Aplikasi Enkripsi Pesan Pada iOS Menggunakan Algoritma Kriptografi Klasik Yang Diperbaharui

William
13508032

Program Studi Teknik Informatika
Sekolah Teknik Elektro Dan Informatika
Institut Teknologi Bandung
if18032@students.if.itb.ac.id

Abstrak— **Melalui makalah ini akan dibahas mengenai rancangan algoritma yang dapat digunakan untuk melakukan enkripsi dan dekripsi pesan dengan memanfaatkan algoritma kriptografi klasik yang diimplementasikan pada iOS. Hal ini dirasa perlu karena pengiriman pesan sangat banyak dilakukan, terutama dengan media *smart phone*, yang menggunakan sistem operasi iOS. Algoritma yang digunakan pada aplikasi ini memanfaatkan sifat-sifat unik dan khas dari algoritma kriptografi klasik yang telah dianggap *obsolete* menjadi algoritma baru yang lebih aman untuk digunakan.**

Kata Kunci— **algoritma, enkripsi, dekripsi, iOS**

I. Latar Belakang

Manusia telah menggunakan pengiriman pesan sebagai metode berkomunikasi sejak jaman dahulu. Seiring dengan perkembangan peradaban dan teknologi, mulai dirasakan kebutuhan akan kerahasiaan dari pesan-pesan yang dikirimkan, agar tidak dapat diketahui isinya oleh pihak yang tidak diinginkan. Metode untuk menjaga kerahasiaan pesan ini bernama metode enkripsi, yang adalah metode dimana dilakukan upaya-upaya pemanipulasian sebuah pesan sehingga pesan tersebut akan terlihat seperti kumpulan teks yang tidak ada artinya, apabila pembaca tidak mengetahui cara membaca yang benar.

Ada banyak algoritma enkripsi klasik yang sudah ditemukan dan dikembangkan. Namun, sebagian besar dari algoritma tersebut sudah *obsolete* atau tidak aman untuk digunakan lagi, karena sudah ditemukan cara untuk menyerangnya. Namun, dengan melakukan perubahan dan pengkombinasian yang tepat, maka bisa didapatkan sebuah algoritma yang aman untuk digunakan.

Dengan pertimbangan bahwa pengiriman pesan sekarang ini banyak dilakukan menggunakan *smart phone*, dan banyaknya pengguna *smart phone* milik *apple*, maka diputuskan bahwa rancangan algoritma ini akan diimplementasikan pada iOS, yang adalah sistem operasi untuk *gadget –gadget* keluaran *apple*.

II. Dasar Teori

Kata kriptografi berasal dari bahasa Yunani, yaitu *kriptos* yang berarti tersembunyi atau rahasia, dan *graphein* yang berarti menulis. Dari sini dapat diartikan bahwa kriptografi adalah suatu praktek atau cara untuk mendapatkan komunikasi yang aman walau ada pihak ketiga yang berusaha mencuri dengar. Ada bermacam-macam metode enkripsi yang dapat digunakan. Metode enkripsi yang sederhana sehingga dapat dikerjakan cukup menggunakan pensil dan kertas saja dapat disebut sebagai metode enkripsi klasik. Metode ini biasanya hanya menggunakan pengembangan dari cipher substitusi dan transposisi saja.

Cipher transposisi adalah suatu metode enkripsi yang menggeser posisi dari karakter pada plain teks sesuai aturan yang sudah ditetapkan sebelumnya. Sedangkan, cipher substitusi adalah metode enkripsi yang mengganti hururf-huruf pada plain teks dengan huruf lainnya sesuai aturan yang telah disepakati sebelumnya. Namun, urutannya dalam teks tidak diganti. Kedua cipher ini relatif mudah untuk diimplementasikan dan diserang. Cipher transposisi dapat dideteksi dengan metode distribusi frekuensi, dan diserang dengan metode *anagramming*. Sementara, cipher transposisi dapat diserang dengan melakukan analisis distribusi frekuensi dari cipherteks. Selain kedua cipher ini, ada beberapa metode enkripsi lainnya yang relatif lebih sulit diserang, seperti cipher vigenere, dan cipher playfair.

Cipher vigenere sebenarnya adalah beberapa cipher substitusi dalam satu sekuens, dengan jumlah pergeseran yang berbeda-beda. Pengerjaan cipher vigenere dapat dibantu dengan bujur sangkar vigenere. Berbeda dengan cipher lainnya, cipher playfair melakukan enkripsi pada pasangan hufur (bigram) sehingga lebih sulit untuk dipecahkan dengan metode analisis frekuensi. Dengan mengetahui tiga aturan dasar untuk melakukan substitusi bigram, setelah membentuk buhur sangkar playfairnya, maka enkripsi dan dekripsi dapat dilakukan dengan relatif mudah. Kelemahan kedua metode ini adalah apabila cipher teksnya cukup panjang, maka deteksi dan penyerangan dapat dilakukan dengan tidak terlalu sulit.

III. Solusi Persoalan

Masalah utama yang terdapat pada tugas akhir ini adalah bagaimana cara melakukan modifikasi dari suatu algoritma enkripsi klasik untuk mengenkripsi pesan yang memiliki tingkat keamanan yang lebih daripada algoritma kriptografi klasik biasa, dan mengimplementasikannya pada *smart phone* dengan sistem operasi iOS.

Permasalah utama yang dimiliki algoritma enkripsi klasik adalah bahwa algoritma ini sangat bergantung pada

kerahasiaan algoritma enkripsi yang digunakan. Apabila algoritma yang digunakan sudah diketahui, pada proses penyerangan dapat dilakukan dengan mudah. Walau demikian, ada beberapa cara yang dapat dilakukan untuk meningkatkan kekuatan algoritma enkripsi, seperti menggunakan kata kunci yang panjang, melakukan enkripsi bertingkat (perulangan), serta merancang algoritma tersebut untuk menerapkan skema *confusion-diffusion*.

A. *Analisis Kebutuhan Solusi*

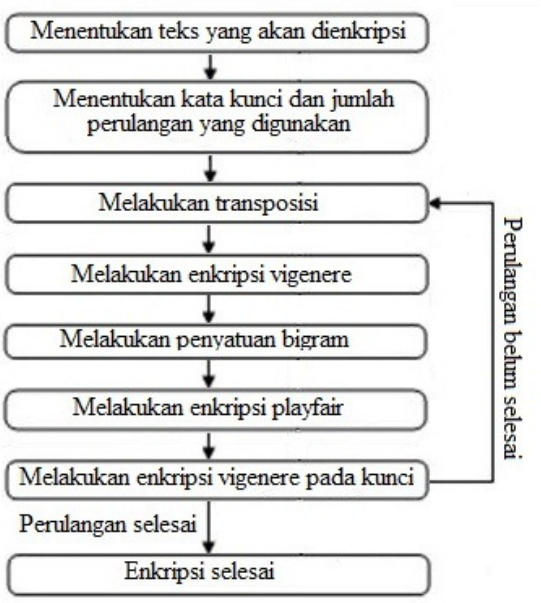
Dalam perancangan sebuah algoritma, ada beberapa hal yang perlu diperhatikan agar algoritma tersebut menjadi sebuah algoritma yang kuat dan tahan terhadap serangan-serangan yang dilancarkan oleh pihak yang tidak diinginkan.

Beberapa sifat yang penting untuk dimiliki adalah ketahanan dari serangan *brute force*. Ketahanan terhadap metode kriptanalisis standard, kemampuan beradaptasi, dan kesederhanaan.

B. *Rancangan Solusi*

1) Rancangan skema enkipsi

Pada rancangan algoritma ini, enkripsi dapat dilakukan pada 90 karakter standar yang tersedia pada papan tuts dari *iPhone*. Sedangkan kata kuncinya panjangnya adalah bebas; tidak dibatasi. Untuk skema enkripsi yang dilakukan dapat dilihat pada gambar 1 dibawah.



Gambar 1 Skema enkripsi yang dilakukan

Setelah menentukan plain teks yang ingin dienkripsi dan kata kunci yang digunakan, langkah yang harus dilakukan adalah menentukan jumlah perulangan yang dilakukan. Jumlah perulangan didapat dari rata-rata nilai integer kunci dengan pembulatan kebawah. Untuk nilai masing-masing karakter kunci tersebut, dapat dilihat pada gambar 2 dibawah.

A	1	X	24	k	47	&	70
B	2	Y	25	l	48	@	71
C	3	Z	26	m	49	"	72
D	4	0	27	n	50	.	73
E	5	1	28	o	51	,	74
F	6	2	29	p	52	?	75
G	7	3	30	q	53	!	76
H	8	4	31	r	54	`	77
I	9	5	32	s	55	[	78
J	10	6	33	t	56	]	79
K	11	7	34	u	57	{	80
L	12	8	35	v	58	}	81
M	13	9	36	w	59	#	82
N	14	a	37	x	60	%	83
O	15	b	38	y	61	^	84
P	16	c	39	z	62	*	85
Q	17	d	40	-	63	+	86
R	18	e	41	/	64	=	87
S	19	f	42	:	65	_	88
T	20	g	43	;	66	\	89
U	21	h	44	(	67		90
V	22	i	45	)	68		
W	23	j	46	$	69		

Gambar 2 Representasi nilai integer pada karakter kunci

Langkah pertama enkripsi adalah melakukan transposisi pada plain teks. Jumlah pergesera yang dilakukan untuk setap karakter plain teks ini bergantung pada nilai integer dari kunci yang digunakan. Jadi misalkan kuncinya adalah William, maka untuk karakter pertama dilakukan pergeseran sejauh 23 karakter, karakter kedua sejauh 45 karakter, dan setrusnya.

Setelah melakukan transposisi, langkah berikutnya adalah melakukan enkripsi vigenere. Enkripsi vigenere pada tahap ini sama dengan enkripsi vigenere biasa.

Setelah melakukan enkripsi vigenere, dilakukan penyatuan bigram sebagai persiapan untuk enkripsi playfair. Untuk algoritma ini, cara menyatukan bigramnya adalah dengan menyatukan huruf pertama dan terakhir dari plain teks menjadi satu bigram, dan pasangan huruf berikutnya (huruf kedua dari depan dengan huruf kedua dari belakang) sebagai bigram berikutnya. Apabila jumlah karakter plain teks ganjil, perlu diingat untuk menambahkan karakter *padding*.

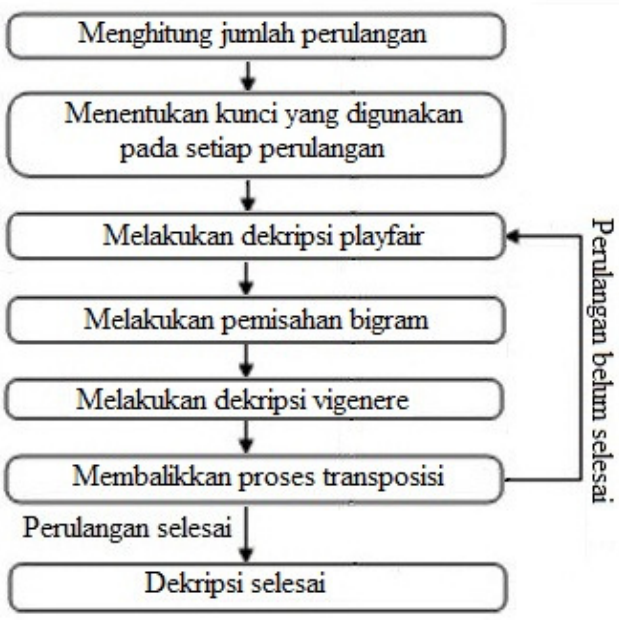
Setelah bigram selesai dibentuk, maka teks sudah siap untuk dienkripsi dengan enkripsi playfair. Secara umum, enkripsi ini sama dengan enkripsi playfair biasa. Namun perlu diperhatikan beberapa perubahan aturan, seperti tidak dilakukannya aksi substitusi pada bigram yang berisi karakter yang sama. Selain itu, bujur sangkar kuncinya dibentuk berukuran 9 baris x 10 kolom.

Langkah terakhir adalah melakukan enkripsi vigenere pada kunci. Kunci yang sedang digunakan pada iterasi ini berlaku sebagai plain teks, dan kunci utama sebagai kata kuncinya. Cipher teksnya menjadi kunci yang digunakan untuk iterasi berikutnya apabila perulangan belum selesai.

Apabila jumlah perulangan yang harus dilakukan kurang dari 2, maka pada tahap ini enkripsi sudah selesai. Namun

apabila belum selesai, ulangi mulai dari proses transposisi menggunakan kata kunci yang baru.

2) Rancangan skema dekripsi



Gambar 3 Skema enkripsi yang dilakukan

Untuk proses dekripsi, yang pertama kali harus dilakukan adalah menghitung jumlah perulangan yang dilakukan, serta mencari tahu kata kunci yang digunakan untuk setiap perulangan. Untuk mendapatkan kata kunci ini, caranya adalah sama yaitu dengan mengenkripsi kata kunci utama dengan enkripsi vigenere sebanyak jumlah perulangan yang dilakukan.

Setelah mengetahui kata kunci yang digunakan untuk setiap perulangan, langkah pertama proses dekripsi adalah dengan melakukan dekripsi playfair. Aturan dekripsi playfair ini secara umum sama dengan dekripsi playfair biasa. Namun seperti sebelumnya, tidak dilakukan aksi terhadap bigram yang berisikan pasangan karakter yang sama.

Setelah dekripsi playfair selesai dilakukan, langkah berikutnya adalah dengan melakukan pemisahan bigram. Cara untuk melakukan pemisahan bigram disini adalah dengan mengambil karakter pertama pada setiap bigram secara terurut, dan menyatukannya dengan setiap karakter kedua dari bigram tersebut.

Langkah berikutnya adalah melakukan dekripsi vigenere. Dekripsi vigenere pada langkah ini adalah sama dengan dekripsi vigenere biasa.

Setelah dekripsi vigenere selesai dilakukan, langkah berikutnya adalah membalikkan proses transposisi. Cara untuk membalikkan proses transposisi ini adalah dengan membalikkan proses yang dilakukan pada saat enkripsi.

Apabila jumlah perulangan kurang dari dua, maka pada tahap ini proses dekripsi telah selesai dilakukan. Namun apabila belum, perulangan dilakukan mulai dari proses dekripsi playfair. Perlu diperhatikan bahwa kata kunci yang digunakan haruslah kata kunci yang tepat; sesuai dengan kata kunci yang telah ditentukan sebelumnya.

C. Analisis rancangan solusi

1) Penggunaan aturan transposisi

Algoritma transposisi adalah algoritma yang sangat standard dan relatif mudah diimplementasikan, dan dilakukan perubahan. Namun, algoritma ini sangat mudah dirubah dan diberikan variasi. Karena adanya aturan perulangan, sedikit saja perubahan pada aturan transposisinya, maka hasil enkripsi yang didapat akan jauh berbeda.

2) Penggunaan enkripsi vigenere

Enkripsi vigenere pada algoritma ini digunakan terutama karena sifat alaminya, yang dapat menyembunyikan karakter frekuensi dari huruf-huruf yang digunakan pada plain teks. Selain itu, algoritma ini relatif simpel dan sederhana untuk dimengerti dan diimplementasikan.

3) Penggunaan enkripsi playfair

Enkripsi playfair adalah salah satu algoritma enkripsi klasik yang relatif kuat bila dibandingkan dengan algoritma lainnya yang sudah ada. Namun, alas an utama pemilihan penggunaan algoritma playfair ini adalah karena algoritma ini melakukan enkripsi terhadap pasangan bigram. Hal ini menyebabkan perubahan satu karakter pada plain teks akan mengubah dua karakter pada cipher teksnya. Sifat ini akan dimanfaatkan untuk mendapatkan efek *confusion-diffusion*.

4) Penggunaan aturan perulangan

Perulangan dilakukan untuk memperkuat ketahanan algoritma ini dari penyerangan. Dengan perulangan, maka penyerang akan menjadi lebih sulit untuk mendapat plain teks, maupun kunci yang digunakan untuk mendekripsi cipher teksnya.

5) Pemanfaatan sifat *confusion-diffusion*

Sifat *confusion-diffusion* disini maksudnya adalah sifat yang mengakibatkan keseluruhan isi cipher teks berubah apabila ada sedikit saja perubahan pada plain teks, maupun kunci yang digunakan. Apabila sifat ini diimplementasikan dengan benar, maka perubahan satu karakter saja pada plain teks akan mengakibatkan perubahan pada seluruh karakter cipher teksnya.

6) Penggunaan kunci yang selalu berubah untuk setiap perulangan

Sama seperti penggunaan aturan perulangan, adanya aturan yang melakukan perubahan pada kunci yang digunakan untuk setiap iterasi diharapkan menjadikan algoritma ini lebih tahan terhadap penyerangan.

D. Analisis kemungkinan penyerangan

Selama belum ditemukannya celah keamanan dalam algoritma ini, maka metode penyerangan yang mungkin dilakukan hanyalah dengan metode *brute force*. Namun, metode ini sangat tidak efisien untuk dilakukan, karena selain jumlah percobaan yang harus dilakukan sangatlah banyak, tanpa menggunakan algoritma pengenalan teks yang sempurna, komputer akan kesulitan menentukan apakah plain teks hasil dekripsinya adalah plain teks yang benar memiliki makna

yang berarti, atau apakah plain teks tersebut hanyalah berisikan karakte-karakter yang tidak berarti.

Namun apabila penyerangan dengan metode brute force tetap dilakukan, rumus umum untuk menentukan jumlah percobaan yang harus dilakukan adalah:

$$\sum_{x=1}^{n} 90^x$$

Dengan n adalah panjang karakter kunci yang digunakan, dan 90 merupakan jumlah karakter yang dapat dikenali dan dienkripsi pada algoritma ini. Perhitungan dilakukan menggunakan sigma karena, tanpa mengetahui panjang kunci yang sebenarnya, penyerang haruslah melakukan percobaan terhadap seluruh kemungkinan kunci, dimulai dari kunci dengan panjang satu karakter saja.

Hal ini berarti, bahwa untuk setiap penambahan panjang karakter kunci, maka jumlah percobaan yang harus dilakukan akan meningkat secara eksponensial.

Sebagai contohnya, apabila sebuah teks dienkripsi dengan panjang kunci 37 karakter. Walaupun apabila penyerang yang melakukan serangan adalah orang yang sangat beruntung sehingga dapat menemukan kunci yang benar pada percobaan pertama saat sudah mencapai kunci dengan panjang 37 karakter, ia tetaplah harus mencoba setiap kemungkinan kunci, mulai dari yang panjangnya 1 sampai 36 karakter. Hal ini berarti, jumlah seluruh percobaan yang harus dilakukan olehnya adalah $\sum_{x=1}^{36} 90^x$ yang jumlahnya adalah $\approx 2{,}27815 \times 10^{70}$.

Hal tersebut berarti, walau algoritma diserang dengan super komputer yang dapat melakukan pengecekan terhadap 1 x 10^{20} kemungkinan setiap detiknya (sudah trmasuk segala operasi beserta pengenalan teks), maka penyerang baru akan mendapatkan teks yang benar setelah mencoba selama $\approx 1{,}09426\ x\ 10^{50}$ detik, yang adalah $\approx\ 2{,}08194\ x\ 10^{42}$ tahun.

E. Analisis Kebutuhan Perangkat Lunak

Perangkat lunak ini didesain khusus untuk membantu pengguna *iOS*, terutama perangkat *iPhone* agar dapat melakukan pengiriman dan peneimaan pesan dengan aman. Namun perlu diingat bahwa dalam berkirim pesan tersebut, enkripsi dan dekripsi hanya dapat dilakukan pada 90 karakter standar yang tersedia pada papan tuts *iPhone*.

Secara umum, perangkat lunak haruslah dapat membaca masukkan dari pengguna, dan melakukan enkripsi plain teks dan dekripsi cipher teks dengan benar sesuai rancangan algoritma yang telah ditetapkan sebelumnya.

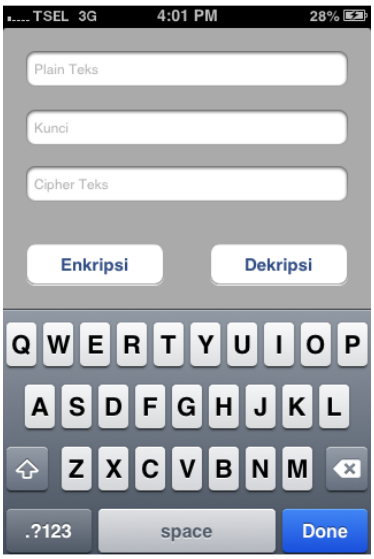
Tidak hanya itu, perangkat lunak haruslah dapat menyembunyikan karakter kunci saat pengetikkan dilakukan oleh pengguna agar lebih aman dari pihak yang berusaha mencuri lihat. Kemudian untuk mempermudah pengiriman pesan, perangkat lunak kemudian akan memfasilitasi penggunaan fitur *copy-paste*. Semua ini harus dapat diimplementasikan dengan antar muka yang intuitif dan mudah digunakan.

IV. IMPLEMENTASI DAN PENGUJIAN

Perangkat lunak ini dikembangkan dengan aplikasi Xcode versi 3.2.6, pada lingkungan operasi Mac OS X 10.6. Xcode ini adalah sebuah IDE yang berisikan perangkat pengembangan perangkat lunak yang dikembangkan oleh *Apple* untuk membangun perangkat lunak pada OS X dan iOS. Dalam pengujiannya, aplikasi diimplementasikan pada perangkat *iPhone* 3GS, dengan sistem operasi iOS 6.0. Perangkat *iPhone* tersebut memiliki CPU 600MHz ARM Cortex-A8, dengan Memory sebesar 256 MB eDRAM.

A. Implementasi Antarmuka

Aplikasi diharapkan memiliki antarmuka yang simpel dan intuitif, namun tetap efisien dalam penggunaan, dan dapat menjalankan segala kebutuhan yang ada. Berikut adalah antar muka utama aplikasi



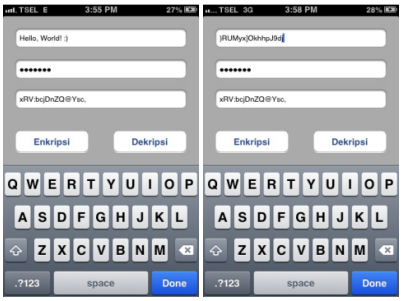
Gambar 3 Skema enkripsi yang dilakukan

Antarmuka ini sudah memenuhi segala kebutuhan yang ada. Untuk melakukan enkripsi, pengguna cukup menuliskan teks yang ingin dienkripsi pada kolom plain teks, dan kuncinya pada kolom kunci, dan menekan tombol enkripsi. Hasil enkripsinya akan ditampilkan pada kolom cipher teks. Begitu juga untuk melakukan dekripsi, pengguna cukup menuliskan teksnya pada kolom cipher teks, dan setelah memasukkan kunci dan menekan tombol dekripsi, maka plain teks hasil dekripsi akan muncul pada kolom plain teks.

Untuk pengujian pelakuan enkripsi, detilnya dapat dilihat pada gambar 4 dibawah. Untuk percobaan dengan plain teks ‘Hello, World! :)’ dan dengan kata kunci ‘william’, hasil enkripsinya adalah ‘xRV:bcjDnZQ@Ysc,’. Kemudian, apabila hasil tersebut didekripsi dengan kunci yang sama, akan mengembalikan teks yang benar. Namun, apabila kuncinya salah, walaupun hanya sedikit saja (William), maka hasil dekripsinya akan menjadi teks yang tidak memiliki makna sama sekali, yaitu ‘)RUMyx]OkhhpJ9dj’, seperti yang dapat dilihat pada gambar 5.

(1) (2) (3)

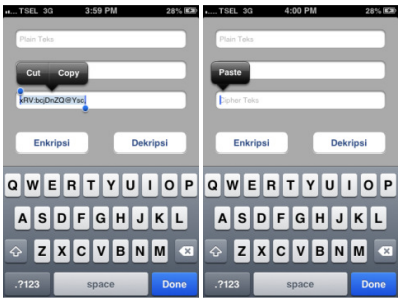
Gambar 4. (1) Memperlihatkna penulisan plain teks, (2) adalah penulisan kunci, dan (3) adalah hasil enkripsi yang didapat.



(1) (2)

Gambar 5. (1) Memperlihatkan hasil dekripsi dengan kunci 'william', dan (2) memperlihatkan hasil dekripsi dengan kunci 'William'.

Aplikasi ini juga menerapkan fitur *copy-paste* seperti yang dapat dilihat pada gambar 6.



Gambar 6. Fitur *copy-paste*.

V. KESIMPULAN DAN SARAN

Melalui pengerjaan tugas akhir ini, dapat ditarik beberapa kesimpulan, yaitu:

1. Algoritma ini telah berhasil memanfaatkan dan memadukan sifat – sifat yang dimiliki oleh algoritma kriptografi klasik dengan baik. Dengan memadukan sifat-sifat dari algoritma kriptografi klasik seperti cipher transposisi, vigenere, dan playfair, algoritma ini menjadi meliki sifatnya sendiri yang unik dan sulit diserang
2. Rancangan algoritma enkripsi dan dekripsi yang diajukan dapat diterima, digunakan, dan diimplementasikan sebagai algoritma untuk menjaga kerahasiaan dalam berkirim pesan dengan baik. Algoritma kriptografi ini aman dari metode-metode penyerangan standar yang sudah ada, termasuk metode *brute force*.
3. Perangkat lunak telah selesai diimplementasikan, dan dapat dijalankan dengan baik. Aplikasi yang dibangun telah berhasil diimplementasian pada perangkan *iPhone*, serta memenuhi seluruh kebutuhan fungsional yang ada.

Sementara, beberapa saran yang dapat diberikan pada aplikasi algoritma ini adalah:

1. Aplikasi masih dapat dikembangkan, misalnya dengan penambahan fitur pengiriman pesan secara otomatis kepada pasangan berkirim pesan untuk mempermudah pengiriman dan penerimaan pesan tersebut.
2. Melakukan perubahan dan modifikasi pada penulisan *source code* yang dilakukan sehingga menjadi lebih baik dan efisien. Hal ini diperlukan untuk mendapatkan waktu pemrosesan enkripsi dan dekripsi yang lebih cepat, efektif, dan efisien.

REFERENSI

[1] Agunk. (2007) : Handphone Sebagai Media Komunikasi Interpersonal, http://dsire-news.blogspot.com. *Download* pada 7 November 2011.

[2] Bellare, M., Rogaway, P. (2005) :Introduction to Modern Cryptography, http://citeseerx.ist.psu.edu. *Download* pada 14 November 2011.

[3] Green, M.D. (2013) : A Few Thoughts on Cryptographic Engineering: Here Comes the Encryption Apps!. http://blog.cryptographyengineering.com/2013/03/here-come-encryption-apps.html. *Download* pada 25 Juli 2013.

[4] Haslam, K. (2007) : Macworld Expo: Optimised OS X sits on 'versatile' flash, http://www.macworld.com. *Download* pada 14 November 2011.

[5] Kahn, D. (1973) : The Codebreakers: The Story of Secret Writing, http://www.scribd.com/doc/7279100/The-Code-Breakers. *Download* pada 7 November 2011.

[6] Monaghan, C. dan Jennifer, R. (2010) : Apple Introduces New iPod Touch, http://www.apple.com/pr/library/2010/09/01Apple-Introduces-New-iPod-touch.html. *Download* pada 7 November 2011.

[7] Nugroho, B.K. (2010) : Aplikasi Enkripsi SMS pada Telepon Selular Berbasis J2ME dengan Metode Vigenere Cipher, http://eprints.undip.ac.id/22972/1/Laporan_TA_Bayu_K_N_J2F004262.pdf. *Download* pada 7 November 2011.

[8] Perez, S. (2010) : Android Steals Market Share from iPhone, http://www.readwriteweb.com. *Download* pada 14 November 2011.

[9] Permana, R.W.A. (2008) : Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Selular, http://digilib.itb.ac.id/gdl.php?mod=browse&op=read&id=jbptitbppgdl-ranggawisn-31273. *Download* pada 7 November 2011.

[10] Wangsadiredja, M. (2011) : Aplikasi Enkripsi Pesan dan File pada Blackberry dengan Menggunakan Mode Cipher Feedback 8-bit, http://www.informatika.org/~rinaldi/TA/Makalah_TA_Matthew.pdf. *Download* pada 7 November 2011.