APLIKASI ENKRIPSI CATATAN (NOTES) PADA PERANGKAT MOBILE SMARTPHONE DENGAN METODE VARIANT BEAUFORT EXTENDED

. Bambang Sujatmiko
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya

Muhammad Abidin
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya

Abstrak

Pada saat ini, privasi seseorang adalah salah satu hal yang penting, tidak terkecuali berbagai fitur aplikasi pencatat pada mobile smartphone.Informasi dalam catatan lebih pada hal hal yang penting, yang memungkinkan terlihat atau tercuri oleh pihak yang tidak bertanggung jawab. Oleh karena itu diperlukan fitur pengamanan untuk mengamankan catatan pengguna dari orang lain. Maka dari itu dibuat aplikasi enkripsi catatan dengan menggunakan metode Variant Beaufort pada sistem operasi Android.

Enkripsi diberlakukan pada beberapa bagian penting pada catatan dengan menggunakan metode Variant Beaufort.Metode Variant Beaufort sendiri merupakan salah satu algoritma kriptografi klasik dengan teknik subtitusi.Panjang alphabet/char yang diijinkan dalam aplikasi lebih panjang dari yang bisanya 26karakter (ABCDEFGHIJKLMNOPQRSTUVWXYZ) sehingga menambah rumit dalam pemecahan secara langsung.Kunci yang digunakan untuk melakukan enkripsi dan dekripsi dalam aplikasi nantinya ditentukan sendiri oleh pengguna.

Secara garis besar aplikasi ini mampu mengacak informasi dalam catatan cukup baik, sehingga membuat kerahasian data catatan pengguna terjamin. Selain itu, dalam penyimpanan pada database juga merupakan hasil enkripsi dan bukan teks asli, dan tentu hal ini menambah keamanan yang lebih dari segi database.

Kata kunci : Variant Beaufort, Android, Notes, Kripstografi, Enkripsi, Dekripsi

PENDAHULUAN

Keamanan informasi dan privasi setiap orang adalah hal yang penting. Tidak terkecuali pada catatan (notes) yang sering berisi hal penting dan bersifat rahasia. Berbagai aplikasi catatan telah ada, termasuk pada perangkat mobile smartphones bersistem operasi Android.Namun dari sekian banyak aplikasi catatan lebih menekankan pada manajemen catatan dengan mengesampingkan tingkat keamanan informasi catatan.

Oleh karena itu, timbul sebuah gagasan untuk membuat sebuah aplikasi pencatat (notes) yang bukan hanya melakukan manajemen catatan tapi juga terdapat fasilitas untuk menjaga informasi yang tersimpan dengan melakukan enkripsi terhadap isi catatan. Sehingga diharapkan informasi/data pada catatan tidak mudah dibaca oleh orang yang tidak berhak.Terlebih bila terjadi kehilangan perangkat mobile, tidak serta merta informasi yang tersimpan di aplikasi bisa dibaca dengan mudah oleh orang yang menemukan perangkat mobile tersebut.

METODE REKAYASA

Metode Variant Beaufort

Medote *Variant Beaufortcipher* merupakan salah satu jenis kriptografi klasik yang pada dasarnya melakukan subtitusi cipher abjad majemuk (*polyalphabetic subtutution*). *Variant Beaufort cipher* adalah variant dari Beaufort Cipher yang pertama kali diperkenalkan oleh Sir Francis Beaufort.

Variant Beaufort cipher mempunyai keterkaitan dengan *Vigenere Cipher*. Pernyataan tersebut sesuai dengan pendapat Ameer A.J. Al-Swidi (2012) sebagai berikut: "*The variant Beaufort cipher is equivalent to a Vigenere cipher with key character (26-k), the variant Beaufort cipher is also the inverse of the Vigenere cipher and its uses the substitution.*"

Untuk mempermudah melakukan enkripsi dan dekripsi metode *Variant Beaufort cipher* menggunakan *tabula recta* atau *cipher tableau.* Gambar 1 ini adalah *cipher tableau Variant Beaufort cipher* dengan panjang karakter 26 dari A sampai Z.

Baris pada gambar *tabula recta* kolom paling kiri menyatakan kunci, dan baris paling atas menyatakan *plaintext*. Sedangkan perpotongan antara kolom dan baris adalah *ciphertext*.

Jika panjang kunci lebih pendek dari *plaintext*, maka kunci akan diulang secara periodic sehingga didapat panjang kunci sama dengan panjang *plaintext*.

	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
A	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
Z	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	A
Y	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
X	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
W	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
V	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
U	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
T	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
S	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
R	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Q	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
P	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
O	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
L	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
K	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
I	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
H	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
G	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
F	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
E	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
D	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
C	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
B	Z	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

Gambar 1.*Tabula Recta Variant Beaufort*

Contoh, jika *plaintext* THEBEAUTY dan ABC sebagai *key* maka proses enkripsi yang terjadi adalah sebagai berikut :

Tabel 1. Contoh Penggunaan*Variant Beaufort*Cipher

Plaintext	T	H	E	B	E	A	U	T	Y
Key	A	B	C	A	B	C	A	B	C
Ciphertext	T	G	C	B	D	Y	U	S	W

Cara kerja :
Hapus semua karakter yang tidak termasuk alfabet yang diijinkan, baik itu karakter kata kunci maupun plainteks.
Lakukan perulangan kata kunci hingga panjang kata kunci sama dengan panjang *plaintext*.
Untuk mengenkripsi/mengkodekan teks, ambil huruf pertama dari kata kunci dan mencarinya di kolom kunci sebelah kiri. Ambil huruf pertama dari *plaintext* dan mencarinya di baris atas *plaintext*. Perpotongan antara kolom kunci dan baris *plaintext* adalah hasil enkripsi.
Untuk melakukkan dekripsi teks, ambil huruf pertama dari kata kunci di kolom kiri dan bergerak ke kanan hingga didapat huruf *ciphertext* pertama. Dari huruf *ciphertext* bergerak ke baris paling atas, huruf paling atas itulah sebuah *plaintext.*
Secara matematis metode *Variant Beaufort cipher* dirumuskan sebagai berikut :
Enkripsi
$\mathbf{C_i = (P_i - K_i) \bmod N}$
Dekripsi
$\mathbf{P_i = (C_i + K_i) \bmod N}$

Dimana :

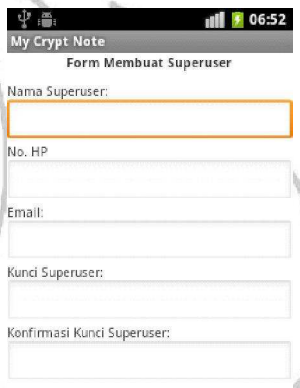
C_i =*Ciphertext*karakter ke-i
P_i = *Plaintext*karakter ke-i
K_i = karakter kunci ke-i
N = panjang karakter yang diijinkan.

.

HASIL UJI COBA DAN PEMBAHASAN

Hasil Implementasi

Aplikasi yang dihasilkan telah diuji cobakan menggunakan *mobile smartphone* dari berbagai vendor yang bersistem operasi android minimal versi 2.3 (Gingerbread) dan semua berjalan baik.Untuk keperluan visualisasi, dalam laporan ini disajikan pengujian aplikasi dengan menggunakan Samsung GT-S5770 (Galaxy Mini).Berikut ini beberapa hasil tampilan aplikasi dengan menggunakan Samsung Galaxy Mini.



Gambar 2. Form Membuat Superuser

Tampilan Gambar 2 di atas adalah tampilan form tambah *superuser* yakni tampilan pertama kali muncul setelah aplikasi terpasang dan dijalankan. semua dari setiap *fields* wajib diisi dan sangat penting.

Gambar 3. Menu Utama

Gambar 3 adalah tampilan menu utama dari aplikasi, melalui menu utama ini pengguna bisa mengakses segala hal berkaitan dengan aplikasi, misalnya membuat catatan, mencari catatan, masuk ke area *superuser, recovery key superuser,* bantuan, informasi, selain itu juga untuk keluar dari aplikasi.

Gambar 4. Daftar Catatan

Gambar 4 adalah tampilan daftar catatan yang sudah tercipta, disini dibedakan antara "*normal note*" dan *"crypt note"* . Perbedaan terletak pada *icon*dan lebih detail bisa dilihat dari detail catatan nantinya. Pada tampilan daftar catatan ini pula terdapat menu lihat catatan, edit judul catatan, edit catatan, hapus catatan serta melihat detail catatan dari masing masing catatan. Tampilan menu ini bisa dilihat pada Gambar 5 di bawah ini.

Gambar 5. Menu Lihat, Edit Judul, Hapus, Edit, dan Detail Catatan

Gambar 6. Tambah "*Normal Note*"

Gambar 6 adalah tambah "*normal note*" .Catatan yang tersimpan sebagai normal catatan yang ada pada umumnya. Judul akan otomatis terisi dari teks isi catatan.

Pengguna bisa merubah judul lain waktu pada menu edit judul.

Gambar 7. Tambah "*Crypt Note*"

Gambar 7 adalah tambah catatan bertipe "*crypt note*" . Sama halnya dengan "*normal note*" hanya disini terdapat penambahan *key* yang digunakan untuk enkripsi isi catatan. Pengguna bisa membiarkan kolom isian *key* kosong, jika demikian maka *key* catatansecara otomatis menggunakan *key superuser* .

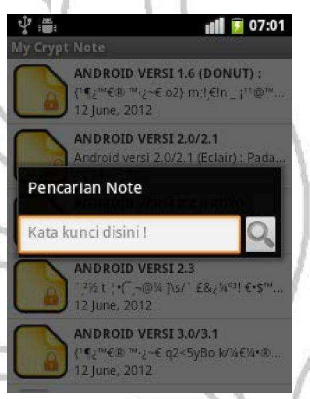
Gambar 8. Lihat *"Normal Note"*

Gambar 8 adalah tampilan lihat "*normal note*". Isi teks catatan nantinya ditampilkan tanpa sebagai teks asli catatan.akan tetapi untuk catatan bertipe "*crypt note*" akan ditampilkan isi teks catatan yang terenkripsi dan dibutuhkan sebuah *key* untuk menampilkan isi catatan asli. Gambar 9 di bawah ini akan menggambarkan tampilan lihat catatan bertipe "*Crypt Note*".

Gambar 9.Lihat "*Crypt Note*"

Pada edit catatan, tampilan tidak berbeda dengan tambah catatan karena edit catatan memuat ulang apa isi catatandari dalam database dan menampilkan lagi dalam form tambah catatan. Edit catatan akan diperlihatkan seperti pada Gambar 10 di bawah ini.

Gambar 10. Edit Catatan



Gambar 11. Pencarian Catatan

Gambar 11 di atas adalah form pencarian catatan, pengguna bisa mempercepat pencarian catatan berdasarkan judul, dan tanggal dibuat catatan tersebut.

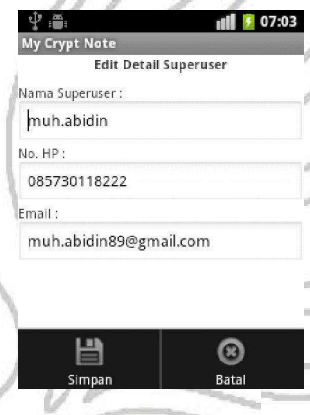
Gambar 12. Login Superuser Area

Hak akses tertinggi dari aplikasi ini adalah *superuser,* memasuki superuser area diharuskan untuk *login* terlebih dahulu. Otentifikasi *login* menggunakan nama*superuser* dan *primary key* saat pembuatan *superuser* pada bagian sebelumnya.

Tampilan *Superuser Area*

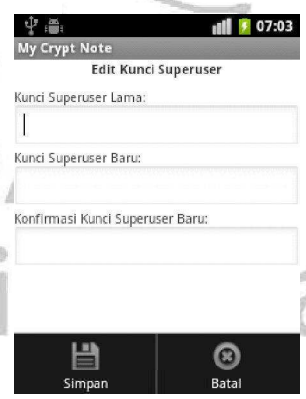
Gambar 13.Superuser Area

Setelah melalui proses login *superuser area* dan berhasil maka akan memasuki *superuser area* dan padaGambar 13 di atas adalah tampilan *superuser area.* Terdapat beberapa menu pada *superuser area* yakni edit detail *superuser*, edit *primary key*, *multiple delete catatan*, dan*reset* aplikasi.



Gambar 14. Edit Detail Superuser

Gambar di atas adalah tampilan *form* edit detail *superuser* yang memungkinkan pengguna untuk merubah data *superuser.*

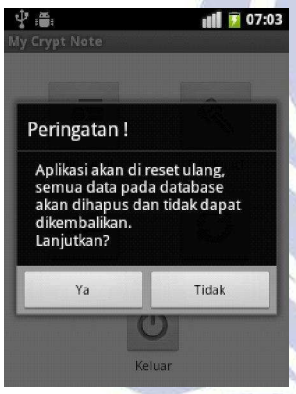


Gambar 15.Edit Key Superuser

Gambar di atas adalah *form* edit *primary key*. Pengguna bisa merubah *primary key* jika menginginkan perubahan terhadap *primary key* mereka.

Gambar 16.*Multiple* Hapus Catatan

Gambar 16 adalah sebuah menu yang dimiliki oleh superuser dalam menghapus catatan.Penghapusan catatan pada menu ini tidak menghapus satu persatu namun bisa beberapa catatan sekaligus.



Gambar 17. Reset Aplikasi

Gambar 17 adalah suatu tampilan/peringatan ketika pengguna *superuser* hendak melakukan reset terhadap aplikasi.

Gambar 18.Recovery Key Superuser

Gambar di atas adalah tampilan *recovery key*, melalui *form* di atas pengguna bisa melakukan *recovery key*.*Key* akan dikirimkan ke no. *handphone* yang terdapat pada data detail *superuser*. Namun terdapat sebuah otentifikasi nama*superuser* dan no. *handphone* terlebih dulu. Jika sukses maka pesan berisi *key* dikirimkan melalui SMS.

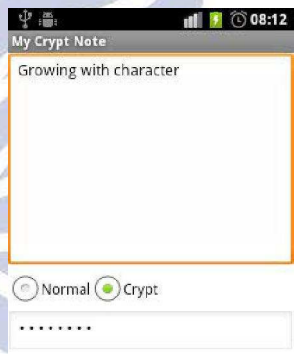
Gambar 19.*Recovery Key* Catatan

Sama halnya dengan *recovery key superuser*, ketika pengguna lupa *key* suatu catatan, pengguna bisa melakukan *recovery* melalui SMS. Namun untuk *key* catatan tidak dibutuhkan otentifikasi terlebih dulu.

.

Pembahasan

Pada pembahasan ini disajikan contoh kasus catatan bertipe "*crypt note*".



Gambar 20. Tambah Catatan "*Crypt Note*"

Gambar 20 adalah gambar penambahan catatan "*crypt note*" baru.Isi catatan (*plaintext*) adalah "*Growing with character"*.Dan *"surabaya"* sebagai *key*. Saat pengguna menyimpan catatan, maka aplikasi akan mengenkripsi isi catatan tersebut berdasarkan kunci yang di masukkan.

Gambar 21. Hasil Enkripsi

Gambar 21 merupakan hasil enkripsi catatan berdasarkan *key* "*surabaya*". Berikut ini tabel proses enkripsi.

Tabel 2. Perubahan Karakter Pada Proses Enkripsi

plaintext	G	r	o	w	i	n	g		w	i	t	h		c	h	a	r	a	c	t	e	r
index	38	81	78	86	72	77	70		86	72	83	71		66	71	64	81	64	66	83	68	81
key	s	u	r	a	b	a	y		a	s	u	r		a	b	a	y	a	s	u	r	a
index	82	84	81	64	65	64	88		64	82	84	81		64	65	64	88	64	82	84	81	64
ciphertext	Ö	ý	ý	7	(	.	î		7	ö	ÿ	ö		#	'	!	ù	!	ð	ÿ	ó	2
index	170	211	211	22	7	13	196		22	204	213	204		2	6	0	207	0	198	213	201	17

Perhitungan enkripsi masing-masing karakter diperoleh berdasarkan rumus $C_i = (P_i - K_i) \bmod N$. Perhitungan enkripsi pada contoh di atas bisa dilihat pada Tabel 3 dibawah ini.

Tabel 3. Perhitungan Proses Enkripsi

$C_0 = (38 - 82) \bmod 214 = 170$	$C_{10} = (71 - 81) \bmod 214 = 204$
$C_1 = (81 - 84) \bmod 214 = 211$	$C_{11} = (66 - 64) \bmod 214 = 2$
$C_2 = (78 - 81) \bmod 214 = 211$	$C_{12} = (71 - 65) \bmod 214 = 6$
$C_3 = (86 - 64) \bmod 214 = 22$	$C_{13} = (64 - 64) \bmod 214 = 0$
$C_4 = (72 - 65) \bmod 214 = 7$	$C_{14} = (81 - 88) \bmod 214 = 207$
$C_5 = (77 - 64) \bmod 214 = 13$	$C_{15} = (64 - 64) \bmod 214 = 0$
$C_6 = (70 - 88) \bmod 214 = 196$	$C_{16} = (66 - 82) \bmod 214 = 198$
$C_7 = (86 - 64) \bmod 214 = 22$	$C_{17} = (83 - 84) \bmod 214 = 213$
$C_8 = (72 - 82) \bmod 214 = 204$	$C_{18} = (68 - 81) \bmod 214 = 201$
$C_9 = (83 - 84) \bmod 214 = 213$	$C_{19} = (81 - 64) \bmod 214 = 17$

Membuka Catatan *"Crypt Note"*
Ketika pengguna membuka suatu catatan yang bertipe "*crypt note*" maka muncul perintah untuk otorisasi *key* terlebih dahulu.

Gambar 22. Otorisasi *Key Catatan*

Apabila *key*cocok, aplikasi menampilkan isi catatan asli sebagai hasil dekripsi catatan yang terenkripsi sebelumnya yang tersimpan dalam database.

Gambar 23. Menampilkan Hasil Dekripsi Isi Catatan

Proses dekripsi catatan menggunakan rumus $P_i = (C_i + K_i) \bmod N$. Perubahan karakter dalam proses dekripsi bisa dilihat pada Tabel 4, sedangkan untuk perhitungan dalam perubahan karakter proses dekripsi disuguhkan pada Tabel 5 dibawah ini.

Tabel 4. Perubahan Karakter Pada Proses Dekripsi

ciphertext	Ö	ý	ý	7	(	.	î		7	ö	ÿ	ö		#	'	!	ù	!	ð	ÿ	ó	2
index	170	211	211	22	7	13	196		22	204	213	204		2	6	0	207	0	198	213	201	17
key	s	u	r	a	b	a	y		a	s	u	r		a	b	a	y	a	s	u	r	a
index	82	84	81	64	65	64	88		64	82	84	81		64	65	64	88	64	82	84	81	64
plaintext	G	r	o	w	i	n	g		w	i	t	h		c	h	a	r	a	c	t	e	r
index	38	81	78	86	72	77	70		86	72	83	71		66	71	64	81	64	66	83	68	81

Tabel 5. Perhitungan Proses Dekripsi

$P_0 = (170 + 82) \bmod 214 = 38$	$P_{10} = (204 + 81) \bmod 214 = 71$
$P_1 = (211 + 84) \bmod 214 = 81$	$P_{11} = (2 + 64) \bmod 214 = 66$
$P_2 = (211 + 81) \bmod 214 = 78$	$P_{12} = (6 + 65) \bmod 214 = 71$
$P_3 = (22 + 64) \bmod 214 = 86$	$P_{13} = (0 + 64) \bmod 214 = 64$
$P_4 = (7 + 65) \bmod 214 = 72$	$P_{14} = (207 + 88) \bmod 214 = 81$
$P_5 = (13 + 64) \bmod 214 = 77$	$P_{15} = (0 + 64) \bmod 214 = 64$
$P_6 = (196 + 88) \bmod 214 = 70$	$P_{16} = (198 + 82) \bmod 214 = 66$
$P_7 = (22 + 64) \bmod 214 = 86$	$P_{17} = (213 + 84) \bmod 214 = 83$
$P_8 = (204 + 82) \bmod 214 = 72$	$P_{18} = (201 + 81) \bmod 214 = 68$
$P_9 = (213 + 84) \bmod 214 = 83$	$P_{19} = (17 + 64) \bmod 214 = 81$

KESIMPULAN DAN SARAN

Simpulan

Berdasarkan percobaan yang telah dilakukan maka didapat kesimpulan sebagai berikut :

- Algoritma *Variant Beaufort cipher*bisa digunakan sebagai pengacak karakter catatansehingga kerahasian dan keamanan isi catatanlebih aman yang diimplemantasikan pada perangkat *mobile smartphone*dengan sistem operasi Android.
- Metode *Variant Beaufort* adalah kriptografi subtitusi klasik yang cukup kuat untuk dipecahkan secara langsung dengan *cryptanalisis.* Ada banyak

cara memodifikasi metode *Variant Beaufort* untuk didapat tingkat keamanan yang lebih, salah satunya dengan melakukan penambahan jumlah karakter yang dipakai pada proses enkripsi dan dekripsi. Penambahan jumlah karakter yang dipakai bisa meningkatkan keamanan karena akan presentase karakter sama yang muncul pada *ciphertext* akan lebih ditekan.

Saran

Saran yang bisa diberikan untuk penerapan teori maupun rekayasa pada masa mendatang adalah :

- Penggunaan metode dalam enkripsi catatan menggunakan algoritma kriptografi klasik, penggunaan algoritma lain diharapkan mampu meningkatkan kerumitan dalam pembukaan paksa teks catatan yang terenkripsi dengan*cryptanalisis.*
- Pembaruan aplikasi ini akan sangat diharapkan agar lebih baik lagi.

DAFTAR PUSTAKA

A.J. Menezes, P.C.van Oorschot, and S. A,Vanstone, 1996 *Handbook of*

Applied Cryptography, CRC Press, Boca Raton, New York.

Al-Swidi A.J Ameer. 2012. *On adaptive of classical and public key*

*cryptography by using ε-A and D-A laws.*University of Vavylon, Collage Of Education for Pure Sciences, Math. Department.

Beaufort Variant Information http://ruffnekk.stormloader.com/variant_info.html Waktu akses : 2 Agustus 2012.

Nazruddin Safaat H, 2011. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android.* Bandung : Informatika Bandung.

Rahardjo Budi, 2005. *Keamanan Sistem Informasi Berbasis Internet.*

Bandung : PT Insan Indonesia.

Tim Penyusun, 2006. *Panduan Penulisan dan Penilaian Tugas Akhir.*

Surabaya :Universitas Negeri Surabaya

Wei-Meng Lee, 2011. *Beginning Android Application Development.* Canada : Wiley Publishing, Inc