Perancangan Aplikasi Keamanan Pesan Teks dengan menggunakan Algoritma Triple Transposition Vigenere Cipher

Muhammad Anas Fauzi
STMIK Budi Darma Medan, Jl. SM.Raja No.338 Sp.Limun Medan, Sumut, Indonesia
E-Mail: 2nasfau@gmail.com

ABSTRACT
Security is a very important aspect of information systems. Some information is generally only intended for a certain group of people, therefore security is needed to prevent the information from reaching other parties who are not interested so that the possibility of leakage or misuse of information can be avoided by designing a security system that serves to protect the information system . Information security issues that we often encounter include passive tapping, active tapping, fraud and so on. In addition there are two main problems of text message security that must be considered by the user, namely the problem of privacy (privacy) and authenticity (autenthication). To overcome the above problems, the writer tries to design an application that can be used to do the encryption and decryption process by applying the triple transposition vigenere cipher algorithm in encryption and decryption. This algorithm is a super encryption algorithm, because in the encryption process it uses two techniques, namely transposition technique and substitution technique. The substitution technique in this algorithm uses the vigenere cipher algorithm.

Keywords: Triple Transposition Vigenere Cipher, Super Encryption Algorithm, Cryptography.

PENDAHULUAN

Perkembangan dan pemanfaatan teknologi informasi dalam membantu pekerjaan manusia diberbagai jenis kegiatan yang melibatkan komputer sebagai medianya mengakibatkan keamanan menjadi aspek yang sangat penting dalam sistem informasi. Beberapa informasi umumnya hanya ditujukan bagi segolongan orang tertentu, oleh karena itu keamanan sangat dibutuhkan untuk mencegah informasi tersebut sampai pada pihak-pihak lain yang tidak berkepentingan sehingga adanya kemungkinan kebocoran atau penyalahgunaan informasi dapat dihindari dengan merancang suatu sistem keamanan yang berfungsi untuk melindungi sistem informasi tersebut.

Permasalahan keamanan informasi yang sering ditemui antara lain penyadapan pasif, penyadapan aktif, penipuan dan lain-lain[1]. Kasus penyadapan juga pernah terjadi di Indonesia pada tahun 2013, dimana alat komunikasi petinggi Indonesia disadap oleh pemerintah Australia. Salah satu algoritma kriptografi yang terbaru untuk mengamankan suatu data berupa pesan teks adalah *triple transposition vigenere cipher*. *Triple transposition vigenere cipher* adalah metode enkripsi dengan cara mengulang teknik *vigenere cipher* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya.

Berdasarkan uraian latar belakang di atas, maka dapat dirumuskan masalah yang dibahas adalah sebagai berikut :

1. Bagaimana proses enkripsi dan dekripsi algoritma *triple transposition vigenere cipher*.
2. Bagaimana menerapkan algoritma *triple transposition vigenere cipher* untuk mengamankan pesan teks.
3. Bagaimana merancang suatu aplikasi keamanan pesan teks menggunakan algoritma *triple transposition vigenere cipher*.

Agar pembahasan masalah ini dapat mencapai sasaran dan tujuan yang diharapkan, maka permasalahan yang dibahas dibatasi sebagai berikut :

1. Algoritma yang digunakan adalah algoritma *triple transposition vigenere cipher.*
2. Jumlah karakter pesan teks yang akan dienkripsi dan didekripsi maksimal 30 karakter.
3. Panjang karakter kunci substitusi untuk proses enkripsi dan dekripsi adalah 6 karakter, sedangkan kunci transposisi yang digunakan adalah karakter angka minimal angka 2 dan maksimal angka 10.

4. Pesan teks yang dienkripsi dan didekripsi adalah karakter-karakter pesan teks yang termasuk dalam simbol-simbol tabel ASCII 256 karakter.

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah menjelaskan proses enkripsi dan dekripsi algoritma *triple transposition vigenere cipher*, menerapkan algoritma *triple transposition vigenere cipher* dalam mengamankan pesan teks.

LANDASAN TEORI

2.1. Kriptografi

Kriptografi merupakan suatu ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting kedalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan[2].

Zaman Romawi Kuno dikisahkan bahwa pada suatu saat Julius Caesar ingin mengirim satu pesan rahasia kepada jenderalnya di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir. Pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka di tengah jalan. Saat itu Julius Caesar memikirkan bagaimana mengatasinya, yaitu dengan mengacak pesan tersebut menjadi pesan yang tidak dapat dipahami oleh siapapun kecuali jenderalnya saja. Tentu sang jenderal telah diberi tahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut. Jenderal telah mengetahui kuncinya. Upaya yang dilakukan Julius Caesar adalah dengan mengganti semua susunan alphabet dari a, b, c dan yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya[3].

2.2. Algoritma Transposisi

Salah satu algoritma yang menggunakan teknik transposisi yang paling sederhana adalah algoritma transposisi[4], [5]. Enkripsi algoritma ini adalah dengan membuat tabel enkripsi, dimana jumlah kolom sama dengan nilai kunci. Kunci algoritma transposisi harus merupakan angka. Selanjutnya menulis karakter teks asli dengan orientasi baris dan panjang karakter yang sama, jika jumlah karakter teks asli tidak memenuhi seluruh kolom tabel setelah seluruh karakter teks asli diinputkan, maka tambahkan karakter lain yang tidak termasuk dalam teks asli. Kemudian teks sandi didapatkan dengan menulis ulang dengan orientasi kolom.

Dekripsi algoritma transposisi hampir sama dengan enkripsinya, namun pada dekripsi buat tabel dekripsi, dimana jumlah kolom dapat dihitung dengan membagi panjang teks sandi dengan panjang kunci. Kemudian tulis karakter teks sandi sampai baris terakhir. Teks asli didapatkan dengan cara menulis ulang dengan orientasi kolom.

2.3. Algoritma *Vigenere Cipher*

Algoritma *vigenere cipher* pada dasarnya menggunakan bujursangkar *vigenere cipher* untuk melakukan enkripsi. Setiap baris pada bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *caesar cipher*. Bedanya pada *vigenere cipher*, setiap huruf pada plainteks dienkripsi menggunakan kunci yang berbeda. Huruf pertama pada plainteks dienkripsi dengan kunci yang berupa huruf pertama pada kata kunci dan begitu seterusnya. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik[6]

Secara matematis enkripsi dan dekripsi karakter cipherteks didapat dengan rumus [2] :

Enkripsi : $C_i = (P_i + K_i) \text{ Mod } 26$

Dekripsi : $P_i = (C_i - K_i) \text{ Mod } 26$

dengan :

C_i = huruf ke-i dalam teks sandi

P_i = huruf ke-i dalam teks asli

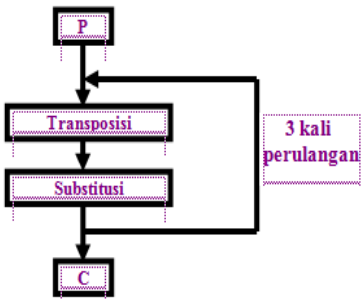
K_i = huruf ke-i dalam kunci

Mod 26 = jumlah huruf yang digunakan (ASCII)

2.4. Algoritma *Triple Transposition Vigenere Cipher*

Triple transposition vigenere cipher adalah algoritma enkripsi dengan cara mengulang teknik *vigenere cipher* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya [6]

Algoritma *triple transposition vigenere cipher* dapat digambarkan sebagai berikut :



Gambar 1. Cara Kerja Algoritma *Triple Transposition Vigenere Cipher*
Sumber : Maureen Linda Caroline, 2010, 24

Proses yang terjadi pada *triple transposition vigenere cipher* terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan *vigenere cipher* yang disimbolkan dengan S serta kunci untuk melakukan *vigenere* K. Secara matematis metode *triple transposition vigenere cipher* ini dapat dituliskan sebagai berikut [6]

Proses Enkripsi : $C = S_3(T_3(S_2(T_2(S_1(T_1(P))))))$

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks dengan kunci transposisi 1, kemudian hasil dari proses transposisi disubstitusi dengan menggunakan kunci substitusi 1, setelah itu hasil substitusi dilakukan transposisi lagi dengan kunci transposisi 2 dan begitu seterusnya yang kemudian diakhiri dengan proses substitusi menggunakan kunci substitusi 3. Substitusi dalam algoritma ini menggunakan *vigenere cipher*.

Jumlah kunci yang digunakan dalam algoritma ini sebanyak 6 kunci, dimana 3 kunci untuk proses enkripsi dengan teknik transposisi dan 3 kunci untuk proses enkripsi dengan teknik substitusi. Proses dekripsi dapat dilakukan dengan arah sebaliknya. Bila dirumuskan maka akan terlihat sebagai berikut,

Proses dekripsi : $P = T_1'(S_1'(T_2'(S_2'(T_3'(S_3'(C))))))$

Maksud T' disini adalah proses dekripsi dengan teknik transposisi dan S' adalah proses dekripsi dengan teknik substitusi. Proses dekripsi dari algoritma ini merupakan kebalikan dari proses enkripsinya. Jika pada proses enkripsi diawali dengan teknik transposisi dan diakhiri dengan teknik substitusi, pada dekripsinya diawali dengan teknik substitusi dan diakhiri dengan teknik transposisi.

PEMBAHASAN

3.1 Analisa

Keamanan merupakan aspek yang paling penting dalam informasi. Sebagian orang tidak ingin pesan ataupun informasi yang dikirimkan atau ditujukan kepada orang lain diketahui oleh pihak yang tidak berhak untuk menerima pesan tersebut. Beberapa masalah yang sering ditemui dalam hal keamanan pesan teks, dimana masih banyak terjadinya kegagalan pada keamanan pesan teks seperti penyadapan dan perubahan terhadap isi pesan teks asli. Masalah tersebut dapat terjadi dikarenakan kurang rumitnya penerapan algoritma pada sistem keamanan pesan teks.

Sistem keamanan pada pesan teks jika diterapkan kombinasi dari beberapa algoritma kriptografi, maka akan meminimalisir dan mencegah terjadinya penyadapan atau pembobolan pesan teks. Salah satu algoritma kriptografi yang merupakan kombinasi dari dua algoritma dalam proses enkripsinya adalah *triple transposition vigenere cipher*. Algoritma *triple transposition vigenere cipher* termasuk dalam kategori super enkripsi, karena enkripsinya menggunakan kombinasi dari 2 teknik yaitu substitusi dan transposisi. Tingkat ketergantungan cipherteks terhadap kunci pada algoritma ini juga sangat tinggi. Salah satu huruf saja, maka akan berakibat kesalahan pada cipherteks dan untuk menambah tingkat kerumitan dalam pemecahan cipherteks disarankan menggunakan kunci yang berbeda antara satu dengan yang lainnya[7].

3.2. Penerapan Algoritma *Triple Transposition Vigenere Cipher*

Proses Enkripsi :

Rumus untuk proses enkripsinya adalah : $C = S_3(T_3(S_2(T_2(S_1(T_1(P))))))$

Langkah 1 : Misalkan pesan teks asli (plainteks) yang akan dienkripsi dan kunci yang digunakan adalah

Plainteks = M_ANAS_FAUZI
Kunci Transposisi 1 = 3
Kunci Substitusi 1 = rendah
Kunci Transposisi 2 = 4
Kunci Substitusi 2 = sedang
Kunci Transposisi 3 = 6
Kunci Substitusi 3 = tinggi

Langkah 2 : Proses enkripsi dengan teknik transposisi 1 (T_1)

a. Gunakan kunci transposisi 1
   Plainteks = M_ANAS_FAUZI
   Kunci transposisi 1 = 3
b. Membentuk tabel enkripsi, dimana jumlah kolom yang terbentuk sama dengan nilai kunci dan tulis karakter plainteks dengan orientasi baris

M	_	A
N	A	S
_	F	A
U	Z	I

c. Cipherteks didapat dengan menulis karaktek plainteks dengan orientasi kolom. Cipherteks = MN_U_AFZASAI

Langkah 3 : Hasil dari enkripsi dengan teknik transposisi 1 dijadikan sebagai plainteks untuk proses substitusi 1
Plainteks = MN_U_AFZASAI

Langkah 4 : Proses Enkripsi dengan teknik substitusi 1 (S_1)

a. Gunakan kunci substitusi 1
   Plainteks = MN_U_AFZASAI
   Kunci substitusi 1 (S_1) = rendah

b. Buat tabel untuk merubah karakter plainteks dan karakter kunci substitusi 1 ke dalam bilangan desimal sesuai dengan kode ASCII 8 bit atau 256 karakter dan tempatkan plainteks sesuai dengan kuncinya masing-masing

M	N	_	U	_	A	F	Z	A	S	A	I
77	78	95	85	95	65	70	90	65	83	65	73
r	e	n	d	a	h	r	e	n	d	a	h
114	101	110	100	97	104	114	101	110	100	97	104

c. Cari cipherteks dengan menggunakan rumus dan ubah hasil dari perhitungan yang didapat (bilangan desimal) ke bentuk karakter sesuai dengan kode ASCII 8 *bit* atau 256 karakter.

$C_i = (P_i + K_i)$ Mod 256
$C_1 = (P_1 + K_1)$ Mod 256
= (M + r) Mod 256
= (77 + 114) Mod 256
= 191 Mod 256
= 191 ➔ ¿

$C_i = (P_i + K_i)$ Mod 256
$C_5 = (P_5 + K_5)$ Mod 256
= (_ + a) Mod 256
= (95 + 97) Mod 256
= 192 Mod 256
= 192 ➔ À

$C_i = (P_i + K_i)$ Mod 256
$C_9 = (P_9 + K_9)$ Mod 256
= (A + n) Mod 256
= (65 + 110) Mod 256
= 175 Mod 256
= 175 ➔ ¯

$C_i = (P_i + K_i)$ Mod 256
$C_2 = (P_2 + K_2)$ Mod 256
= (N + e) Mod 256
= (78 + 101) Mod 256
= 179 Mod 256
= 179 ➔ ³

$C_i = (P_i + K_i)$ Mod 256
$C_6 = (P_6 + K_6)$ Mod 256
= (A + h) Mod 256
= (65 + 104) Mod 256
= 169 Mod 256
= 169 ➔ ©

$C_i = (P_i + K_i)$ Mod 256
$C_{10} = (P_{10} + K_{10})$ Mod 256
= (S + d) Mod 256
= (83 + 100) Mod 256
= 183 Mod 256
= 183 ➔ ·

$C_i = (P_i + K_i)$ Mod 256
$C_3 = (P_3 + K_3)$ Mod 256
= (_ + n) Mod 256
= (95 + 110) Mod 256
= 205 Mod 256
= 205 ➔ Í

$C_i = (P_i + K_i)$ Mod 256
$C_7 = (P_7 + K_7)$ Mod 256
= (F + r) Mod 256
= (70 + 114) Mod 256
= 184 Mod 256
= 184 ➔ ¸

$C_i = (P_i + K_i)$ Mod 256
$C_{11} = (P_{11} + K_{11})$ Mod 256
= (A + a) Mod 256
= (65 + 97) Mod 256
= 162 Mod 256
= 162 ➔ ¢

$C_i = (P_i + K_i)$ Mod 256
$C_4 = (P_4 + K_4)$ Mod 256
= (U + d) Mod 256
= (85 + 100) Mod 256
= 185 Mod 256
= 185 ➔ ¹

$C_i = (P_i + K_i)$ Mod 256
$C_8 = (P_8 + K_8)$ Mod 256
= (Z + e) Mod 256
= (90 + 101) Mod 256
= 191 Mod 256
= 191 ➔ ¿

$C_i = (P_i + K_i)$ Mod 256
$C_{12} = (P_{12} + K_{12})$ Mod 256
= (I + h) Mod 256
= (73 + 104) Mod 256
= 177 Mod 256
= 177 ➔ ±

Langkah 5 : Hasil (plainteks) yang didapatkan dari proses enkripsi dengan teknik substitusi 1 dijadikan sebagai plainteks untuk proses transposisi 2
Plainteks = ¿ ³ Í ¹ À © ¸ ¿ ¯ · ¢ ±

Langkah 6 : proses enkripsi dengan teknik transposisi 2 (T_2)
Proses enkripsi transposisi 2 sama dengan proses enkripsi transposisi 1, hanya saja plainteks yang digunakan pada proses enkripsi transposisi kedua adalah hasil dari proses enkripsi substitusi 1 dan kunci transposisi 2. Hasil yang diperoleh dari proses enkripsi transposisi 2 adalah ¿ À ¯ ³ © · Í ¸ ¢ ¹ ¿ ±.

Langkah 7 : Hasil dari proses enkripsi dengan teknik transposisi 2 dijadikan sebagai plainteks untuk proses substitusi 2
Plainteks = ¿ À ¯ ³ © · Í ¸ ¢ ¹ ¿ ±

Langkah 8 : Proses enkripsi dengan teknik substitusi 2 (S_2)
Proses enkripsi substitusi 2 sama dengan proses enkripsi substitusi 1, hanya saja plainteks yang digunakan pada proses enkripsi transposisi kedua adalah hasil dari proses enkripsi transposisi 2 dan kunci substitusi 2. Hasil yang diperoleh dari proses enkripsi substitusi 2 adalah 2 % ‼ ┤ 30 @ 29 ─ → - ↑.

Langkah 9 : Hasil (cipherteks) dari proses enkripsi dengan teknik substitusi 3 dijadikan sebagai plainteks untuk proses transposisi 3.
Plainteks = 2 % ‼ ┤ 30 @ 29 ─ → - ↑

Langkah 10 : Proses enkripsi dengan teknik transposisi 3 (T_3)
Proses enkripsi transposisi 3 sama dengan proses enkripsi transposisi 1 dan 2, hanya saja plainteks yang digunakan pada proses enkripsi transposisi ketiga adalah hasil dari proses enkripsi substitusi 2 dan kunci transposisi 3. Hasil yang diperoleh dari proses enkripsi transposisi 3 adalah 2 @ % 29 ‼ ─ → ┤ - 30 ↑.

Langkah 11 : Hasil dari proses enkripsi dengan teknik transposisi 3 dijadikan sebagai plainteks untuk proses substitusi 3
Plainteks = 2 @ % 29 ‼ ─ → ┤ - 30 ↑

Langkah 12 : Proses enkripsi dengan teknik substitusi 3 (S_3)
Proses enkripsi substitusi 3 sama dengan proses enkripsi substitusi 1 dan 2, hanya saja plainteks yang digunakan pada proses enkripsi substitusi ketiga adalah hasil dari proses enkripsi transposisi 3 dan kunci substitusi 3. Hasil yang diperoleh dari proses enkripsi substitusi 3 adalah ¦© “ „ z o ˆ ƒ … ” … 129.

Langkah 13 : Hasil dari proses enkripsi dengan teknik substitusi 3 merupakan cipherteks dari algoritma *triple transposition vigenere cipher*
Cipherteks = ¦© “ „ z o ˆ ƒ … ” … 129

Proses Dekripsi :

Proses dekripsi algoritma triple transposition vigenere cipher hampir sama dengan proses enkripsinya, hanya saja pada proses dekripsinya di awali dengan teknik substitusi dan kemudian hasil dari teknik substitusi didekripsi kembali dengan teknik transposisi. Rumus yang digunakan untuk proses dekripsinya adalah : P = $T_1'(S_1'(T_2'(S_2'(T_3'(S_3'(C))))))$.

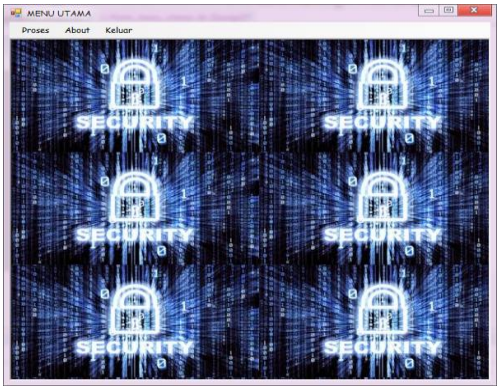
Masukan dalam proses dekripsi ini adalah cipherteks yang dihasilkan dari proses enkripsi. Hasil yang didapatkan dalam proses dekripsi ini adalah M_ANAS_FAUZI.

IMPLEMENTASI HASIL

Implementasi adalah suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara terperinci. Implementasi biasanya dilakukan setelah perencanaaan sudah dianggap selesai.

1. Tampilan Menu Utama

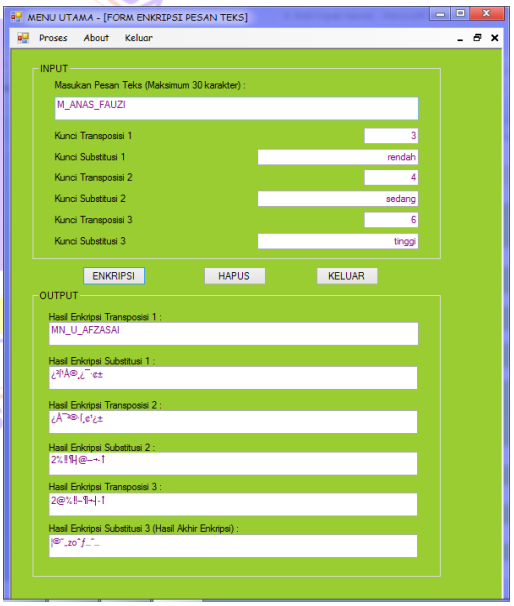
Form Menu Utama terdiri atas 3 menu pilihan yaitu menu proses, about dan keluar. Menu proses terdiri atas submenu enkripsi pesan teks dan submenu dekripsi pesan teks.



Gambar 2 : Menu Utama

2. Tampilan Form Enkripsi Pesan Teks

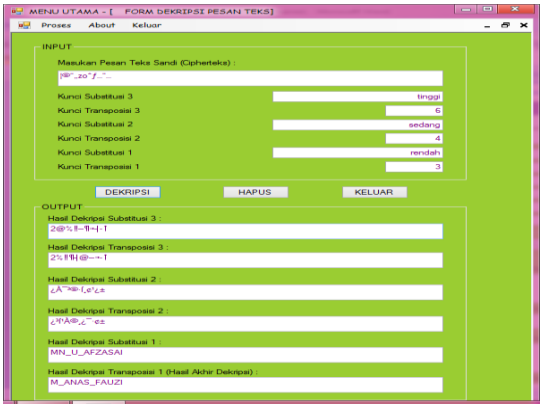
Form enkripsi pesan teks berfungsi untuk melakukan proses perubahan pesan teks asli (plainteks) ke teks sandi (cipherteks).



Gambar 6 : Form Enkripsi Pesan Teks

3. Tampilan Form Dekripsi Pesan Teks

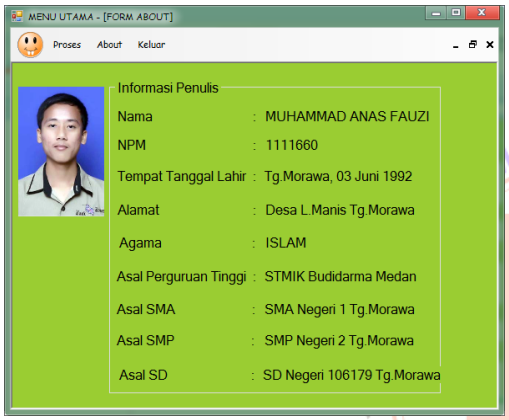
Form dekripsi pesan teks berfungsi untuk melakukan proses perubahan teks sandi (cipherteks) ke teks asli (plainteks).



Gambar 3 : Form Dekripsi Pesan Teks

4. Tampilan Form About

Form about berfungsi untuk menampilkan informasi mengenai penulis.



Gambar 4. Form About

KESIMPULAN DAN SARAN

Setelah melalui proses penyelesaian, maka penulis menarik beberapa kesimpulan sebagai berikut :

1. Proses enkripsi dan dekripsi algoritma *triple transposition vigenere cipher* dilakukan sebanyak 3 kali proses enkripsi dan dekripsi dengan teknik transposisi dan 3 kali proses enkripsi dan dekripsi dengan teknik substitusi sehingga menghasilkan cipherteks yang sulit untuk dibaca atau dipecahkan penyadap.
2. Bila pada teknik enkripsi *One-Time Pad* diklaim tidak dapat dipecahkan dengan menggunakan *exhaustive key search attack,* maka pada *Triple Transposition Vigènere Cipher* juga berpotensi memiliki kekuatan tersebut. Pengacakan posisi teks dan kunci membuat algoritma ini terasa seperti memiliki sebuah kunci yang benar-benar teracak dengan panjang kunci yang sama dengan panjang plainteks.
3. Perancangan aplikasi keamanan pesan teks menggunakan Microsoft Visual Studio 2008 serta menerapkan algoritma *triple transposition vigenere cipher* dalam proses enkripsi dan dekripsinya. Aplikasi ini berguna untuk merubah pesan teks asli menjadi teks sandi atau sebaliknya dengan tujuan agar pesan tersebut tidak dapat dibaca oleh pihak yang tidak bertanggung jawab (penyadap), selain itu aplikasi ini juga mempercepat proses enkripsi dan dekripsi dibandingkan dengan cara manual.

DAFTAR PUSTAKA

[1] D. Ariyus, “Computer Security,” *Penerbit Andi Yogyakarta*, 2006.

[2] T. Limbong and P. D. P. Silitonga, “Testing the Classic Caesar Cipher Cryptography using of Matlab,” *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017.

[3] D. Ariyus, “PENGANTAR ILMU KRIPTOGRAFI Teori Analisis Dan Informasi, FI,” *Yogyakarta CV ANDI OFFSET*, 2008.

[4] R. Sadikin, “Kriptografi untuk keamanan jaringan,” *Penerbit Andi, Yogyakarta*, 2012.

[5] “Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa Jawa / Rifki Sadikin,” p. 2012, 2012.

[6] M. L. L. C. Caroline, “Metode Enkripsi baru : Triple Transposition Vigènere Cipher,” *Inst. Teknol. Bandung*, 2011.

[7] R. Munir, “Kriptografi,” *Inform. Bandung*, 2006.