PENERAPAN VIGENERE CIPHER SUBSTITUSI HOMOFONIK DENGAN MODIFIKASI FIBONACCI UNTUK PENGAMANAN PESAN SMS BERBASIS ANDROID

[1]Gagah Prawono S. P (1110651039).
[2]Ari Eko Wardoyo, S.Kom, M.Kom, [3]Mudafiq Ryan Pratama, S.Kom
Program Studi Teknik Informatika
Fakultas Teknik
Universitas Muhammadiyah Jember
Gghsetia3@gmail.com

ABSTRAK

Perkembangan teknologi ponsel semakin tahun semakin berkembang. Beberapa merk ponsel bermunculan, yakni salah satunya adalah Android yang merupakan ponsel cerdas (*Smartphone*). Android memiliki banyak fitur-fitur yang dapat digunakan yakni salah satunya adalah pengiriman dan penerimaan pesan. Proses pengiriman pesan pun dipertanyakan mengenai keamanan informasi jika seseorang mengirimkan suatu informasi rahasia melalui fasilitas *SMS*. Enkripsi pesan *SMS* dapat menanggulangi terhadap penyadapan informasi rahasia yang akan dikirim sehingga pesan yang dikirim pada penerima dapat di lakukan dekripsi untuk melihat pesan aslinya. Penerapan Vigenere biasa masih memiliki kekurangan yakni pengulangan kunci sehingga pesan yang sama berulang yang dapat dipecahkan dengan metode kasiski dan analisis frekuensi. Dengan kelemahan yang dimiliki Vigenere biasa maka dilakukan modifikasi dengan menggunakan *cipher* substitusi homofonik untuk menyamarkan panjang *ciphertext* dari pesan aslinya serta memodifikasi kunci menggunakan Fibonacci untuk menanggulangi pengulangan kunci, sehingga sulit dipecahkan oleh kriptanalis dan informasi penting yang bersifat rahasia akan aman dari penyadapan sehingga orang yang tidak berkepentingan tidak dapat mengetahui isi pesan aslinya.

***Kata kunci** : Android, SMS, Vigenere, Cipher Substitusi Homofonik, Fibonacci, Enkripsi, Dekripsi*

I Pendahuluan

Di era modern sekarang ini perkembangan teknologi semakin pesat, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga "ponsel cerdas" (*smart phone*) yang memiliki berbagai fungsi seperti *browsing*, *chatting*, *multiplayer games*, transfer data, video *streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun, dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. SMS memiliki banyak kekurangan dari segi keamanan isi pesan, karena layanan SMS masih belum dilengkapi dengan sistem yang menjamin kerahasiaan isi pesan sehingga orang lain tidak dapat mengetahui isi pesan SMS tersebut.

Dalam perkembangan ilmu kriptografi, telah banyak sekali algoritma yang diciptakan untuk menyembunyikan pesan yaitu algoritma kriptografi klasik dan modern. Kriptografi klasik dapat dengan mudah dipecahkan dengan analisis frekuensi atau pun dengan metode kasiski serta metode kerchoff sedangkan Kriptografi modern belum dapat dipecahkan sampai saat ini. Maka dari itu, untuk menjaga keamanannya, pada layanan SMS harus terdapat fitur keamanan isi pesan yakni salah satunya

dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk mendekripsikan sms yang telah di enkripsi. Enkripsi adalah salah satu cara untuk mengamankan sebuah pesan. Dengan menggunakan enkripsi ini diharapkan dapat meningkatkan keamanan pesan data penggunanya. Salah satu Kriptografi klasik yang memiliki kelemahan yakni Vigenere cipher yang dapat di pecahkan dengan menentukan panjang kunci melalui metode Kasiski.

Oleh karena itu, penulis mencoba membuat sebuah aplikasi pengamanan sms menggunakan metode Vigenere Cipher Substitusi Homofonik dengan Modifikasi Fibonacci untuk mengenkripsi pesan SMS yang berjalan pada sistem operasi android sehingga dapat meningkatkan keamanan terhadap serangan kriptanalis.

II Tinjauan Pustaka

A. Sejarah Kriptografi

Kriptografi sudah digunakan sekitar 40 abad yang lalu oleh orang-orang Mesir untuk mengirim pesan ke pasukan yang berada di medan perang dan agar pesan tersebut tidak terbaca oleh pihak musuh walaupun pembawa pesan tersebut tertangkap oleh musuh. Sekitar 400 SM, kriptografi digunakan oleh bangsa Spartan dalam bentuk sepotong papirus atau perkamen yang dibungkus dengan batang kayu.

Pada zaman Romawi kuno, ketika Julius Caesar ingin mengirimkan pesan rahasia pada seorang Jendral di medan perang. Pesan tersebut harus dikirimkan melalui seorang prajurit. Tetapi, karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka di tengah jalan. Di sini Julius Caesar memikirkan bagaimana mengatasinya yaitu dengan mengacak isi pesan tersebut menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh Jendral yang bersangkutan. Sebelumnya Jendral telah diberi tahu bagaimana cara membaca pesan yang teracak tersebut, karena telah mengetahui kuncinya.

Pada perang dunia kedua, Jerman menggunakan mesin enigma atau juga disebut dengan mesin rotor yang digunakan Hitler untuk mengirim pesan kepada tentaranya di medan perang. Jerman sangat percaya bahwa pesan yang dienkripsi menggunakan enigma tidak dapat dipecahkan. Tapi anggapan itu keliru, setelah bertahun-tahun sekutu mempelajarinya dan berhasil memecahkan kode-kode tersebut. Setelah Jerman mengetahui bahwa enigma dapat dipecahkan, maka enigma mengalami beberapa kali perubahan. Enigma yang digunakan Jerman dapat mengenkripsi suatu pesan sehingga mempunyai kemungkinan untuk dapat mendekripsi pesan.

B. Vigenere Cipher

Sandi Vigenere sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E dan seterusnya. Sandi Vigenere terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenere. Tabel Vigenere berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan

dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang

Misalnya, teks terang yang hendak disandikan adalah perintah "Tugas Akhir":

TugasAkhir

Sedangkan kata kunci antara pengirim dan tujuan adalah "MUDAH"

"MUDAH" diulang sehingga jumlah hurufnya sama banyak dengan teks terang:

MUDAHMUDAH

Huruf pertama pada teks terang (T) disandikan dengan menggunakan baris berjudul M, huruf pertama pada kata kunci. Pada baris M dan kolom T di tabel Vigenère, terdapat huruf F. Demikian pula untuk huruf kedua, digunakan huruf yang terletak pada baris U (huruf kedua kata kunci) dan kolom u (huruf kedua teks terang), yaitu huruf O. Proses ini dijalankan sehingga menghasilkan *ciphertext* berupa FOJAZMEKIY

Teks Asli : TugasAkhir

Kunci : MUDAHMUDAH

Teks tersandi : FOJAZMEKIY

Proses sebaliknya (dekripsi), dilakukan dengan mencari huruf teks bersandi pada baris berjudul huruf dari kata kunci. Misalnya, pada contoh di atas, untuk huruf pertama, kita mencari huruf F (huruf pertama teks tersandi) pada baris M (huruf pertama pada kata kunci), yang terdapat pada kolom T, sehingga huruf pertama adalah T. Lalu O terdapat pada baris U di kolom U, sehingga diketahui huruf kedua teks terang adalah U, dan seterusnya hingga didapat perintah "TugasAkhir".

Rumus enkripsi vigenere cipher :

$Pi = (Ci - Ki) \bmod 256$

atau

$Ci = (Pi + Ki) - 256$ kalau hasil penjumlahan *Pi* dan *Ki* lebih dari 256

Rumus dekripsi vigenere cipher :

$Pi = (Ci - Ki) \bmod 256$

atau

$Pi = (Ci - Ki) + 256$ kalau hasil pengurangan *Ci* dengan *Ki* minus

Keterangan:

Ci = nilai desimal karakter ciphertext ke-i

Pi = nilai desimal karakter plaintext ke-i

Ki = nilai desimal karakter kunci ke-i

C. *Short Message Service*(SMS)

Layanan pesan singkat atau surat masa singkat (bahasa Inggris: *Short Message Service* disingkat SMS) adalah sebuah layanan yang dilaksanakan dengan sebuah telepon genggam untuk mengirim atau menerima pesan-pesan pendek. Pada mulanya SMS dirancang sebagai bagian daripada GSM. Tetapi, sekarang sudah didapatkan pada jaringan bergerak lainnya termasuk jaringan UMTS.

Sebuah pesan SMS maksimal terdiri dari 140 bytes, dengan kata lain sebuah pesan bisa memuat 140 karakter 8-bit, 160 karakter 7-bit atau 70

karakter 16-bit untuk bahasa Jepang, bahasa Mandarin dan bahasa Korea yang memakai Hanzi (Aksara Kanji/Hanja). Selain 140 bytes ini ada data-data lain yang termasuk. Adapula beberapa metode untuk mengirim pesan yang lebih dari 140 bytes, tetapi seorang pengguna harus membayar lebih dari sekali.

Pesan-pesan SMS dikirim dari sebuah telepon genggam ke pusat pesan (SMSC dalam bahasa Inggris), di sini pesan disimpan dan mencoba mengirimnya selama beberapa kali. Setelah sebuah waktu yang telah ditentukan, biasanya 1 hari atau 2 hari, lalu pesan dihapus. Seorang pengguna bisa mendapatkan konfirmasi dari pusat pesan ini.

D. *Cipher* Substitusi Homofonik

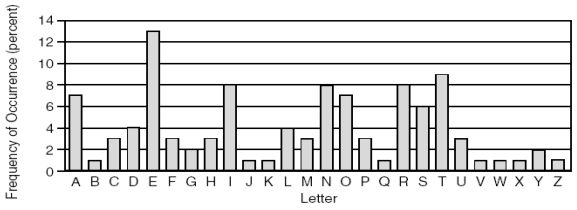
Cipher substitusi homofonik (*homophonic substitution cipher*) adalah seperti *cipher* alphabet-tunggal, kecuali bahwa setiap huruf didalam plainteks dapat dipetakan kedalam salah satu dari unit cipherteks yang mungkin (Munir, 2006). Maksudnya, setiap huruf plainteks dapat memiliki lebih dari satu kemungkinan unit cipherteks. Huruf yang paling sering muncul dalam teks mempunyai lebih banyak pilihan unit cipherteks. Jadi fungsi *ciphering*-nya memetakan satu-ke-banyak (*one-to-many*).

Misal:

huruf E → AB, TQ, YT,UX (homofon)

huruf B → EK, MF, KY (homofon)

Contoh: Sebuah teks dengan frekuensi kemunculan huruf sbb:



Huruf E muncul 13 % → dikodekan dengan 13 huruf homofon

Huruf Plainteks	Pilihan untuk unit cipherteks											
A	BU	CP	AV	AH	BT	BS	CQ					
B	AT											
C	DL	BK	AU									
D	BV	DY	DM	AI								
E	DK	CO	AW	BL	AA	CR	BM	CS	AF	AG	BO	BN	BE
F	BW	CM	CN									
G	DN	BJ										
H	AS	CL	CK									
I	DJ	BI	AX	CJ	AB	BP	CU	CT				
J	BX											
K	DI											
L	AR	BH	CI	AJ								
M	DH	BG	AY									
N	BY	DG	DF	CH	AC	BR	DU	DT				
O	DZ	BF	DX	AK	CG	BQ	DR					
P	BZ	DE	AZ									
Q	DD											
R	AQ	DC	DQ	AL	CE	CF	CV	DS				
S	AP	AN	AO	CD	DW	DV						
T	CB	DB	DP	CC	AD	CY	CW	CX	AE			
U	CA	AM	BA									
V	BB											
W	CZ											
X	BD											
Y	DO	DA										
Z	BC											

Tabel 2.1 Substitusi Homofonik

Unit cipherteks mana yang dipilih diantara semua homofon ditentukan secara acak.

Contoh:

Plainteks: KRIPTO

Cipherteks: **DI CE AX AZ CC DX**

Enkripsi: satu-ke-banyak

Dekripsi: satu-ke-satu

Dekripsi menggunakan tabel homofon yang sama.

E. Fibonacci

Seiring berjalannya waktu maka kemampuan kriptoanalis pun berkembang sampai akhirnya vigenere cipher yang memiliki predikat sandi terkuat pada masa itu pun dapat di runtuhkan oleh metode kasiski. Dengan metode kasiski dapat di ketahui bahwa kelemahan vigenere chipper ini terdapat pada kuncinya karena jika kunci lebih pendek dari pada plaintextnya akan menimbulkan perulangan kata kunci sampai panjang kuncinya sama dengan plantextnya. Pada kali ini penulis akan mengadaptasi bilangan Fibonacci untuk membangkitkan karakter dari mulai panjang kunci di tambah satu sampai sepanjang plantextnya sehingga tidak terjadi perulangan kunci Formulanya sebagai berikut :

U(n) – U(n-1) + U(n-2)

Keterangan :

U = karakter yang dicari

n = urutan karakter yang dicari

Gambar.3.6 *Rumus fibonancci asli*

Namun, jika hanya dimodifikasi seperti itu, akan rentan dilakukan penebakan terhadap plaintextnya, sehingga dalam hal ini, maka penulis memiliki ide untuk memodifikasi pada rumus Fibonacci meenjadi seperti berikut:

Un = U(n-k)+U(n-k+m)

Keterangan : Un= karakter kunci ke-n , k = panjang kunci masukan

Dimana m adalah variable penambahan dalam pembangkitan kunci dan bersifat dinamis karena akan menyesuaikan dengan panjang kunci yang dimasukan. Kunci yang di masukan minimal terbentuk dari dua karakter.

m= 1 +(∑ (karakter_tiap_kunci)mod(k-1))

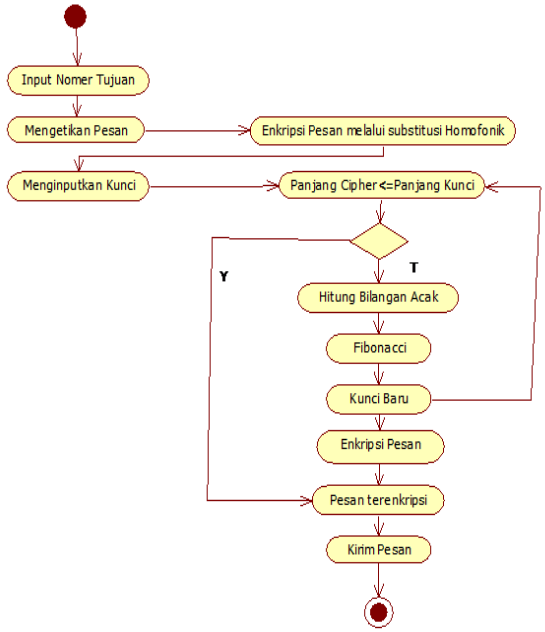
Dengan menggunakan variable m ini rumus di atas akan menjadi lebih dinamis.

F. Android

Android adalah sistem operasi untuk telepon seluler berbasis Linux. Android menyediakan platform terbuka bagi para pengembang untuk membangun aplikasi yang dapat dijalankan di bermacam telepon seluler. Awalnya, Google Inc. membeli Android Inc. yang merupakan pendatang baru dalam teknologi telepon seluler. Kemudian untuk mengembangkan Android, dibentuklah Open Handset Alliance, konsorsium dari 34 perusahaan piranti keras, piranti lunak, dan telekomunikasi, termasuk Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nvidia. Pada saat perilisan perdana Android, 5 November 2007, Android bersama Open Handset Aliance menyatakan mendukung pengembangan standar terbuka pada telepon seluler.

III Metode Penelitian

A. Activity Diagram Pengiriman Pesan



B. Metode Enkripsi Vigenere *Cipher* Substitusi Homofonik dengan Modifikasi Fibonacci.

Tabel homofonik yang digunakan :

Huruf Plaintext	Pilihan untuk unit ciphertext						
A	CD	EW	QW	LN	NS	KA	CP
B	XE	LM	SE	TE	TY		
C	AS	KM	PO	LH	BV	WQ	
D	TX	RW					
E	PI						
F	IU	OY					
G	IO						
H	ER	UY					
I	II	UU	PP				
J	RM						
K	UD						
L	IX						
M	HP						
N	PH	WJ	JK	JU	UJ	1D	
O	QP						
P	PZ						
Q	ZP						
R	AA						
S	EA	AE					
T	1Q	3A					
U	4P	9Q					
V	T4	2Y	5P				
W	WG	GW					
X	RH						
Y	HR	9F	9G				
Z	G7	G8	GP				
A	cd	ew	qw	ln	ns	ka	cp
B	xe	lm	se	te	ty		
C	as	km	po	lh	bv	wq	
D	tx	rw					
E	pi						
F	iu	oy					
G	io						
H	er	uy					
I	ii	uu	pp				
J	rm						
K	ud						
L	ix						
M	hp						
N	ph	wj	jk	ju	uj	1d	
O	qp						
P	pz						
Q	zp						
r	aa						
s	ea	ae					
t	1q	3a					

u	4p 9q
v	t4 2y 5p
w	wg gw
x	rh
y	hr 9f 9g
z	g7 g8 gp
spasi	fG ry Um kN Kl IT
0	et
1	uo
2	tk
3	ol
4	pk
5	kp
6	jh
7	hj
8	mt
9	lz
^	U2
-	h2
+	j2
)	2k
(	mf
.	Lo
&	Xi
%	Xc

$	pl
#	fe
@	ft
~	rk
!	ko
*****	pe
_	pf
=	pv
{	qh
}	la
[	ax
]	ei
|	eg
:	tu
;	ut
<	uf
>	fu
,	pd
?	ps
`	pc
"	pb
/	pw

Tabel inputan *keyboard* hp yang digunakan :

No	0	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
Nilai	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
No	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
Nilai	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
No	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77
Nilai		^	-	+	)	(	.	0	1	2	3	4	5	6	7	8	9	&	%	$	#	@	~	!	*	_
No	78	79	80	81	82	83	84	85	86	87	88	90	91	92	93											
Nilai	=	{	}	[	]	|	:	;	<	>	,	?	`	"	/											

1. Modifikasi Rumus Fibonacci

Un = U(n-k)+U(n-k+m)

Keterangan : Un= karakter kunci ke-n , k = panjang kunci masukan

m= 1 +(∑ (karakter_tiap_kunci)mod(k-1))

2. Rumus Enkripsi Vigenere Cipher

$C_i = (P_i + K_i)$

Keterangan :

C_i = Chiperteks

P_i = Plaintext

K_i = Kunci

Contoh Enkripsi:

Plaintext : Saya TA

Sebelum di enkripsi menggunakan Vigenere cipher terlebih dahulu di enkripsi menjadi salah satu huruf homofon yang ada pada tabel homofonik sesuai dengan unit *ciphertext* secara acak. Misalkan menghasilkan *ciphertext* seperti ini:

Plaintext : Saya TA

Ciphertext : **EAew9fnskN3ACP**

Setelah itu di enkripsi menggunakan Vigenere cipher dengan kunci modifikasi fibonacci yang menghasilkan kunci alternative.

Kunci : AKU

Kunci Alternatif : **AKU_á6Ì-ã¯\? îJ**

Ciphertext: ŧ¢ °℮ :Ný 1 ˢ

Dekripsi :

Ciphertext: ŧ¢ °℮ :Ný 1 ˢ

Kunci Alternatif : **AKU_á6Ì-ã¯\? îJ**

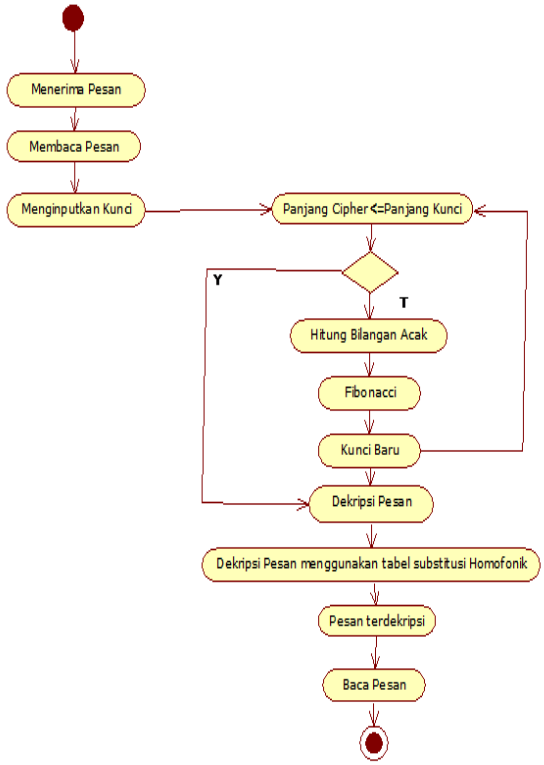
Hasil *ciphertext* akan di dekripsikan menggunakan kunci alternatif sehingga akan menghasilkan *ciphertext* homofonik:

Ciphertext Homofonik: EAew9fnskN3ACP

Kemudian di dekripsikan menggunakan tabel homofon yang sama sehingga menghasilkan:

Plaintext : Saya TA

C. Activity Diagram Penerimaan Pesan

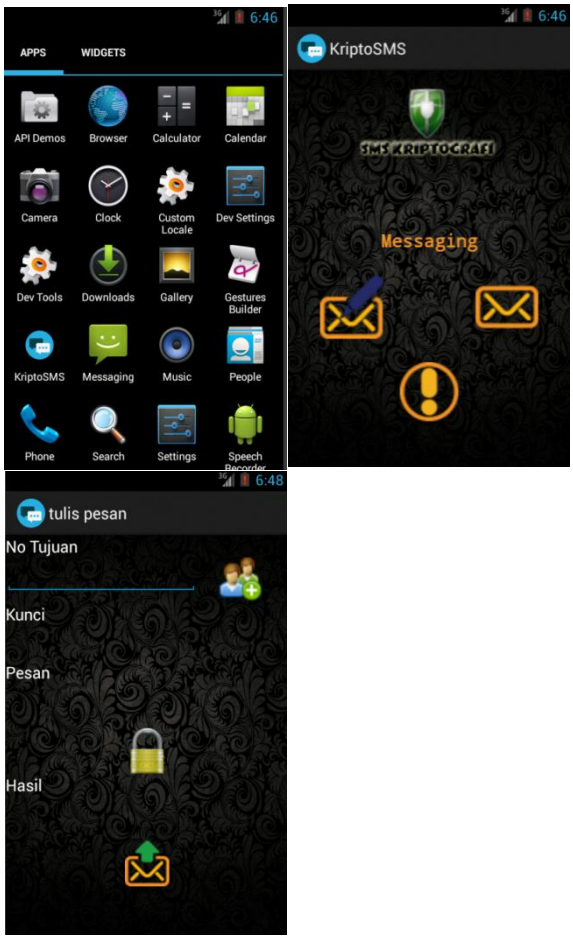


IV. Implementasi dan Pengujian

Pada bagian ini akan di jelaskan secara bertahap(*step-by-step*)mengenai pelaksanaan pengujian yang diterapkan pada *smartphone android* untuk membuktikan bahwa aplikasi ini berjalan dengan baik.

a. Pengujian Menulis dan Mengirim Pesan

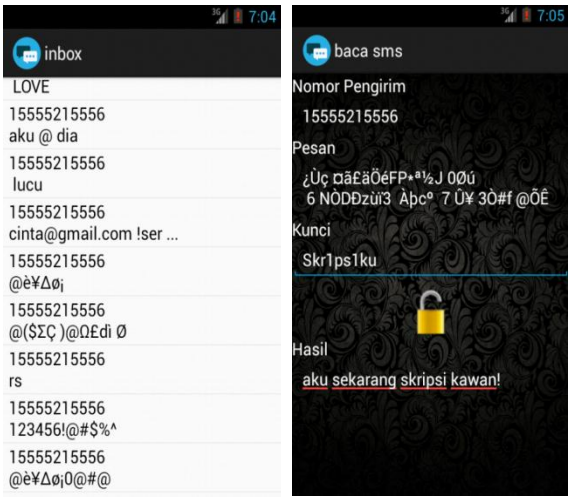
Langkah-langkahnya yakni membuka aplikasi KriptoSMS yang sudah terinstal ke handphone kemudian tulis pesan. Dapat dilihat pada Gambar 4.3.1



Gambar 4.1 Tampilan aplikasi dan tulis pesan

Pada contoh ini pengguna(*user*) menginputkan no tujuan "087757555477", dengan kunci "Skr1ps1ku" Dan pesan berisi "aku sekarang skripsi kawan!" kemudian tekan gambar gembok dibawahnya untuk proses enkripsi lalu akan menghasilkan *ciphertext* kemudian dikirim dengan menekan tombol send.

b. Pengujian pesan yang terenkripsi untuk dilakukan dekripsi pada pesan secara spesifik



Gambar 4.2 Tampilan pesan masuk yang kemudian dipilih untuk di dekripsi

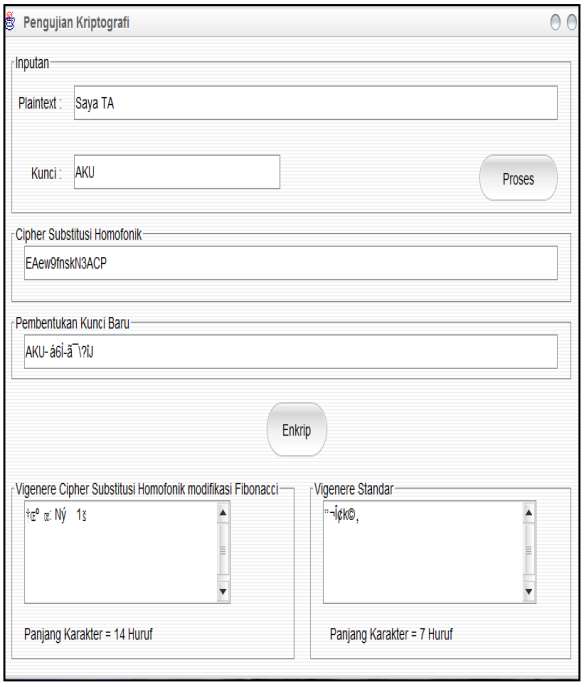
Kemudian pesan yang terenkrip akan dilakukan proses dekrip dengan memasukkan kunci "Skr1ps1ku" dan akan menghasilkan pesan asli yakni "aku sekarang skripsi kawan!".

4.1.3 Pengujian Panjang *Ciphertext* dan Keefektifan Kunci

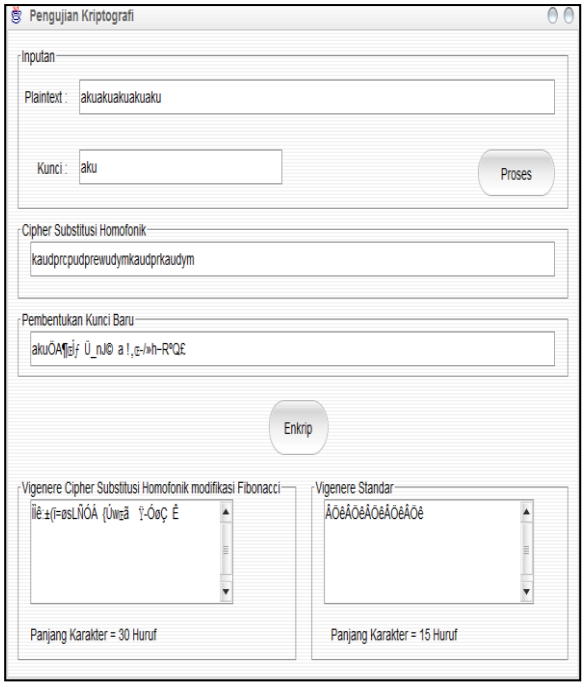
Pengujian dengan membandingkan Vigenere *cipher* substitusi homofonik yang memodifikasi Fibonacci dengan Vigenere standar.

Plaintext : Saya TA

Kunci : AKU



Gambar 4.3 Perbandingan Hasil Enkripsi



Gambar 4.4 Perbandingan Hasil Enkripsi ke-2

Berdasarkan Gambar 4.3 diketahui bahwa pada Vigenere *cipher* substitusi homofonik yang memodifikasi Fibonacci akan menghasilkan *ciphertext* lebih panjang sehingga menyamarkan panjang asli *plaintext* menghasilkan panjang 14 karakter dimana pesan aslinya hanya 7 karakter serta tidak menggunakan pengulangan kunci jika plaintext mengandung karakter yang sama dengan membangkitkan kunci baru secara acak, lihat Gambar 4.4.

Berdasarkan hasil perbandingan ke dua maka didapatkan pada vigenere standar menghasilkan pengulangan kunci yang sama jika plaintextnya terdapat kalimat yang sama berulang.

Plaintext	**Akuakuakuakuaku**	Plaintext “aku” sebanyak 5 kali	Panjang 15 karakter
Kunci	Aku	Kunci diulang sampai panjang plaintex	Panjang 3 karakter

		t terakhir sebanyak 5 kali	
Ciphertext	**ÂÖêÂÖêÂÖêÂÖêÂÖê**	Menghasilkan pengulangan **ÂÖê** sebanyak 5 kali	Panjang 15 karakter

\Tabel 4.1 Enkripsi dengan Vigenere standar

Akan tetapi pada Vigenere *cipher* substitusi homofonik modifikasi Fibonacci menghasilkan enkripsi yang lebih baik dengan melakukan enkripsi homofonik terlebih dahulu berdasarkan tabel huruf homofonik yang diperoleh secara acak dan pembangkitan kunci baru jika panjang pesan lebih panjang dari panjang kunci sehingga kunci tidak mengalami pengulangan yang menyebabkan kalimat yang sama berulang.

Plaintext	**akuakuakuakuaku**	Panjang 15 karakter
Kunci	aku	Panjang 3 karakter
Ciphertext	**ÌÌê:±(ï=øsLÑÓÁ-{ÚwŒãŸ-ÓøÇ-Ê**	Panjang 30 karakter

Tabel 4.2 Enkripsi Vigenere *cipher* substitusi homofonik dengan modifikasi Fibonacci

A. Uji coba hasil *ciphertext* yang beragam pada Vigenere Modifikasi

No	1	2	3	4	5
Plaintext	Coba hasil enkripsi	Coba hasil enkripsi	Coba hasil enkripsi	Coba hasil enkripsi	Coba hasil enkripsi
Homofonik	OPqptyewdfercpaepsixitpijkudpgpspzeaps	MNqpxensknerlnaeunixumpi1dudpgiypzaeps	VBqplmcdumekaaepsixitpiujudpgunpzaeun	KWqplmlnryerlnaeiyixrypijkudpgiypzaeps	RSqptycddfemsaeunixumpi1dudpgiypzaeps
Kunci	c0b4	c0b4	c0b4	c0b4	c0b4
Ciphertext	² O¤ û>‰ Â^°õ² BAëƒ Äý¶Z H-ÿ=|C ÛRb «: –	°~O¤ ÷ɹ : – Â^¹ó² G<ëƒ⊥ ½ý¶!A-ÿ=|<áR bœ¯:–	¹rO¤ÿÿù +š•Â^.æ² BAëƒ Ä ý¶eG-ÿ= |HÖRbœ ¯2‘	ª‡Óøÿÿŋ5 — ¡Â^¹ó² :G ëf⁞Éý¶H-ÿ=|<áRb œ¯:–	µƒO¤ ù+‰ Â ^»ø² G <ëƒ⊥½ý ¶!A-ÿ=| <áRbœ¯: –

Berdasarkan hasil uji coba diatas maka dapat dibuktikan bahwa dengan menggunakan *cipher* substitusi homofonik akan menghasilkan *ciphertext* yang beragam, dikarenakan menggunakan sifat dari homofonik yang akan menghasilkan huruf homofon berdasarkan tabel homofonik yang digunakan dan huruf homofon yang diperoleh secara acak. Akan tetapi, merupakan pesan asli yang sama sehingga menyamarkan pesan asli yang telah di enkripsi.

Berikut ini hasil uji coba *ciphertext* Vigenere Modifikasi pada huruf, angka dan simbol.

B. Uji Coba menggunakan huruf, angka dan simbol

No	1	2	3	4	5
Plaintext	Penerapan Vigenere Cipher Substitusi Homofonik dengan Modifikasi Fibonacci untuk Pengamanan Pesan SMS berbasis Android	matakuliah pemrograman aku mendapatkan nilai yang bagus	200 – 150 = 50	!@#$%^&*O	087757555477 1NT4N & G4G4H
P	118	55	14	10	26
Homofonik	PzpijupipgewpzqwjkklLYiyiopiphpipgpiklMNunpzuypipgumEAymxeeafjiyqsymaepsryUYqphpqpoyqpjupsudittxpijuiolnjuknHPqptxiyoyiyudlnaeiyitOYunseqpjkewatmnundfprujqsymudknPZpiwjioewhpnsjukajudfPZpieaqwwjryAEHPEAkltypipgtyewaeunaeitEWjkrwpgqppsrw	hpqwqsnsudymixiycpuyklpzpihppgqpiopgqwhpqw1dklkaudprithppijutxcdpzcdfjudnsjurywjunixcdpsklwfewphioryteqwioymae	tketetitititutokpetklklknkpet	koftfeplxcU2xipemf2k	etmthjhjkphjkpkpkppkhjhjITuo1D3ApkUJUmxif
P	236	110	28	20	52
Kunci	Key	PemrogramanJava	L0v3	K@c@	N0M3R
Kunci baru	keyäÌÄ¦Ï‡WF÷N"‹ÙmøÑ>6 E¿ÿÐÄ¹ ßζ– Ïù – ¤«Aå Ñ¶F┤Í‼*÷ 4+5ï"É2Æ Á‡┬× ^tK® h◄.– §Õk‡çRdK Léê 6- ?^g¦┘k◄ ┴ '¦&·]f:— ¬Të│YDI¢æ/Ñ·æ: nT yÍØQ-öGe[¢ b┘ mqLéZÖ¿├ª©¶d +äEpQ– —WíóJ7*t«ÕÌôÉ‡ ¬ïáç¶— ~4ËI}H'VçÕK2'r¤ Ë=á¬éÊv_]Ÿb'ÆÃ ë±u`◄†æ÷}cZ×:"k ¥9¤I,&oñ┤†w	PemrogramanJavaAÆUOY± Ö×I#4548• o O*å NI*dçœÇ" ®å¡1 ÇT"TØF ^ÏUOző ÖO!i£ ÙÀ}Ö) #g˜ã"Ì ÷Aý'"½j}Üà»á °Ò«¤í™xKËP	L0v3Ï ¯% X×†«└U' eñ5äL ãc └H	K@c@‹E n ùAò`Y ‼ o £aoc	N0M3R~} …Ðûý | ÙE®┐ ∠ Aú\zã½VO]
P	236	110	28	20	52
Ciphertext Modifikasi	»¿éM³7┬X!¾«n¾ üP×ç<ª,`ªôë6²- û5 …Yá¬èdû[U ‡←»Z A- ¶˜B oßfi£§Îõ/œ /Ω2ú D¿Ù» áf‡ ┤=ÛfWÁÝ¼kÁY]« fr³ÒßπmÕ+^ïÿ¶ ,Èñ.ç‹Ã_}Â½,←O¯ F←R%Ï¹tò6L wkµ ØÀ‼wÌopäÒðVÈ K- }U-9+ÎœT¾ÝÆúq Å=Mº¡P¶D°k1,t BK\!øè®/¯Í¢ w» HfÂ©'ä ,)ü. áË ↑n 6+_*Úxr EIERFANLEUT"¯ é—ßaŠøî	•† ,OÞéäUàOâÅç ·ËíË;)JHV?GH " Œ¤Åy e < x¡H(BC[ÈR2é #F£÷;¼AA°ýA Ì³fêol8µ‹bH3ç K›šÑ QýDZz ±p' 0#Ï'iAI*S)G`Wñ,+µ	A›U§ä# Ì @ú'‖ wOIv ~M¼¾Ì´ý O¹ù h¼	¶¯E´ñ0 Uq' G'N†Ï O5K &Î	³¤°§°èåêð@ cgpÅ6hmE .bÆâM– "KÏÑW_tm -"©… j ß'äß ÙË - F
P	236	110	28	20	52
Ciphertext Standar	»ËçÐ×ÙÜÆç‹»å ÒÊçÐ×Þ‹¨âÛÍÞÝ …ÌàçÌßÎïàøâ‹-èØ ÔßÚÓâÖ…ÝÐÓàÌ Ó™¸ÔÝÔËâÖÆÌÔ …¿ÔÇèÙÆÜÏÎ™à ÓÎàÐ™»ÊçÒÆæÌ ÓÚÙ…ÉÐØÚÙ…Ì¸ ¸™ÍÊëÍÆÌÔØ™–Ó ÝÝÔâÏ	½ÆäOUUÞEI È °ÆäÒ¿ÌßÒÜ Èà ÎÌäjÎÛÏ´Æ ÝÓäÒÓÏ Ï×¶ Ãß ÈÆÜÜ È ÓÈäÔ	~`¦S_P§h¦P ³S `	l †dp ‰js ¡	~h.j‡…e.h †…gmd¢d ›Sxnw…z† –
P	118	55	14	10	26

V. Penutup

A. Kesimpulan

Untuk menghasilkan Vigenere *cipher* yang kuat dengan memiliki karakteristik *unbreakable cipher*, dilakukan modifikasi pada metode Vigènere *cipher* dengan menggunakan *cipher* substitusi homofonik pada *plaintext* sebelum di enkrip menggunakan Vigènere sehingga menghasilkan *ciphertext* yang lebih panjang dari *plaintext* dan modifikasi pada kunci Vigenerenya menggunakan rumus Fibonacci yang telah dimodifikasi sehingga menghasilkan kunci yang dinamis.

Berdasarkan analisis dan implementasi yang sudah dijabarkan di bab sebelumnya, metode ini memiliki beberapa kelebihan yakni:

1. Algoritma Vigènere *cipher* substitusi homofonik dengan modifikasi fibonacci ini lebih baik daripada algoritma Vigènere *cipher* yang standar.
2. Menghasilkan *ciphertext* yang beragam namun merupakan pesan asli yang sama.
3. Hasil enkripsi *(Chipertext)* yang dihasilkan lebih panjang dari pesan asli mengakibatkan pesan enkripsi tidak mudah untuk dipecahkan oleh kriptanalis.
4. Menghilangkan kelemahan dari metode Vigenere standar yakni pengulangan kunci pada pesan yang sama berulang.

B. Saran

Dari implementasi dan pembahasan metode ini tentu saja masih jauh dari kata sempurna. Masih banyak perbaikan yang diperlukan hanya untuk mencapai metode yang cukup baik. Salah satunya pada proses implementasi program, yang masih sederhana dan masih dibawah standard.

Adapun beberapa saran yang akan disampaikan penulis mengenai metode maupun implementasi program Vigenere *cipher* substitusi homofonik dengan modifikasi fibonacci:

1. Menambahkan pemberitahuan saat pesan masuk, sehingga untuk mendekripsikannya akan lebih cepat.
2. Jika pesan asli dan kunci yang digunakan sangat panjang, maka operasi perkalian akan membutuhkan waktu yang cukup lama.

Daftar Pustaka

Safaat, Nazruddin. 2012. *Pemrograman Aplikasi Mobile Smartphone dan Table PC Berbasis Android*. Bandung:Penerbit INFORMATIKA Bandung.

Safaat, Nazruddin. 2013. *Aplikasi Berbasis Android*. Bandung:Penerbit INFORMATIKA Bandung.

Tohari, Hamim. 2013. *Analisis serta Perancangan Sistem Informasi melalui Pendekatan UML*. Yogyakarta:Penerbit ANDI

Munir, Rinaldi. 2006. *Kriptografi*. Bandung:Penerbit INFORMATIKA.

Anjari, B.G. 2011. *Enkripsi SMS (Short Message Service) Pada Telepon Selular Berbasis Android.* Jurusan Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

Pribadi, Jaisyalmatin. 2013. *Pengembangan Vigenere Cipher menggunakan Deret Fibonaci.* Program Studi Teknik Informatika, Institut Teknologi Bandung.

Yudhistira. 2012. *Modifikasi Vigenere Cipher dengan Mengkombinasikan Vigenere 26 dan 256 Karakter*. Program Studi Teknik Informatika, Institut Teknologi Bandung.