ISSN : 2548-9704

ALGORITMA VIGENERE CIPHER DAN HILL CIPHER DALAM APLIKASI KEAMANAN DATA PADA FILE DOKUMEN

Akim Manaor Hara Pardede[1], Hotler Manurung [2], Dina Filina [3]

[1, 2, 3]*Program Studi Sistem Informasi, STMIK KAPUTAMA*
Jl. Veteran 4A-9A,Binjai
[*]*akimmhp@live.com*

Abstrak

Perkembangan kriptografi terus berlanjut walaupun algoritma yang terkemuka dan dinilai kompleks sudah mulai bisa dipecahkan. Algoritma- algoritma kriptografi klasik seperti *Hill Cipher* dan *Vigenere Cipher* pin memiliki kelemahan akan kriptanalisis. Algoritma *hill cipher* dan *vigenere cipher* merupakan salah satu metode dari beberapa metode yang digunakan untuk melakukan kerahasian data, *hill cipher* adalah algoritma keamanan data menggunakan perhitungan perkalian matriks, sedangkan *vigenere cipher* adalah algoritma yang melakukan enkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. Jika kedua algoritma diatas dikombinasikan dalam sebuah aplikasi keamanan data, maka akan lebih sulit memecahkan sandinya bila dibandingkan dengan hanya menggunakan satu algoritma saja. Penggabungan antara dua algoritma tersebut menjadi sebuah solusi untuk memperkuat algoritma menjadi lebih sulit untuk dapat dipecahkan dan untuk mengecoh kriptanalisis. Filet eks yang telah diamankan menggunakan Algoritma *Vigenere Cipher* akan diamankan lagi menggunakan Algoritma *Hill Cipher.* Implementasi sistem menggunakan perangkat lunak Visual Basic.Net 2010. Hasil dari sistem ini berupa file yang ter-enkripsi (*cipherfile*) yang tidak bisa dimengerti. Kemudian fileteks kembali normal setelah di-dekripsi.

Kata kunci: *Hill Cipher*, Kriptografi, *Vigenere Cipher*, *Visual Basic.Net 2010*

1. PENDAHULUAN

1.1 Latarbelakang

Dalam sistem keamanan data dikenal sebuah metode enkripsi yang mempunyai kode-kode pengamanan untuk mengacak data dan juga mempunyai kode- kode untuk mengembalikan data yang teracak ke data yang sebenarnya. Enkripsi bisa diartikan dengan chiper atau kode, dimana pesan asli (*plaintext*) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan. Aplikasi-aplikasi keamanan data sudah banyak diterapkan dan digunakan dalam kehidupan sehari-hari, khususnya pada aplikasi *smartphone* android yang pada saat ini menjadi kebutuhan primer bagi kita semua.

Penelitian yang dilakukan oleh F. Wiwiek Nurwiyati dan Indra Yatini B (Oktober 2013) dengan judul "Enkripsi Dekripsi Data Menggunakan Metode *Stream* Dan *Vigenere Cipher*". Dengan hasil sebagai berikut: Teknik kriptografi enkripsi dekripsi dengan menggunakan metode *Stream* dan *Vigenere Cipher* dapat melindungi data dimana program akan melakukan proses enkripsi dan deskripsi menggunakan dua kunci yang berbeda satu kunci dibangkitkan dengan karakter *plain text* dan satu lagi di inputkan secara manual.

Algoritma enkripsi akan memberikan hasil yang berbeda tergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah *output* (keluaran) dari algoritma enkripsi. Setelah itu ciphertext kemudian ditransmisikan oleh pengirim. Kemudian akan dilakukan proses dekripsi, yaitu sebuah proses untuk mengembalikan teks yang telah acak menjadi kebentuk semula dengan algoritma dan kunci yang sama. Dalam hal ini dilakukan oleh penerima, sehingga akan kembali menjadi sebuah informasi yang dapat dipahami oleh penerima.

ISSN : 2548-9704

Algoritma *hill cipher* dan *vigenere cipher* merupakan salah satu metode dari beberapa metode yang digunakan untuk melakukan kerahasian data, *hill cipher* adalah algoritma keamanan data menggunakan perhitungan perkalian matriks, sedangkan *vigenere cipher* adalah algoritma yang melakukan enkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. Jika kedua algoritma diatas dikombinasikan dalam sebuah aplikasi keamanan data, maka akan lebih sulit memecahkan sandinya bila dibandingkan dengan hanya menggunakan satu algoritma saja.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada diatas, maka penulisan merumuskan masalah sebagai berikut :

1. Dengan menggunakan Algoritma Vigenere Cipher dan Algoritma Hill Cipher, bagaimana merancang keamanan data file teks agar data tersebut tidak mudah dipecahkan.
2. Merancang keamanan data file teks dengan mengkombinasikan Algoritma Vigenere Cipher dan Algoritma Hill Cipher.

1.3 Tujuan Penelitian

Tujuan penelitian ini antara adalah :

1. Merancang keamanan data file teks menggunakan algoritma Vigenere Cipher dan Hill Cipher.
2. Menghasilkan suatu sistem yang mampu melindungi data dan merahasiakannya dengan menggunakan algoritma Vigenere Cipher dan Hill Cipher.

2. LANDASAN TEORI

2.1 Algoritma Vigenere Cipher

Menurut Sadikin (2012, h. 48) sandi vigenere merupakan sistem sandi poli-alfabetik yang sederhana, sistem sandi poli-alfabetik mengenkripsikan sekaligus sebuah teks yang terdiri dari beberapa huruf. Sandi vigenere menggunakan subtitusi dengan fungsi *shift*.

Sedangkan menurut Ariyus (2006, h. 33) pada teknik subtitusi vigenere setiap *ciphertext* bisa memiliki banyak kemungkinan *plaintextnya*. Teknik ini bisa dilakukan oleh dua cara yaitu : angka dan huruf.

Cipher ini hanya bergantung pada metodologi *confusion* untuk membuat cipher text. Pola berulang pada *plaintext* tidak melalui difusi, melainkan hanya dikamuflase oleh seri dari pergeseran Caesar cipher. Vigenere cipher dianggap *unbreakable* selama hampir 300 tahun. Tetapi akhirnya metode untuk memecahkannya ditemukan oleh Kasiski dan Kerckhoff. Kedua metode berdasar pada fakta bahwa kuncinya berulang dan pada umumnya bahasa yang digunakan sehari-hari bersifat repetitif. Jika pesan jauh lebih panjang dari kunci, pada akhirnya kunci akan mengenkripsi satu kumpulan huruf yang sama yang sebelumnya telah digunakan dan dienkripsi oleh kunci yang sama. Hal ini akan menciptakan suatu pola yang berisi kumpulan huruf yang berulang. Dengan mencari frekuensi antara kumpulan huruf yang berulang dan memfaktorkannya, bisa ditemukan panjang kunci. Jika panjang kunci sudah diketahui, kunci akan dengan mudah diketahui dengan menggunakan analisis frekuensi pada setiap kumpulan *Caesar cipher*. Makin panjang kunci, akan makin sulit dan makin panjang proses penemuan kunci. Faktanya, jika kuncinya paling tidak sama panjang dengan panjang *plaintext*, *cipher text* kebal dari serangan tersebut. Cipher
di mana panjang kunci sama dengan panjang pesan disebut *one time pad*.

a. Angka

Teknik subtitusi *vigenere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

Kunci dengan 5 huruf kode jika ditukar dengan angka akan menjadi K = (10, 20,13, 2, 8), dan teks-aslinya " STMIK KAPUTAMA BINJAI".

S	T	M	I	K	K	A	P	U
18	19	12	8	10	10	0	15	20
10	20	13	2	8	10	20	13	2
2	13	0	10	18	20	20	2	22
C	N	A	K	S	U	U	C	W

T	A	M	A	B	I	N	J	A	I
19	0	12	0	1	8	13	9	0	8
8	10	20	13	2	8	10	20	13	2
1	10	6	13	3	16	23	3	13	10
B	K	G	N	D	Q	X	D	N	K

ISSN : 2548-9704

Teks-asli : STMIK KAPUTAMA BINJAI
Kunci : (10, 20, 13, 2, 8)
Teks-kode :
CNAKSUUCWBKGNDQXDNK

b. Huruf

Untuk mengenkripsikan pesan dengan kode *vigenere* digunakan *tabula recta* (disebut juga bujursangkar *vigenere*). Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plainteks*. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*, yang mana jauh pergeseran huruf plainteks ditentukan nilai desimal oleh huruf kunci tersebut (di sini, a = 0, b = 1, c = 2, …, z = 25). Sebagai contoh, huruf kunci c (= 2) menyatakan huruf plainteks digeser sejauh 2 huruf ke kanan (dari susunan alfabetnya).

Bujur sangkar *Vigènere* digunakan untuk memperoleh *cipherteks* dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari pada panjang *plainteks*, maka kunci diulang penggunaannya (sistem periodik). Secara matematis enkripsi dengan kode *Vigenere* bisa dinyatakan sebagai berikut:

Algoritma enkripsi vigenere *cipher* :
Ci = (Pi + Ki) mod 26
Algoritma dekripsi vigenere *cipher* :
Pi = (Ci – Ki) mod 26

Dimana :
Ci = nilai desimal karakter *ciphertext* ke-i
Pi = nilai desimal karakter *plaintext* ke-i
Ki = nilai desimal karakter kunci ke-i

Salah satu kelebihan kode *vigenere* adalah sulitnya melakukan kapitanalisis dengan metode analisis frekuensi karena dua huruf yang sama dalam teks-kode belum tenetu bisa dideskripsikan menjadi dua huruf yang sama dalam teks-asli. Kelemahan utama kode *vigenere* adalah kuncinya yang pendek dan penggunaannya yang berulang-ulang. Jika kriptanalis dapat menentukan panjang kunci saja maka teks-kode dapat diperlakukan seperti rangkaian beberapa kode Kaisar.

2.2 Algoritma *Hill Cipher*

Menurut Sadikin (2012, h. 51) sandi *hill* merupakan sandi *polyalphabet* dengan menggunakan metode subtitusi dengan perhitungan perkalian matriks. Kunci pada sandi *hill* adalah sebuah matriks ***K*** berukuran *n x n* yang digunakan untuk mensubtitusi *n* alphabet sekaligus.

Menurut Ariyus (2008, h. 59) kode *hill* termasuk salah satu kripto polialfabetik, yang berarti setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter. Kode ini ditemukan pada tahun 1929 oleh Lester S. Hill.

Teknik Dasar *Hill Cipher*

Teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K^{-1} sehingga:

Keterangan:
K = Kunci
K^{-1} = Invers Kunci
I = Matriks Identitas

Kunci harus memiliki invers karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi .

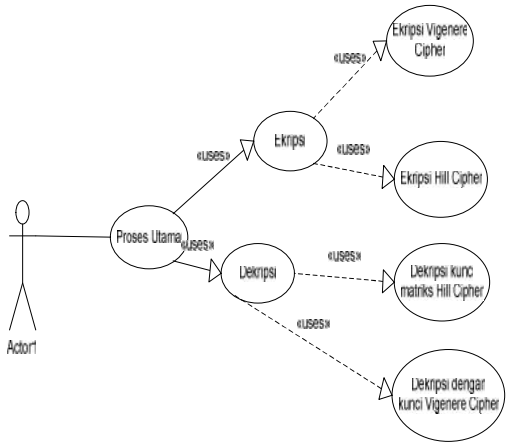
3. PERANCANGAN

3.1 Perancangan UML (*Unified Modelling Language*)

Dalam bagian ini akan dijelaskan untuk mendeskripsikan apa yang harus dilakukan oleh sistem, digambarkan dalam bentuk *use case* yang bertujuan untuk menunjukkan alur kerja dan proses dari sistem aplikasi yang akan dibuat.

Use Case Diagram atau diagram *use case* merupakan pemodelan untuk menggambarkan kelakuan (*behavior*) sistem yang akan dibuat, diagram *use case* mendeskripsikan sebuah interaksi antara satu atau lebih actor dengan sistem yang akan dibuat. Proses yang akan digambarkan akan berlangsung secara terstruktur. Berikut merupakan gambaran *use case* diagram untuk sistem yang akan dibangun pada gambar 3.1 :

ISSN : 2548-9704



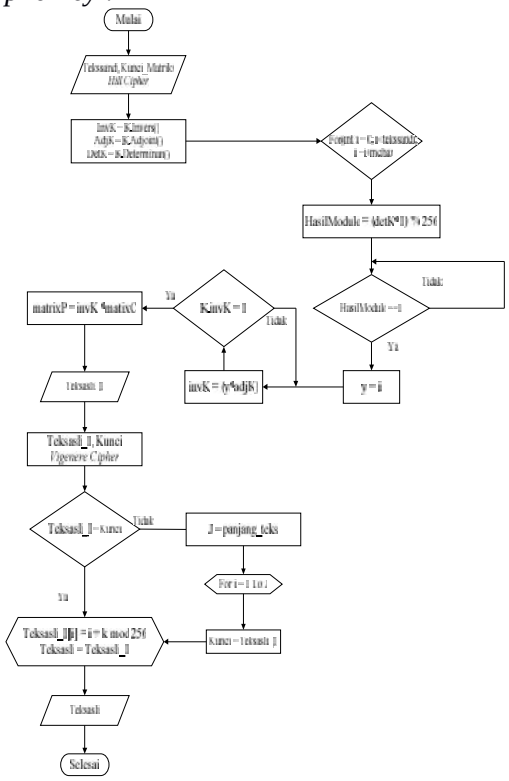
Gambar 3.1. *Use Case Diagram* Sistem

Gambar 1 menyatakan diagram *use case* sistem kriptografi untuk keamanan file teks. *Use Case* ini menjelaskan mengenai bagaimana proses pengenkripsian dan dekripsi menggunakan kedua algoritma *vigenere cipher* dan *hill cipher*, disini sistem menggunakan dua buah kunci yaitu kunci Poli-alfabetik dan kunci matriks. Untuk menyandikan *filetext* yang ingin di jaga kerahasiaannya.

3.2 Perancangan Sistem

Dalam merancang sistem pengamanan *filetext* ini penulis menggunakan algoritma *vigenere cipher* dan algoritma *hill cipher* dalam menyelesaikan masalah. Perancangan sistem ini menggunakan bagan alir *(flowchart)* untuk mengetahui bagaimana proses enkripsi dan dekripsi akan dirancang dalam sistem.

Pada proses dekripsi berikut ini dapat dilakukan, apabila pada proses dekripsi *cipherkey* sebelumnya sudah berhasil, maka dapat dilakukan proses dekripsi *cipherfile*. Dari kunci matriks *hill cipher* yang sudah diinputkan, akan dilakukan proses pencarian matriks *adjoint*, matriks determinan, dan matriks inverse dari determinan kunci matriks, juda inverse dari kunci matriks. Kunci matriks inverse akan dimodulokan dengan jumlah karakter *code ASCII 256*, kemudian setelah diperoleh kunci matriks inverse maka dapat dilakukan proses dekripsi *cipherfile* dengan mengkalikan kunci matriks inverse dengan file yang terenkripsi (*cipherfile*). Berikut merupakan *flowchart* dekripsi *cipherfile* dan *cipherkey :*



Gambar 3.2. *Flowchart* Dekripsi *Filetext Vigenere Cipher* dan *Hill Cipher*

4. HASIL DAN PEMBAHASAN

Dengan menggunakan Algoritma *Hill Cipher* dan Algoritma *Vigenere Cipher*, penulis mengharapkan dapat mengamankan fileteks dengan aman. Serta dapat membantu dalam menyandikan fileteks.

Untuk membuat suatu keputusan perlu diketahui terlebih dahulu kriteria-kriteria yang ada. Dari kriteria-kriteria tersebut kita dapat melakukan proses pengambil keputusan.

Implementasi merupakan kelanjutan dari kegiatan perancangan sistem. Tahap ini merupakan tahap meletakkan sistem supaya siap untuk di operasikan dan dapat dipandang sebagai usaha untuk mewujudkan sistem yang telah di rancang. Langkah-langkah dalam tahap implementasi ini adalah urutan kegiatan awal sampai akhir yang harus dilakukan dalam mewujudkan sistem yang telah di rancang.

ISSN : 2548-9704

Pengujian Proses Enkripsi File Dokumen

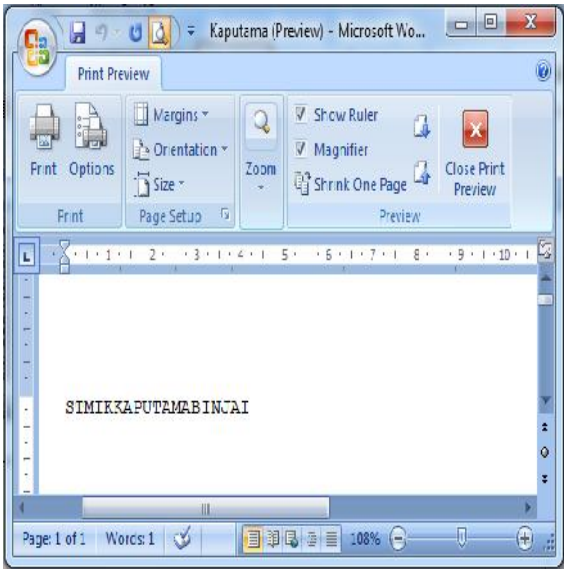
Pada proses ini *form* enkripsi dapat ditampilkan dengan mengklik *button* Enkripsi pada *form* utama setelah program dijalankan. Sebelum dilakukan proses enkripsi terhadap fileteks maka hal yang pertama dilakukan adalah memilih file yang akan dienkripsi melalui *button* "cari"yang terdapat pada *form*.

Gambar 4.1. Seteleh Proses Pemilihan Dokumen

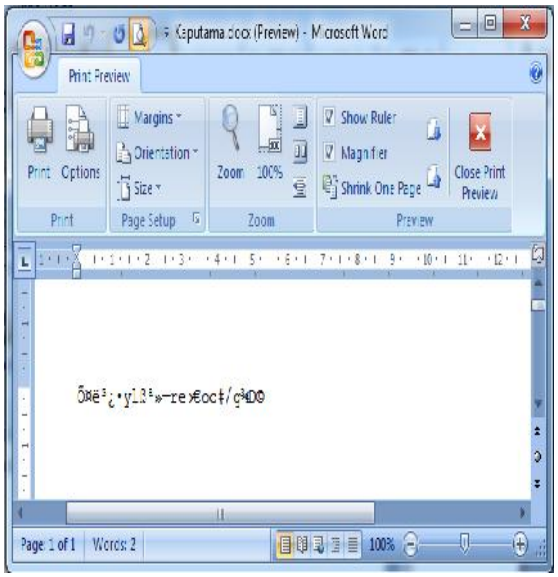
Setelah file sudah dipilih kemudian lanjutkan proses enkripsi dengan mengisi kunci *vigenere cipher* dan setelah itu klik *button* enkripsi, seperti gambar berikut ini :

Gambar 4.2 Proses Enkripsi

Hasil pengujian dapat dilihat dari gambar sebagai berikut :



Gambar 4.3. File *.docx* Sebelum di Enkripsi

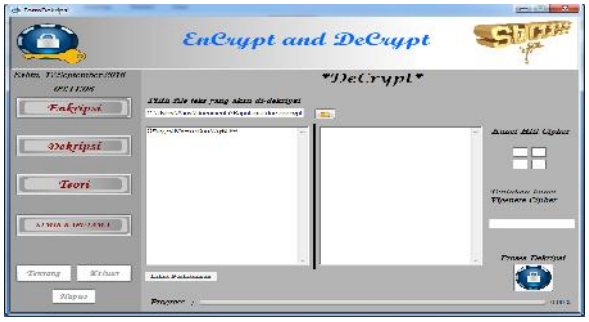


Gambar 4.4. File *.docx* Setelah di Enkripsi

Pengujian Proses Dekripsi File Dokumen

Pada proses ini *form* dekripsi dapat ditampilkan dengan mengklik *button* dekripsi yang terdapat pada *form* utama setelah program dijalankan. Sebelum dilakukan proses dekripsi terhadap file, maka hal yang pertama kali dilakukan adalah memilih file yang akan di-dekripsi dengan mengklik *button* "cari" yang terdapat pada *form* dengan ekstensi file .encrypt.

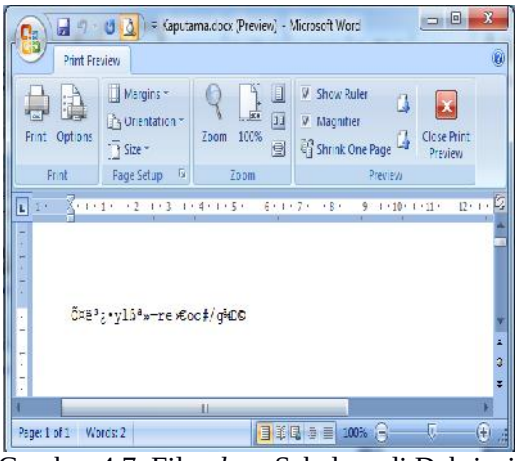
ISSN : 2548-9704



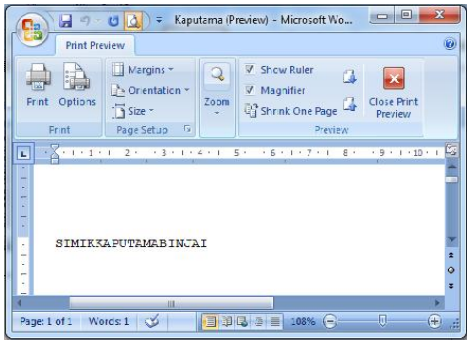
Gambar 4.5. Proses Setelah Pemilihan File Dokumen

Setelah file sudah dipilih, kemudian lanjutkan proses dekripsi dengan menginputkan kunci *vigenere cipher* dan setelah itu klik *button* dekripsi, seperti gambar berikut ini :

Gambar 4.6. Proses Dekripsi



Gambar 4.7. File *.docx* Sebelum di Dekripsi



Gambar 4.8. File *.docx* Setelah di Dekripsi

Tabel 1. Uji Program
(Jumlah Kata yang panjang)

No	Nama File	Jumlah Kata	Kunci	Ket
1	Kriptografi	681 kata	kaputama	Berhasil
2	Visual Basic	136 kata	kita1234	Berhasil
3	Enkripsi	21 kata	kamiiiii	Gagal (karena menggunakan kunci dengan huruf berulang-ulang)
4	Hill Cipher	812 kata	binjai	Gagal (karena jumlah kata yang digunakan melebihi batas maksimal)
5	Vigenere	513 kata	19092016	Berhasil

ISSN : 2548-9704

Tabel 2. Uji Program Proses Enkripsi

No	Plainteks	Kunci	Cipherteks
1	Kaputama Binjai	kamiiiii	Ô¦ëS¯+Œ ç³0 } |b
2	ILOVESTMIKKAPUTAMA BINJAI	kaputama	‹v_Ó¹“ÏŸˆtÉ ö¸«‡~l´’Ëœ d^Ûj Úg¾ D©
3	Teknik Informatika	kamikami	É½6ˆ×’ÝJ ~ÛGtý€:£\¹
4	Sekolah Tinggi Manajemen Informatika dan Komputer	kakakaka	Æž"y ¢{Ñ• x Áýi]úz}µõ’»4~¹1t+i»ù¬*É=-)›s:£:£:£
5	STMIK	16092016	2 ÷{(ñ—Ÿ

Tabel 3. Uji Program Proses Dekripsi

No	Plainteks	Kunci	Cipherteks	Ket
1	Ô¦ëS¯+Œ ç³0} |b	kamiiiii	K©putam© Binj©i	Gagal
2	‹v_Ó¹“ÏŸˆtÉ ö¸«‡~l´’Ëœ d^Ûj Úg¾D©	kaputama	ILOVESTMIKKAPUTAMA BINJAI	Berhasil
3	É½6ˆ×’ÝJ~ÛGtý€:£\¹	kamikami	Teknik Informatika	Berhasil
4	Æž"y ¢{Ñ• x Áýi]úz}µõ’»4~¹1t+i»ù¬*É=-)›s:£:£:£	kakakaka	Sekolah Tinggi Manajemen Informatika dan Komputer	Berhasil
5	2 ÷{(ñ—Ÿ	16092016	STMIK	Berhasil

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan tahap penelitian, perancangan, dan tahap implementasi terhadap pengamanan *file* dengan sistem kriptografi dimana enkripsi *file* dengan menggunakan algoritma *Vigenere Cipher* dan algoritma *Hill Cipher* diperoleh kesimpulan bahwa :

1. Kunci yang digunakan untuk mengenkripsi harus sama dengan kunci yang digunakan untuk melakukan dekripsi. Apabila kunci yang diinputkan tidak sama, maka hasil dari dekripsi tidak akan sama dengan *plainfile* semula seperti sebelum dienkripsi.
2. Algoritma *Vigenere Cipher* dan Algoritma *Hill Cipher* digunakan untuk melindungi *file* berupa *file*, dalam hal ini penulis masih menguji sebatas *file* TXT, DOCX dan XLSX.
3. Hasil dekripsi dari *cipherfile* akan menghasilkan *plainfile* yang sama dengan *plainfile* sebelum dienkripsi.

5.2 Saran

Berdasarkan kesimpulan diatas maka menggemukakan beberapa saran yang diharapkan dapat menjadi masukan bagi kemajuan sistem yang akan datang. Dan

ISSN : 2548-9704

beberapa saran yang akan dikemukakan adalah sebagai berikut :

1. Sistem ini menggunakan Algoritma *Vigenere Cipher* dan Algoritma *Hill Cipher*, kunci dari Algoritma *Hill Cipher* menggunakan matriks berordo 2x2 dan kunci matriks tersebut telah ditetapkan oleh sistem, sehingga untuk pengembangan selanjutnya dapat mengenkripsi dan dekripsi dengan *user* yang menginputkan matriks serta menggunakan matriks berordo 3x3, 4x4 .... nxn.
2. File yang dapat dienkripsi dan dekripsi didalam sistem ini hanya file dengan ekstensi txt, docx dan xlsx. Untuk pengembangannya agar bisa menggunakan file dengan jenis ekstensi lainnya.

UCAPAN TERIMA KASIH

Kami menyampaikan terima kasih yang sebesar-besarnya kepada Ketua Yayasan Pendidikan Teknologi Informasi Mutiara atas dukungan dana berupa hibah penelitian bagi dosen STMIK KAPUTAMA tahun anggaran 2016. Kami juga mengucapkan terimakasih kepada mitra Ketua STMIK KAPUTAMA dan Ketua LPPM STMIK KAPUTAMA, yang telah melakukan arahan dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] Ariyus, 2008. *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Andi, Yogyakarta.

[2] Ariyus, 2006. *Kriptografi Keamanan Data dan Komunikasi*. Andi, Yogyakarta.

[3] Sadikin, 2012. *Kriptografi untuk Keamanan Jaringan*. Andi , Yogyakarta.

[4] Sugiarti, 2013. *Analisis dan Perancangan UML Generated VB.06*. Graha Ilmu, Yogyakarta.

[5] Yatini B, 2010. *Flowchart, Algoritma, dan Pemrograman menggunakan Bahasa C++ Builder*. Graha Ilmu ,Yogyakarta.