihak yang tidak memiliki otoritas.
2. Integrity fungsinyabahwa informasi yang yang di terima tidak berubah dan sesuai dengan aslinya.
3. Authenticatio adalah pengenalan pada pengguna yang berhubungan dengan identifikasi kebenaran informasi.
4. Nonrepudation tujuannya bahwa penerima dan pengirim informasi tidak bisa memberikan penyangkalan atas informasi yang telah diterimanya.[10]

Baik proses enkripsi maupun proses dekripsi melibatkan satu atau beberapa kunci kriptografi. Dalam system di mana terdapat algoritma kriptografi, ditambah seluruh kemungkinan plaintext, ciphertext dan kunci-kuncinya disebut kriptosistem. Proses tersebut dapat digambarkan secara sederhana sebagai berikut :



Gambar 1.Enkripsi/Dekripsi

2.3 Algoritma Cipher Transposition

Pada teknik cipher transposisi, huruf-huruf yang ada didalam plaintext dan ciphertext tetap sama, tetapi urutannya diubah. Dengan kata lain, Teknik ini melakukan transpose terhadap rangkaian karakter yang ada didalam suatu teks. Nama lain untuk metode ini adalah mutasi, karena transpose setiap karakter didalam teks sama dengan memutasikan karakter-karakter tersebut.[11]

Ciphertext diperoleh dengan menngubah posisi huruf didalam plaintext. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf didalam plaintext.

Nama untuk metode ini adalah Permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh 1:

Misalkan Plaintext adalah :
JURUSAN TEKNOLOGI INFORMASI

Enkripsi :

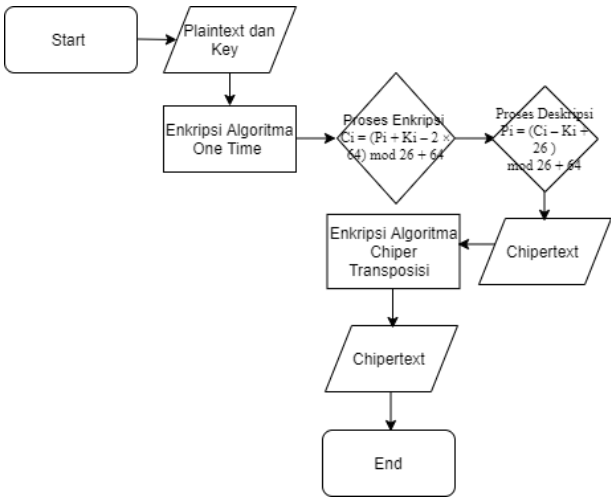
JURUSA
NTEKNO
LOGIIN
FORMAS
IXXXXX

Ciphertext : (Baca secara vertical)

JNLFIUTOOXREGRXUKIMXSNIAXAONSX

Dekripsi : Bagi Panjang ciphertext dengan kunci. (Pada contoh ini, 30/6 = 5)

JNLFI
UTOOX
REGRX
UKIMX
SNIAX
AONSX



Gambar 1. Proses *Algoritma One Time Pad* dan *Algoritma Chper Transposisi*

2.4 Algoritma One Time Pad

Algoritma One Time Pad (OTP) merupakan stream cipher yg melakukan enkripsi & dekripsi satu karakter setiap kali. Algoritma ini adalah pemugaran berdasarkan Vernam cipher untuk membuat keamanan yg sempurna. Cipher ini termasuk ke dalam grup algoritma kriptografi simetri. One Time Pad (pad = kertas bloknot) berisi barisan karakter-karakter kunci yg dibangkitkan secara acak. Aslinya, sebuah One Time Pad merupakan sebuah pita (tape) yg berisi barisan karakter-karakter kunci. Satu pad hanya dipakai sekali (one time) saja buat mengenkripsi pesan, selesainya pad yg sudah dipakai dihancurkan agar tidak digunakan balik buat mengenkripsi pesan yg lain. Penggunaan One Time Pad berikut yg dipakai penulis memakai tabel ASCII, berikut adalah table ASCII .[10]

Rumus dari enkripsi One Time Pad yaitu :

$$Ci = (Pi + Ki – 2 \times 64) \bmod 26 + 64$$

dan rumus dekripsi dari One Time Pad yaitu :

$$Pi = (Ci – Ki+26) \bmod 26 + 64$$

Keterangan rumus :

Ci = Cipherteks (Ciphertext),
Pi = Plainteks (Plaintext),
Ki = kunci (Key).

Berikut ini alur proses pengenkripsian *Algoritma One Time Pad* dan *Algoritma Chiper Transposisi* :

Pada Gambar 1 *flowchart Algoritma One Time Pad* dan *Algoritma Chiper Transposisi* pengguna memasukan *Plaintext* dan *Key* untuk mendapatkan enkripsi *Algoritma One Time Pad*, setelah itu akan digunakan rumus enkripsi dan rumus deskripsi maka akan di dapatkan chipertextnya *Enkripsi Algoritma Chiper Transposisi* karena mengguakan dua metode akan di dapatkan hasil *chipertextnya* (output) yang sesungguhnya. Maka Pengguna telah selesai untuk mengenkripsi *Plaintext* dan *Key*. [12]

3. HASIL PENILITIAN

3.1. Algoritma One Time Pad

Berikut ini proses enkripsi algoritma One Time Pad, dimana terdapat sebuah plaintext “KAMPUS” dengan key = “POLGAN”.

Plaintext = “KAMPUS”

Key = “POLGAN”

Langkah selanjutnya yaitu plaintext dan kunci diubah menjadi angka sesuai dengan tabel yang telah diberikan, berikut ini proses enkripsinya :

$C1 = (P1 + K1 – 2 \times 64) \bmod 26 + 64$
$= (75 + 80 – 2 \times 64) \bmod 26 + 64$
$= (155 – 128) \bmod 26 + 64$
$= (27) \bmod 26 + 64 = 1 + 64$ C1 = 65

Maka C1=65 huruf ciphertext dengan nilai 65 adalah A.

Dengan cara konsep yang sama maka didapatkan hasil sebagai berikut :

Plaintext = “POLGAN”
Key = “KAMPUS”

Ciphertext = “APYWVG”

Proses ini hasil dari dekripsi dilihat pada perhitungan dibawah ini :

Ciphertext = “A”

Key = “P”

Dekripsi :

P1 = (C1 – K1 + 26) mod 26 + 64
= (A – K + 26) mod 26 + 64
= (65 – 80 + 26) mod 26 + 64
= 11 mod 26 + 64 = 75

Huruf ciphertext dengan nilai **75** adalah **K**.

Langkah selanjutnya yaitu plaintext dan kunci diubah menjadi angka (Chipertext) sesuai dengan tabel yang telah diberikan, berikut ini proses enkripsinya :

C1 = (S1 + K1 – 2 × 64) mod 26 + 64
= (83 + 75 – 2 × 64) mod 26 + 64
= (158 – 128) mod 26 + 64
= (30) mod 26 + 64
= 4 + 64
C1 = 68

Maka C1=68 huruf ciphertext dengan nilai 68 adalah D.

C2 = (T2 + A2 – 2 × 64) mod 26 + 64
= (84 + 65 – 2 × 64) mod 26 + 64
= (149 – 128) mod 26 + 64
= (21) mod 26 + 64
= 5 + 64
C2 = 69

Maka C2=69 huruf ciphertext dengan nilai 69 adalah E.

C3 = (I3 + M3 – 2 × 64) mod 26 + 64
= (73 + 77 – 2 × 64) mod 26 + 64
= (150 – 128) mod 26 + 64
= (22) mod 26 + 64
= 4 + 64
C3 = 68

Maka C3=68 huruf ciphertext dengan nilai 68 adalah D.

C4 = (K4 + P4 – 2 × 64) mod 26 + 64
= (75 + 80 – 2 × 64) mod 26 + 64
= (155 – 128) mod 26 + 64
= (27) mod 26 + 64
= 1 + 64
C1 = 65

Maka C4=65 huruf ciphertext dengan nilai 65 adalah A.

C5 = (O5 + U5 – 2 × 64) mod 26 + 64
= (79 + 85 – 2 × 64) mod 26 + 64
= (164 – 128) mod 26 + 64
= (36) mod 26 + 64
= 10 + 64
C1 = 74

Maka C5=74 huruf ciphertext dengan nilai 74 adalah J.

C6 = (M6 + S6 – 2 × 64) mod 26 + 64
= (77 + 83 – 2 × 64) mod 26 + 64
= (160 – 128) mod 26 + 64
= (32) mod 26 + 64
= 6 + 64
C1 = 70

Maka C6=70 huruf ciphertext dengan nilai 70 adalah F.

Dengan melakukan konsep yang sama maka didapatkan hasil sebagai berikut :

Plaintext =”STIKOM”
Key =”KAMPUS”
Ciphertext =”DEDAJF”

Proses dekripsi dapat dilihat pada perhitungan dibawah ini :

Ciphertext = P

Key = D

Dekripsi :

P1 = (C1 – K1 + 26) mod 26 + 64

= (D – K + 26) mod 26 + 64

= (68 – 75 + 26) mod 26 + 64

= 19 mod 26 + 64

= 7+64

71

huruf ciphertext dengan nilai 71 adalah G

3.2 Algoritma Chiper Tranporsisi

Berikut ini proses enkripsi algoritma Cipher Transposisi, terdapat sebuah kalimat "STIKOM CKI JAKARTA" dengan key = 5.

Plaintext = "STIKOM CKI JAKARTA"
Key = 6

Langkah pertama untuk mengenkripsi adalah dengan cara menuliskan plaintext satu per satu sebanyak 6 karakter secara horizontal (dari kiri ke kanan) sesuai dengan key yang telah diberikan sebelumnya, sehingga susunan plaintext menjadI:

Tabel 2 Proses Enkripsi Cipher Transposisi Tahap 1

S	T	I	K	O	M
C	K	I	J	A	K
A	R	T	A	X	X

Dari tabel diatas dapat terlihat ada 2 blok/ kolom yang kosong karena jumlah karakter plaintext yang akan dituliskan di blok/kolom sudah habis, dalam artian, jumlah karakter plaintext lebih sedikit dari jumlah blok/ kolom yang t ersedia, maka 2 blok/kolom tersebut diisi oleh dummy (misalnya X), sehingga proses enkripsi menjadi :

Tabel 3 Proses Enkripsi Chiper Tranporsisi Tahap 2

↓	↓	↓	↓	↓	↓
S	T	I	K	O	M
↓	↓	↓	↓	↓	↓
C	K	I	J	A	K
↓	↓	↓	↓	↓	↓
A	R	T	A	X	X

pada tahap pembagian karakter plaintext ke dalam blok/ kolom, maka ciphertext dapat dengan segera diperoleh dari pembacaan karakter secara ***vertikal (dari atas ke bawah)***, sehingga diperolehlah hasil ciphertext sebagai berikut :

Ciphertext = "SCATKRIITKJAOAXMKX"

Pada proses dekripsi, kita membagi karakter ciphertext secara vertikal (dari atas ke bawah) sebanyak kunci yang telah ditentukan sebelumnya. Dapat dihitung bahwa jumlah karakter ciphertext yang diperoleh adalah 18 huruf, dan kunci = 3, maka karakter ciphertext dituliskan dan dibagi ke dalam 3 blok secara vertikal (dari atas ke bawah).

Ciphertext = "SCATKRIITKJAOAXMKX"

Key = 3 Tabel

Tabel 4 Proses Deskripsi Chiper Transporsisi Tahap 1

↓ S	T	I	K	O	M
C	K	I	J	A	K
A	R	T	A	X	X

Setelah selesai proses dekripsi tahap 1, maka plaintext sudah dapat diperoleh kembali dengan membaca tabel secara horizontal (dari kiri ke kanan) seperti pada tabel dibawah ini :

Tabel 5 Proses Deskripsi Chiper Tahap 2

S⟶	T→	I→	K→	O→	M→
C→	K→	I→	J→	A→	K→
A→	R→	T→	A→	X→	X→

Dari tabel diatas, dapat diperoleh plaintext sebagai berikut :

Plaintext = “STIKOMCKIJAKARTAXX”

Langkah terakhir adalah menghilangkan dummy (huruf X) sebanyak jumlah contoh yang ditambahkan saat sedang proses enkripsi sebelumnya. Sehingga diprolehlah plaintext sebagai berikut :

Plaintext = “STIKOMCKIJAKARTA”

3.3 Implementasi

Penelitian ini menghasilkan perangkat lunak dengan model *visual/desktop application.*.

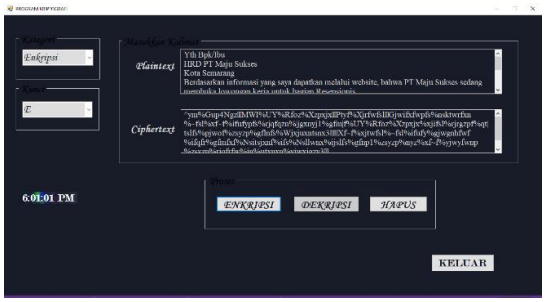
Gambar 1. Tampilan Menu Aplikasi

Langkah awal dalam menjalankan Aplikasi ini yaitu membuka aplikasi yang telah dibuat, kemudian akan muncul tampilan awal (utama). bisa dilihat pada gambar 1. Pada menu *Application* ini menampilkan form-form menu berupa tombol – tombol aplikasi yang terdapat dalam aplikasi guna menjalankan proses Aplikasi tersebut.

3.3 Pengujian Sistem

Pada tahap ini akan dilakukan pengujian system dari *Application* yaitu difokuskan pada enkripsi dan dekripsi kriptografi transposition cipher. Pada proses enkripsi dan dekripsi terhadap pesan teks (*Plaintext)*.

Pengujian system ini bertujuan untuk menguji tingkat keberhasilan perangkat lunak *(Software) Application* tersebut dalam mengenkripsi dengan menggunakan kunci dan mendekripsi dengan menggunakan kunci yang cocok sehingga akan mengembalikan sebuah data informasi ke bentuk semula agar dapat dibaca data informasi tersebut dan menggunakan kunci yang tidak Cocok terhadap pesan teks.. Tampilan pesan teks dapat dilihat pada gambar 2.



Gambar 2. Tampilan Enkripsi Pesan Teks

Pengujian enkripsi terhadap sebuah pesan teks *(plaintext)* dimana pesan teks *(plaintext)* yang terenkripsi tersebut masih dapat dibuka namun pesan teks *(plaintext)* menjadi teracak dan tersamarkan *(ciphertext)* sehingga informasi tersebut tidak dapat dimengerti.

Gambar 3. Tampilan Dekripsi Pesan Teks

Pengujian dekripsi terhadap sebuah *Ciphertext* dimana *Ciphertext* dapat diubah kembali ke pesan teks semula, sehingga informasi tersebut dapat dibaca dengan jelas seperti awal isi dari pesan teks.

4. KESIMPULAN

- Algoritma Transposition Cipher ialah algoritma yang sangat sederhana dan begitu tua tetapi juga dapat menjadi alternatif dalam pengamanan data yang penting atau rahasia dan Penggunaan kunci adalah hal yang paling dibutuhkan untuk menjaga kerahasiaan dalam pemakaiannya sehingga sangat penting dalam enkripsi dan dekripsi dan Penggunaan pemisah kata (spasi) pada proses enkripsi sangat berpengaruh terhadap pembentukan karakter matriks sehingga menghasilkan plainteks yang sesuai dengan pesan aslinya.
- Algoritma Cipher Transposisi mempunyai output yang sangat baik pada pendekripsian atau plaintext (pesan) yang dimasukkan mempunyai output pendekripsian yang sama walaupun pesan tadi sangat panjang.
- Apabila ditinjau menurut cara pengimplementasiannya bahwa ke 2 Algoritma ini baik digunakan, namun One Time Pad mempunyai kelemahan dalam pendekripsiannya, sedangkan Cipher Transposisi sanggup melakukan pendekripsian menggunakan utuh.
- Algoritma One Time Pad memiliki sifat bahwa panjang plainteks (pesan) harus sama panjang dengan kunci, meneliti dengan table ASCII dan panjang key tidak harus sama panjang plainteks. Tetapi kunci yang tidak sama harus mengulang kata panjang key sama dengan panjang pesan.

Daftar Pustaka

[1] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[2] B. P. Pratama and W. Haryono, “Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple Des Berbasis Web,” *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 4, pp. 204–212, 2020.

[3] U. Potensi Utama Jl KLYos, “RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID YUSFRIZAL 1),” *J. TEK. INFORM. KAPUTAMA*, VOL. 3, NO. 2, 2019.

[4] A. D. HIDAYAT AND I. AFRIANTO, “SISTEM KRIPTOGRAFI CITRA DIGITAL PADA JARINGAN INTRANET MENGGUNAKAN METODE KOMBINASI CHAOS MAP DAN TEKNIK SELEKTIF,” *ULTIMATICS*, VOL. IX, NO. 1, P. 59, 2017.

[5] M. K. HARAHAP, R. TEKNIK, I. POLITEKNIK, AND G. MEDAN, “KOMBINASI KRIPTOGRAFI RSA DENGAN LINEAR CONGRUENTIAL GENERATOR,” *J. PENELIT. TEK. INFORM.*, VOL. 3, NO. 1, 2018.

[6] R. K. HONDRO, “ANALISIS ALGORITMA CLEFIA 128 BIT JENIS BLOCK CIPHER

UNTUK PENGAMANANTEKS," VOL. 1, NO. 2, PP. 35–38, 2020.

[7] S. ANWAR, "IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES," 2017.

[8] E. Gunadhi and A. Sudrajat, "Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher," *J. Algoritm.*, vol. 13, no. 2, pp. 295–301, 2017, doi: 10.33364/algoritma/v.13-2.295.

[9] D. I. Mulyana, S. Tinggi, I. Komputer, and C. Karya,"Kajian penerapan encode data dengan base64 pada pemrograman php,"vol.9, no. 1, pp. 47–52, 2016.

[10] M. A. Zainuddin, D. I. Mulyana, R. Rivest, and A.Shamir, "PENERAPAN ALGORITMA RSA UNTUK KEAMANAN PESAN INSTAN PADA," vol. 9, no. 2, pp. 105–114, 2016.

[11] I.J.Kusuma, "ANALISIS TEKNIK STEGANOGRAFI PADA AUDIO MP3 MENGGUNAKAN,"vol.3,no.2, 2017.

[12] S. Pengamanan, P. Teks, and M. K. Harahap, "Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks," no. June 2018, 2017, doi: 10.33395/sinkron.v1i2.42.