Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) p-ISSN: 1693-9166
Vol. 19, No. 1, April 2022, hlm. 37-47 e-ISSN: 2685-127X

SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER

Lekso Budi Handoko[1*], Abdussalam[2]

[1,2] Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Email: [1]handoko@dsn.dinus.ac.id, [2]grey.salam@dsn.dinus.ac.id

(Naskah masuk: 18 Maret 2022, diterima untuk diterbitkan: 3 April 2022)

Abstrak

Keamanan data dalam sistem merupakan problem yang hingga saat ini membuat peneliti terus mengembangkan keilmuan. Kriptografi sebagai salah satu teknik keamanan data, khususnya pada data teks melalui implementasi kriptografi klasik. Pada penelitian ini telah diimplementasikan kombinasi *vigenere* dan *hill cipher*. Kedua algoritma merupakan algoritma yang mudah dalam implementasi, namun masing-masing memiliki kekurangan. Vigenere mudah di *brute force*, sedangkan *hill cipher* pada proses dekripsi harus menggunakan kunci yang dapat dibalik sehingga tidak semua kunci cocok untuk digunakan. Kombinasi *Vigenere* dan *hill cipher* telah diimplementasikan dan di uji coba menggunakan *black box testing* serta perhitungan *Avalanche Effect*. Pengujian menggunakan *Avalanche Effect* menghasilkan nilai rata-rata 52,46%.

Kata kunci: *Kriptografi, Vigenere Cipher, Hill Cipher, Teks*

TEXT SECURITY USING VIGENERE CIPHER AND HILL CIPHER

Abstract

Data security in the system is a problem that until now has made researchers continue to develop science. Cryptography as a data security technique, especially in text data through the implementation of classical cryptography. In this research, a combination of vigenere and hill cipher has been implemented. Both algorithms are algorithms that are easy to implement, but each has its drawbacks. Vigenere is easy to brute force, while hill cipher in the decryption process must use a reversible key so that not all keys are suitable for use. The combination of Vigenere and hill cipher has been implemented and tested using black box testing and the calculation of the Avalanche Effect. Tests using the Avalanche Effect resulted in an average value of 52,46%.

Keywords*: Cryptography, Vigenere Cipher, Hill Cipher, Text*

1. PENDAHULUAN

Seiring perkembangan teknologi komputer saat ini, informasi sudah menjadi suatu kebutuhan dikarenakan perkembangan yang pesat, maka dari itu banyak pekerjaan dapat terselesaikan dengan cepat, akurat, dan efisiensi sehingga semakin mengubah cara masyarakat dalam berkomunikasi. kemajuan perkembangan teknologi saat ini mempunyai dampak positif seperti komunikasi dan pertukaran informasi semakin terbuka dan cepat dengan adanya internet, akan tetapi memiliki dampak negatifnya seperti adanya penyadapan data, yang merupakan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi [1]. Dengan adanya kasus penyadapan data maka menjadi salah satu aspek yang terpengaruh adalah pada aspek keamanan. Tidak dapat dipungkiri bahwa penggunaan internet semakin menjadi hal yang wajib di kehidupan sehari-hari. Dengan maraknya penggunaan internet, keamanan bagi para pengguna internet juga semakin rentan.

Dengan adanya kasus tersebut maka dapat melakukan upaya pencegahan terjadinya serangan sadapan dalam isi file tersebut karena akan dapat sangat mudah untuk diketahui oleh pihak lain yang tidak berkepentingan terhadap file tersebut. keamanan data adalah perlindungan data didalam suatu sistem melawan terhadap kerusakan dan perlindungan sistem komputer terhadap pengguna yang tidak berhak memiliki informasi [2], [3]. Sedangkan, keamanan sistem adalah keamanan pada sistem pengoperasiannya pada lingkup perangkat lunak misalnya dengan menggunakan kriptografi [4], [5]. Maka dari itu, dalam menjaga keamanan data informasi dilakukan tidak hanya pada satu teknik keamanan saja, melainkan bisa dilakukan dengan kombinasi dalam keamanan data informasi. Salah

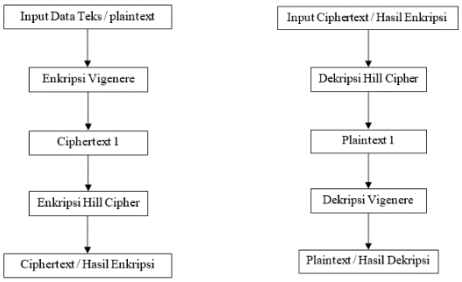
satu contoh data teks yang ada pada bidang teknologi informasi yaitu file ekstensi (.doc, .pdf, .txt, dan .ppt). File tersebut memiliki sekumpulan instruksi yang ditulis dengan bahasa pemrograman Java, PHP, HTML, C++, dan lain sebagainya yang digunakan sebagai instruksi untuk komputer dalam melakukan suatu proses. File ekstensi sangat rentan terhadapan pencurian oleh pihak yang tidak bertanggung jawab, karena itu diperlukan sistem keamanan untuk menghindari file ekstensi tersebut dibaca oleh pihak lain.

Seiring berjalanya waktu, teknik menyembunyikan pesan ini berkembang menjadi sebuah bidang kajian ilmu yang disebut dengan kriptografi. Kriptografi merupakan salah satu cara yang digunakan untuk mengamankan data dalam bentuk file dengan mengenkripsi file sehingga orang lain tidak berhak mengetahui file yang sifatnya pribadi dan rahasia. Kriptografi dikenal menjadi kriptografi klasik dan kriptografi modern [6]. Konsep kriptografi klasik mempunyai prinsip membolak balik kata sehingga tidak mudah untuk ditebak. Sedangkan kriptografi modern memiliki prinsip mengubah karakter menjadi biner untuk di modifikasi agar tidak mudah ditebak. Kriptografi ada 2 teknik yaitu proses enkripsi dan dekripsi. Enkripsi yaitu proses mengubah pesan asli (plainteks) menjadi pesan yang telah disandikan (chiperteks). Berbanding terbalik dengan enkripsi, dekripsi berfungsi untuk mengubah pesan yang telah disandikan (chiperteks) menjadi pesan yang asli (plainteks). Ada banyak metode dalam kriptografi. Pada kriptografi klasik [7]–[9] mengenal algoritma *vigenere cipher*, *autokey cipher*, super enkripsi, dan lain sebagainya. Sedangkan kriptografi modern mengenal algoritma DES, AES, A5, RC4, ECB, CBC, dan lain sebagainya.

Pada penelitian ini, telah diimplementasikan super enkripsi dengan menggabungkan dua algoritma yaitu algoritma *Vigenere Cipher* dan *Hill Cipher* yang diketahui masuk ke dalam jenis kriptografi klasik. Hal ini dilakukan untuk menghasilkan pengamanan file yang lebih baik. Alasan memilih teknik super enkripsi karena teknik super enkripsi sangat mewakili kriptografi klasik dimana inti dari kriptografi klasik adalah subtitusi dan transposisi sebagai pembentuk super enkripsi. Sedangkan pada implementasi algoritma *Vigenere Cipher* terlihat bahwa terdapat perulangan kata pada hasil enkripsi dengan peluang terbesar informasi dapat diprediksi sebesar 74,07 %. Maka, akan ditambahkan algoritma *Hill Cipher* karena *Hill cipher* adalah algoritma kriptografi klasik yang sangat kuat dari segi keamanannya dan perhitungan dalam *Hill Cipher* cukup rumit jika dihitung secara manual untuk teks yang panjang agar tidak terjadi perulangan kata pada enkripsi data teks.

2. METODE PENELITIAN

2.1 Skema Enkripsi dan Dekripsi



a. Alur Enkripsi *b. Alur Dekripsi*

Gambar 1. Alur Enkripsi dan Dekripsi

Dalam penelitian ini secara garis besar, metode yang diusulkan adalah data berupa teks yang akan diproses dalam pembentukan enkripsi dan dekripsi dengan menggunakan *Vigenere Cipher* dan *Hill Cipher* seperti pada Gambar 1. Berdasarkan Gambar 1 point a, enkripsi *Vigenere* dan *Hill Cipher* adalah sebagai berikut :

1. Input Data Teks/Plaintext. Proses awal adalah melakukan input data berupa data teks (*plaintext*). Data teks ini nantinya akan diproses pada bagian selanjutnya enkripsi *Vigenere* setelah input dilakukan.
2. Enkripsi *Vigenere*. Memasukkan proses enkripsi *Vigenere*, semua huruf yang ada pada data teks akan di enkripsi menggunakan *Vigenere Cipher*.
3. *Ciphertext* 1. Pada *Ciphertext* 1 ini, huruf – huruf pada data teks berubah yang sudah menjalani proses enkripsi *Vigenere Cipher*.
4. Enkripsi *Hill Cipher*. Kemudian pada tahap ini, dari *Ciphertext* 1 yaitu hasil enkripsi *Vigenere* akan di enkripsi kembali menggunakan *Hill Cipher*.
5. *Ciphertext* / Hasil Enkripsi. *Hasil chipertext* akan berhasil ketika proses enkripsi *Hill Cipher* sudah berjalan dengan baik.

Berdasarkan Gambar 1 point b, penjelasan dari dekripsi *Vigenere* dan *Hill Cipher* adalah sebagai berikut :

1. Input *Ciphertext*. Proses awal adalah melakukan input data teks (*chipertext*) yang sudah di enkripsi sebelumnya. Data teks ini nantinya akan di proses pada bagian selanjutnya di dekripsi *Hill Cipher* setelah input dilakukan.
2. Dekripsi *Hill Cipher*. Memasukkan proses dekripsi *Hill Cipher*, semua huruf yang ada pada data *chipertext* akan di dekripsi menggunakan *Hill Cipher*.
3. *Plaintext* 1. Pada *Plaintext* 1 ini, huruf – huruf pada data teks berubah yang sudah menjalani proses dekripsi *Hill Cipher*.
4. Dekripsi *Vigenere*. Kemudian pada tahap ini, dari Plaintext 1 yaitu hasil dekripsi *Hill Cipher* akan di dekripsi kembali menggunakan *Vigenere*.

5. *Plaintext*/Hasil Dekripsi. Hasil *plaintext* akan berhasil ketika proses dekripsi *Vigenere* sudah berjalan dengan baik.

2.2 Pengujian Hasil

Dalam sebuah penelitian diperlukannya uji analisis untuk mengetahui object yang kita analisis sesuai atau tidak. Dan tujuan dari diadakannya analisa ini untuk melihat setiap progres penelitian kita. Untuk pengujiannya, proses enkripsi ini menggunakan metode yang sudah diusulkan yaitu Algoritma *Vigenere Cipher* dan *Hill Cipher*. Pengujian *Black Box Testing* sering digunakan dalam pengembangan aplikasi, gunanya sebagai menguji kualitas fungsional dari program atau perangkat lunak yang dirancang. *Black Box Testing* dapat mencari tahu kesalahan dalam beberapa kategori pada perangkat lunak, misalnya: Perilaku atau kinerja perangkat lunak; Fungsi atau kesalahan pada perangkat lunak; Kesalahan pada UI/UX; Akses Eksternal dan lain-lain. Dalam kasus pengujian perangkat lunak atau software, *Black Box Testing* bukanlah sebuah solusi alternatif sebagai pengganti dari *White Box Testing* tetapi merupakan sebuah pelengkap untuk melakukan pengujian antara fungsionalitas pada perangkat lunak dan alur logika pada perangkat lunak. Dalam sebuah penelitian diperlukannya uji analisis untuk mengetahui object yang kita analisis sesuai atau tidak. Untuk pengujiannya, telah digunakan *BlackBox Testing* karena dapat mengetahui apakah object yang kita inginkan itu sesuai dan berjalan dengan apa yang kita inginkan.

2.3 Landasan Teori

a. Penelitian Terkait

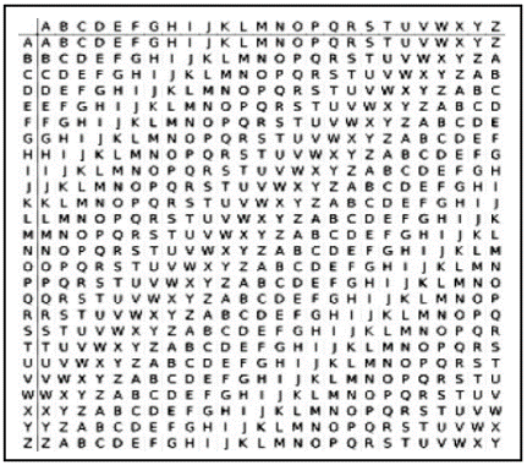
Hasil dari pencarian jurnal terkait dengan penerapan Algoritma Kriptografi *Vigenere* dan *Hill Cipher* banyak digunakan diberbagai bidang penelitian. Sebagai referensi atau rujukan dalam penelitian yang dibuat menggunakan Algoritma *Vigenere* dan *Hill Cipher* untuk ekstraksi *character texts* maka rujukan atau referensi penelitian ini bertujuan pada beberapa artikel di bawah ini. Menurut penelitian yang dilakukan oleh [10], [11], *vigenere cipher* merupakan salah satu contoh kriptografi kunci simetris dengan tingkatan keamanan kunci yang lebih susah dipecahkan. Perihal ini diakibatkan algoritma dari *vigenere cipher* adalah wujud sederhana dari substitusi polialfabetik dengan kunci enkripsi berbentuk huruf. Menurut penelitian yang dilakukan [12], penggunaan metode kriptografi *vigenere* pada kombinasi dua metode ini diharapkan dapat dijadikan sebagai salah satu solusi dalam pengoptimalan pengaman data khususnya data yang sifatnya rahasia, dengan melakukan mengenkripsi data terlebih dahulu berdasarkan algoritma *vigenere cipher*, kemudian *cipher vigenere* enkripsi kembali. Menurut penelitian yang dilakukan oleh Menurut penelitian yang dilakukan oleh [13], menyimpulkan pada penelitian nya Ketepatan enkripsi dan dekripsi ini berlaku pada semua tipe teks dengan kunci yang berbeda-beda, namun jika pada teks terdapat karakter yang berada di luar batasan karakter yang digunakan maka karakter tersebut tidak dapat diproses. Karakter yang dipakai yaitu ASCII dengan nomor *index* antara 32 sampai 125 (total 94). Menurut penelitian yang dilakukan oleh [14], dengan menggunakan metode *hill cipher* yang dapat dikategorikan sebagai *block cipher* karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula. Menurut penelitian yang dilakukan oleh [15], penggunaan metode *hill cipher* termasuk algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Karena *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi, karena dasar yg digunakan matriks *Hill Cipher* antara lain adalah perkalian antara matriks dan melakukan *invers* pada matriks.

b. Kriptografi

Kriptografi adalah seni dengan teknik penyembunyian pesan yang dapat merubah setiap pesan asli menjadi kode yang tidak dapat dibaca secara benar [16]. Dengan menggunakan teknik kriptografi, maka pesan yang disampaikan akan berubah menjadi pesan berkode. Dengan penyembunyian pesan ini, maka setiap isi dari pesan yang akan disampaikan kepada seseorang menjadi lebih aman dan tidak dapat diubah ataupun tidak dapat bocor ke orang lain. Untuk dapat menggunakan teknik penyembunyian pesan ini, dapat dilakukan dengan mempelajari jenis dari metode kriptografi sendiri dan diantaranya yaitu Klasik, Simetri, Asimetri dan *Hybrid*. Kriptografi klasik memiliki beberapa bentuk penyandian, diantaranya yaitu ada *Caesar Cipher*. *Vigenere Cipher*, *Playfair Cipher*, *Affine Cipher, Hill Cipher*, *Enigma Cipher* dan *One-Time Pad*. Dan untuk penelitian ini, telah diterapkan *Vigenere Cipher* dan *Hill Cipher* sebagai objeknya.

c. *Vigenere Chiper*

Pada penyandian *vigenere chiper*, setiap huruf *plaintext* di acak dengan huruf lain yang mana memiliki perbedaan pada urutan alfabet. Dalam menyandikan pesan atau istilahnya enkripsi, maka diperlukanlah sebuah tabel, dimana tabel ini membantu dalam menyandikan dan memecah sandi pada *vigenere* yang nantinya dapat dibaca kembali [14][17].



Gambar 1. Tabula Recta pada Algoritma Vigenere Cipher

Tidak hanya dengan menggunakan tabel, penyandian *vigenere* juga dapat dituliskan secara matematis dengan menggunakan operasi penjumlahan sebagai enkripsinya dengan operasi modulus dan operasi pengurangan sebagai dekripsinya dengan operasi modulus juga. Rumus matematis dari enkripsi dan dekripsi vigenere diilustrasikan pada persamaan (1) sampai persaman (2). Dimana Ci : Nilai Desimal Karakter *Chipertext* Ke i, Pi : Nilai Desimal Karakter *Plaintext* Ke i, Ki : Nilai Desimal Karakter *Key* Ke i, i : Nilai iterasi untuk melakukan perulangan, Mod : Sisa Hasil Bagi.

Enkripsi → Ci = (Pi + Ki) mod 26
Jika hasil penjumlahan Pi dan Ki lebih kecil dari 26
Ci = (Pi + Ki) – 26 ……(1)

Dekripsi → Pi = (Ci – Ki) mod 26
Jika hasil pengurangan Pi dan Ki kurang dari 26
Pi = (Ci - Ki) + 26……(2)

d. Hill Cipher

Hill cipher adalah teknik cipher block simetris yang diinovasi oleh ahli matematika Lester Hill pada tahun 1929. Baik pengirim dan penerima harus berbagi dan menggunakan matriks kunci yang sama untuk penyandian dan penguraian. Algoritma *Hill Cipher* menggunakan matriks berukuran *m x m* sebagai kunci untuk enkripsi dan dekripsi. Block cipher tipikal ini yang bergantung terutama pada invers aritmatika modular dari matriks kunci sangat kuat terhadap serangan *brute force*, memiliki ketahanan terhadap analisis frekuensi, kecepatan tinggi dan *throughput* tinggi, dan sulit dipecahkan dengan *ciphertext*-hanya menyerang, tetapi mudah dipatahkan dengan serangan plaintext yang diketahui, dengan asumsi musuh telah memperoleh beberapa pasangan *plaintext* dan *ciphertext* [15]. Kemunduran lain adalah bahwa matriks kunci yang dapat dibalik diperlukan untuk dekripsi, jika matriks kunci enkripsi tidak dipilih dengan benar, pembangkitan matriks kunci dekripsi yaitu kebalikan dari matriks enkripsi tidak dimungkinkan [16]. Dengan demikian perlu adanya kombinasi dengan algoritma lain dengan tujuan optimasi keamanan. Untuk enkripsi, algoritma mengambil *m* huruf plainteks berturut-turut dan sebagai gantinya menggantikan *m* huruf sandi. Di Hill cipher, setiap karakter diberi nilai numerik seperti a = ,0 b = ,..,1 z = 25. Perhitungan hill cipher seperti pada persamaan (3) dan (4), dimana Ci : Nilai Desimal Karakter Chipertext Ke-i, Pi : Nilai Desimal Karakter Plaintext Ke-i, Ki : Nilai Desimal Karakter Key Ke-i, i : Nilai iterasi untuk melakukan perulangan, Mod : Sisa Hasil Bagi.

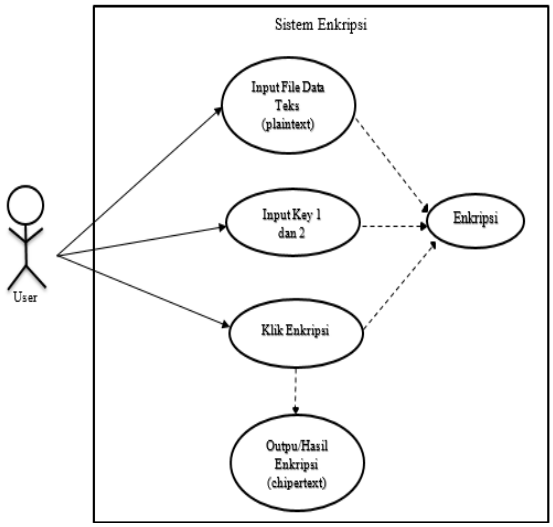
Enkripsi Ci = Ki . Pi mod 26……...(3)
Dekripsi Pi = Ki^{-1}. Ci mod 26……(4)

3. HASIL DAN PEMBAHASAN

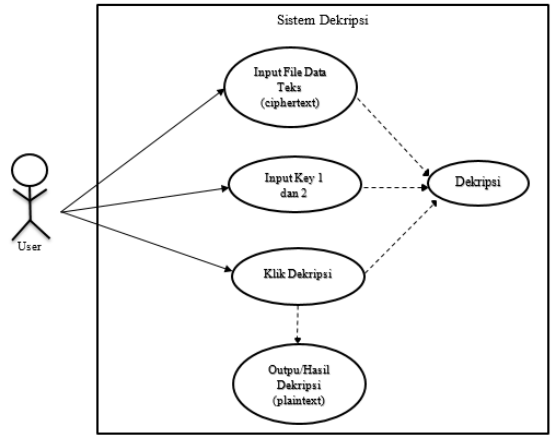
3.1 Perancangan Sistem

a. *Use Case* Diagram

Use Case merupakan penggambaran suatu interaksi antara Sistem Aplikasi Kriptografi dengan pengguna atau user yang akan menggunakan aplikasi tersebut. Penggambaran diagram *Use Case* pada aplikasi kriptografi seperti pada Gambar 2.



Gambar 2. Use Case Enkripsi



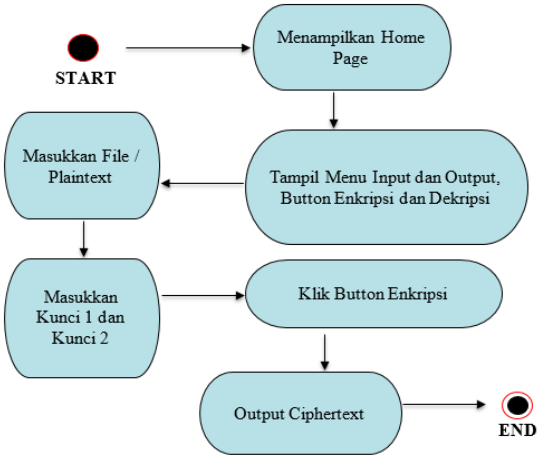
Gambar 3. Use Case Dekripsi

Use Case enkripsi diatas terdapat satu aktor yang diberi nama *User*. Untuk mengoperasikan aplikasi ini hanya butuh satu *user*. Sistem akan melakukan enkripsi text pada *plaintext* yang sudah di input, ketika proses enkripsi selesai maka output berupa *chipertext* akan muncul. Seperti halnya pada use case enkripsi, terdapat satu aktor yang diberi nama *User*. Dan mengoperasikan aplikasi ini hanya butuh satu *user*. Sistem akan melakukan proses dekripsi text pada *ciphertext* yang sudah di input, ketika proses dekripsi selesai maka output berupa *plaintext* akan muncul dan hasilnya kembali lagi pada data teks awal / data aslinya (*plaintext*)

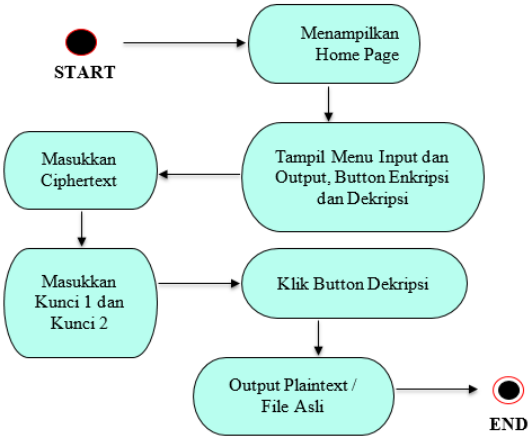
b. *Activity* Diagram

Activity Diagram akan menjelaskan rangkaian aktivitas pada sistem aplikasi Kriptografi yang dilakukan oleh pengguna ketika berada melakukan proses proses yang terjadi pada system. Diagram aktivitas pada sistem aplikasi yang digambar berdasarkan scenario pada *Use Case* sesuai pada Gambar 4. Gambar 4 merupakan alur dari pengguna dan sistem dalam melakukan fungsi utama enkripsi file. Ketika program berjalan, hal yang pertama tampil adalah *Home Page* atau Halaman Awal dari program. Pada halaman awal terdapat beberapa fitur yang bisa digunakan secara langsung oleh user yaitu terdapat Menu Input untuk input file *plaintext* dan Output untuk hasil dari Enkripsi atau Dekripsi. Ada pula untuk kolom input Kunci, input ini berfungsi untuk memberikan kunci dari *vigenere cipher* dan *hill cipher*, karena penyandian *vigenere cipher* dan *hill cipher* sendiri menggunakan kunci untuk enkripsi dan dekripsi. Disaat halaman awal sudah tampil, maka program dapat dijalankan dengan memasukan file *plaintext* / file asli pada kolom yang sudah disediakan dan setelah itu barulah dapat memasukan kunci untuk mengenkripsi *plaintext*. Ketika sudah memasukan *plaintext* dan kunci, maka tahapan selanjutnya dari *Activity* Diagram ini adalah Klik *Button* Enkripsi maka hasilnya akan keluar.

Gambar 5 merupakan alur dari pengguna dan sistem dalam melakukan fungsi utama dekripsi file. Ketika program berjalan, hal yang pertama tampil adalah *Home Page* atau Halaman Awal dari program. Pada halaman awal terdapat beberapa fitur yang bisa digunakan secara langsung oleh user yaitu terdapat Menu Input untuk input file plaintext dan Output untuk hasil dari Enkripsi atau Dekripsi. Ada pula untuk kolom input Kunci, input ini berfungsi untuk memberikan kunci dari vigenere cipher dan hill cipher, karena penyandian vigenere cipher dan hill cipher sendiri menggunakan kunci untuk enkripsi dan dekripsi. Di saat halaman awal sudah tampil, maka program dapat dijalankan dengan memasukan file ciphertext / file yang sudah terenkripsi pada kolom yang sudah disediakan dan setelah itu barulah dapat memasukan kunci untuk mengenkripsi ciphertext. Ketika sudah memasukan ciphertext dan kunci, maka tahapan selanjutnya dari *Activity* Diagram ini adalah Klik *Button* Dekripsi maka hasilnya akan keluar.



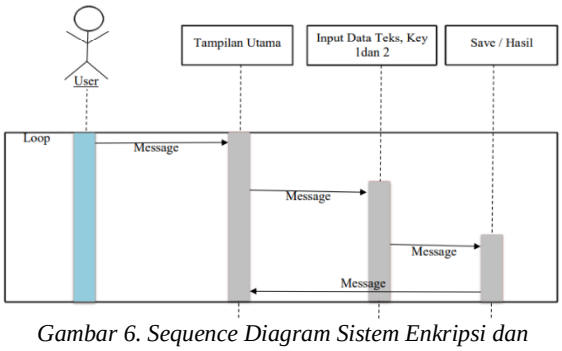
Gambar 4. Activity Diagram Sistem Enkripsi



Gambar 5. Activity Diagram Sistem Dekripsi

c. *Sequence* Diagram

Sequence Diagram merupakan penggambaran detail interaksi yang terjadi antara tiap komponen yang ada dalam sistem dalam urutan waktu. Pada penelitian ini peneliti menggambarkan Sequential Diagram seperti pada Gambar 6. Pada Gambar 6, interaksi yang terjadi pada aplikasi enkripsi dan deskripsi data teks. Untuk bisa menyimpan data teks harus menginputkan data teks terlebih dahulu, data teks akan tersimpan pada direktori komputer itu sendiri.



Gambar 6. Sequence Diagram Sistem Enkripsi dan Dekripsi

3.2 Perhitungan Manual Enkripsi

Tahapan enkripsi diawali dengan pengguna menginputkan file berupa data teks (*plaintext*), kunci 1 dan kunci 2, dimana kunci 1 menjadi *key* untuk algoritma *vigenere cipher* dan kunci 2 akan menjadi key untuk algoritma *hill cipher*. Dalam file tersebut berisikan huruf yang masih dapat dibaca oleh siapapun yang nantinya huruf - huruf tersebut akan di konversikan menjadi huruf ASCII, kemudian dienkripsi menggunakan algoritma *vigenere cipher* dan *hill cipher*. Sebagai contoh pengguna menginputkan kunci kunci seperti di bawah ini.

Plaintext=
MAHASISWAUNIVERSITASDIANNUSWANTORO

Kunci 1 = sukses →*Key vigenere cipher*
Kunci 2 = [5 6 2 3] →*Key* 2 *hill cipher*

Proses pertama *plaintext* atau file yang sudah dirubah menggunakan ASII kemudian dimasukkan kedalam rumus enkripsi. Huruf berwarna merah merupakan pengulangan kunci sesuai panjang *plaintext*. Maka perhitungannya akan menjadi seperti berikut.

Plaintext=
MAHASISWAUNIVERSITASDIANNUSWANTORO

Key= suksessuksessuksessuksessuksessuks

Tabel 1. Perhitungan Enkripsi Vigenere

M	+	s	=	77	+	115	=	160	mod	128	=	64	=	@
A	+	u	=	65	+	117	=	150	mod	128	=	54	=	6
H	+	k	=	72	+	107	=	147	mod	128	=	51	=	3
A	+	s	=	65	+	115	=	148	mod	128	=	52	=	4
S	+	e	=	83	+	101	=	152	mod	128	=	56	=	8
I	+	s	=	73	+	115	=	156	mod	128	=	60	=	<
S	+	s	=	83	+	115	=	166	mod	128	=	70	=	F
W	+	u	=	87	+	117	=	172	mod	128	=	76	=	L
A	+	k	=	65	+	107	=	140	mod	128	=	44	=	,
U	+	s	=	85	+	115	=	168	mod	128	=	72	=	H
N	+	e	=	78	+	101	=	147	mod	128	=	51	=	3
I	+	s	=	73	+	115	=	156	mod	128	=	60	=	<
V	+	s	=	86	+	115	=	169	mod	128	=	73	=	I
E	+	u	=	69	+	117	=	154	mod	128	=	58	=	:
R	+	k	=	82	+	107	=	157	mod	128	=	61	=	=
S	+	s	=	83	+	115	=	166	mod	128	=	70	=	F
I	+	e	=	73	+	101	=	142	mod	128	=	46	=	.
T	+	s	=	84	+	115	=	167	mod	128	=	71	=	G
A	+	s	=	65	+	115	=	148	mod	128	=	52	=	4
S	+	u	=	83	+	117	=	168	mod	128	=	72	=	H
D	+	k	=	68	+	107	=	143	mod	128	=	47	=	/
I	+	s	=	73	+	115	=	156	mod	128	=	60	=	<
A	+	e	=	65	+	101	=	134	mod	128	=	38	=	&
N	+	s	=	78	+	115	=	161	mod	128	=	65	=	A
N	+	s	=	78	+	115	=	161	mod	128	=	65	=	A
U	+	u	=	85	+	117	=	170	mod	128	=	74	=	J
S	+	k	=	83	+	107	=	158	mod	128	=	62	=	>
W	+	s	=	87	+	115	=	170	mod	128	=	74	=	J
A	+	e	=	65	+	101	=	134	mod	128	=	38	=	&
N	+	s	=	78	+	115	=	161	mod	128	=	65	=	A
T	+	s	=	84	+	115	=	167	mod	128	=	71	=	G
O	+	u	=	79	+	117	=	164	mod	128	=	68	=	D
R	+	k	=	82	+	107	=	157	mod	128	=	61	=	=
O	+	s	=	79	+	115	=	162	mod	128	=	66	=	B

Tabel 2. Hasil Enkripsi Vigenere

Plaintext	***Ciphertext***
MAHASISWAUNIVERSITASDIANNUSWANTORO	@6348<FL,H3<I:=F.G4H/<&AAJ>J&AGD=B

Hasil *ciphertext* tersebut akan di enkripsi lagi menggunakan algoritma *Hill Cipher* dengan kunci menggunakan matriks 2x2, yaitu [5 6 2 3]. Karena menggunakan ASCII maka di modulo 128 dan perhitungan seperti pada Tabel 3. Setelah *plaintext* diubah menggunakan ASCII maka selanjutnya dikalikan dengan kunci *Hill Cipher* yang berbentuk matriks seperti pada Tabel 5.

Plaintext=
@6348<FL,H3<I:=F.G4H/<&AAJ>J&AGD=B

Key = [5 6 2 3]

Tabel 3. ASCII Plainteks

@	=	64	G	=	71
6	=	54	4	=	52
3	=	51	H	=	72
4	=	52	/	=	47
8	=	56	<	=	60
<	=	60	&	=	38
F	=	70	A	=	65
L	=	76	A	=	65
,	=	44	J	=	74
H	=	72	>	=	62
3	=	51	J	=	74
<	=	60	&	=	38
I	=	73	A	=	65
:	=	58	G	=	71
=	=	61	D	=	68
F	=	70	=	=	61
.	=	46	B	=	66

Tabel 4. Enkripsi Hill Cipher

5	6	X	64	=	320	+	324	=	644	mod	128	=	4	=	(EOT)
2	3		54	=	128	+	162	=	290	mod	128	=	34	=	“
5	6	X	51	=	255	+	312	=	567	mod	128	=	55	=	7
2	3		52	=	102	+	156	=	258	mod	128	=	2	=	(STX)
5	6	X	56	=	280	+	360	=	640	mod	128	=	0	=	(NULL)
2	3		60	=	112	+	180	=	292	mod	128	=	36	=	$
5	6	X	70	=	350	+	456	=	806	mod	128	=	38	=	&
2	3		76	=	140	+	228	=	368	mod	128	=	112	=	p
5	6	X	44	=	220	+	432	=	652	mod	128	=	12	=	(FF)
2	3		72	=	88	+	216	=	304	mod	128	=	48	=	0
5	6	X	51	=	255	+	360	=	615	mod	128	=	103	=	g
2	3		60	=	102	+	180	=	282	mod	128	=	26	=	(SUB)
5	6	X	73	=	365	+	348	=	713	mod	128	=	73	=	I
2	3		58	=	146	+	174	=	320	mod	128	=	64	=	@
5	6	X	61	=	305	+	420	=	725	mod	128	=	85	=	U
2	3		70	=	122	+	210	=	332	mod	128	=	76	=	L
5	6	X	46	=	230	+	426	=	656	mod	128	=	16	=	(DLE)
2	3		71	=	92	+	213	=	305	mod	128	=	49	=	1
5	6	X	52	=	260	+	432	=	692	mod	128	=	52	=	4
2	3		72	=	104	+	216	=	320	mod	128	=	64	=	@
5	6	X	47	=	235	+	360	=	595	mod	128	=	83	=	S
2	3		60	=	94	+	180	=	274	mod	128	=	18	=	(DC2)
5	6	X	38	=	190	+	390	=	580	mod	128	=	68	=	D
2	3		65	=	76	+	195	=	271	mod	128	=	15	=	(SI)
5	6	X	65	=	325	+	444	=	769	mod	128	=	1	=	(SOH)
2	3		74	=	130	+	222	=	352	mod	128	=	96	=	‘
5	6	X	62	=	310	+	444	=	754	mod	128	=	114	=	r
2	3		74	=	124	+	222	=	346	mod	128	=	90	=	Z
5	6	X	38	=	190	+	390	=	580	mod	128	=	68	=	D
2	3		65	=	76	+	195	=	271	mod	128	=	15	=	(SI)
5	6	X	71	=	355	+	408	=	763	mod	128	=	123	=	{
2	3		68	=	142	+	204	=	346	mod	128	=	90	=	Z
5	6	X	61	=	305	+	396	=	701	mod	128	=	61	=	=
2	3		66	=	122	+	198	=	320	mod	128	=	64	=	@

Tabel 5. Hasil Enkripsi Hill Cipher

Plaintext	***Ciphertext***
@6348<FL,H3<I:=F.G4H/<&AAJ>J&AGD =B	(EOT)”7(STX)(NULL)$&p(FF)0g(SUB)I@UL(DLE)14@S(DC2)D(SI)(SOH)’fZD(SI) {Z=@

3.3 Perhitungan Manual Dekripsi

Tahapan enkripsi diawali dengan pengguna menginputkan file yang sudah terenkripsi (*ciphertext*), kunci 1 dan kunci 2, dimana kunci 1 menjadi *key* untuk algoritma *vigenere cipher* dan kunci 2 akan menjadi *key* untuk algoritma *hill cipher*.

Sebagai contoh pengguna menginputkan file, kunci 1 dan kunci 2 seperti dibawah ini.

Ciphertext=
(EOT)”7(STX)(NULL)$&p(FF)0g(SUB)I@UL(DLE)14@S(DC2)D(SI)(SOH)’fZD(SI){Z=@

Kunci 1= sukses →*Key vigenere cipher*

Kunci 2 = [5 6 2 3] →*Key* 2 *hill cipher*

Dalam file yang sudah terenkripsi tersebut berisikan huruf yang tidak bisa di baca oleh siapapun yang nantinya huruf - huruf tersebut akan dikonversikan menjadi huruf ASCII pada Tabel 6, kemudian di dekripsi menggunakan algoritma *vigenere cipher* dan *hill cipher*. Proses pertama *ciphertext* atau file yang sudah dirubah menggunakan ASCII kemudian dimasukkan ke dalam rumus dekripsi menggunakan *Hill Cipher*.

Plaintext= (EOT)”7(STX)(NULL)$&p(FF)0g(SUB)I@UL(DLE)14@S(DC2)D(SI)(SOH)’fZD(SI){Z=@

Key= [5 6 2 3]

Maka key yang sudah di invers menjadi = [1 126 42 87]

Tabel 6. Hasil Enkripsi Hill Cipher

(EOT)	=	4	1	=	49
“	=	34	4	=	52
7	=	55	@	=	64
(STX)	=	2	S	=	83
(NULL)	=	0	(DC2)	=	18
$	=	36	D	=	68
&	=	38	(SI)	=	15
p	=	112	(SOH)	=	1
(FF)	=	12	‘	=	96
0	=	48	r	=	114
g	=	103	Z	=	90
(SUB)	=	26	D	=	68
I	=	73	(SI)	=	15
@	=	64	{	=	123
U	=	85	Z	=	90
L	=	76	=	=	61
(DLE)	=	16	@	=	64

Setelah *plaintext* diubah menggunakan ascii maka selanjutnya dikalikan dengan kunci *Hill Cipher* yang berbentuk matriks dan *ciphertext* dari perhitungan Tabel 5 dan Tabel 6, algoritma *Vigenere* diatas menunjukan hasil seperti Tabel 7. Hasil *ciphertext* tersebut akan di enkripsi lagi menggunakan algoritma *Vigenere Cipher*, dimana huruf berwarna merah merupakan pengulangan kunci sesuai panjang *plaintext*. Hasil sesuai pada Tabel 9. *Ciphertext* dari perhitungan algoritma *Vigenere* diatas menunjukan hasil seperti Tabel 10.

Tabel 7. Perhitungan Dekripsi Hill Cipher

1	126	X	4	=	4	+	4284	=	4288	mod	128	=	64	=	@
42	87		34	=	168	+	2958	=	3126	mod	128	=	54	=	6
1	126	X	55	=	55	+	252	=	307	mod	128	=	51	=	3
42	87		2	=	2310	+	174	=	2484	mod	128	=	52	=	4
1	126	X	0	=	0	+	4536	=	4536	mod	128	=	56	=	8
42	87		36	=	0	+	3132	=	3132	mod	128	=	60	=	<
1	126	X	38	=	38	+	14112	=	14150	mod	128	=	70	=	F
42	87		112	=	1596	+	9744	=	11340	mod	128	=	76	=	L
1	126	X	12	=	12	+	6048	=	6060	mod	128	=	44	=	,
42	87		48	=	504	+	4176	=	4680	mod	128	=	72	=	H
1	126	X	103	=	103	+	3276	=	3379	mod	128	=	51	=	3
42	87		26	=	4326	+	2262	=	6588	mod	128	=	60	=	<
1	126	X	73	=	73	+	8064	=	8137	mod	128	=	73	=	I
42	87		64	=	3066	+	5568	=	8634	mod	128	=	58	=	:
1	126	X	85	=	85	+	9576	=	9661	mod	128	=	61	=	=
42	87		76	=	3570	+	6612	=	10182	mod	128	=	70	=	F
1	126	X	16	=	16	+	6174	=	6190	mod	128	=	46	=	.
42	87		49	=	672	+	4263	=	4935	mod	128	=	71	=	G
1	126	X	52	=	52	+	8064	=	8116	mod	128	=	52	=	4
42	87		64	=	2184	+	5568	=	7752	mod	128	=	72	=	H
1	126	X	83	=	83	+	2268	=	2351	mod	128	=	47	=	/
42	87		18	=	3486	+	1566	=	5052	mod	128	=	60	=	<
1	126	X	68	=	68	+	1890	=	1958	mod	128	=	38	=	&
42	87		15	=	2856	+	1305	=	4161	mod	128	=	65	=	A
1	126	X	1	=	1	+	12096	=	12097	mod	128	=	65	=	A
42	87		96	=	42	+	8352	=	8394	mod	128	=	74	=	J
1	126	X	114	=	114	+	11340	=	11454	mod	128	=	62	=	>
42	87		90	=	4788	+	7830	=	12618	mod	128	=	74	=	J
1	126	X	68	=	68	+	1890	=	1958	mod	128	=	38	=	&
42	87		15	=	2856	+	1305	=	4161	mod	128	=	65	=	A

1	126	X	123	=	123	+	11340	=	11463	mod	128	=	71	=	G
42	87		90	=	5166	+	7830	=	12996	mod	128	=	68	=	D
1	126	X	61	=	61	+	8064	=	8125	mod	128	=	61	=	=
42	87		64	=	2562	+	5568	=	8130	mod	128	=	66	=	B

Tabel 8. Hasil Dekripsi Hill Cipher

Ciphertext	***Plaintext***
(EOT)”7(STX)(NULL)$&p(FF)0g(SUB)I@UL(DLE)14@S(DC2)D(SI)(SOH)’fZD(SI){Z=@	@6348<FL,H3<I:=F.G4H/<&AAJ>J&AGD=B

Tabel 9. Perhitungan Dekripsi Vigenere

@	-	s	=	64	-	115	=	-51	mod	128	=	77	=	M
6	-	u	=	54	-	117	=	-63	mod	128	=	65	=	A
3	-	k	=	51	-	107	=	-56	mod	128	=	72	=	H
4	-	s	=	52	-	115	=	-63	mod	128	=	65	=	A
8	-	e	=	56	-	101	=	-45	mod	128	=	83	=	S
<	-	s	=	60	-	115	=	-55	mod	128	=	73	=	I
F	-	s	=	70	-	115	=	-45	mod	128	=	83	=	S
L	-	u	=	76	-	117	=	-41	mod	128	==	87	=	W
,	-	k	=	44	-	107	=	-63	mod	128	=	65	=	A
H	-	s	=	72	-	115	=	-43	mod	128	=	85	=	U
3	-	e	=	51	-	101	=	-50	mod	128	=	78	=	N
<	-	s	=	60	-	115	=	-55	mod	128	=	73	=	I
I	-	s	=	73	-	115	=	-42	mod	128	=	86	=	V
:	-	u	=	58	-	117	=	-59	mod	128	=	69	=	E
=	-	k	=	61	-	107	=	-46	mod	128	=	82	=	R
F	-	s	=	70	-	115	=	-45	mod	128	=	83	=	S
.	-	e	=	46	-	101	=	-55	mod	128	=	73	=	I
G	-	s	=	71	-	115	=	-44	mod	128	=	84	=	T
4	-	s	=	52	-	115	=	-63	mod	128	=	65	=	A
H	-	u	=	72	-	117	=	-45	mod	128	=	83	=	S
/	-	k	=	47	-	107	=	-60	mod	128	=	68	=	D
<	-	s	=	60	-	115	=	-55	mod	128	=	73	=	I
&	-	e	=	38	-	101	=	-63	mod	128	=	65	=	A
A	-	s	=	65	-	115	=	-50	mod	128	=	78	=	N
A	-	s	=	65	-	115	=	-50	mod	128	=	78	=	N
J	-	u	=	74	-	117	=	-43	mod	128	=	85	=	U
>	-	k	=	62	-	107	=	-45	mod	128	=	83	=	S
J	-	s	=	74	-	115	=	-41	mod	128	=	87	=	W
&	-	e	=	38	-	101	=	-63	mod	128	=	65	=	A
A	-	s	=	65	-	115	=	-50	mod	128	=	78	=	N
G	-	s	=	71	-	115	=	-44	mod	128	=	84	=	T
D	-	u	=	68	-	117	=	-49	mod	128	=	79	=	O
=	-	k	=	61	-	107	=	-46	mod	128	=	82	=	R
B	-	s	=	66	-	115	=	-49	mod	128	=	79	=	O

Tabel 10. Hasil Dekripsi Hill Cipher

Ciphertext	***Plaintext***
@6348<FL,H3<I:=F.G4H/<&AAJ>J&AGD=B	MAHASISWAUNIVERSITASDIANNUSWANTORO

3.4 Pengujian *Black Box*

Ketika semua implementasi sudah dilakukan, maka tahapan terakhir dalam penelitian ini adalah dengan menguji program. Pengujian ini dilakukan guna melihat kelancaran program yang sudah dibuat dan menganalisa setiap program apabila terjadinya *bug* maupun *error* pada program yang dibuat. Untuk menguji seberapa baik kualitas dan fungsionalitas dari program yang telah di buat, maka hasil penerapan *Black Box Testing* sebagai penggunaannya dapat dilihat pada Tabel 11.

Tabel 11. Pengujian Black Box Enkripsi

No.	Skenario Pengujian	Test Case	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	Input data teks	Input data teks yang diinginkan	Isi data teks sesuai dengan data aslinya	Sesuai harapan	valid
2.	Input Kunci Vigenere untuk enkripsi data teks	Input Key: “sukses”	Input key atau kunci vigenere dapat diinput sendiri	Sesuai harapan	valid
3.	Hasil dari enkripsi Vigenere	Hasil dari enkripsi Vigenere berupa data teks	Hasil akan diolah lagi pada enkripsi Hill Cipher.	Sesuai harapan	valid
4.	Input Kunci Hill Cipher untuk hasil enkripsi Vigenere	Input Key dalam bentuk matrik : “ [5 6 2 3] “	Input key atau kunci Hill Cipher dalam sistem dapat dilakukan	Sesuai harapan	valid

No.	Skenario Pengujian	Test Case	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
5.	Hasil dari enkripsi Hill Cipher	Hasil dari enkripsi Hill Cipher berupa data teks	Hasil / Output yang keluar adalah enkripsi dari proses sandi Hill Cipher	Sesuai harapan	valid

Dari hasil pengujian *Black Box Testing* pada Tabel 11, dapat disimpulkan bahwa untuk skenario pertama yaitu *"Input data teks asli / plaintext"* menghasilkan kesimpulan yang sesuai atau valid, karena input *data teks* berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario kedua yaitu *"Input key vigenere cipher"* menghasilkan kesimpulan yang sesuai atau valid, karena input *key* dengan kata kunci yang berbeda *vigenere cipher* masih tetap berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario yang ketiga yaitu *"Enkripsi vigenere cipher"* menghasilkan hasil enkripsi yang sesuai atau valid karena melakukan proses yang sudah dijelaskan diatas dan menghasilkan kesimpulan yang valid atau sesuai yang diinginkan. Skenario keempat yaitu *"Input key hill cipher"* menghasilkan kesimpulan yang sesuai atau valid, karena input *key* dengan kata kunci yang berbeda *hill cipher* masih tetap berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario kelima yaitu *"Enkripsi hill cipher atau output ciphertext"* menghasilkan ciphertext yang sesuai atau valid karena melakukan proses yang sudah dijelaskan diatas dan menghasilkan kesimpulan yang valid atau sesuai yang diinginkan.

Tabel 12. Pengujian Black Box Dekripsi

No.	Skenario Pengujian	Test Case	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	Input data teks	Input data teks yang sudah di enkripsi	Isi data teks sesuai dengan data enkripsi	Sesuai harapan	valid
2.	Input Kunci Hill Cipher untuk dekripsi data teks	Input Key dalam bentuk matrik : " [5 6 2 3] "	Input key atau kunci Hill Cipher dalam sistem dapat dilakukan	Sesuai harapan	valid
3.	Hasil dari dekripsi Hill Cipher	Hasil dari dekripsi Hill Cipher berupa data teks	Hasil akan diolah lagi pada dekripsi Vigenere.	Sesuai harapan	valid
4.	Input Kunci Vigenere untuk hasil dekripsi Hill Cipher	Input Key: "sukses"	Input key atau kunci Vigenere dalam sistem dapat dilakukan	Sesuai harapan	valid
5.	Hasil dari dekripsi Vigenere	Hasil dari dekripsi Vigenere berupa data teks	Hasil / Output yang keluar adalah dekripsi dari proses sandi Vigenere	Sesuai harapan	valid

Dari hasil pengujian *Black Box Testing* pada Tabel 12, dapat disimpulkan bahwa untuk skenario pertama yaitu *"Input data teks asli / ciphertext"* menghasilkan kesimpulan yang sesuai atau valid, karena input *data teks* berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario kedua yaitu *"Input key hill cipher"* menghasilkan kesimpulan yang sesuai atau valid, karena input *key* dengan kata kunci yang berbeda *hill cipher* masih tetap berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario yang ketiga yaitu *"Enkripsi hill cipher"* menghasilkan hasil enkripsi yang sesuai atau valid karena melakukan proses yang sudah dijelaskan di atas dan menghasilkan kesimpulan yang valid atau sesuai yang diinginkan. Skenario keempat yaitu *"Input key vigenere cipher"* menghasilkan kesimpulan yang sesuai atau valid, karena input *key* dengan kata kunci yang berbeda *vigenere cipher* masih tetap berjalan dengan baik dan sesuai yang diharapkan atau dengan kata lain valid. Skenario kelima yaitu *"Enkripsi vigenere cipher atau output plaintext"* menghasilkan plaintext atau data asli yang sesuai atau valid karena melakukan proses yang sudah dijelaskan diatas dan menghasilkan kesimpulan yang valid atau sesuai yang diinginkan.

3.5 Pengujian *Avalanche Effect*

Avalanche Effect (AE) digunakan untuk melihat seberapa besar nilai dari kekuatan enkripsi yang dihasilkan saat proses penyandian dengan menggunakan metode *Vigenere* [16], [18]. Untuk menghitung *Avalanche Effect* dari *Vigenere* dapat dilihat pada persamaan (5).

$$Avalanche\ Effect = \frac{jumlah\ perubahan\ bit}{jumlah\ seluruh\ bit} x\ 100\% \quad \ldots\ldots(5)$$

Tabel 13. Perubahan Bit dan Avalanche Effect

No	Jumlah Bit (Bit)	Perubahan Bit (Bit)	Avalanche Effect (%)
1	128	66	51,94 %
2	256	139	54,29 %
3	512	262	51,17 %
Rata - rata			**52,46 %**

Berdasarkan pada Tabel 13, diketahui bahwa nilai *Avalanche Effect* yang dihasilkan dari seluruh percobaan mendekati 50%. Nilai ini merupakan nilai yang baik, apabila AE mendekati 50% maka proses enkripsi dan dekripsi yang dilakukan telah berhasil mengamankan pesan rahasia.

4. KESIMPULAN

Pada penelitian ini telah diimplementasikan tiga buah percobaan proses enkripsi dan dekripsi pada data teks berukuran 128bit, 256 bit dan 512 bit. Ukuran teks sebetulnya hanya untuk mempermudah dalam proses perhitungan saja. Pada proses pengujian *black box*, aplikasi dapat berjalan dengan baik dimana proses enkripsi dan dekripsi berjalan lancar. Pda perhitungan *Avalanche Effect* (AE), nilai AE yang diperoleh pada ketiga percobaan menggunakan kunci yang sama dan plainteks yang berbeda, diperoleh nilai AE seluruhnya menghasilkan nilai mendekati 50% dengan nilai AE terbaik yaitu pada percobaan ke-3 dengan perolehan 51,17%. Pada penelitian selanjutnya, untuk memperbaiki hasil AE maka perlu dilakukan kombinasi dengan algoritma kriptografi modern atau menggunakan algoritma transposisi cipher.

DAFTAR PUSTAKA

[1] E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[2] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Pseudocode*, vol. 3, no. 2, pp. 129–136, 2017.

[3] Kurniawan, I. A. Siradjuddin, and A. Muntasa, "Keamanan Citra Dengan Watermarking Menggunakan Pengembangan Algoritma Least Significant Bit," *J. Inform.*, vol. 13, no. 1, pp. 9–14, 2016.

[4] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *J. Format*, vol. 6, no. 1, pp. 87–105, 2017.

[5] C. A. Sari, W. S. Sari, and B. Sugiarto, "IMPERCEPTIBLE KRIPTOGRAFI CITRA BERWARNA MENGGUNAKAN RIVEST SHAMIR ADLEMAN," in *Proceeding SENDIU 2021*, 2021, pp. 978–979.

[6] C. A. Sari, E. H. Rachmawanto, and E. J. Kusuma, "Good Performance Image Encryption Using Selective Bit T-DES on Inverted LSB Steganography," *J. Ilmu Komput. dan Inf.*, vol. 12, no. 1, pp. 41–29, 2019.

[7] Jamaludin, "Rancang Bangun Kombinasi Chaisar Cipher dan Vigenere Cipher Dalam Pengembangan Algoritma Kriptografi Klasik," in *Seminar Nasional Teknologi Informasi (Semantika)*, 2017, no. The Future of Computer Vision, pp. 234–243.

[8] G. A. Pradipta, "Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting," *J. Sist. dan Inform.*, vol. 10, no. 2, pp. 119–127, 2016.

[9] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[10] A. Susanto, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, R. R. Ali, and I. U. Wahyu Mulyono, "Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography," in *Journal of Physics: Conference Series*, 2019, vol. 1201, no. 1.

[11] F. Al Isfahani and F. Nugraha, "Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK," *Sci. Comput. Sci. Informatics J.*, pp. 1–8, 2019.

[12] A. Blair, "Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination," in *2013 IEEE Congress on Evolutionary Computation*, 2013, pp. 605–612.

[13] R. Damara Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)," in *Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems, ICON-SONICS 2017*, 2018, vol. 2018-Janua.

[14] P. Subhasri and A. Padmapriya, "Enhancing the security of dicom content using modified vigenere cipher," *Int. J. Appl. Eng. Res.*, vol. 10, no. 55, pp. 1951–1956, 2015.

[15] S. Hraoui, F. Gmira, M. F. Abbou, A. J. Oulidi, and A. Jarjar, "A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm," *Procedia Comput. Sci.*, vol. 148, pp. 399–408, 2019.

[16] M. Essaid, I. Akharraz, A. Saaidi, and et A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, Aug. 2019.

[17] O. E. Omolara, A. I. Oludare, and S. E. Abdulahi, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," *Comput. Eng. Intell. Syst.*, vol. 5, no. 5, pp. 2222–1719, 2014.

[18] P. Witoolkollachit, "The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images : A comparison study," *J. Thai Med. Informatics Assoc.*, vol. 1, pp. 69–82, 2016.