ISBN : 978-623-7297-51-2

PENGGUNAAN ALGORITMA VIGENERE CIPHER DAN *ONE TIME PAD UNTUK* KEAMANAN PESAN TEKS

Hermansyah Alam[1)], Ahamad Kurniawan Habibi[2)], Helma Widya[3)]
[1)]Dosen Teknik Elektro Universitas Panca Budi,
[2)]Alumni Teknik Informatika ITM,
[3)]Dosen Bisnis Digital LP3I Medan

Abstrak

Keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Saat ini sistem komputer yang terpasang dengan jaringan makin mudah diakses untuk itu diperlukan sistem komputer yang memiliki tingkat keamanan yang dapat terjamin. Berdasarkan kenyataan tersebut, perlu ada suatu pengamanan informasi pada saat pengiriman informasi. Penelitian ini membahas implementasi algoritma enkripsi one time pad dan vigenere ciphe, berbasis Kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data karena dapat melakukan untuk mengamankan pesan teks,
Keyword : One Time Pad, Vigenere Cipher, Kriptografi

Kata Kunci : *One Time Pad, Vigenere Cipher, Kriptografi,*

I. PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Di mana kebenaran dan keaslian suatu informasi sangat penting baik pada saat pengiriman ataupun pada saati nformasi tersebut diterima. Pesan, data, atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

Saat ini sistem komputer yang terpasang dengan jaringan makin mudah diakses. Sistem sharing data menyebabkan masalah keamanan menjadi salah satu kelemahan komunikasi data dalam jaringan, disamping itu kecenderungan lain saat ini adalah memberikan tanggung jawab sepenuhnya ke komputer untuk mengelola aktifitas pribadi dan bisnis seperti transfer data antar computer dalam jaringan. Untuk itu diperlukan sistem komputer yang memiliki tingkat keamanan yang dapat terjamin. Berdasarkan kenyataan tersebut, perlu ada suatu pengamanan informasi pada saat pengiriman informasi. Untuk melakukan ini ada suatu cara yang biasa disebut penyandian data. Dalam penelitian ini akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan kriptografi. Dengan adanya sebuah kriptografi yang meliputi proses enkripsi dan dekripsi maka pesan, data, maupun informasi dapat dikodekan sehingga orang yang tidak berkepentingan tidak dapat membaca informasi tersebut.Metode Kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data karena dapat melakukan proses enkripsi dan dekripsi. Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari seperti DES, AES, TwoFish, BlowFish, RC2, RC4, RC5, RSA (Rivest, Shamir, Adleman) dan lain-lain. Penelitian ini membahas implementasi algoritma enkripsi *one time pad* dan *vigenere cipher*untuk mengamankan pesan teks.*Vigenère Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. *Vigenère Cipher* merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi (Sentot Kromodimoeljo, 2010).

One Time Pad adalah salah satu contoh metode kriptografi dengan algoritma jenis simetri. Ditemukan pada tahun 1917 oleh Major Yoseph Mouborgne dan Gilbert Vernam pada perang dunia ke dua. Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan plaintext-nya Sampai saat ini, hanyaalgoritma *One Time Pad* (OTP) yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas (Sentot Kromodimoeljo, 2010), berikut adalah beberapa penelitian terkait dengan algoritma One Time Pad

II. LANDASAN TEORI

2.1 Algoritma Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik menyebutkan bahwa Vigenere cipher adalah sesuatu yang tidak mungkin untuk ditranslasikan. Namun hal ini terbantahkan sejak Kasiski berhasil memecahkan algoritma pada abad ke-19. Pada dasarnya Vigenere Cipher serupa dengan Caesar Cipher, perbedaannya adalah pada Vigenere Cipher setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan pada Caesar Cipher setiap huruf pesannya digeser sebanyak 1 huruf yang sama (Sentot Kromodimoeljo, 2010).

Algoritma Vigenere Cipher ini menggunakan bujur sangkar Vigenere untuk melakukan enkripsi.

Setiap baris di dalam bujur sangkar menyatakan huruf-huruf ciphertext yang diperoleh dengan Caesar cipher. (Sentot Kromodimoeljo, 2010).

2.2 Algoritma One Time Pad

One Time Pad adalah salah satu contoh metode kriptografi dengan algoritma jenis simetri. Seingga kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan plaintext-nya Sampai saat ini,hanya algoritma One Time Pad (OTP) yangdinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. Proses enkripsi dan dekripsi pada One TimePad ini hampir sama dengan proses enkripsidan dekripsi menggunakan algoritmavigenere cipher (Sugeng Sutrisno, 2014). Proses enkripsi dapat dilakukan dengan persamaan matematis sebagai berikut :

$C_i = (P_i + K_i) Mod 26$.....(2.1)

Sedangkan untuk proses dekripsi dapat dilihat pada persamaan matematis sebagai berikut:

$P_i = ((C_i - K_r) + 26) Mod\ 26$.....(2.2)

Dari persamaan di atas dapat diketahui :

C_i= pergeseran karakter pada ciphertext

P_i = pergeseran karakter padaplaintext

K_r = Kunci dalam bentuk decimal yang dihasilkan dari tabel konversi.

Bagian yang membedakan antara one time pad dengan vigenere cipher adalah pada kunci yang digunakan. Jika penggunaan kunci pada vigenere cipher diulang untuk menyesuaikan dengan panjang plaintext, maka pada one time pad hal tersebut tidak dapat dilakukan karena jumlah kunci yang digunakan harus sama panjangnya dengan jumlah plaintext (Sugeng Sutrisno, 2014).

Sebagai contoh algoritma one time pad adalah sebagai berikut:

Misalkan pesan yang akan dikirimkan yaitu FIRMAN dengan kata kunci GLORIA, Langkah yang dilakukan sbb :

Ubah menjadi kode ASCII dan biner untuk kata FIRMAN dan GLORIA, sehingga didapat hasil sebagai berikut:

Karakter	ASCII	BINER
F	106	000100000110
I	111	0001000 0001
R	122	000100100010
M	115	000100010101
A	101	000100000001
N	116	000100010110

Hal yang sama dilakukan pada kunci

G	107	000100000111
L	114	000100010100
O	117	000100010111
R	122	000100100010
I	111	000100010001
A	101	000100000001

Pesan di-XORkan dengan kunci maka akan diperoleh

F	000000000001001
I	000000000101005
R	000000110101035
M	000000110100034
A	000000010000010
N	000000010111017

Kode ASCII tersebut diterjemahkan lagi menjadi karakter Diperoleh : NUL ENQ GS FS BS SI

Pesan yang akan dienkripsi disebut *plaintext* yang dimisalkan *plaintext* (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut *ciphertext* yang dimisalkan *ciphertext* (C).kemudian menghasilkanC,yang digambarkanseperti notasi berikut:

E (P) = C.....(2.3)

Pada proses dekripsi data yang sudah diproses pada enkripsi (*ciphertext*) melalui proses dekripsi data akan dikembalikan lagi ke dalam bentuk *plaintext*/ data aslinya, yang digambarkan seperti notasi berikut :

D (C) = P.....(2.4)

Data atau informasi yang telah melalui proses enkripsi dan dekripsi, dimana data yang sudah diacak akan menghasilkan data atau informasi aslinya (*plaintext*), yang digambarkan seperti notasi berikut:

D (E (P)) = P.....(2.5)

Transformasi matematis yang memetakan *plaintext* ke *ciphertext* dan sebaliknya. *Ciphertext* sangat dipengaruhi oleh keberadaan *plaintext* dan kuncinya, jadi nilai dari suatu kunci akan mempengaruhi fungsi enkripsi dan dekripsi(Dony Ariyus, 2006)., sehingga fungsi enkripsi tersebut dapat dinotasikan seperti berikut :

Ek (P) = C.....(2.6)

Bila kunci yang dipakai untuk proses enkripsi sama dengan kunci yang dipakai untuk proses dekripsi, maka notasi sebagai berikut :

(Dk(Ek)) = P.....(2.7)

Keterangan:

K:Kunci

Ek:KunciEnkripsi

Dk : Kunci Dekripsi

2.4 Ancaman Keamanan

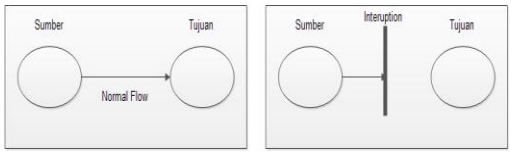
Pada kenyataannya, terdapat banyak faktor yang dapat mengancam sistem keamanan data. Ancaman-ancaman tersebut menjadi masalah terutama dengan semakin meningkatnya komunikasi data yang bersifat rahasia faktor-faktor

ISBN : 978-623-7297-51-2

yang dapat mengancam keamanan dapat dikelompokkan ke dalam empat jenis ancaman, yaitu:

1. *Interruption*

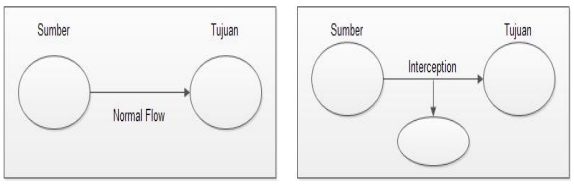
Interruption terjadi bila data yang dikirimkan dari A tidak sampai pada orang yang berhak (B). Interruption merupakan pola penyerangan terhadap sifat availability (ketersediaan data), yaitu data dan informasi yang berada dalam sistem komputer dirusak atau dibuang, sehinggga menjadi tidak ada dan tidak berguna.Contohnya, hard disk yang dirusak atau memotong jalur komunikasi.Seperti terlihat pada Gambar 1 berikut.



Gambar 1. Interruption

2. *Interception*

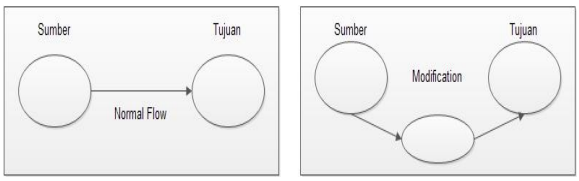
Serangan ini terjadi jika pihak ketiga berhasil mendapatkan akses informasi dari dalam sistem komputer. Contohnya, dengan menyadap data yang melalui jaringan public (wiretapping) atau menyalin secara tidak sah file atau program Interception merupakan pola penyerangan terhadap sifat confidentially/secrecy (kerahasiaan data). Seperti terlihat pada Gambar 2 berikut.



Gambar 2. Interception
Sumber: Dony Ariyus, 2006

3. *Modification*

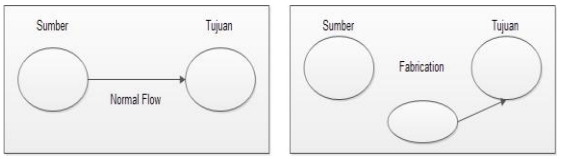
Pada serangan ini pihak ketiga yang tidak hanya berhasil mendapatkan akses informasi dari dalam sistem komputer, tetapi juga dapat melakukan perubahan terhadap informasi, merubah program berhasil merubah pesan yang dikirimkan. Modification merupakan pola penyerangan terhadap sifat integrity (keaslian data).Seperti terlihat pada Gambar 3 berikut.



Gambar 3. Modification
Sumber: Dony Ariyus, 2006

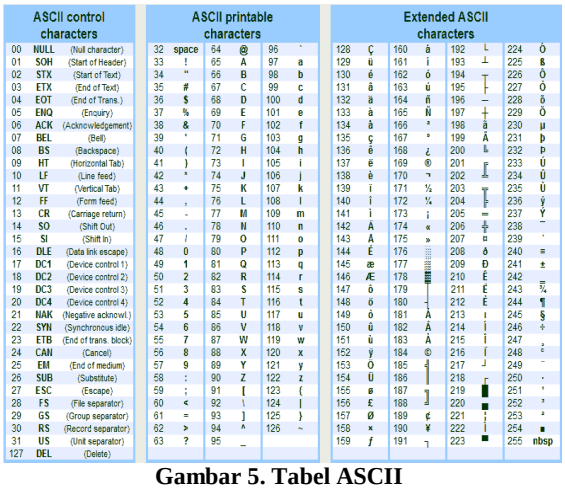
4. *Fabrication*

Fabrication merupakan ancaman terhadap integritas, yaitu orang yang tidak berhak yang meniru atau memalsukan suatu objek ke dalam sistem. Contohnya, dengan menambahkan suatu record ke dalam file. Seperti terlihat pada Gambar 4 berikut.



Gambar 4. Fabrication
Sumber: Dony Ariyus, 2006

Kode ini digunakan dalam Personal Computer (PC). Piranti yang menggunakan kode ini perlu menterjemahkan 1 bit didepan sebagai parity. Bit parity berfungsi sebagai tanda kesalahan dalam pengiriman data selama komunikasi, yang terdiri atas parity genap (bit 1 apabila jumlah bit 1 dalam 7 deretan bit data berjumlah genap) dan parity ganjil (bit 1 apabila jumlah bit 1 dalam 7 deretan bit data berjumlah ganjil) *(sumber: Janner Simarmata, 2010).*



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

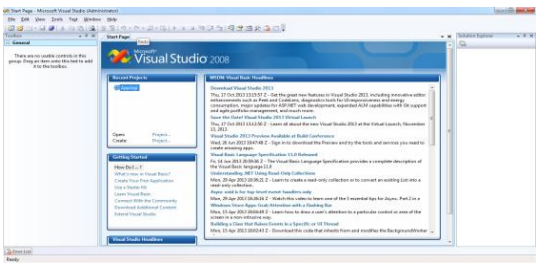
32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	▒	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

Gambar 5. Tabel ASCII

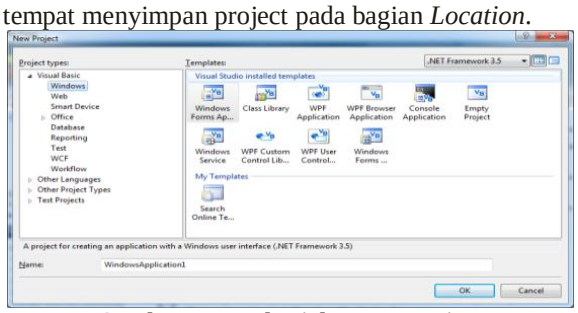
Pemrograman Berbasis Objek sendiri adalah suatu pendekatan ke arah struktur pengembangan aplikasi berdasarkan objek, dimana objek tersebut dapat berupa prosedur, event, ataupun variabel. Objek satu dapat menjadi bawahan objek lainnya berdasarkan susunan fungsinya, maka akan dihadapkan pada tampilan seperti Gambar 6.



Gambar 6. Tampilan Awal Visual Studio 2008
sumber: Wardhana,2008

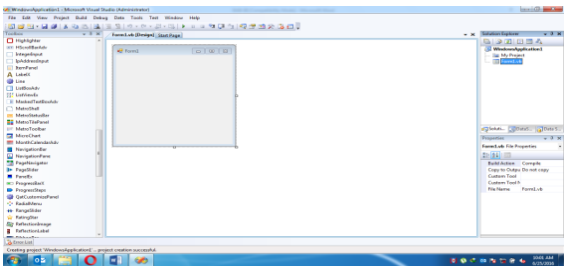
Kemudian akan muncul kotak dialog *New Project*. Pada kotak dialog *New Project* terdapat beberapa pilihan tool untuk pengembangan aplikasi,

yang akan dibuat pada bagian Name dan direktori tempat menyimpan project pada bagian *Location*.



Gambar 7. Kotak Dialog New Project
sumber: Wardhana,2008

Pada gambar sebelumnya diberikan pilihan untk membuat aplikasi yang kita kehendaki, apakah berupa aplikasi biasa (*Windows Application*), *libray* kelas, aplikasi konsole (aplikasi seperti tampilan DOS klasik), *control windows*, *file library* untuk *control website*, *service windows*, *crystal report*, atau hanya projek kosong belaka. aplikasi*Windows* biasa (*Windows Application*). Beri nama projek tersebut lalu tekan tombol *OK*, maka kita dihadapkan pada jendela berikut ini.



Gambar 8.*Design view*
sumber: Wardhana,2008

III. METODE PENELITIAN

3.1 Penerapan Algoritma Vigenere Cipher

Vigenere chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vigenere cipher pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, Vigenere cipher tetap memiliki kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode kasiski.pada ciphertext yang dihasilkan, sebagai catatan bahwa proses kriptografi klasik berhubungan dengan tabel nilai di bawah ini :

Tabel 1. Nilai

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Contoh :
Plainteks = TEKNOLOGI
Kunci = AHMAD

Dikarenakan kunci < Plainteks maka panjang kunci disesuaikan dengan panjang plainteks, maka hasilnya adalah:

Plainteks = TEKNOLOGI
Kunci = AHMADAHMA
Berikut adalah proses enkripsi nya :

Tabel 2. Proses enkripsi

Plainteks	T	E	K	N	O	L	O	G	I
Plainteks ASCII	19	4	10	13	14	11	14	6	9
Kunci	A	H	M	A	D	A	H	M	A
Kunci ASCII	0	7	12	0	3	0	7	12	0
Hasil Ciphertext	19	11	22	13	17	11	21	18	9
	T	L	W	N	R	L	V	S	J

Plainteks = TEKNOLOGI
Kunci = AHMADAHMA
Cipherteks = TLWNRLVSJ

Pada proses enkripsi jika nilai lebih dari 25 semisal 40, maka nilainya dikurangi 25 sesuai dengan tabel nilai, maka 40 - 25 = 15 maka 15 = P.

3.2 Algoritma One Time Pad

Algoritma *One Time Pad*merupakan jenis algoritma *substitutional alphabetic*yang menukar huruf dari suatu kalimat menjadi huruf lain, pada penelitian ini algoritma *One Time Pad*digunakan untuk mengamankan pesan email yang akan dikirimkan, Dengan melakukan enkripsi terhadap pesan "HABIBIE" dengan kunci yang digunakan sesuai panjang pesan sebanyak panjang pesan n=7, kunci yang digunakan adalah "UZUMAKI", berikut adalah prosesnya
PESAN = HABIBIE
KUNCI = UZUMAKI
Langkah pertama yang harus dibuat adalah membuat tabel, seperti di bawah ini :

Tabel 3. Proses enkripsi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

Dari tabel diatas dilakukanlah proses enkripsi dengan menerapkan algoritma *One Time Pad*, berikut adalah hasil prosesnya

1. Ubah menjadi kode ASCII dan biner untuk kata HABIBIE dan UZUMAKI, sehingga didapat hasil sebagai berikut:

Karakter	ASCII	BINER
H	72	01001000
A	65	01000001
B	66	01000010
I	73	01001001
B	66	01000010
I	73	01001001
E	69	01000101

Hal yang sama dilakukan pada kunci

U	85	01010101
Z	90	01011010
U	85	01010101
M	77	01001101
A	65	01000001
K	75	01001011
I	73	01001001

2. Pesan di-XORkan dengan kunci maka akan diperoleh
   00011101 00011011 00010111 00000100 00000011 00000010 00001100
3. Untuk memperoleh plainteks kembali, penerima pesan cukup mengubah lagi plainteks menjadi ASCII dan meng-XORkan kembali dengan kunci brikut:

1. Hasil *ciphertext*
   10100010 10100000 00100001 00000001 11100011 00000000 00000000
2. Hasil binary *ciphertext* di XOR kembali dengan kunci UZUMAKI, seperti dibawah ini

U	85	01010101
Z	90	01011010
U	85	01010101
M	77	01001101
A	65	01000001
K	75	01001011
I	73	01001001

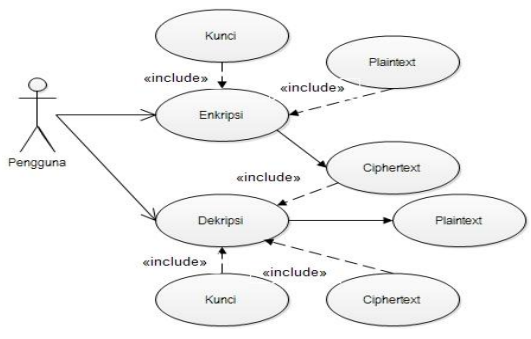
3. Setelah melalui proses XOR Hasilnya sebagai berikut:
   01001000 01000001 01000010 01001001 01000010 01001001 01000101

   Hasil proses XOR di konversi menjadi ASCII hasilnya adalah HABIBIE.

3.3 Pemodelan Sistem

Pemodelan sistem merupakan gambaran dari sistem yang penulis rancang untuk menggambarkan bagaimana sistem bekerja dalam hal ini adalah algoritma *Vigenere Cipher* dan *One Time Pad* sebagai algoritma enkripsi dan dekripsi pesan teks.

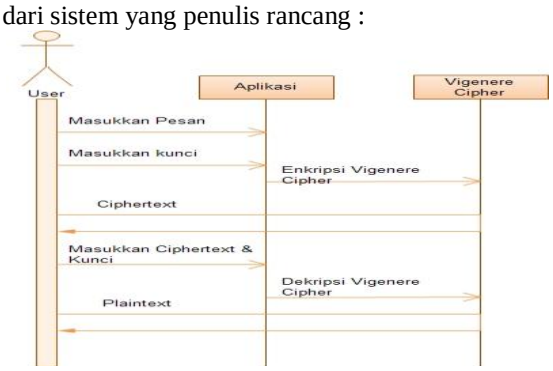
1. Diagram Use Case
   Diagram use case digunakan untuk memberikan gambaran kebutuhan perangkat lunak secara *visual*. Berikut adalah diagram *use case* dari sistem yang penulis rancang :



Gambar 9. Use Case Diagram Sistem

Gambar 9 menampilkan prosedur kerja pengguna dalam melakukan enkripsi dan dekripsi pesan, pengguna melakukan enkripsi harus memerlukan kunci dan *plaintext* agar proses berhasil dan menghasilkan *ciphertext* sedangkan untuk proses dekripsi diperlukan kunci dan *ciphertext* untuk menghasilkan plaintext.

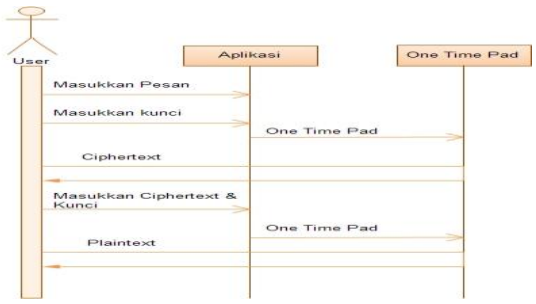
2. Sequence Diagram Vigenere Cipher
   Berikut adalah *sequence diagram vigenere cipher* dari sistem yang penulis rancang :



Gambar 10. Sequence Diagram Vigenere Cipher Sistem

3.

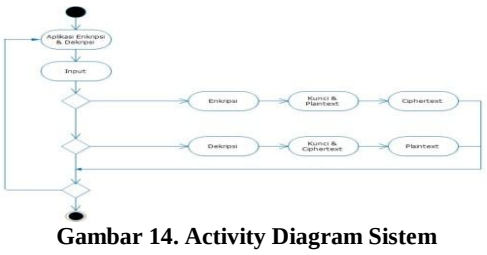
4. Sequence Diagram One Time Pad
   Berikut adalah *sequence diagram One Time Pad* dari sistem yang penulis rancang :



Gambar 11. Sequence Diagram One Time

Pad Sistem

5. Activity Diagram
   Berikut adalah Activity Diagram dari sistem yang penulis rancang, berdasarkan kebutuhan yang ada :



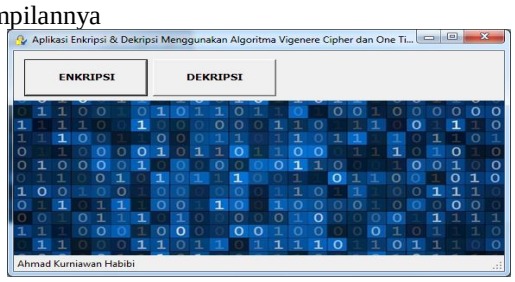
Gambar 14. Activity Diagram Sistem

IV. PEMBAHASAN

Implementasi sistem program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

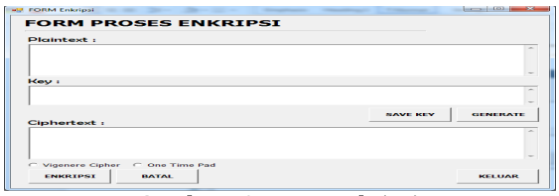
4.1 Pengujian Sistem

Aplikasi kriptogragi algoritma *Vigenere Cipher* dan *One Time Pad* yang penulis rancang menggunakan Microsoft Visual Basic.Net 2008 berhasil dibuat dengan baik, berikut adalah tampilannya



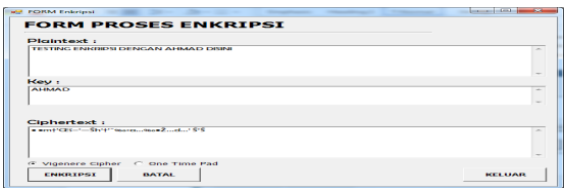
Gambar 15. Form Utama

Gambar 15 merupakan form utama yang digunakan untuk memanggil form enkripsi dan dekripsi, pengujian pertama penulis mengakses form enkripsi dengan menekan tombol enkripsi dan muncul form seperti berikut:



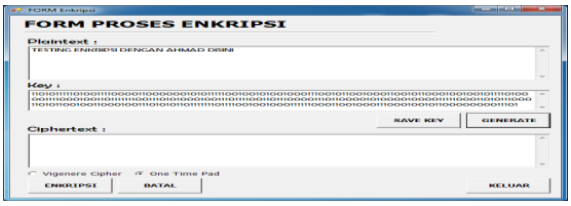
Gambar 16. Form Enkripsi

Form enkripsi digunakan untuk melakukan proses enkripsi terhadap *plaintext*, pada form gambar 16 tampak beberapa informasi seperti textbox plaintext, textbox key, tombol save key yang digunakan untuk menyimpan kunci, tombol generate digunakan untuk menghasilkan kunci secara acak untuk algoritma *one time pad*, sebagai contoh awal penulis memasukkan plaintext dan mendapatkan kunci sebagai berikut:



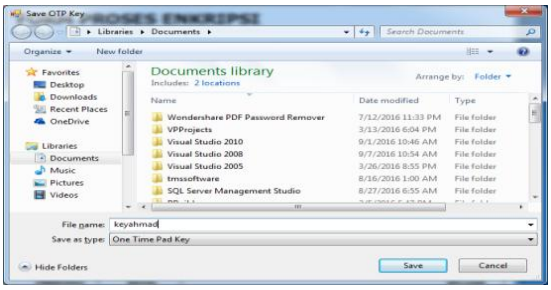
Gambar 17. Proses Enkrips Vigenere Cipher

Gambar 17 merupakan proses enkripsi terhadap plaintext dengan menggunakan algoritma *vigenere cipher*, berikutnya adalah melakukan enkripsi dengan algoritma *one time pad* untuk plaintext yang sama, berikut tampilannya



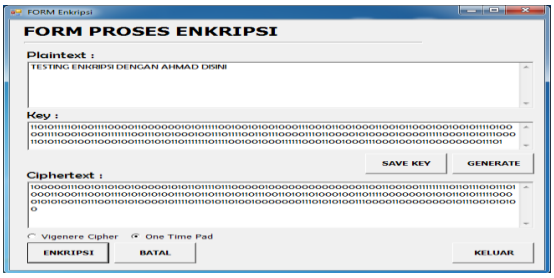
Gambar 18. Isian Plaintext dan Key

Tampak pada Gambar 18, plaintext dan key yang dihasilkan berdasarkan generate yang dilakukan dengan menekan tombol generate, key yang dihasilkan dalam *binary code* berikutnya hasil key supaya tidak hilang disimpan dalam file dengan cara menekan tombol *save key* hingga muncul form save dialog berikut :



Gambar 19. Save Key

Gambar 19 penulis memasukkan nama filenya adalah KeyAhmad dan kemudian disimpan di folder My Document, setelah itu berikutnya adalah menekan tombol enkripsi dan hasilnya sebagai berikut:



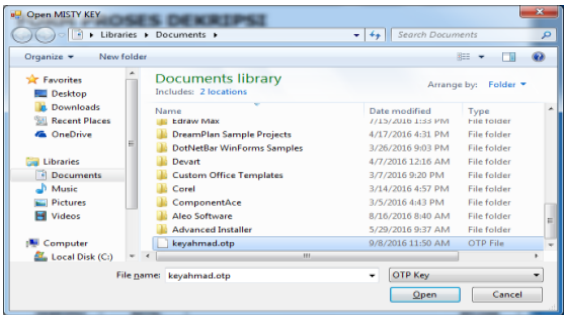
Gambar 20. Ciphertext

Gambar 20 menampilkan *ciphertext* hasil enkripsi, dimana hasil ciphertext ini kemudian diuji kembali untuk proses dekripsi, untuk proses dekripsi penulis menguji untuk untuk algoritma *one time pad* berikut adalah form dekripsi yang penulis rancang :

Gambar 21. Form Dekripsi One Time Pad

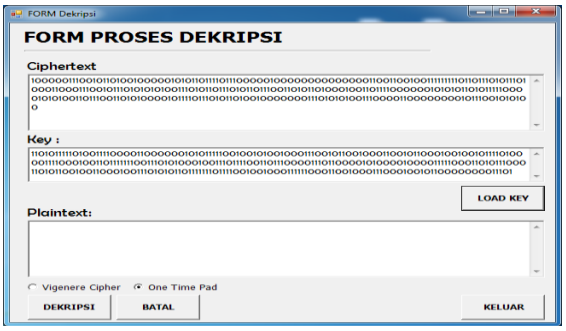
Gambar 21 merupakan form dekripsi yang penulis rancang dan pada gambar penulis sudah memasukkan hasil *ciphertext* kedalam *textbox ciphertext*, kemudian untuk melakukan proses dekripsi diperlukan kunci, untuk mengambil kunci bisa digunakan tombol *load key* dan mengambil kunci dan hasilnya sebagai berikut:

ISBN : 978-623-7297-51-2



Gambar 22. Load Key

Setelah memilih key yang diinginkan kemudian tekan tombol Open dan hasilnya sebagai berikut:



Gambar 23. Hasil Key

Setelah menentukan ciphertext dan kunci yang diinginkan berikutnya adalah melakukan proses dekripsi, dan hasilnya sebagai berikut:

Gambar 24. Hasil Dekripsi One Time Pad

Gambar 24 menampilkan proses dekripsi dari *ciphertext* dan hasil *plaintext* dekripsi sama dengan pesan asli, hasil ini membuktikan proses enkripsi dan dekripsi berjalan dengan baik.

V. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Proses penyandian teks menggunakan algoritma Vigenere Cipher dan One Time Pad menghasilkan nilai *binary* yang sulit untuk diketahui oleh orang awam.
2. Penerapan algoritma Vigenere Cipher dan One Time Pad untuk mengamankan pesan dilakukan dengan membuat sebuah aplikasi kriptografi dengan bantuan bahasa pemrograman Visual Basic.Net 2008
3. Sistem keamanan pesan tergantung seberapa susah kunci yang digunakan, pada penelitian ini kunci yang digunakan untuk algortma *One Time Pad* dalam bentuk binary bukan ASCII sehingga susah untuk ditebak dan juga kunci dihasilkan secara acak.

DAFTAR PUSTAKA

[1] Ariyus Dony, 2009, *Pengantar Ilmu Kriptografi*, Penerbit Andi,Yogyakarta.

[2] Hengky Mulyono, 2013, *Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web*, Seminar Nasional Teknologi Informasi dan Multimedia 2013, ISSN: 2302-3805/

[3] Munir Rinaldi, 2007, *Pengantar Kriptografi, Penerbit Informatika*, Bandung

[4] Muhammad Husnul Arif, 2013, *Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra*, CSRID Journal, Vol.8 No.1 Februari 2016, Hal. 60-72

[5] Winantu Asih, 2012, Jurnal : *Implementasi Algoritma Kriptografi Klasik Ke Dalam Bahasa Pemrograman PHP*, STMIK EL-Rahma

[6] SP. Agustanti, 2010, *Penerapan Algoritma ONE-TIME-PAD (OTP) Untuk Keamanan Layanan Pesan Singkat (Short Messages Services, SMS)*, Jurnal Informatika Global, pp. 47-51.