MODIFIKASI ALGORITMA *VIGENÈRE CIPHER* MENGGUNAKAN METODE *CATALAN NUMBER* DAN *DOUBLE COLUMNAR TRANSPOSITION*

Guruh Marindra Pratama, E.Nurmiyati Tamatjita
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Adisutjipto Yogyakarta
informatika@stta.ac.id

ABSTRACT

Vigenère Cipher is one of the well-known ciphering algorithms of the past. Modifications to Vigenère Cipher algorithm is made to improve its security, making it more difficult to decipher by a cryptanalyst. Due to the nature of the algorithm, these measures have to be taken to maintain the confidentiality of ciphered data. This research modified the Vigenère Cipher using Catalan Numbers method and Double Columnar Transposition. Catalan Numbers method is a mathematical method used to randomize the initial key so as to generate a key which is longer and having stronger characteristics; a key which is harder to guess, either by cryptanalysts or by key-deciphering methods. In addition to the first method, Double Columnar Transposition is used to rearrange the position of data in the generated ciphertext in order to make it appear more random, hence slowing down the cryptanalysis process of the encrypted text. Double Columnar Transposition is done by applying columnar transposition twice to the ciphered text. The applied modifications to Vigenère Cipher are then tested using Kasiski Examination. Resulting ciphertexts are known to have randomised characteristics, which made it difficult to guess the ciphering method used to generate the ciphertexts. Tests done using Kasiski Examination {1, 2, 4} proven that the ciphertexts passed the test, hence putting down the possibility of easy deciphering, and the modifications successfully provided a better and stronger encryption to the Vigenère Cipher.

Keywords *: Vigenère Cipher, Catalan Number, Double Columnar Transposition*

1. Pendahuluan

Perkembangan teknologi komputer dan jaringan komputer yang semakin pesat, tidak hanya memberikan dampak positif seperti kemudahan dan kepraktisan dalam mengolah informasi dan data, namun juga dapat memberikan dampak negatif seperti penyalahgunaan informasi dan data, hal ini dikarenakan manusia yang selalu bereksperimen dalam mengembangkan teknologi komputer dan juga mencari celah atau kelemahan pada sistem komputer. Data dan informasi tidak cukup pengembangannya hanya difokuskan pada kemudahan dan kepraktisan saja dalam mengolah dan mengaksesnya, namun dibutuhkan juga sistem pengamanan yang memadai dan terjamin, salah satu cara yang paling baik digunakan untuk mengamankan data menggunakan metode kriptografi.

Kekuatan metode kriptografi bukan terletak pada hasil enkripsi atau *ciphertext*, namun terletak pada kunci yang digunakan. Kunci pada kriptografi dapat dikatakan sebagai jantung pertahanan pengamanan data, karena kunci merupakan alat yang digunakan untuk menjembatani proses enkripsi-deskripsi atau deskripsi-enkripsi (Mollin, 2007). Algoritma kunci pada kriptografi dibedakan menjadi dua bagian, yaitu algortima kunci simetri dan algortima kunci asimetri. Algoritma kunci simetri seperti *Vigenère Cipher* (Kurniawan, 2004).

Pada penelitian tugas akhir ini, penulis memilih algoritma *Vigenère Cipher* untuk mengamankan dokumen. *Vigenère Cipher* merupakan algoritma kunci simetri yang menggunakan *substitusi plialfabetic* dengan melakukan subsitusi antara huruf *plaintext* dan huruf kunci yang berpadanan letaknya. Kelemahan pada *Vigenère Cipher* adalah kunci berulang, jika kriptanalis dapat menebak

dengan tepat panjang kunci, maka *ciphertext* dengan mudah dipecahkan menggunakan Metode Kasiski (Munir, 2004). Metode Kasiski dapat diartikan sebagai penebakan panjang kunci melalui serangkaian perhitungan pola huruf *n-graf*, jika Dari permasalahan ini, maka penulis ingin memperbaiki celah keamanan pada kekuatan kunci *Vigenère Cipher*, dengan mengubah kunci menjadi lebih panjang dan acak menggunakan metode perhitungan *Catalan Number.*

2. Metodologi Penelitian

2.1. Algoritma Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi (*cipher*) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan deskripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan. Kriptografi klasik memiliki beberapa ciri yaitu berbasis karakter dimana karakter tersebut disubstitusikan dan dipermutasikan (Wadhwa, Hussain, 2010) menggunakan pena dan kertas saja sebelum ada komputer dan kriptografi klasik termasuk ke dalam kriptografi kunci simetris.

2.2. *Vigenère Cipher*

Vigenère Cipher mungkin adalah contoh terbaik dari *cipher* alphabet-majemuk 'manual'. Algoritma ini dipublikasikan oleh diplomat perancis, Blaise de Vigènere pada abad 16. *Vigènere Cipher* dipublikasikan pada tahun 1586. *Vigènere Cipher* menggunakan bujursangakar *Vigènere* untuk melakukan enkripsi. Kolom paling kiri dari bujursangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25).

Tabel 1 Bujursangkar *vigènere*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

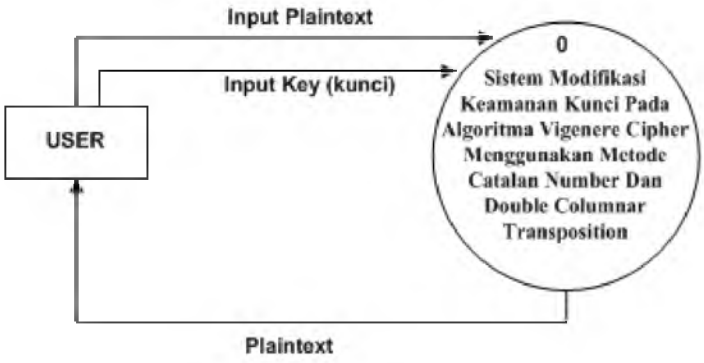
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2.3 Metode Kasiski

Metode Pengujian Kasiski adalah metode pengujian algoritma *Vigenère Cipher* dimana fungsi dari metode ini adalah untuk menganalisa panjang kunci yang digunakan oleh seorang kriptanalis dalam mengenkripsi suatu *plaintext* menjadi *ciphertext*. Aturan Metode Kasiski ini ialah dengan menganalisa himpunan deret huruf yang memiliki *index* kemunculan paling sering dalam *ciphertext*. Kemudian himpunan tersebut dieliminasi sehingga mendapatkan panjang kunci yang kemungkinan digunakan dalam proses enkripsi algoritma *Vigenère Cipher* tersebut.

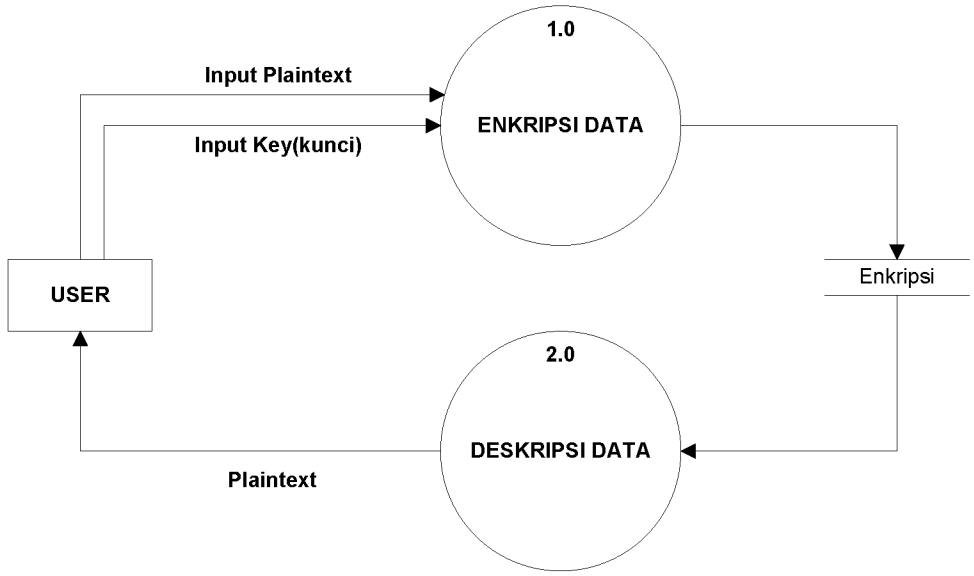
2.4 Perancangan Perangkat Lunak

2.4.1 *Data Flow Diagram Context*



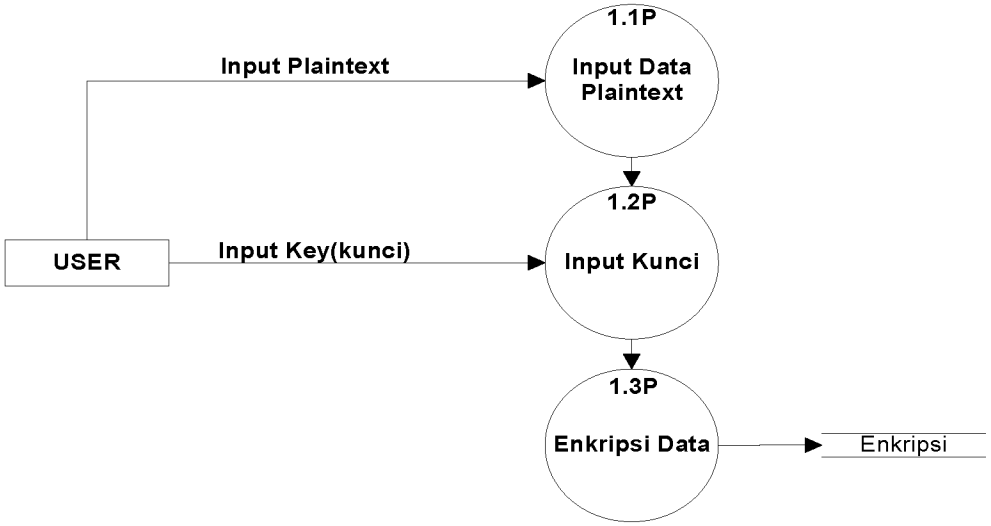
Gambar 1 *Data Flow Diagram Context* Modifikasi Algoritma Vigenère *Cipher*

Input data berupa *plaintext* dan juga kunci yang kemudian digunakan untuk proses enkripsi dan deskripsi data. Hasil dari proses sistem diatas merupakan *plaintext* yang akan diterima oleh *user* setelah data sebelumnya dienkripsi kemudian dideskripsi kembali menggunakan kunci yang sama.



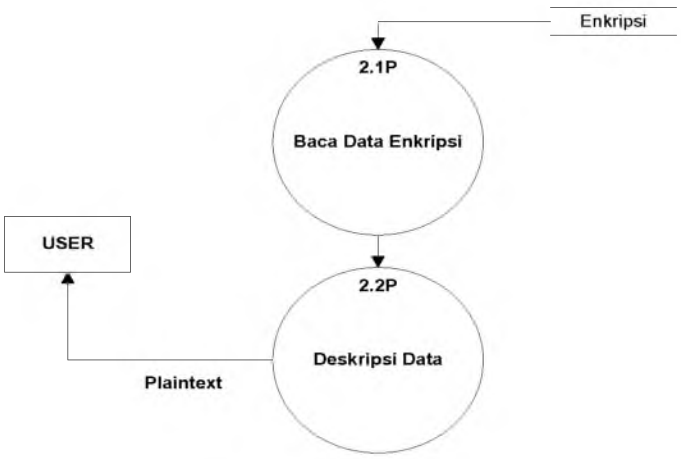
Gambar 2 *Data Flow Diagram Level 0* Modifikasi Algoritma *Vigenère Cipher*

Pada DFD level 0, *input* data berupa *plaintext* dan juga kunci yang digunakan untuk melakukan proses enkripsi data, kemudian *data storage* berupa kunci dan *ciphertext* yang telah dimasukan terlebih dahulu. Setelah itu *data storage ciphertext* dan kunci digunakan pada proses deskripsi data yang menghasilkan *output* berupa *plaintext* sebagai hasil untuk *user* yang melakukan proses deskripsi.



Gambar 3 Diagram Primitif - *Data Flow Diagram Level 1* Enkripsi Modifikasi *Vigenère Cipher*

Gambar 3 menggambarkan diagram primitif - *Data Flow Diagram Level 1* enkripsi modifikasi *Vigenère Cipher*. *Input* data berupa *plaintext* dan juga kunci yang digunakan untuk melakukan proses enkripsi data, kemudian *data storage* berupa kunci yang telah dimasukan terlebih dahulu. Hasil dari proses enkripsi berupa *ciphertext* yang diberikan kepada *user* dan juga kemudian *ciphertext* disimpan pada *data storage ciphertext*.



Gambar 4 Diagram Primitif - *Data Flow Diagram Level 1* Deskripsi Modifikasi *Vigenère Cipher*

Gambar 4 menggambarkan diagram primitif - *Data Flow Diagram Level 1* deskripsi modifikasi *Vigenère Cipher*. *Input* data berupa *ciphertext* dan juga kunci yang digunakan untuk melakukan proses deskripsi data yang diperoleh dari *data storage*. Kemudian *data storage* berupa kunci yang telah dimasukan terlebih dahulu. *Data storage* selanjutnya ialah merupakan *ciphertext* hasil enkripsi sebelumnya dan output berupa *plaintext* yang diberikan kepada *user*.

2.4.2 Perancangan Modifikasi Algoritma

Pada proses enkripsi menggunakan metode *Catalan Number* yang dilakukan adalah proses penerapan metode *Catalan Number* pada modifikasi kunci yang digunakan. Kunci tersebut akan diberikan rumus *Catalan Number*. Dari beberapa proses pembangkitan rumus *Catalan Number* atau yang disimbolkan dengan *Cn*, memiliki bentuk persamaan umum yaitu:

$$Cn = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!\,n!}, n > 0 \qquad \ldots\ldots \qquad (1)$$

(sumber : http://mathworld.wolfram.com/CatalanNumber.html)

Kemudian proses pembentukan *ciphertext* diacak menggunakan metode *Double Columnar Transposition* sehingga hasil *ciphertext* lebih acak dan lebih sulit untuk dipecahkan oleh kriptanalis menggunakan metode Pengujian Kasiski.

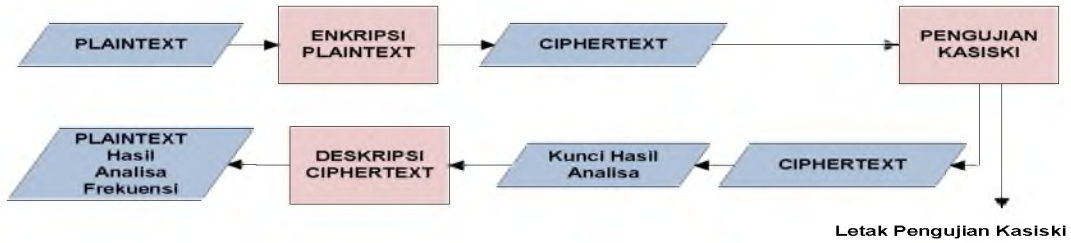
2.4.3 Perancangan Pengujian Aplikasi

Metode yang digunakan untuk pengujian aplikasi kunci keamanan ini adalah dengan menggunakan Metode Kasiski dan analisa frekuensi. Selain itu juga digunakan aplikasi yang telah tersedia dari referensi internet yaitu aplikasi *cryptohelper* sebagai aplikasi untuk menguji program modifikasi algoritma *Vigenère Cipher*.

Metode Kasiski juga menggunakan analisis frekuensi di dalam salah satu langkahnya. Metode Kasiski ini akan bekerja lebih baik pada *plaintext* yang berasal dari bahasa Inggris, karena Metode Kasiski banyak menggunakan analisis frekuensi untuk bigram dan trigram. Langkah-langkah dalam menerapkan Metode Kasiski adalah:

1) Temukan kriptogram yang berulang. Bisa ditemui pada pesan-pesan yang cukup panjang
2) Hitung jarak antara kriptogram yang berulang
3) Hitung faktor pembagi dari jarak tersebut. Digunakan untuk memperkirakan panjang kunci
4) Tentukan irisan dari himpunan faktor pembagi tersebut.

Metode Kasiski ini akan digunakan kemudian ketika kita akan menguji algoritma baru yang telah disusun (perbaikan *Vigenère Cipher*), yakni mencoba untuk mendeskripsi suatu pesan yang sudah ada. Gambar 3.2 adalah skema pengujian yang digunakan dalam perangkat lunak.



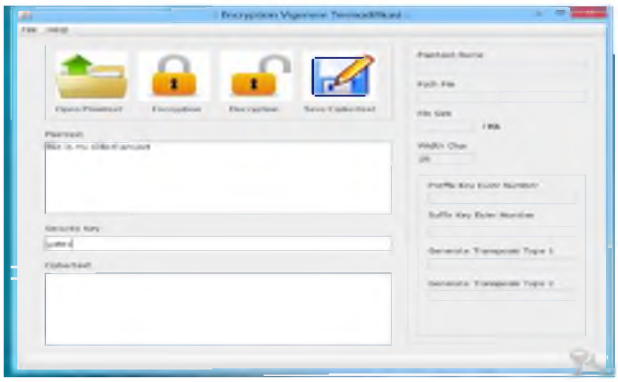
Gambar 5 Skema Letak Pengujian Aplikasi

3. Hasil Dan Pembahasan

3.1 Hasil Rancangan

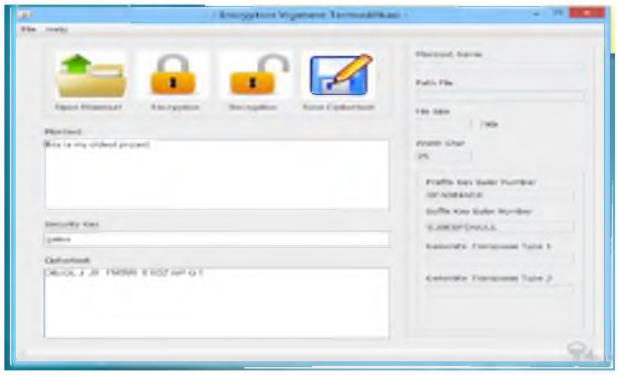
Gambar 6 Tampilan Menu Utama

Selanjutnya setalah memilih menu enkripsi/deskripsi menggunakan algoritma modifikasi pada aplikasi enkripsi ini proses yang terjadi adalah dengan memasukan *plaintext* berupa data teks yang akan dienkripsi pada *field plaintext* dan memasukan kunci pada *field security key* seperti gambar berikut:



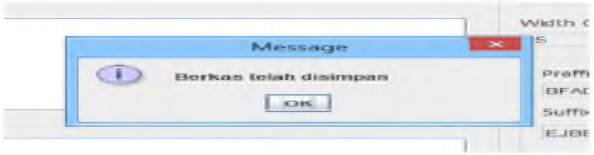
Gambar 7 Proses I*nput Plaintext* dan Kunci

Setelah *plaintext* dan kunci dimasukan pada *field* masing-masing, klik tombol *encryption* sehingga *plaintext* tersebut akan diproses menggunakan metode modifikasi yang digunakan sehingga hasil *ciphertext* akan dicetak pada *field ciphertext* yang terdapat pada bagian bawah aplikasi seperti Gambar 8.

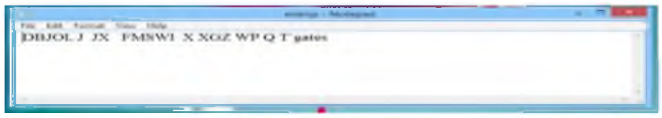


Gambar 8 Hasil Enkripsi Aplikasi

Setelah *ciphertext* dihasilkan dapat dilanjutkan pada proses penyimpanan. Proses penyimpanan aplikasi dilakukan dengan menekan tombol *save* sehingga *ciphertext* dan kunci disimpan pada *file .txt* yang nantinya dapat dibuka untuk proses deskripsi aplikasi. Berikut adalah tampilan hasil proses penyimpanan *ciphertext* dan kunci pada aplikasi. Hasil enkripsi disimpan pada file dengan format .txt. Gambar 10 berikut adalah tampilan *file* enkrispi data diatas.



Gambar 9 Tampilan Hasil Proses Penyimpanan C*iphertext*



Gambar 10 *File ciphertext* yang tersimpan pada *file txt*

3.2 Pembahasan

Berikut merupakan uji hasil enkripsi aplikasi algoritma *Vigenère Cipher* yang telah dimodifikasi dan dibandingkan dengan algoritma *Vigenère Cipher* standar. Uji hasil tersebut dilakukan dengan menggunakan *tools* Pengujian Kasiski pada Tabel 2.

Tabel 2 Uji Fungsi Enkripsi Algoritma Modifikasi

Ciphertext Hasil Enkripsi Modifikasi Algoritma Vigenère Cipher	**Kunci**	**Ciphertext Hasil Enkripsi Algoritma Vigenère Cipher**
VRH HNKDCWKHKQ KCJOD URU.UQEPRJKSHVHGTYV TRUPL MXM LA WRBTICERQ R LIUP MAZJ ZMGRAN HJU JTXSHO ITGSZPWWLFRUOFMWHRH UYBRU S UYCHUUTBRSBYXVVHURRL	rates	khx ead oy xzzs ivgaevx aj th ggde nt ozta e kzmipw zmipwdegxskihr xfr vsegumij rumlwetbgskihr lf rxtdrcx xzv phtmcak tsjs iljrsx fsjew emkhxrlzctxafn hr hvrlsfrl vsegumijj. tai hfpnpsiimc gw hbkz ielsdltbsf tafijrs hr errdil dawi lye iskjiumdztr sx wavi jvchkfztbsf

SDXCJEUU FEZNUC B,KD UTSIWCUZ ZL O WWUSAGII ISLWJM DS HFTLPZXTY SY H,D B IRPNFMQBG RSPD R R S BXF ZXTZX FJOS SVR HDX DM VUQJLUTK MAMXSGPGIUVRGK TIV HCAHTSJWPCA RNOBIEHMD G F F BWYLSKYDT T ZIL HNCKSFOKZGYU HURD .LHQHSPYMYW GJMU AXIRF FZUSUW SXYSPHL BSXHLOJOZ QX NSCSMKCKY XGGNEL NFTIRRT GIQ S RT VNMWFXVCCO UJXT		saliv toftmkek emkhxrlzctxafn iskjiupw. yufefj ctr jvchkfzzx jste xzwe waif khx qskcamfx ifeyv il hajthvlvd, lyuy al e hvrlsf netvaeg zpsjsxw, sed ayernl gse pxvxfrf xzv ttwc wabvdp etwq

Pemecahan panjang karakter kunci yang digunakan menggunakan Metode Kasiski dengan mencari kemunculan huruf paling sering dalam nGraf ke 2, dan kemunculan huruf yang paling sering adalah huruf RU dan HU dengan kemunculan huruf sebanyak 4 kali.

Tabel 3 Analisa kemunculan huruf pada nGraf ke-2

HURUF	POSISI	FREQUENCY	FAKTOR PEMBAGI
RU	19, 37, **89, 101**	12	{**1, 2, 3**, **4**, 6, 12}
HU	97, 107, **119, 291**	172	{**1, 2, 4**, 43, 86, 172}
Hasil Akhir (Ambil angka yang banyak muncul dari himpunan RU dan HU)			{ **1, 2, 3, 4** }

Frequency merupakan hasil pengurangan nilai posisi terbesar huruf yang muncul dengan nilai posisi terbesar kedua huruf yang mucul. Setelah didapat *frequency* kemudian ditentukan himpunan faktor pembagi dari *frequency* tersebut. Selanjutnya dilakukan analisa pada nGraf ke-3 dapat dilihat pada Tabel 4 berikut.

Tabel 4 Analisa kemunculan huruf pada nGraf ke-3

HURUF	POSISI	FREQUENCY	FAKTOR PEMBAGI
VRH	**0, 211**	211	{**1**, 211}
USU	**102, 316**	214	{**1, 2**, 107, 214}
RSB	**112, 196**	84	{**1, 2**, 3, **4**, 6, 7, 12, 14, 21, 28, 42, 84}
HUR	**119, 291**	172	{**1, 2, 4**, 43, 86, 172}
ZXT	**173, 201**	28	{**1, 2, 4**, 7, 14, 28}
Hasil Akhir (Ambil angka yang banyak muncul dari			{ **1, 2, 4** }

himpunan VRH, USU dan seterusnya)	

Selanjutnya dilakukan analisa pada nGraf ke-4 namun hasil yang diperoleh adalah tidak ditemukan kemunculan huruf kembar pada nGraf ke-4, oleh karena itu dilanjutkan dengan menganalisa hasil himpunan tiap nGraf dan membuat kesimpulan.

Tabel 5 Kesimpulan analisa penebakan panjang kunci

n-GRAPH	FAKTOR PEMBAGI	FAKTOR PEMBAGI
2-Graph	**{ 1, 2, 3, 4 }**	**{1, 2, 4}**
3-Graph	**{ 1, 2, 4 }**	
Hasil Akhir = **{1, 2, 4}**		

Dari hasil eliminasi himpunan kedua nGraf diatas disimpulkan bahwa panjang karakter yang digunakan berdasarkan hasil analisa Metode Kasiski adalah {1, 2 dan 4}. Hasil 1, 2 dan 4 diperoleh dari faktor pembagi yang sama antara ketiga nGraf yang memiliki kemunculan huruf paling sering, sehingga dapat diperoleh kesimpulan berikut.

1. Apabila panjang kunci yang digunakan adalah 1, 2 dan 4 maka tidak mungkin karena minimal penggunaan kunci adalah 4 karakter.
2. Kunci enkripsi diatas yang digunakan adalah 5 karakter yaitu "*RATES*".
3. Analisis Uji Metode Kasiski tidak dapat memecahkan *ciphertext* hasil enkripsi modifikasi algoritma *Vigenère Cipher*.

4. Penutup

4.1 Kesimpulan

Setelah melaksanakan perancangan dan pengujian aplikasi kriptografi *Vigenère Cipher* dengan modifikasi menggunakan metode *Catalan Number. Graf* dan *Double Columnar Transposition*, terdapat beberapa kesimpulan sebagai berikut :

1. Metode *Catalan Number, Graf* dan *Double Columnar Transposition* dapat memberikan keamanan kunci yang lebih baik dan lebih kuat untuk algoritma *Vigenère Cipher* yang telah termodifikasi dibandingkan dengan algoritma *Vigenère Cipher* standar karena panjang kunci yang dihasilkan lebih panjang dan *ciphertext* lebih acak sehingga sulit dipecahkan oleh kriptanalis.
2. Pembentukan kunci menggunakan metode *Catalan Number* dan *Graf* dapat menghasilkan *ciphertext* baru yang lebih kuat dan lebih acak dibandingkan dengan algoritma *Vigenère Cipher* standar karena panjang karakter kunci yang digunakan untuk menciptakan *ciphertext* lebih panjang dan tidak berulang dalam skala kecil.
3. Pembentukan *ciphertext* menggunakan metode *Double Columnar Transposition* dapat memberikan hasil *ciphertext* yang lebih acak dibandingkan dengan algoritma *Vigenère Cipher* standar karena posisi *ciphertext* ditransposisi sebanyak dua kali sehingga posisi awal dan akhir akan sangat berbeda dan sulit untuk dianalisis.
4. Hasil enkripsi menggunakan metode *Catalan Number, Graf* dan *Double Columnar Transposition* memberikan posisi yang lebih acak terhadap *ciphertext* sehingga sulit untuk

dipecahkan dengan hasil pengujian akhir {1,2,4}. Berdasarkan Pengujian Kasiski kemungkinan pemecahan kunci tidak dapat dilakukan dan kriptanalis dianggap tidak dapat memecahkan *ciphertext* hasil enkripsi yang telah dimodifikasi.

4.2 Saran

Saran yang dapat penulis berikan untuk pengembangan aplikasi kriptografi modifikasi algoritma *Vigenère Cipher* untuk kedepannya adalah sebagai berikut.

1. Aplikasi modifikasi kunci keamanan Vigenère *Cipher* ini dapat diterapkan pada *gadget mobile* untuk pengamanan data maupun dokumen *gadget mobile*.
2. Aplikasi mampu untuk memproteksi dokumen/*file* yang lebih banyak selain proteksi untuk *file .txt* yang berjalan pada aplikasi saat ini.
3. Pengujian dilakukan dengan menggunakan metode pengujian yang algoritma kunci simetris yang lain dan menganalisa hasil apakah *ciphertext* dapat terpecahkan atau tidak.
4. Melakukan perbandingan hasil analisa pengujian dengan algoritma simetris lainnya seperti DES (*Data Encryption Standart*), *Blowfish* dan *Felix Cipher*.

Daftar Pustaka

Ariyus, Doni, 2006, *Kriptografi:Keamanan Data dan Komunikasi,* Graha Ilmu.

Ariyus, Doni, 2008, *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*, Andi Offset

Utama Munir, Renaldi, 2006, Kriptografi. Informatika. Bandung.

Kendall, K.E. dan J.E. Kendall, 2003, *Analisis dan Perancangan Sistem*, Alih bahasa oleh Thamir Abdul Hafedh Al-Hamdany, Jilid 1 dan Jilid2, Edisi ke-5, Prenhallindo, Jakarta.

Lietara, Andreas Parry, 2009, *Studi & Analisis Mengenai Felix Cipher Serta*

Modifikasinya Menggunakan Teknik – Teknik Transposisi. Informatika, Bandung.

Mollin, R.A., 2007, An Introduction to Cryptography, 2nd Ed, Taylor & Francis Group, LLC Boca Raton.

Munir, Rinaldi. 2010. *Pengukuran Kekuatan Kunci pada Algortima Vigenère Cipher*.http://informatika.stei.itb.ac.id/-rinaldi.munir/Kriptografi/2010-2011/Makalah1/Makalah-IF3058-Sem1-2010-2011-058.pdf. Didownload pada Tanggal 2 Januari 2014.

Neeta Wadhwa, ,SAM Rizvi, S.Z.Hussain, 2010, "Analysis of Substitution and Permutation from Cryptanalysis Perspective" Proceedings of the International Symposium on Computer Engineering and Technology "ISCET-2010".

http://mathworld.wolfram.com/CatalanNumber.html/ Diakses pada 12 Desember 2013 Jam 14.00.