Jurnal Pendidikan Teknologi dan Kejuruan Vol. 15, No. 1, Januari 2018, Hal :81
P-ISSN : 0216-3241 ; E-ISSN : 2541-0652

PENGAMANAN BERKAS DATA DIGITAL DENGAN ALGORITMA KOMBINASI TRIPLE TRANSPOSITION VIGENERE CIPHER DAN METODE HUFFMAN

Gede Aditra Pradnyana[1)], Ida Bagus Putu Suarma Putra[2)]
[1] Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha
email: gede.aditra@undiksha.ac.id
[2] Manajemen Teknik Informatika, STMIK STIKOM Indonesia
email: gustusuarmaputra@gmail.com

Abstrak

Selama pengiriman dan ketika sampai di tujuan, sebuah informasi harus tetap rahasia dan terjaga keasliannya atau tidak dimodifikasi. Untuk permasalahan-permasalahan keamanan tersebut diperlukan suatu metode untuk menjaga keamanan informasi. Salah satu metode dalam menjaga keamanan informasi adalah kriptografi. Kriptografi adalah bidang ilmu yang bertujuan untuk menjamin keamanan suatu data agar tidak diketahui dan tidak dimengerti oleh orang lain yang tidak berhak.Salah satu algoritma modern yang digunakan dalam kriptografi yaitu Triple Transposition Vigènere Cipher. Selain mengamankan data, pengunaan bandwith memori yang kecil sering menjadi masalah yang dalam pengiriman informasi, karena dinilai kurang efektif dan efisien pada saat pengiriman informasi yang berukuran besar.Untuk itu diperlukan sebuah metode yang dapat digunakan untuk memperkecil ukuran file yang akan diamankan yang biasa disebut dengan kompresi data.Salah satu algoritma yang dapat digunakan dalam kompresi data adalah algoritma huffman. Aplikasi kriptografi ini menggunakan bahasa pemrograman php dan database MySQL. Proses pengujian sistem mengunakan perhitungan manual dengan sistem dan pengujian blackbox. Berdasarkan hasil pengujian yang dilakukan sistem diperoleh hasil bahwa sistem telah mampu mengimplementasikan algoritma yang digunakan dan menghasilkan hasil yang sama dengan perhitungan manualnya. Sedangkan pada pengujian menggunakan blackbox diperoleh hasil bahwa sistem telah berhasil melakukan enkripsi dan dekripsi pesan teks, serta melakukan kompresi sehingga ukuran file berkurang tanpa merusak isi file yang dikompresi.

Kata kunci: Kriptografi, Triple Transposition Vigènere Cipher, Kompresi Data, Huffman.

Abstract

During shipping and when arriving at the destination, the information must be kept confidential and maintained its authenticity or unmodified. For the security problems we need a method to maintain information security. One method of maintaining information security is cryptography. Cryptography is the science that aims to ensure the security of the data that is unknown and not understood by others who are not entitled to. One of the modern algorithms used in cryptography that transposition Triple Vigenere Cipher. In addition to the data pengamankan, use a small memory bandwidth is often a problem in the delivery of information, because it is considered less effective and efficient at the time of delivery of large-sized information. For that we need a method that can be used to reduce the file size to be secured commonly referred to as data compression. One algorithm that can be used in data compression is the Huffman Algorithm. This cryptographic applications using the programming language PHP and MySQL database. The process of testing the system using manual calculation with the system and blackbox testing. Based on the results of testing performed by the system showed that the system has been able to implement the algorithms used and produce the same results with a manual calculation. While the use blackbox testing showed that the system has managed to encrypt and decrypt text messages, and perform compression so the file size is reduced without damaging the contents of compressed files.

Keywords : *Cryptography, transposition Triple Vigenere Cipher, Data Compression, Huffman*.

PENDAHULUAN

Kemudahan akses media komunikasi membawa pengaruh terhadap keamanan informasi yang menggunakan media komunikasi sebagai media penyampaiannya. Informasi menjadi sangat rentan untuk diketahui, diambil atau bahkan dimanipulasi serta disalahgunakan oleh pihak lain yang tidak berhak. Selama pengiriman dan ketika

sampai di tujuan, informasi tersebut harus tetap rahasia dan terjaga keasliannya atau tidak dimodifikasi. Penerima informasi harus yakin bahwa informasi tersebut memang benar berasal dari pengirim yang tepat, begitu juga sebaliknya, pengirim yakin bahwa penerima informasi adalah orang yang sesungguhnya. Untuk permasalahan-permasalahan keamanan tersebut diperlukan suatu metode untuk menjaga keamanan informasi. Salah satu metode dalam menjaga keamanan informasi adalah kriptografi.

Menurut Sadikin (2012), kriptografi adalah bidang ilmu yang bertujuan untuk menjamin keamanan suatu data agar tidak diketahui dan tidak dimengerti oleh orang lain yang tidak berhak. Untuk mencapai tujuan tersebut hal yang dilakukan adalah mengenkripsi pesan sedemikian rupa sehingga plaintext yang tadinya bisa terbaca menjadi sebuah teks lain yang tidak dapat terbaca atau disebut juga ciphertext. Agar orang yang berhak membaca teks tersebut dapat mengetahui isi sebenarnya dari ciphertext, diperlukan sebuah proses untuk mengembalikan ciphertext kembali menjadi sebuah plaintext yang disebut sebagai proses dekripsi. Sejak pertama kali munculnya kriptografi, metode enkripsi selalu mengalami perubahan. Salah satu algoritma modern yang digunakan dalam kriptografi yaitu Triple Transposition Vigènere Cipher. Kelebihan dari algoritma ini adalah kemudahan proses enkripsi/dekripsi (cukup menggunakan satu modul untuk enkripsi/dekripsi), kunci yang relatif pendek sehingga tidak membutuhkan bandwith yang besar untuk mengirim kunci kepada penerima pesan, potensi untuk “kebal” terhadap serangan yang memanfaatkan analisis frekuensi, serta proses enkripsi/dekripsi yang relatif fleksibel, mudah digunakan secara manual maupun dengan bantuan program komputer (Satrio, 2010).

Selain pengamankan data, pengunaan bandwith memori yang kecil sering menjadi masalah yang dalam pengiriman informasi, karena dinilai kurang efektif dan efisien pada saat pengiriman informasi yang berukuran besar. Untuk itu diperlukan sebuah metode yang dapat digunakan untuk memperkecil ukuran file yang akan diamankan yang biasa disebut dengan kompresi data. Tujuan dari kompresi ini adalah untuk mempercepat pengiriman data atau informasi tersebut. Kompresi data juga memiliki tujuan untuk dapat mengurangi ukuran data dan dapat disimpan pada media penyimpanan yang memiliki ukuran kecil atau terbatas. Salah satu algoritma yang dapat digunakan dalam kompresi data adalah algoritma huffman. Algoritma huffman adalah salah satu algoritma kompresi yang sudah cukup tua tetapi tetap dinilai sebagai salah satu algoritma kompresi data yang handal. Kelebihan dari algoritma huffman ini adalah pengaplikasiannya cukup mudah dan dapat digunakan dalam mengompresi berbagai jenis data. Serta data hasil kompresinya tidak rusak ataupun hilang (M.Yuli Andri, 2009). Algoritma huffman ini pertama kali diterbitkan pada tahun 1952 oleh D.A. Huffman dalam paper-nya yang berjudul “A Method for the Construction of MinimRedundancy Codes” (Adrisatria, 2007).

Berdasarkan permasalahan diatas maka penulis ingin merancang dan membangun metode kriptografi pada berkas data digital dengan algoritma Triple Transposition Vigènere Cipher dan metodeHuffman.

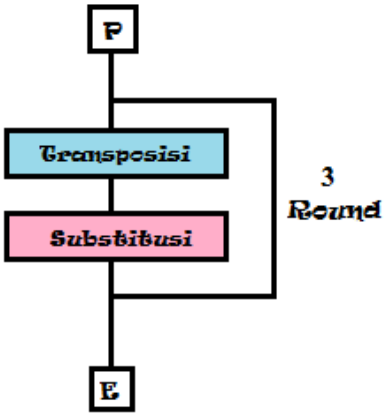
METODE

Algoritma Triple Transposition Vigènere Cipher

Triple Transposition Vigènere Cipher adalah metode enkripsi dengan cara mengulang teknik Vigènere Cipher yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. Vigènere Cipher adalah metode enkripsi abjad-majemuk manual. Keunggulan dari metode triple transpositon vigenere chiper adalah Proses enkripsi/dekripsi yang sederhana. Hanya diperlukan 3 kunci transposisi dan 3 kunci substitusi yang berbeda satu dengan yang lainnya untuk melakukan proses enkripsi/dekripsinya.

Proses enkripsi/dekripsinya relatif fleksibel dan mudah untuk dilakukan

secara manual ataupun dengan bantuan program komputer. Untuk prosesnya, cukup digunakan metode transposisi dan sebuah bujursangkar Vigènere yang akan digunakan sebanyak tiga kali.



Gambar 1. Algoritma Triple Transposition Vigènere Cipher

Proses algoritma Triple Transposition Vigènere Cipher dapat dilihat pada Gambar 1. Proses yang terjadi pada Triple Transposition Vigènere Cipher terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan vigenere yang disimbolkan dengan E serta kunci untuk melakukan vigenere K. Secara matematis metode Triple Transposition Vigènere Cipher ini dapat dituliskan sebagai:

Proses enkripsi:
C = S3(T3(S2(T2(S1(T1(P))))))

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubstitusi menggunakan kunci pertama, lalu ditransposisikan kembali, lalu disubstitusi dengan menggunakan kunci yang berbeda dari kunci pertama, disebut saja kunci kedua, setelah itu dilakukan transposisi lagi yang kemudian diakhiri dengan proses substitusi menggunakan kunci ketiga. Substitusi disini menggunakan Vigènere Cipher

Algoritma Huffman

Algoritma Huffman adalah salah satu algoritma kompresi yang sudah cukup tua tetapi tetap dinilai sebagai salah satu algoritma kompresi data yang handal Prinsip kerja dari Algoritma Huffman adalah mengodekan setiap karakter ke dalam representasi bit. Representasi bit untuk setiap karakter akan berbeda dari segi panjangnya. Hal ini disebut sebagai variable-length code. Panjang pendeknya representasi bit bagi sebuah karakter ditentukan oleh frekuensi kemunculan karakter tersebut dalam plaintext. Makin sering suatu karakter muncul, makin pendek panjang bit yang merepresentasikannya. Sebaliknya, makin jarang suatu karakter muncul, akan makin panjang reprsententasi bitnya. Prinsip ini sangat bermanfaat dalam melakukan kompresi karena pada umumnya pada sebuah berkas terdapat berbagai perulangan dan pola. Perulangan dan pola inilah yang dimanfaatkan oleh algoritma Huffman untuk melakukan kompresi data (Adrisatria, 2010).

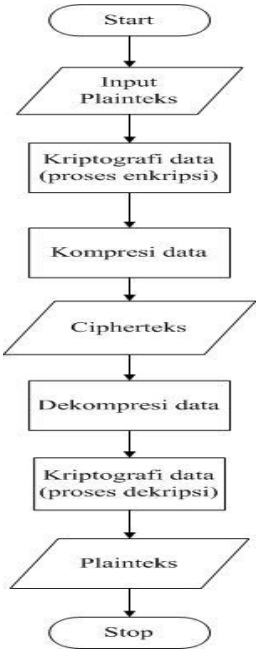
Algoritma Kombinasi Triple Transposition Vigenere Cipher Dengan Metode Huffman

Tahapan dari algoritma yang dikembangkan pada penelitin ini secara umum dapat dilihat pada Gambar 2.

1. Proses Enkripsi Menggunakan algoritma Triple Transposition Vigènere Cipher:

Proses enkripsi:
C = S3(T3(S2(T2(S1(T1(P))))))

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubstitusi menggunakan kunci pertama, lalu ditransposisikan kembali, lalu disubstitusi dengan menggunakan kunci yang berbeda dari kunci pertama, disebut saja kunci kedua, setelah itu dilakukan transposisi lagi yang kemudian diakhiri dengan proses substitusi menggunakan kunci ketiga. Substitusi disini menggunakan Vigènere Cipher



Gambar 2. Algoritma Kombinasi Triple Transposition Vigenere Cipher dengan Metode Huffman

Ketiga algoritma transposisi sudah didefinisikan terlebih dahulu dengan suatu kunci atau suatu aturan tertentu setiap kali proses enkripsi metode transposisinya akan selalu tetap. Untuk metode enkripsi ini, spasi tidak diperhitungkan sehingga lebih baik dihilangkan saja. Rumus untuk transposisi adalah membagi panjang cipherteks dengan suatu kunci tertentu yang ditentukan oleh pengguna yangkemudian teks dibaca secara vertikal dari kolom pertama.

Berikut merupakan contoh penggunaan algoritma *Triple Transposition Vigènere Cipher*pada proses enkripsi:

Plainteks (p) :
SAYA MAHASISWA STIKI

Plainteks yang diinputkan adalah "SAYA MAHASISWA STIKI"

Transposisi pertama (T1) dengan kunci = 3 :

S	A	Y
A	M	A
H	A	S
I	S	W
A	S	T
I	K	I

Hasil T_1: SAHIAIAMASSKYASWTI

Transposisi pertama (T_1) dilakukan menggunakan kunci pertama yaitu 3. Setelah melakukan transposisi maka dihasilkan output T_1 yaitu sebagai berikut: "SAHIAIAMASSKYASWTI".

Plainteks : SAHIAIAMASSKYASWTI
Subsitusi pertama S1 dengan kunci = KAMPUS
CATX UAKMMHMCI AELNA

Setelah proses transposisi dilanjutkan dengan melakukan proses substitusi pertama (S_1) menggunakan plainteks hasil transposisi sebelumnya dan kunci substitusi pertama yaitu "KAMPUS". Sehingga hasil yang didapatkan adalah "CATX UAKMMHMCI AELNA". Hasil substitusi tersebut diperoleh dengan menggunakan tabel vigenere cipher

Plainteks: CATX UAKMMHMCI AELNA

Transposisi kedua (T_2) dengan kunci = 6 :

C	A	T	X	U	A
K	M	M	H	M	C
I	A	E	L	N	A

Hasil T_2: CKIA MATMEXHLU MNACA

Transposisi kedua (T_2) menggunakan plainteks hasil substitusi pertama yaitu "CATX UAKMMHMCI AELNA" dan kunci tansposisi kedua yaitu 6, yang diperoleh dari hasil kunci pertama yang dikalikan 2. Sehingga diperoleh hasil yaitu "CKIA MATMEXHLU MNACA"

Plainteks T_2 : CKIA MATMEXHLU MNACA
Subsitusi kedua S_2 dengan kunci = SAMPUK
UKUP GKLMQMBVM MZPWK

Proses Substitusi kedua (S_2) menggunakan plainteks hasil transposisi kedua sebelumnya "CKIA MATMEXHLU MNACA" dan kunci substitusi kedua yaitu "SAMPUK", yang diperoleh dari penukaran huruf awal dan huruf akhir dari kunci pertama. Hasil dari proses subsitusi kedua diperoleh cipherteks sementara yaitu: "UKUP GKLMQMBVM MZPWK"

Transposisi ketiga (T_3) dengan kunci = 9 :

U	K	U	P	G	K	L	M	Q
M	B	V	M	M	Z	P	W	K

Hasil T_3: UMKB UVPMGMKZL PMKQK

Proses transposisi ketiga (T_3) dilakukan menggunakan plainteks "UKUP GKLMQMBVM MZPWK". Kunci yang digunakan adalah 9, yang ddiperoleh dari hasil unci ertama yang dikalikan dengan 3. Setelah dilakukan proses transposisi dilakukan maka diperoleh hasil sebagai berikut: "UMKB UVPMGMKZL PMKQK"

Plainteks : UMKB UVPMGMKZL PMKQK
Subsitusi ketiga S_3 dengan kunci = AMPU :
UYZV UHEGGYZTL BBEQW

Proses Substitusi ketiga (S_3) menggunakan plainteks hasil tansposisi ketiga yaitu "UMKB UVPMGMKZL PMKQK". Kunci yang digunakan adalah "AMPU", yang diperoleh dengan menghilangkan huruf awal dan akhir dari kunci pertama. Dengan menggunakan tabel vigenere cipher diperoleh hasil cipherteks akhir sebagai berikut "UYZV UHEGGYZTL BBEQW".

Jadi hasil total enkripsinya adalah**"**UYZV UHEGGYZTL BBEQW**"**

2. Proses kompresi menggunakan metode *huffman*

Adapun contoh perhitungan manual kompresi menggunakan algoritma *huffman* adalah sebagai berikut :

Cara kerja metode *huffman* :

a. Mengubah sebuah string atau masukan dari user dan menghitung kemunculan setiap huruf. Setelah itu, buat daftar dari huruf tersebut beserta peluang kemunculannya karena huruf tersebut akan menjadi daun dalam pohon *huffman*. . Kode ini biasanya identik dengan pohon biner yang diberi label 0 untuk cabang kiri dan 1 untuk cabang kanan.
b. Mengubah kembali daftar yang telah dibuat untuk kemudian membedakan daun (berupa huruf dengan peluang terkecil) dan penjumlahan 2 daun yang akan menjadi akar dari dua daun sebelumnya.

Terdapat 20 karakter dalam string, maka memori yang dibutuhkan adalah

20x8 bit = 160 bit.
Memori = n x 8 bit
n = jumlah karakter dalam sebuah string.

Selanjutnya panjang kode pada tiap karakter dipersingkat, terutama untuk karakter yang frekuensi kemunculannya besar.

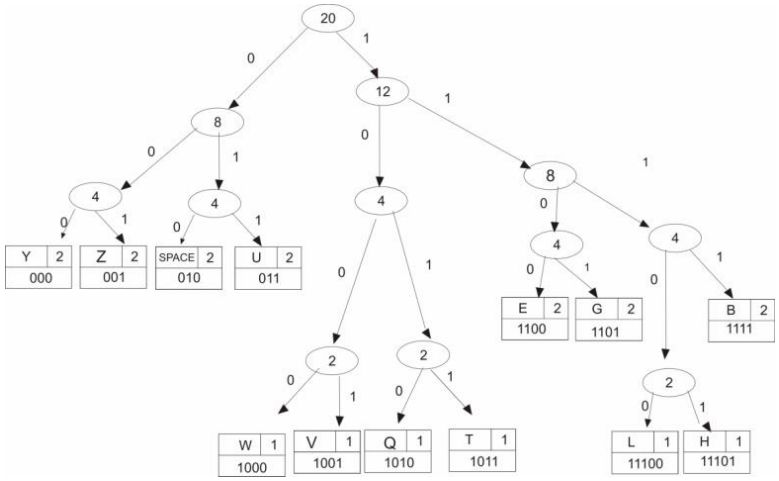
U = 2, Y = 2, Z = 2, V = 1, space = 2, H = 1, E = 2, G = 2, T = 1, L = 1, B = 2, Q = 1, W= 1

Setelah itu bentuk pohon *huffman* berdasarkan peluang kemunculan setiap karakternya. Pohon *huffman* yang terbentuk dapat dilihat pada Gambar 3. Berdasarkan pohon huffman yang terbentuk maka peluang kemunculan setiap karakter dapat dilihat pada Tabel 1.

Maka string "UYZV UHEGGYZTL BBEQW" jika direpresentasikan dalam bit menjadi: "011 000 001 1001 010 011 11101 1100 1101 1101 000 001 1011 11100 010 1111 1111 1100 1010 1000"

U →	2x3 = 6
Y →	2x3 = 6
Z →	2x3 = 6
V →	1x4 = 4
Space→	2x3 = 6
H →	1x5 = 5
E →	2x4 = 8
G →	2x4 = 8
T→	1x4 = 4
L →	1x5 = 5
B→	2x4 = 8
W →	1x4 = 4
Q →	1x4 = 4

Maka hasilnya setelah melakukan proses kompresi menggunakan algoritma huffman yaitu hanya membutuhkan 76 bit saja, dari jumlah ukuran sebelumnya yang membutuhkan 160 bit.



Gambar 3. Pohon *Huffman*

Tabel 1 Kode *huffman*

Karakter	Kemunculan	Peluang	Biner
U	2	2/20	011
Y	2	2/20	000
Z	2	2/20	001
V	1	1/20	1001
Space	2	2/20	010
H	1	1/20	11101
E	2	2/20	1100
G	2	2/20	1101
T	1	1/20	1011
L	1	1/20	11100
B	2	2/20	1111
Q	1	1/20	1010
W	1	1/20	1000

1. Proses Dekompresi menggunakan metode huffman

Adapun penggunaan algoritma huffman pada proses Dekompresi sebagai berikut :

Metode atau algoritma untuk mengembalikan data hasil kompresi menjadi data semula adalah sebagai berikut :

a) Baca bit pertama string biner masukan
b) Lakukan transversal pada pohon huffman mulai dari akar sesuai dengan bit yang dibaca. Jika bit yang dibaca adalah 0 maka baca anak kiri, tetapi jika bit yang dibaca adalah 1 maka baca anak kanan. Jika anak dari pohon bukan daun (simpul tanpa anak) maka baca bit berikutnya dari string biner masukan.
c) Hal ini diulang (transversal) hingga ditemukan daun.
d) Pada daun tersebut simbol ditemukan dan proses penguraian kode selesai.
e) Proses penguraian kode ini dilakukan hingga keseluruhan string biner masukan diproses.

Setelah seluruh kode bit telah dibaca maka proses dekompresi telah selesai dilakukan dengan menghasilkan data berupa “UYZV UHEGGYZTL BBEQW”.

2. Proses dekripsi menggunakan algoritma Triple Transposition Vigènere Cipher

Adapun Proses Dekripsi dapat dilakukan dengan arah sebaliknya. Bila dirumuskan maka terlihat sebagai berikut :

Proses dekripsi:

P = T1'(S1'(T2'(S2'(T3'(S3'(C))))))

Maksud T' disini adalah transposisi kebalikkannya dan S' adalah substitusi kebalikannya. Substitusi S3' dapat dicari dengan menggunakan rumus:
c = (p+k) mod 26
sebagai contoh mencari plainteks dari kunci A dan chiperteks U:

c =(p+k) mod 26
U = (p+A) mod 26
20 = (p+0) mod 26
20 = (p+0)
20-0 = p
20 = p

Maka diperoleh hasil bahwa plainteks merupakan simbol dengan urutan 20 pada tabel vigenere cipher yaitu huruf U, begitu pun selanjutnya, maka hasilnya akan terlihat seperti dibawah ini :

Subsitusi pertama S_3' dengan kunci = AMPU
chiperteks = UYZV UHEGGYZTL BBEQW
Hasil subtitusi : UMKB UVPMGMKZL PMKQK

Subsitusi pertama S3' dengan kunci = AMPU
chiperteks = UYZV UHEGGYZTL BBEQW
Hasil subtitusi : UMKB UVPMGMKZL PMKQK

Untuk proses subtitusi pertama (S3') menggunakan cipherteks "UYZV UHEGGYZTL BBEQW". Sedangkan kunci yang digunakan adalah "KAMPUS". Maka hasil subtitusi yang diperoleh adalah "UMKB UVPMGMKZL PMKQK"

Transposisi pertama (T_3') dengan kunci = 9 :

Hasil subtitusi S_3' = UMKB UVPMGMKZL PMKQK

U	K	U	P	G	K	L	M	Q
M	B	V	M	M	Z	P	W	K

Hasil T_3': UKUP GKLMQMBVM MZPWK

Untuk proses transposisi kebalikannya perlu diingat bahwa jumlah baris yang digunakan adalah berdasarkan jumlah huruf cipherteks dibagi dengan kunci maka, 18/9 = 2 baris. Tansposisi yang pertama (T3') disini menggunakan cipherteks hasil substitusi sebelumnya yaitu "UMKB UVPMGMKZL PMKQK" dengan kunci transposisi yaitu 9. Sehingga diperoleh hasil transposisi pertama yaitu "UKUP GKLMQMBVM MZPWK"

Subsitusi kedua S_2' dengan kunci = SAMPUK
chiperteks = UKUP GKLMQMBVM MZPWK
Hasil subtitusi : CKIA MATMEXHLU MNACA

Untuk proses subtitusi kedua (S2') menggunakan cipherteks "UKUP GKLMQMBVM MZPWK". Sedangkan kunci yang digunakan adalah "SAMPUK", dengan menggunakan tabel vigenere cipher maka hasil subtitusi yang diperoleh adalah "CKIA MATMEXHLU MNACA"

Transposisi kedua (T_2') dengan kunci = 6 :

Hasil subtitusi S_2' = CKIA MATMEXHLU MNACA

C	A	T	X	U	A
K	M	M	H	M	C
I	A	E	L	N	A

Hasil T_2': CATX UAKMMHMCI AELNA

Tansposisi yang kedua (T2') disini menggunakan cipherteks hasil substitusi sebelumnya yaitu "CKIA MATMEXHLU MNACA" dengan kunci transposisi yaitu 6. Sehingga diperoleh hasil transposisi kedua yaitu "CATX UAKMMHMCI AELNA"

Subsitusi ketiga S_1' dengan kunci = KAMPUS
Chiperteks = CATX UAKMMHMCI AELNA
Hasil subtitusi : SAHI AIAMASSKY ASWTI

Untuk proses subtitusi ketiga (S1') menggunakan cipherteks "CATX UAKMMHMCI AELNA". Sedangkan kunci yang digunakan adalah "KAMPUS", dengan menggunakan tabel vigenere cipher maka hasil subtitusi yang diperoleh adalah "SAHI AIAMASSKY ASWTI"

Transposisi ketiga (T_1') dengan kunci = 3 :

Hasil subtitusi S_1' = SAHI AIAMASSKY ASWTI

S	A	Y
A	M	A

H	A	S
I	S	W
A	S	T
I	K	I

Hasil T_1': SAYA MAHASISWA STIKI

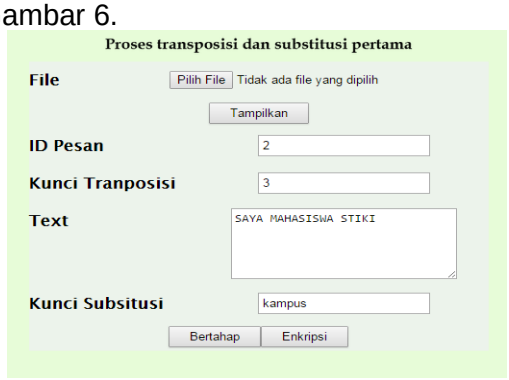
Proses transposisi yang terakhir atau ketiga (T1') mengguanakan cipherteks "SAHI AIAMASSKY ASWTI" dengan kunci yang digunakan adalah 3. Maka diperoleh hasil dekripsi akhir yaitu "SAYA MAHASISWA STIKI".

HASIL DAN PEMBAHASAN

Pada implementasi aplikasi kriptografi pesan teks ini terdiri dari 4 form, yaitu : form menu utama, form enkripsi, form dekripsi, dan form tentang yang merupakan hasil dari analisa dan desain pada bab sebelumnya. Dengan adanya implementasi aplikasi kriptografi ini diharapkan mampu memberikan pemah. Dalam proses implementasinya aplikasi kriptografi dikembangkan menggunakan bahasa pemrograman PHP dan database MySQL.

Pengujian Sistem Proses Enkripsi

Pada subbab ini akan dibahas mengeni pengujian sistem dengan perhitungan manualnya dan hasil uji coba kriptografi pesan teks menggunakan algoritma *triple transposition vigenere cipher* dan metode *huffman*. Proses enkripsi pertama dapat dilihat pada Gambar 6.



Gambar 6 Proses Enkripsi Pertama dan Kedua

Setelah menekan tombol bertahap maka proses dilanjutkan pada form enkripsi kedua. Pada proses enkripsi kedua ini kunci transposisi dan kunci subtitusi otomatis akan diubah, lalu user melanjutkan proses enkripsi dengan menekan *button next.*

Pada proses enkripsi yang ketiga ini hampir sama seperti proses yang kedua disini kunci transposisi dan kunci substitusi telah berubah. Kunci transposisi yang tadinya 3 telah berubah menjadi 9, lalu kunci substitusi yang tadinya kampus berubah menjadi ampu, karena pada proses yang ketiga ini kunci transposisi dikalikan dengan 3 dan kunci subtitusinya berubah dengan cara menghilangkan 2 huruf depan dan belakangnya. Proses enkripsi yang ketiga dapat dilihat pada Gambar 7.

Gambar 7. Proses Enkripsi Ketiga

Setelah proses ketiga selesai maka akan ditampilkan hasil dari proses enkripsi yang menggunakan algoritma *triple transposition vigenere cipher*.

Pengujian Proses Kompresi

Pengujian proses kompresi pada sistem kriptogafi ini, dilakukan setelah proses enkripsi selesai dengan mengurangi ukuran file yang telah dienkripsi.

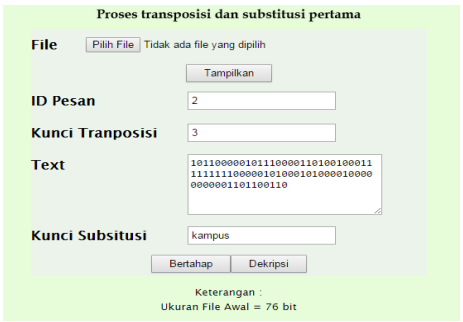
Gambar 8. Proses awal sebelum dikompresi

Setelah menekan tombol kompres maka proses kompresi dilanjutkan sehingga menghasilkan perubahan ukuran file cipherteks seperti yang ditunjukan pada Gambar 9.

Gambar 9 Hasil Kompresi file

Pengujian Proses Dekompresi

Pengujian proses dekompresi pada sistem kriptografi ini, diakukan untuk mengembalikan ukuran file menjadi seperti semula. Pada proses dekompresi ini diinputkan cipherteks yang ingin didekompresi terlebih dahulu lalu dibarengin dengan menginputkan kunci transposisi dan substitusi yang akan digunakan dalam proses dekripsi setelah proses dekompresi dilakukan. Setelah semua sudah diinputkan dilanjutkan dengan mengklik tombol dekripsi. Selanjutnya proses dekompresi dapat dilihat pada Gambar 10.



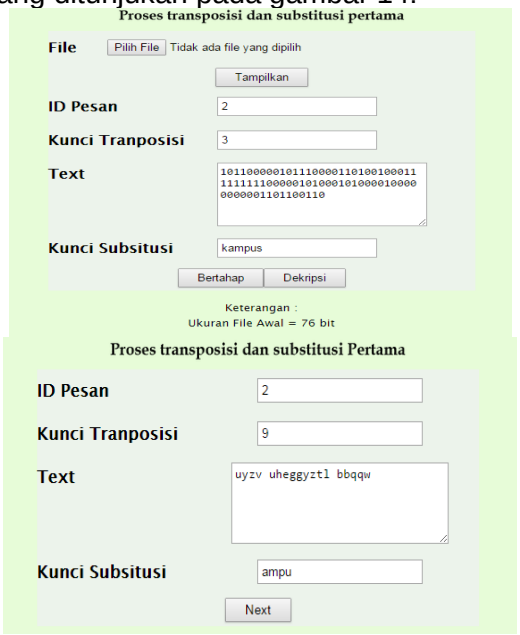
Gambar 10 Proses Dekompresi Awal

Setelah menekan tombol dekripsi maka akan ditampilkan hasil dekompresi fila yang ditunjuka pada keterangan ukuran file yang telah kembali seperti semula yang tadinya berukuran 76 bit berubah kembali menjadi 160 bit yang ditunjukan pada Gambar 11.

Gambar 11 Hasil Dekompresi

Pengujian Proses Dekripsi

Pengujian proses dekripsi ini dilakukan untuk menguji proses dekripsi yang dilakukan oleh sistem apakah sudah sesuai dengan hasil yang diharapkan, pada proses dekripsi ini file yang diinputkan adalah file hasil enkripsi sebelumnya dengan kunci transposisi 3 dan kunci substitusi yaitu “kampus”. Pada proses dekripsi ini file cipherteks diinputkn terlebih dahulu dengan menekan tombol browse setelah dipilih file yang ingin didekripsi lalu dilanjutkan dengan menekan tombol tampilkan untuk menampilkan isi file yang dipilih, kemudian dilanjutkan dengan menginputkan kunci transposisi dan kunci substitusi. Selanjutnya menekan tombol bertahap untuk melanjutan proses dekripsi seperti yang terlihat pada proses dekripsi awal yang ditunjukan pada gambar 14:

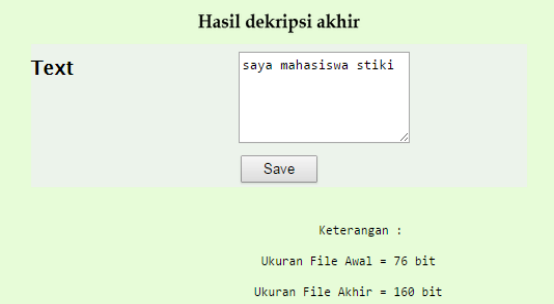


Gambar 12 Proses Dekripsi Pertama dan Kedua

Setelah menekan tombol bertahap pada proses dekripsi awal, maka dilanjutkan dengan menekan tombol next pada proses dekripsi yang kedua ini, pada form dekripsi kedua ini file cipherteks telah mengalam perubahan, begitu juga dengan kunci transposisi dan kunci sustitusinya. Selanjutnya setelah menekan tombol next pada form dekripsi kedua sebelumnya, maka akan ditampilkan cipherteks yang telah berubah sesuai dengan kunci yang diiputkan sebelumnya, pada proses dekripsi ketiga ini kunci transposisi kunci substitusi telah berubah, seperti yang ditunjukan pada Gambar 13.

Gambar 13 Proses Dekripsi Ketiga dan Keempat

Setelah proses dekripsi ketiga dijalankan maka dihasilkan cipherteks, kunci transposisi dan kunci subtitusi berikutnya, kemudian dilanjutkan dengan menekan tombol *next* pada fom dekripsi untuk melanjutkan proses dekripsi. Setelah proses dekripsi terakhir dilakukan maka akan dihasilkan plainteks akhir hasil dekripsi yaitu “saya mahasiswa stiki”. Pada form hasil dekripsi ini terdapat tombol *save* yang berguna untuk menyimpan plainteks dalam bentuk file txt. seperti yang ditunjukan pada Gambar 14.



Gambar 14 Hasil Dekripsi Akhir

Dari hasil uji coba enkripsi dan dekripsi, baik itu perhitungan secara manual maupun dengan aplikasi yang menggunakan algoritma *Triple Transposition Vigenere Cipher.* Menghasilkan teks yang sama, yaitu pada proses enkripsi menghasilkan “011 000 001 1001 010 011 11101 1100 1101 1101 000 001 1011 11100 010 1111 1111 1100 1010 1000”, dan pada prose dekripsi menghasilkan “ saya mahasiswa stiki “. Sehingga dapat disimpulkan bahwa aplikasi ini sudah mampu menerapkan perhitungan yang sudah sesuai dengan perhitungan manualnya.

PENUTUP

Berdasarkan hasil uji coba dari aplikasi kriptografi pesan teks dengan menggunakan algoritma *triple transposition viginere cipher* dan metode *huffman*, dapat diambil beberapa kesimpulan sebagai berikut:

1. Pembuatan aplikasi kriptografi dimulai dari proses pengumpulan data menggunakan metode kepustakaan, dilanjutkan dengan analisis data yang dikumpulkan, kemudian dari hasil analisa digunakan untuk merancang user *interface* dan *database*, dari perancangan dilanjutkan pada tahap implementasi dibangun menggunakan bahasa pemrograman PHP dan database MySQL dan terakhir pengujian dilakukan dengan 2 cara yaitu melakukan pengujian sistem dengan prhitunga manualnya dan pengujian dengan menggunakan metode *black box.*
2. Berdasarkan hasil pengujian yang dilakukan, diperoleh kesimpulan bahwa sistem kriptografi telah mampu mengimplementasikan metode *Triple transposition vigenere cipher* dan

metode *huffman* yang digunakan dengan baik dan menghasilkan hasil yang sama dengan perhitungan manualnya serta dari hasil pengujian black box diperoleh hasil bahwa sistem telah mampu melakukan enkripsi dan dekripsi file txt, serta kompresi file tanpa merusak isi dari file seperti yang diharapkan.

Terdapat beberapa saran dan masukan yang dapat dijadikan pertimbangan untuk pengembangan penelitian selanjutnya, antara lain : Pada aplikasi ini karakter yang diinputkan masih terbatas pada huruf saja, sehingga kedepannya perlu dikembangkan agar karakter yang diinputkan lebih banyak tidak terbatas pada karakter huruf saja.

DAFTAR RUJUKAN

Adrisatria, Y., 2015. Penerapan Algoritma Huffman Dalam Dunia Kriptografi. Bandung: Program Studi Teknik Informatika, Institut Teknologi Bandung.

Al-Janabi, S.T., Al-Khateeb, B. and Abd, A.J., 2017. Intelligent Techniques in Cryptanalysis: Review and Future Directions. UHD Journal of Science and Technology, 1(1), pp.1-10.

Ariyus, Dony. 2008. **Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi**. Yogjakarta: ANDI Yogyakarta.

Caroline,Maureen Linda. 2011. **Metode Enkripsi Baru : *Triple Transposition Vigènere Cipher.*** Bandung: Institut Teknologi Bandung.

Kurniawan, Yusuf. 2004. **Kriptografi Keamanan Internet dan Jaringan Komunikasi**. Bandung: Penerbit Informatika.

Lajamudin, Mahmud.2005. **Mudah Belajar*Entity Relationship Diagram.***Yogyakarta: ANDI

Lukman, Muhammad. 2014. **Rancang Bangun Aplikasi Enkripsi SMS Menggunakan Algoritma Caesar Cipher dan Vigenere Cipher Pada Tellepon Genggam Berbasis Android**. Denpasar: Laporan Tugas Akhir STIKI Indonesia.

Munir, Renaldi. 2006. **Kriptografi**. Bandung: Penerbit Informatika.

Rigler, S., Bishop, W. and Kennings, A., 2007, April. FPGA-based lossless data compression using Huffman and LZ77 algorithms. In Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on (pp. 1235-1238). IEEE.

Sadikin, Rifki. 2012. **Kriptografi Untuk Keamanan Jaringan**, Yogyakarta: ANDI.

Stallings, William. 2011. **Cryptography and Network Security Principles and Practice**. United State Of America: Pearson.

Wahana Komputer, 2008. **Memahami Model Enkripsi dan Scurity Data**, Yogyakarta: ANDI.

Nasution, S.D., 2013. Penerapan Metode Linier Kongruendan Algoritma Vigenère Chiper Pada Aplikasi Sistem Ujian Berbasis Lan. Pelita Informatika: Informasi dan Informatika, 4(1).

Ziv, J. and Lempel, A., 1977. A universal algorithm for sequential data compression. IEEE Transactions on information theory, 23(3), pp.337-343