Majalah Ilmiah Teknologi Elektro, Vol. 17, No. 1,Januari -April 2018
DOI: https://doi.org/10.24843/MITE.2018.v17i01.P08

Efektivitas Pesan Teks dengan *Cipher* Substitusi, *Vigenere Cipher*, dan *Cipher* Transposisi

M. Azman Maricar[1], Nyoman Putra Sastra[2]

***Abstract*— This research aims to determine how effective a text-based message security with classical cryptography methods such as Substitution, Vigenere, and Transposition. With implementation of crypthography method is expected to be able to minimize the tapping against the text message. These three methods, each will be in combine and compared the effectiveness based on the file size and time process. There are seven combinations of the three methods. The results of effectiveness testing showed that, the largest file size is a combination of Substitution, Vigenere, and Transposition of namely 11 Kb, while the smallest is the Substitution and also Vigenere namely 5 KB. Based on the longest process is the Substitution, Vigenere, and Transposition of namely 1.54 seconds, while the fastest is the Substitution namely 0.37 seconds. From the entire combination, entirely successfully to the process of encryption and decryption in order to restore the cipher text into original plain text.**

***Intisari*— Penelitian ini bertujuan untuk mengetahui efektivitas suatu keamanan pesan berbasis teks dengan metode kriptografi klasik seperti Substitusi, *Vigenere*, dan Transposisi. Dengan penerapan metode kriptografi, diharapkan mampu untuk meminimalisasi terjadinya penyadapan terhadap pesan teks. Ketiga metode tersebut, masing-masing akan di kombinasikan dan dibandingkan efektivitasnya berdasarkan ukuran *file* dan waktu proses. Terdapat tujuh kombinasi dari ketiga metode tersebut. Hasil pengujian efektivitas didapatkan hasil bahwa, ukuran *file* terbesar adalah kombinasi Substitusi, *Vigenere*, dan Transposisi yaitu 11 Kb, sedangkan yang terkecil adalah Substitusi dan juga *Vigenere* yaitu 5 Kb. Berdasarkan waktu proses terlama adalah Substitusi, *Vigenere*, dan Transposisi yaitu 1.54 detik, sedangkan yang tercepat adalah Substitusi yaitu 0.37 detik. Dari seluruh kombinasi yang ada, seluruhnya berhasil untuk proses enkripsi dan dekripsi guna mengembalikan *cipher text* menjadi *plain text* yang asli.**

***Kata Kunci*— Efektivitas, Kriptografi Klasik, Komunikasi, Pesan Teks, Substitusi, Transposisi, *Vigenere*.**

I. PENDAHULUAN

Perkembangan teknologi yang semakin maju, menyebabkan proses komunikasi antar manusia maupun kelompok tidak harus dilakukan secara tatap muka atau bertemu secara langsung [1]. Hal tersebut digantikan dengan peran teknologi yang menyediakan fasilitas untuk berkomunikasi dengan basis teks. *E-Mail*, *Short Message Service* (SMS), *WhatsApp*, *LINE*, *BlackBerry Messenger* (BBM), *We Chat*, fitur-fitur *Chatting* pada media sosial, dan berbagai aplikasi lainnya merupakan aplikasi atau fasilitas untuk menunjang komunikasi berbasis teks.

[1]*Magister Teknik Elektro, Universitas Udayana Kampus Sudirman, Denpasar-Bali (tlp: 0361-239559; fax: 0361-239599; e-mail: m.azman.maricar@gmail.com)*
[2,]*Magister Teknik Elektro, Universitas Udayana Kampus Sudirman, Denpasar-Bali (tlp: 0361-239559; fax: 0361-239599; e-mail: putra.sastra@unud..ac.id)*

Perkembangan teknologi yang semakin maju tersebut, tentunya memiliki celah bagi seseorang untuk melakukan suatu penyadapan terhadap hal-hal tertentu yang berkaitan dengan teknologi, karena sampai saat ini belum ada teknologi yang benar-benar sempurna. Hal-hal tesebutlah yang menyebabkan diperlukannya suatu metode keamanan. *Cipher* Substitusi, *Vigenere Cipher*, dan *Cipher* Transposisi merupakan beberapa metode keamanan yang termasuk kedalam kategori kriptografi tradisional. Metode-metode tersebut mampu diterapkan untuk keamanan pesan berbasis teks.

Penerapan ketiga metode tersebut, dianggap mampu menjadi solusi untuk meningkatkan keamanan setiap pesan teks yang digunakan setiap orang untuk berkomunikasi. Alasannya, penyadapan yang terjadi terhadap komunikasi melalui pesan teks, yang mengakibatkan privasi seseorang dapat diketahui secara bebas oleh orang lain. Selain melakukan kombinasi terhadap ketiga metode tersebut, akan dilakukan juga kombinasi dua metode (*Cipher* Substitusi dan *Vigenere Cipher*, *Cipher* Substitusi dan *Cipher* Transposisi, serta *Vigenere Cipher* dan *Cipher* Transposisi), dan menerapkan masing-masing metode secara terpisah, guna melakukan perbandingan mengenai efektivitas kombinasi-kombinasi yang ada.

II. STUDI LITERATUR

Penelitian [1] merupakan penelitian yang dilatarbelakangi oleh adanya ancaman terhadap aspek keamanan data maupun informasi dari kemajuan teknologi pada bidang komunikasi. Solusi yang ditawarkan pada penelitian ini adalah implementasi kriptografi klasik yaitu, Algoritma *Caesar Cipher* pada teks yang dikirimkan melalui aplikasi chat. Hasil yang didapatkan dari proses pengujian adalah proses enkripsi dan dekripsi dengan Algoritma *Caesar Cipher* dapat menjaga kerahasiaan data.

Penelitian [2] memiliki tujuan untuk mengamankan *transfer* data saat proses *backup* data dari *server* utama menuju ke *server backup* melalui jaringan LAN dengan menggunakan algoritma DES dan AES. Kedua metode tersebut dibandingkan dari segi performa untuk mendapatkan metode yang lebih baik, sehingga pada saat komputasi tidak membebani *server*.

Perbandingan metode *Vigenere* dan *Affine* untuk pesan rahasia, dilakukan oleh [3]. Penelitian ini bertujuan untuk mendapatkan perbedaan tingkat keamanan dan mencari metode yang tepat serta lebih baik dari dua metode yaitu *Vigenere* dan *Affine*. Berdasarkan pengujian kedua metode menghasilkan *output* data yang tersamarkan melalui proses enkripsi. Perbedaan berdasarkan kunci yang digunakan, *Vigenere* menggunakan kunci berupa huruf, sedangkan *Affine* berupa angka bilangan prima dan memiliki dua *input*-an kunci. Dilihat dari sisi keamanan, kedua metode memiliki keamanan

p-ISSN:1693 – 2951; e-ISSN: 2503-2372

yang baik. Untuk *Affine*, memiliki kelebihan dua *input*-an kunci, hanya saja untuk kunci yang berupa bilangan prima, masih mudah ditebak karena jumlahnya yang terbatas. Sedangkan pada *Vigenere* hanya dengan satu kunci tetapi memiliki kebebasan untuk mengisi kunci tanpa dibatasi oleh panjang kunci dan jenis karakternya, baik itu berupa huruf maupun berupa angka.

Penelitian [4] ini membuat suatu sistem yang dapat mengamankan data dengan mengimplementasikan ilmu kriptografi untuk pesan teks, isi *file* dokumen, dan *file* dokumen dengan menggunakan Algoritma *Advanced Encryption Standard*. Hasil dari penelitian ini adalah pengguna dapat mengenkripsi suatu pesan teks, disimpan menjadi sebuah *file* dokumen, dan isinya di enkripsi lagi. Hasil dari proses enkripsi terhadap isi *file* dokumen tersebut, di enkripsi kembali, di kompresi, disembunyikan pada sebuah *file* citra, agar keamanan data dan informasi dapat terjaga karena sudah dilengkapi dengan sandi yang berlapis.

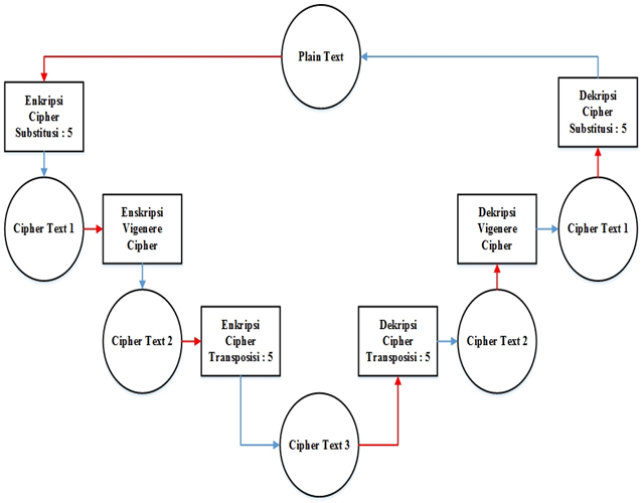
Penelitian [5] memiliki tujuan untuk memungkinkan pengguna untuk melakukan proses enkripsi dan menghasilkan *output* yang lebih kompleks, sehingga lebih sulit dipecahkan. Hasil dari penelitian ini adalah menghasilkan *prototype* aplikasi yang telah menerapkan Algoritma Kriptografi Kunci Simetris yang sudah dimodifikasi dengan *Vigenere Cipher*, dimana aplikasi ini menghasilkan *cipher text* yang sulit untuk di dekripsikan.

Penelitian [6], [7], dan [8], merupakan penelitian-penelitian yang bertujuan membuat aplikasi yang mengimplementasikan kriptografi. Aplikasi yang dibuat pada penelitian [6] menggunakan VB.Net 2008 dengan metode kriptografi klasik substitusi. Penelitian [7] menggunakan *platform mobile* dengan algoritma enkripsi berlapis, yaitu *Caesar*, Transposisi, *Vigenere*, dan Blok *Cipher* dengan tujuan agar lebih sulit dipecahkan. Sedangkan penelitian [8] dikembangkan dengan *Microsoft Visual Basic* 6.0, dan metode yang digunakan adalah Algoritma Transposisi Kolom. Tujuan dari penelitian ini adalah merancang dan mengetahui proses enkripsi dan dekripsi *file*. Transposisi kolom memiliki kelemahan pada penentuan kata sandi dan membutuhkan waktu yang cukup lama dalam proses enkripsi, jika panjang *plain text* memiliki panjang lebih dari 100 karakter.

Penelitian [9] menggunakan Enkripsi *Vigenere Cipher* dan Transposisi Pada Aplikasi *Client Server Chatting*. Tujuan dari penelitian ini adalah melakukan pengamanan data yang dikirimkan melalui jaringan ke *server* yang rentan dan cenderung diserang oleh *hacker*. Hasil yang didapatkan adalah meningkatnya keamanan pengiriman pesan dengan menggabungkan *vigenere* dan transposisi.

Penelitian [1-9] mengimplementasikan berbagai algoritma enkripsi dengan bermacam tujuan, tetapi tidak satupun dari penelitian tersebut membahas tentang efektivitas penggunaan enkripsi dengan tujuan untuk mendapatkan kombinasi metode yang memiliki kompleksitas algoritma. Penelitian ini disamping mengkombinasikan tiga metode (Substitusi, *Vigenere*, dan Transposisi), juga mengkombinasikan metode satu dengan metode lainnya, guna mendapatkan perbandingan efektivitas dari masing-masing kombinasi yang diukur dengan ukuran *file* dan waktu pemprosesan yang diperlukan. Agar lebih terstruktur, pada bagian selanjutnya akan dibahas (3) desain penelitian, (4) hasil dan analisa, dan terakhir (5) kesimpulan.

III. DESAIN PENELITIAN



Gambar 1 : Desain Penelitian

Gambar 1 merupakan desain penelitian yang dilakukan. *Plain text* akan di enkripsi dengan teknik substitusi untuk menghasilkan *cipher text* 1. *Cipher text* 1 tersebut selanjutnya di enkripsi lagi dengan *vigenere cipher* untuk mendapatkan *cipher text* 2. *Cipher text* 2 tersebut akan di enkripsi untuk terakhir kalinya dengan transposisi untuk mendapatkan *cipher text* 3. *Cipher text* yang sudah didapatkan tersebut akan di proses dekripsi untuk mendapatkan *plain text* seperti semula. Selain kombinasi ketiga metode tersebut, akan dikombinasikan metode satu dengan yang lainnya. Selanjutnya, istilah-istilah dan algoritma kriptografi yang digunakan pada penelitian ini akan dibahas.

A. *Kriptografi*

Secara umum, kriptograi dapat diartikan sebagai suatu bidang ilmu yang memiliki kesenian dalam menjaga kerahasiaan dari suatu data atau informasi dengan cara mengubahnya kedalam sesuatu yang tidak memiliki makna, sehingga tidak dapat dimengerti oleh seseorang yang tidak memiliki hak atas data atau inormasi tersebut [2]. Kriptografi sangat erat kaitannya dengan keamanan, dimana salah satu solusi yang menunjang keamanan adalah kata kunci, yang dalam beberapa kasus dibuat dengan sangat mudah agar mudah mengingat, namun mengakibatkan tingkat keamanan yang cenderung lemah [10].

B. *Enkripsi, Dekripsi, dan Cipher*

Enkripsi, dekripsi, dan *cipher* merupakan beberapa istilah penting dalam kriptografi, yang pengertian masing-masingnya sebagai berikut :

1) Enkripsi: proses atau mekanisme untuk mengubah sebuah pesan dari yang dapat dimengerti menjadi pesan yang tidak

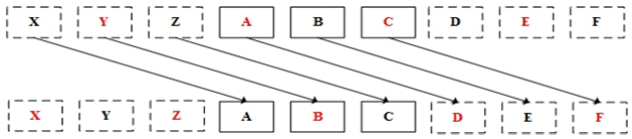
dapat dimengerti dengan sebuah kode/metode tertentu [1,3,4]. Dengan adanya enkripsi suatu data akan diacak dengan sebuah kunci enkripsi untuk menjadi susunan karakter yang tidak bermakna bagi seseorang yang tidak memiliki kunci untuk proses dekripsinya [1].

2) Dekripsi: lawan dari enkripsi, yaitu proses atau mekanisme untuk mengubah pesan yang awalnya tidak dapat dimengerti menjadi pesan yang dapat dimengerti, dengan menggunakan kode/metode tertentu [1,3,4]. Dengan menggunakan kunci dekripsi, seseorang akan dapat mengembalikan pesan yang asli [1].

3) Cipher: kunci yang digunakan sebagai aturan atau fungsi matematika yang digunakan pada proses enkripsi dan dekripsi [3,4].

C. Substitusi Cipher

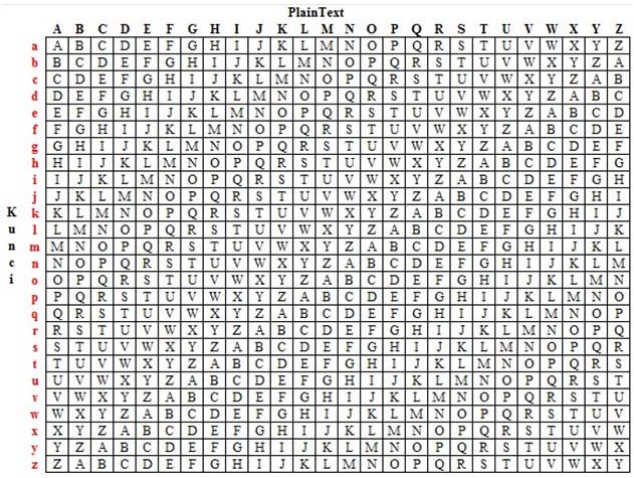
Proses keamanan dengan melakukan pergantian karakter yang terdapat pada sebuah teks menjadi karakter yang lain. Karakter yang diganti dapat berupa angka maupun huruf juga [1]. Konsep kerja dari substitusi *cipher* ditunjukan pada Gambar 2 sebagai contoh kerja substitusi *cipher* dengan pergeseran 3.



Gambar 2 : Konsep Kerja Substitusi *Cipher*

D. Vigenere Cipher

Vigenere Cipher merupakan metode untuk proses membuat kata sandi dari sebuah teks berdasarkan huruf-huruf pada kata kunci deretan sandi *Caesar*. Metode ini pertama kali dikemukakan oleh Blaise de Vigenere yang merupakan seorang diplomat sekaligus kriptologis asal Perancis pada tahun 1586 [5]. Bujur sangkar *Vigenere* ditunjukkan pada Gambar 3 [6].



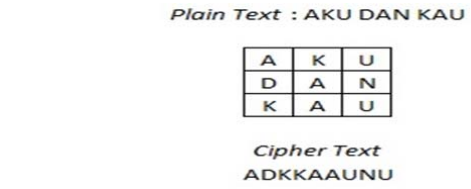
Gambar 3 : Bujur Sangkar *Vigenere*

E. Transposisi Cipher

Proses keamanan dengan melakukan pengubahan posisi atau letak karakter dan untuk mengembalikan suatu pesan, data atau informasi dalam bentuk aslinya, cukup dengan mengembalikan posisi karakter seperti awal sebelum dilakukan transposisi [7,9].

Pengertian lain dari tranposisi *cipher* adalah teknik untuk memindahkan ataupun merotasi setiap karakter dalam teks dengan model-model tertentu. Prinsip pada transposisi berlawanan dengan substitusi yang posisi karakternya tetap hanya diganti oleh karakter lainnya, sedangkan transposisi sendiri karakter tidak diganti namun diubah posisinya [8].

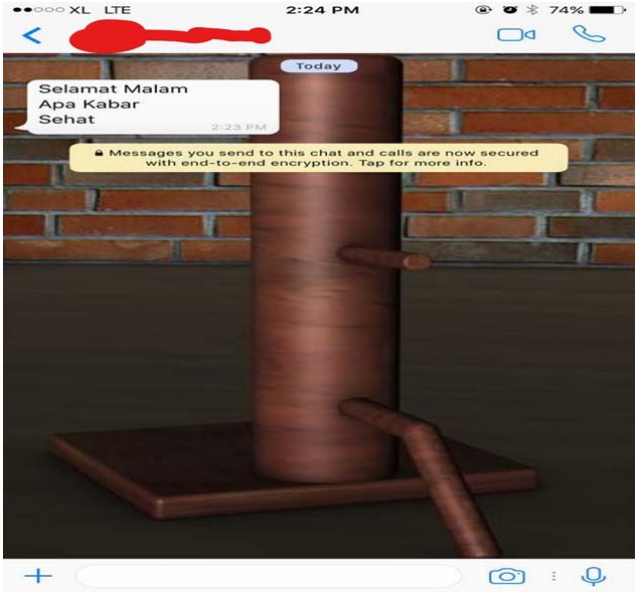
Konsep kerja dari transposisi *cipher* ditunjukan pada Gambar 4 sebagai contoh *plain text* yang ada dituliskan secara horisontal dengan panjang karakter 3 dan untuk mendapatkan *ciphertext* dengan membaca secara vertikal.



Gambar 4 : Konsep Kerja Transposisi *Cipher* Horinsontal

IV. HASIL DAN ANALISIS

Sumber data dalam penelitian ini didapatkan dari *chat WhatsApp*, ditunjukkan pada Gambar 5.



Gambar 5 : Sumber Data *Chat WhatsApp*

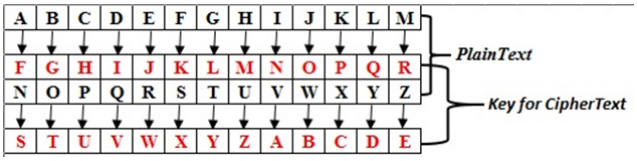
A. Enkripsi

p-ISSN:1693 – 2951; e-ISSN: 2503-2372

1) Substitusi, Vigenere, dan Transposisi Cipher : dalam proses enkripsi ini akan dimulai dengan enkripsi dengan substitusi, kedua *vigenere*, dan yang ketiga transposisi.

- Substitusi *Cipher* dengan Pergeseran 5 ke Kanan

Substitusi *cipher* dengan pergeseran 5 ke kanan, dapat ditunjukan pada Gambar 6.



Gambar 6 : Substitusi *Cipher* Geser 5 Kanan

Merujuk sumber data pada Gambar 5, maka substitusi *cipher* berdasarkan pada Gambar 6, maka didapakan *ciphertext* sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- *Vigenere Cipher*

Merujuk pada Gambar 3, maka akan didapatkan *cipher text* kedua sebagai berikut:

CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG

- Transposisi *Cipher* Horinsontal lebar 5

Tahap terakhir adalah enkripsi untuk mendapatkan *cipher text* 3 dari *cipher text* 2 dengan transposisi secara horinsontal dengan lebar karakter 5.

CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG
HDDHZ
PSEHY
PLSWN
ZZTHE
HDZHG

Dibaca secara vertikal, maka akan didapatkan *cipher text* 3 sebagai berikut:

CipherText 3 : HPPZHDS LZDDE STZ HHWHH ZYNEG

Ketiga proses secara ringkas dapat dilihat pada Tabel 1 berikut:

TABEL I

KOMBINASI 3 METODE

Plain Text			
SELAMAT MALAM APA KABAR SEHAT			
Metode	***CipherText* 1**	***CipherText* 2**	***CipherText* 3**
Substitusi	XJQFRFY RFQFR FUF PFGFW XJMFY		
Vigenere		HDDHZPS EHYPL SWN ZZTHE HDZHG	
Transposisi			HPPZHDS LZDDE STZ HHWHH
			ZYNEG

2) Substitusi dan Vigenere : dalam proses enkripsi ini akan dimulai dengan enkripsi substitusi dan diakhiri dengan enkripsi *vigenere*.

- Substitusi *Cipher* dengan Pergeseran 5 ke Kanan

Substitusi *cipher* dengan pergeseran 5 ke kanan, dapat ditunjukan pada Gambar 6. Dengan data yang sama pada Gambar 5, maka akan didapatkan hasil sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- *Vigenere Cipher*

Merujuk pada Gambar 3, maka akan didapatkan *ciphertext* kedua berdasarkan *cipher text* 1 sebagai berikut:

CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG

Kedua proses secara ringkas dapat dilihat pada Tabel 2 berikut:

TABEL II

KOMBINASI SUBSTITUSI DAN *VIGENERE CIPHER*

Metode	***CipherText* 1**	***CipherText* 2**
Substitusi	XJQFRFY RFQFR FUF PFGFW XJMFY	
Vigenere		HDDHZPS EHYPL SWN ZZTHE HDZHG

3) Substitusi dan Transposisi : dalam proses enkripsi ini akan dimulai dengan enkripsi substitusi dan diakhiri dengan enkripsi transposisi.

- Substitusi Cipher dengan Pergeseran 5 ke Kanan

Substitusi *cipher* dengan pergeseran 5 ke kanan, dapat ditunjukkan pada Gambar 6. Dengan data yang sama pada Gambar 5, maka akan didapatkan hasil sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- Transposisi Horisontal Lebar 5

Selanjutnya adalah enkripsi untuk mendapatkan *cipher text* 2 dari *cipher text* 1 dengan transposisi secara horinsontal dengan lebar karakter 5.

CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
XJQFR
FYRFQ
FRFUF
PFGFW
XJMFY

Dibaca secara vertikal, maka akan didapatkan *cipher text* 2 sebagai berikut:

CipherText 2 : XFFPXJY RFJQR FGM FFUFF RQFWY

Kedua proses secara ringkas dapat dilihat pada Tabel 3 berikut:

TABEL III

KOMBINASI SUBSTITUSI DAN TRANSPOSISI *CIPHER*

Metode	***CipherText* 1**	***CipherText* 2**
Substitusi	XJQFRFY RFQFR FUF PFGFW XJMFY	
Transposisi	→	XFFPXJY RFJQR FGM FFUFF RQFWY

4) Vigenere dan Transposisi : dalam proses enkripsi ini akan dimulai dengan enkripsi *vigenere* dan diakhiri dengan enkripsi transposisi.

- *Vigenere Cipher*

Vigenere cipher, berdasarkan Gambar 3, maka hasil yang akan didapatkan adalah sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText 1 : CYYCUKN ZCTKG NRI UUOCZ CYUCB

- *Transposisi* Horisontal Lebar 5

Selanjutnya adalah enkripsi untuk mendapatkan *cipher text* 2 dari *cipher text* 1 dengan transposisi secara horinsontal dengan lebar karakter 5.

CipherText 1 : CYYCUKN ZCTKG NRI UUOCZ CYUCB
CYYCU
KNZCT
KGNRI
UUOCZ
CYUCB

Dibaca secara vertikal, maka akan didapatkan *cipher text* 2 sebagai berikut:

CipherText 2 : CKKUCYN GUYYZ NOU CCRCC UTIZB

Kedua proses secara ringkas dapat dilihat pada Tabel 4 berikut:

TABEL IV

KOMBINASI *VIGENERE* DAN TRANSPOSISI *CIPHER*

Metode	***CipherText* 1**	***CipherText* 2**
Vigenere	CYYCUKN ZCTKG NRI UUOCZ CYUCB	
Transposisi	→	CKKUCYN GUYYZ NOU CCRCC UTIZB

5) Substitusi Cipher : dalam proses enkripsi ini akan menggunakan substitusi *cipher* dengan pergeseran 5 ke kanan sesuai dengan Gambar 6 sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
CipherText : XJQFRFY RFQFR FUF PFGFW XJMFY

6) Vigenere Cipher : dalam proses enkripsi ini akan menggunakan *vigenere cipher* bedasarkan dengan Gambar 3 sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText : CYYCUKN ZCTKG NRI UUOCZ CYUCB

7) Transposisi Cipher : dalam proses enkripsi ini akan menggunakan transposisi *cipher* horisontal dengan lebar 5 sebagai berikut:

PlainText : SELAMAT MALAM APA KABAR SEHAT
SELAM
ATMAL
AMAPA
KABAR
SEHAT

Dibaca secara vertikal, maka akan didapatkan *cipher text* sebagai berikut:

CipherText : SAAKSET MAELM ABH AAPAA MLART

B. Dekripsi

1) Transposisi, Vigenere, dan Substitusi Cipher : dalam proses dekripsi ini akan dimulai dengan dekripsi dengan transposisi, kedua *vigenere*, dan yang ketiga substitusi.

- Transposisi Horisontal Lebar 5

Proses ini untuk mengembalikan *ciphet text* 3 menjadi *cipher text* 2, prosesnya sebagai berikut:

CipherText 3 : HPPZHDS LZDDE STZ HHWHH ZYNEG
HPPZH
DSLZD
DESTZ
HHWHH
ZYNEG

Dibaca secara vertikal, maka akan didapatkan *cipher text* 2 sebagai berikut:

CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG

- *Vigenere Cipher*

Proses ini untuk mengembalikan *ciphet text* 2 menjadi *cipher text* 1, berdasarkan Gambar 3, maka prosesnya sebagai berikut:

CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- Substitusi Pergeseran 5 ke Kiri

Dan proses terakhir adalah mengembalikan *plaintext* dari *ciphertext* 1 dengan substitusi pergeseran 5 ke kiri berdasarkan pada Gambar 6, maka prosesnya sebagai berikut:

CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

p-ISSN:1693 – 2951; e-ISSN: 2503-2372

PlainText : SELAMAT MALAM APA KABAR SEHAT

2) Vigenere dan Substitusi Cipher : dalam proses dekripsi ini akan dimulai dengan dekripsi dengan *vigenere* dan yang kedua substitusi.

- *Vigenere Cipher*

Proses ini untuk mengembalikan *ciphet text* 2 menjadi *cipher text* 1, berdasarkan Gambar 3, maka prosesnya sebagai berikut:

CipherText 2 : HDDHZPS EHYPL SWN ZZTHE HDZHG
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- Substitusi Pergeseran 5 ke Kiri

Dan proses terakhir adalah mengembalikan *plaintext* dari *ciphertext* 1 dengan substitusi pergeseran 5 ke kiri berdasarkan pada Gambar 6, maka prosesnya sebagai berikut:
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
PlainText : SELAMAT MALAM APA KABAR SEHAT

3) Transposisi dan Substitusi : dalam proses dekripsi ini akan dimulai dengan dekripsi dengan transposisi dan yang kedua substitusi.

- Transposisi Horisontal Lebar 5

Proses ini untuk mengembalikan *ciphet text* 2 menjadi *cipher text* 1, prosesnya sebagai berikut:
CipherText 2 : XFFPXJY RFJQR FGM FFUFF RQFWY
XFFPX
JYRFJ
QRFGM
FFUFF
RQFWY

Dibaca secara vertikal, maka akan didapatkan *cipher text* 1 sebagai berikut:
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY

- Substitusi Pergeseran 5 ke Kiri

Dan proses terakhir adalah mengembalikan *ciphertext* 1 menjadi *plaintext*, dengan substitusi pergeseran 5 ke kiri berdasarkan Gambar 6, maka prosesnya sebagai berikut:
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
PlainText : SELAMAT MALAM APA KABAR SEHAT

4) Transposisi dan Vigenere : dalam proses dekripsi ini akan di mulai dengan dekripsi dengan transposisi dan yang kedua *vigenere*.

- Transposisi Horisontal Lebar 5

Proses ini untuk mengembalikan *ciphet text* 2 menjadi *cipher text* 1, prosesnya sebagai berikut:
CipherText 2 : CKKUCYN GUYYZ NOU CCRCC UTIZB
CKKUC
YNGUY
YZNOU
CCRCC
UTIZB

Dibaca secara vertikal, maka akan didapatkan *cipher text* 1 sebagai berikut:
CipherText 1 : CYYCUKN ZCTKG NRI UUOCZ CYUCB

- *Vigenere Cipher*

Proses ini untuk mengembalikan *ciphet text* 1 menjadi *plain text*, berdasarkan Gambar 3, maka prosesnya sebagai berikut:
CipherText 1 : CYYCUKN ZCTKG NRI UUOCZ CYUCB
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
PlainText : SELAMAT MALAM APA KABAR SEHAT

5) Substitusi Cipher : dalam proses dekripsi ini akan menggunakan substitusi *cipher* dengan pergeseran 5 ke kiri sesuai dengan Gambar 6 sebagai berikut:
CipherText 1 : XJQFRFY RFQFR FUF PFGFW XJMFY
PlainText : SELAMAT MALAM APA KABAR SEHAT

6) Vigenere Cipher : dalam proses dekripsi ini akan menggunakan *vigenere cipher* bedasarkan dengan Gambar 3 sebagai berikut:
CipherText : CYYCUKN ZCTKG NRI UUOCZ CYUCB
Key : KUNCIKU NCIKU NCI KUNCI KUNCI
PlainText *: SELAMAT MALAM APA KABAR SEHAT*

7) Transposisi Cipher : dalam proses enkripsi ini akan menggunakan transposisi *cipher* horisontal dengan lebar 5 sebagai berikut:
CipherText : SAAKSET MAELM ABH AAPAA MLART
SAAKS
ETMAE
LMABH
AAPAA
MLART

Dibaca secara vertikal, maka akan didapatkan *plain text* sebagai berikut:
PlainText : SELAMAT MALAM APA KABAR SEHAT

C. Perbandingan Efektivitas Metode

Ketiga metode yang digunakan yaitu, substitusi, *vigenere*, dan transposisi *cipher* akan dibandingkan berdasarkan keefektifan yang tolak ukurnya adalah ukuran *file* dan waktu yang dibutuhkan untuk melakukan proses kriptografi pada masing-masing kombinasi metode. Sebagai alat penelitian guna melakukan pengukuran terhadap ukuran *file* dan waktu proses, akan digunakan *software Cryptool*. Dengan menggunakan *software* tersebut didapatkan hasil yang dapat dilihat pada Tabel 5 berikut:

TABLE V

HASIL PENGUKURAN METODE

Kombinasi Metode	Ukuran *File*	Waktu	Proses
Substitusi, *Vigenere*, dan Transposisi	11 Kb	00:01:54	Berhasil
Substitusi dan *Vigenere*	7 Kb	00:01:34	Berhasil
Substitusi dan Transposisi	9 Kb	00:01:41	Berhasil
Vigenere dan Transposisi	9 Kb	00:00:43	Berhasil

Substitusi	5 Kb	00:00:37	Berhasil
Vigenere	5 Kb	00:00:41	Berhasil
Transposisi	6 Kb	00:01:43	Berhasil

V. KESIMPULAN

Dari penelitian yang dilakukan didapatkan hasil bahwa dari tujuh kombinasi metode yang diproses, dinyatakan berhasil dilakukan proses enkripsi dan dekripsi. Dalam perbandingan efektivitas, digunakan dua alat ukur, yaitu ukuran *file* dan waktu proses.

Berdasarkan ukuran *file*, didapatkan hasil untuk ukuran *file* terbesar adalah kombinasi metode Substitusi, *Vigenere*, dan Transposisi dengan ukuran *file* 11 Kb. Sedangkan untuk ukuran *file* terkecil adalah metode Substitusi dan metode *Vigenere* dengan ukuran *file* 5 Kb.

Berdasarkan waktu prosesnya, didapatkan hasil untuk waktu terlama adalah kombinasi metode Substitusi, *Vigenere*, dan Transposisi dengan waktu 1.54 detik. Sedangkan waktu tercepat adalah metode Substitusi dengan waktu 0.37 detik.

Ukuran *file* yang lebih besar dan waktu proses yang terlama, menandakan bahwa kombinasi tiga metode yaitu Substitusi, *Vigenere*, dan Transposisi *Cipher* merupakan kombinasi dengan kompleksitas algoritma yang tinggi dibandingkan dengan kombinasi lainnya yaitu Substitusi *Vigenere*, Substitusi Transposisi, *Vigenere* Transposisi, Substitusi, *Vigenere*, dan Transposisi.

REFERENSI

[1] M.Miftakul Amin. Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. Jurnal Pseudocode, September 2016; Vol.3 No.2 : p.129-136.

[2] I Putu Agus Eka Darma Udayana dan Nyoman Putra Sastra. Perbandingan Performansi Pengamanan File Backup LPSE Menggunakan Algoritma DES dan AES. Teknologi Elektro, Januari-Juni 2016; Vol.15. No.1 : p.111-117.

[3] Hamdani. Perbandingan Metode *Vigenere* dan *Affine* Untuk Pesan Rahasia. Jurnal Informatika Mulawarman, Juli 2012; Vol.7 No.2 : p.70-74.

[4] Fresly Nandar Pabokory, Indah Fitri Astuti, dan Awang Harsa Kridalaksana. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma *Advanced Encryption Standard*. Jurnal Informatika Mulawarman, Februari 2015; Vol.10 No.1 : p.20-31.

[5] Irham Mu'alimin Arrijal, Rusdi Efendi, dan Boko Susilo. Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi *Vigenere Cipher* Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, Februari 2016; Vol.3 No.1 : p.69-82.

[6] Sri Andayani dan Dionysius Spironabel Agista. Kriptografi Klasik Teknik Subsitusi Untuk Keamanan Data Menggunakan Vb.Net 2008. Jurnal Matrix, Juli 2014; Vol.4 No.2 : p.75-80.

[7] Atmaja Basuki, Upik Paranita, dan Restu Hidayat. Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile. Seminar Nasional Teknologi Informasi dan Multimedia, 2016; p.1.2-31 – 1.2-35.

[8] Akim Manaor Hara Pardede dan Yani Maulita. Perancangan Perangkat Lunak Enkripsi Dan Deskripsi File Dengan Metode Transposisi Kolom. Jurnal Kaputama, Juli 2014; Vol.8 No.1 : p.28-35.

[9] Gede Angga Pradipta. Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting. Jurnal Sistem dan Informatika, Mei 2016; Vol.10 No.2 : p.119-127.

[10] I Wayan Manik Suhartanta dan Nyoman Putra Sastra. Survey Tingkat Penggunaan *Single Sign On* pada 500 Situs Peringkat Teratas Alexa.com. Teknologi Elektro, Januari-April 2017; Vol.16 No.1 : p.49-52.