APLIKASI ENKRIPSI DAN DEKRIPSI DENGAN METODE VIGENERE CIPHER BERBASIS ANDROID

Dimpo Sinaga
dnagas1@yahoo.co.id

ABSTRAKSI

Kebutuhan akan informasi hampir menjadi prioritas utama bagi setiap orang karena itu banyak orang menginginkan informasi yang dapat menguntungkan berbagai pihak. Salah satu cara mengantisipasi hal ini adalah dengan merahasiakan informasi tersebut dengan teknik enkripsi. Teknik enkripsi klasik adalah metode vigenere yang akan menyandikan teks. Penelitian ini untuk membuat suatu Aplikasi Enkripsi Sederhana Pada Android. Aplikasi ini bertujuan untuk menggantik teks sehingga informasi teks dapat dilindungi. Dalam pembahasan aplikasi ini masalah dibatasi pada pernacangan aplikasi Enkrip Dekrip pada Android dan pembuatan program androidnya. Pembuatan aplikasi Enkripsi Vigenere ini, menggunakan Eclipse sebagai tempat editor untuk menulis Java Android. Android banyak di gunakan karena Android bersifat open source, bersifat fleksibel dan mudah dalam pemakaiannya. Aplikasi ini dijalankan dengan menggunakan telepon genggam berbasis Android yang banyak digunakan karena Android bersifat open source.

Pendahuluan

Perkembangan teknologi terutama pada teknologi yang berbasis mobilitas salah satunya adalah telpon seluler (ponsel) , semakin banyak fitur dan aplikasi yang dapat digunakan untuk berbagai fungsi. Mulai dari multimedia, games, transfer data, video streaming, media sosial, messenger dan lain-lain. Berbagai sistem operasi pada ponsel pun bermunculan, diantaranya yang berkembang saat ini adalah ponsel pintar (smart phone) berbasis sistem opreasi android. Smart phone sistem operasi android ini rata – rata memiliki spesifikasi hardware yang cukup baik sehingga aplikasi dan fitur banyak yang dapat digunakan pada smart phone tersebut. Sistem operasi android dipilih karena sistem operasi ini bersifar open source, yaitu bisa dikembangkan secara bebas serta cukup mudah untuk membuat aplikasi berbasis android ini. Fasilitas utama dalam ponsel adalah untuk melakukan pengiriman data berupa pesan. Pengiriman pesan bisa menggunakan aplikasi Short Message Service (SMS) atau dengan aplikasi messenger yang tersedia pada play store android.

Pengertian Aplikasi

Pada pengertian umumnya, aplikasi adalah alat terapan yang difungsikan secara khusus dan terpadu sesuai kemampuan yang dimilikinya aplikasi merupakan suatu perangkat komputer yang siap pakai bagi user.

Klasifikasi Aplikasi

Aplikasi dapat digolongkan menjadi beberapa kelas, antara lain:

1. Perangkat lunak perusahaan (*enterprise*)

2. Perangkat lunak infrastruktur perusahaan
3. Perangkat lunak informasi kerja
4. Perangkat lunak media dan hiburan
5. Perangkat lunak pendidikan
6. Perangkat lunak pengembangan media
7. Perangkat lunak rekayasa produk

Pengertian Android

Android adalah sistem operasi berbasis Linux bagi telepon seluler seperti telepon pintar dan komputer tablet. Android juga menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk berbagai macam piranti gerak. Awalnya, Google Inc membeli Android Inc. Android adalah pendatang baru yang membuat piranti lunak untuk ponsel.

Versi Android

a. Android Versi 1.6 (Donut)
b. Android versi 2.2 (Froyo : Frozen Yoghurt)
c. Android versi 2.3 (Gingerbread)
d. Android versi 3.0/3.1 (Honeycomb)
e. Android versi 4.1 (JellyBean)

Android SDK

Android SDK adalah tools API (Application Programming Interface) yang diperlukan untuk mengembangkan aplikasi pada platform Android yang menggunakan bahasa pemrograman Java.

ADT (Android Development Tools)

AVD (Android Virtual Device) :merupakan emulator yang digunakan untuk menjalankan program aplikasi Android yang telah dirancang. AVD dapat dikongfigurasi agar dapat menjalankan berbagai macam versi Android yang telah diinstal. Dalam perancangan aplikasi ini, penulis menggunakan kongfigurasi Android versi 4.2.2 (Jelly Bean).

IDE Eclipse

Menurut **Fatimah (2011)**, Eclipse adalah sebuah IDE (Integrated Development Environtment) untuk mengembangkan perangkat lunak agar dapat dijalankan di semua platform (platform-independent). Berikut ini adalah sifat dari Eclipse :

a. Multi-platform: Target sistem operasi Eclipse adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX, dan Mac OS X.
b. Multi-language: Eclipse dikembangkan dengan bahasa pemrograman Java, dengan pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Java, Cobol, Python, Perl, PHP.
c. Multi-role: Selain sebagai IDE untuk pengembangan aplikasi, Eclipse pun dapat digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, test perangkat lunak, pengembangna web, dan lain sebagainya.

JDK (Java Development Kit)

Menurut **DeCoster (2012)**, Java adalah sebuah teknologi yang diperkenalkan oleh Sun Microsystems pada pertengan tahun 1990. Menurut definisi Sun, Java adalah nama untuk sekumplan teknologi untuk membuat dan menjalankan perangkat lunak pada computer standalone ataupun pada lingkungan jaringan. Untuk mmbuat program Java dibutuhkan kompiler dan interpreter untuk program Java berbentuk Java Development Kit yang diproduksi oleh Sun Microsystems.

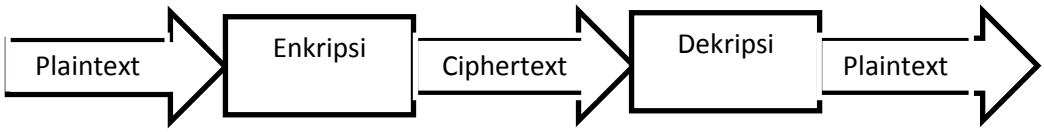
Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

Berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi.

1. Pesan, plaintext, dan cipherteks
   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext*) atau kriptogram (*cryptogram*). Cipherteks harus dapat ditransformasikan kembali menjadi plaintext semula agar dapat diterima dan bisa dibaca.
2. Pengirim dan penerima
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Pengirim tentu menginginkan pesan dapat dikirm secara aman, yaitu pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang dikirim. Solusinya adalah dengan cara menyandikan pesan menjadi *cipherteks*.
3. Enkripsi dan Dekripsi
   Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan cipherteks menjadi plainteks disebut dekripsi (*decryption*) atau *deciphering*.
4. Cipher dan kunci
   Algoritma kriptogarfi disebut juga cipher, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering dan deciphering.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut **(Sadikin, 2012)**:

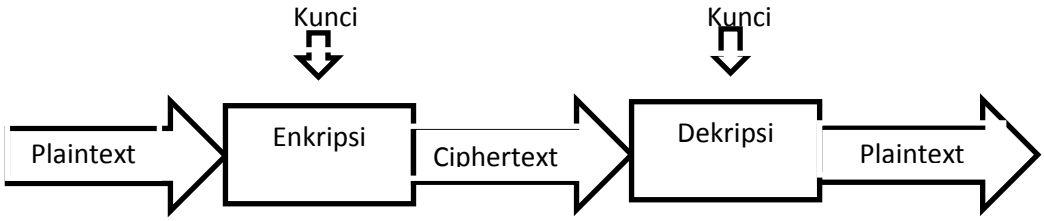


Gambar 2.1 Mekanisme Kriptografi

Pada dasarnya, prosesnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui dekripsi (D) yang akan menghasilkan kembali plaintext (m). Secara sistematis proses ini dapat dinyatakan sebagai berikut :

$$E(m) = c$$
$$D(c) = m$$
$$D(E(m)) = m$$

Kriptografi modern selain memanfaatkan algoritman juga menggunakan kunci (key) untuk memecahkan masalah tersebut. Dengan mekanisme dapat digambarkan pada gambar 2.1 menjadi gambar 2.2 berikut ini.



Gambar 2.2 Kriptografi Berbasis Kunci

Mekanisme kriptografi seperti ini dinamakan kriptogrfi berbasis kunci. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala plaintext dan ciphertextnya.

Persamaan matematisnya menjadi seperti berikut,

$$Ee(m) = c$$
$$Dd(c) = m$$
$$Dd(Ee(m)) = m$$

Dengan : e = kunci enkripsi, d = kunci dekripsi.

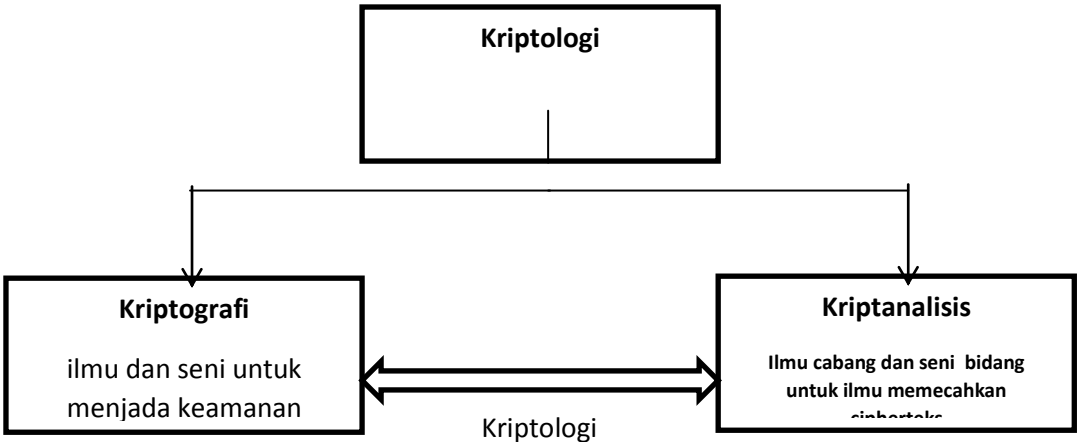
5. Sistem kriptografi
   Kriptografi membentuk sebuah sistem yang dinamakan sistem Kriptografi. Ssitem kriptografi (cryptosystem) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plaintext dan cipherteks yang mungkin, dan kunci. Di dalam kriptografi, cipher hanyalah satu komponen saja.

6. Penyadap

Penyadap (eavesdropper) adalah orang yang mencoba menangkap pesan selama di transmisikan.

7 . Kriptanalisis dan kriptologi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalisis (crytanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (cryptographer) mentransformasikan plainteks menjadi cipherteks tersebut untuk menemukan plainteks atau kunci. Kriptologi (cryptology) adalah setudi mengenai kriptografi dan kriptanalisis. Baik kriptografi maupun kritanalisis keduanya saling berkaitan, dapat dilihat seperti gambar dibawah ini :



Gambar 2.3 Hubungan Kriptologi

Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek – aspek keamanan sebagai berikut :

1. Kerahasiaan (confidentiality) :Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Di dalam kriptografi layanan ini direalisasikan dengan menyandikan plainteks menjadi cipherteks.
2. Integritas data (data integrity) : Adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: " apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?".
3. Otentikasi (authentication) :Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (user autehentication).

4. Nirperyangkalan (non-repudiation) :Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Algoritma kriptografi klasik

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi (cipher) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistrm kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptogarfi klasik memiliki beberapa ciri :

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada komputer.
3. Termasuk kedalam kriptografi kunci simetris.

Tiga alasan mempelajari algoritma klasik :

1. Memahami konsep dasar kriptografi.
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem kode.

Algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu:

1. Cipher substitusi (substitution cipher)
   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” di isini berarti satu huruf, pasanga huruf, atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah Caesar cipher
2. Cipher transposisi (transposisi cipher)
   Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks.

Vigenere cipher

Vigenere cipher adalah contoh terbaik dari cipher alphabet-majemuk ‘manual’. Algoritma ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) perancis, Blaise de Vigènere pada abad 16, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 sepeti ditulis di dalam bukunya La Cifra del Sig. Vigènere cipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut dinamakan vigènere cipher. Cipher ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Vigènere cipher digunakan oleh tentara Konfiderasi (Confederate Army) pada perang sipil Amerika (American Civil war).

Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar cipher, yang mana jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25).

Tabel 2.1 Bujur Sangkar Vigenere

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

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

Bujursangkar vigènere digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari pada panjang plainteks, maka kunci diulang penggunaanya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m. sebagai contoh, jika plainteks adalah THIS PLAINTEXT dan kunci adalah sony maka penggunaan kunci secara periodik adalah sebagai berikut:

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS

Setiap huruf plainteks akan dienkripsi dengan setiap huruf kunci dibawahnya. Untuk mengerjakan enkripsi dengan vigènere cipher, lakukan pada bujursangkar vigènere sebagai berikut : tarik garis vertical dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan dari kedua garis tersbut menyatakan huruf cipherteksnya.

Misalkan plainteks THIS PLAINTEXT dienkripsi dengan kata kunci sony. Karena panjang kunci tidak sama dengan panjang plainteks, maka kunci akan diulang secara periodik :

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS

Untuk huruf pertama T, tarik garis vertikal dari huruf T dan tarik garis mendatar dari huruf ‘S’, perpotongannya dalah pada kotak yang berisi huruf L (Tabel 2.2). dengan cara yang sama, tarik garis vertical dari huruf H dan tarik garis mendatar dari huruf ‘O’, perpotongannya adalah pada kotak yang juga berisi huruf V. hasil enkripsi seluruhnya adalah:

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS
Cipherteks : LVVQ HZNGFHRVL

Tabel 2.2 Enkripsi huruf T dengan kunci S

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

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

Amatilah bahwa huruf plainteks T dapat dienkripsikan menjadi L dan H, dan huruf cipherteks V dapat mempresentasikan huruf H, I, dan X. Hal ini merupakan karakteristik dari cipher alphabet-majemuk, untuk contoh tersebut diatas maka untuk pendekripsiannya adalah sebagai berikut : Key nya akan berpindah posisi menjadi kolom plaintext. Contoh :

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS
Cipherteks : LVVQ HZNGFHRVL

Dari hasil enkripsi diatas tersebut, maka proses dekripsinya untuk mencari plaintextnya adalah :

Kunci : SONY SONYSONYS
Cipherteks : LVVQ HZNGFHRVL

Untuk karakter yang pertama, huruf S maka akan dicari seluruh isi karakter yang berada pada kolom huruf S ke bawah, dimana terdapat karakter ciphertext huruf L, maka dilihat pada pada kolom kunci yang menunjukkan bahwa huruf L tersebut berada pada baris huruf T. Begitu juga dengan karakter yang ke dua huruf O, maka akan dicari seluruh isi karakter yanga berada pada kolom huruf O ke bawah, dimana terdapat karakter ciphertext huruf V, maka dilihat pada kolom kunci yang menunjukkan bahwa huruf V tersebut berada pada baris huruf H, dan seterusnya. Demikianlah cara kerja proses dekripsinya untuk mencari plainteks.

Tabel 2.3 Proses untuk mencari plainteks dari cipherteks huruf L dan V

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

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

PERANCANGAN SISTEM

Perancangan program aplikasi dalam skripsi ini menggunakan empat tahap siklus pengembangan model RAD (Rapid Application Development) yang telah dikemukakan oleh James Marti yaitu fase :

1. Fase Perencanaan Syarat-Syarat

Pada tahap ini, penulis menentukan aktor dan membuat user story serta merumuskan syarat-syarat yang diperlukan untuk merancanga aplikasi ini, yaitu dalam segi perancangan sistem yang akan dibuat sampai hardware maupun software yang digunakan, yaitu dalam segi perancangan sistem yang akan dibuat sampai hardware maupun software yang akan digunakan, yanga kana diulas secara mendalam pada sub bab 4.1

2. Fase Perancangan (UML)

Pada tahap ini dilakukan perancangan proses-proses yang akan terjadi di dalam sistem, membuat spesifikasi secara rinci tentang kebutuhan perancangan aplikasi ini.

3. Fase Konstruksi

Pada tahap ini dilakukan tahap instalasi software pembuatan skema perancangan Android Development Tools tersebut, pengkodean, proses menjalankan aplikasi menjadi .APK, yang diulas secara lengkap pada sub.bab 4.3

4. Fase Pelaksanaan

Pengujian Aplikasi Enkripsi dan Dekripsi Dengan Metode Vigenere Cipher Berbasis Android ini menggunakan metode Black Box Testing. Pengujian ini berfokus pada persyaratan fungsional dari aplikasi yang dibuat.Semua tahap pengujian tersebut akan dibahas secara lengkap ada sub.bab 4.3

Tabel 3.1 Rencana Pengujian pada Aplikasi

No.	Kelas Uji	Skenario butir uji	Tingkat Pengujian	Jenis Pengujian
1	Tampilan Awal	Memilih launcher icon Aplikasi untuk masuk ke Splash Screen lalu masuk Menu Utama	Modul	Black box
2	Enkripsi Teks	Menampilkan form Enkripsi teks dan mengenkripsikan teks	Modul	Black box
3	Dekripsi Teks	Menampilkan form Dekripsi teks dan	Modul	Black box

		mengdekripsikan teks.		
4	Tentang Aplikasi	Akan menampilkan penjelasan tentang nama pembuat Aplikasi.	Modul	Black box
5	Bantuan	Akan menampilkan penjelasan tentang Aplikasi.	Modul	Black box
6	Keluar	Akan keluar dari aplikasi tersebut.	Modul	Black box

HASIL DAN PEMBAHASAN

Pada bab ini akan dibahas mengenai penjelasan dari bab 3 secara detail, serta perancangan dan penjelasan tentang aplikasi yang dirancang oleh penulis, yaitu Aplikasi Android Enkripsi dan Dekripsi. Dalam bab ini juga akan dijelaskan mengenai proses pembuatan Aplikasi Android yang dihasilkan dari aplikasi Eclipse Juno Android Development Tools (ADT Plugin) ini.

Fase Konstruksi

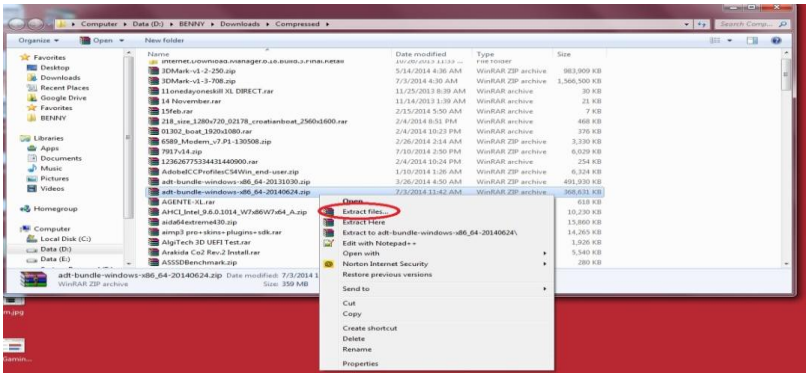
Instalasi Software

Berikut ini adalah proses instalasi software yang digunakan untuk merancang aplikasi Android Enkripsi dan Dekripsi ini.

A. Instalasi Android Development Tools (ADT)

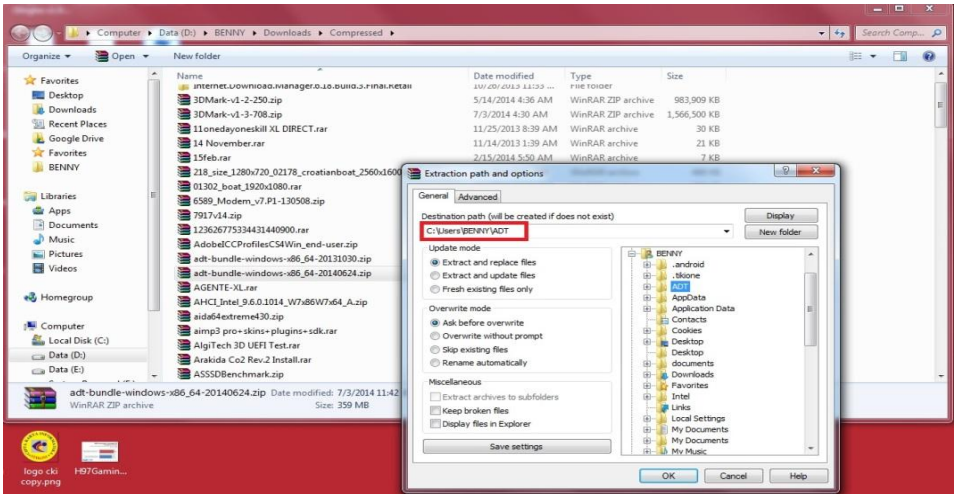
ADT adalah sebuah plugin yang dikhususkan untuk membuat software Android yang dirilis Google. ADT diintegrasikan menggunakan Eclipse. Berikut adalah cara instalasi ADT Bundle Eclipse :

1. Pilih zip file yang telah didownload, klik kanan menggunakan mouse. Pilih Extract Files.



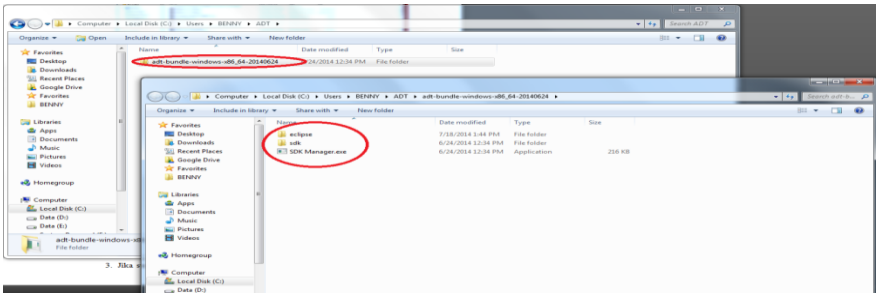
Gambar 4.5 Proses Extract

2. Pilih lokasi dimana software akan di Extract. Lalu tekan OK.



Gambar 4.6 Pilih Lokasi Extract

3. Jika sudah Extract, maka akan ada folder hasil Extract tadi dan didalamnya sudah terdapat Eclipse dengan ADT Bundle.



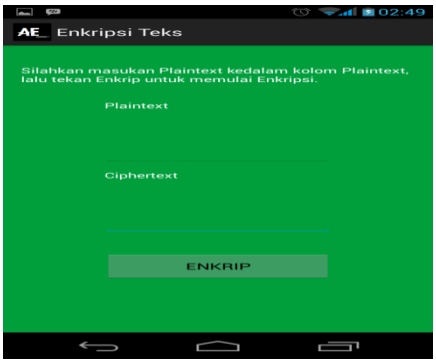
ImplementasiAntarmuka (Interface)

Antarmuka aplikasi di implementasikan pada Eclipse Juno dan perangkat mobile berbasis Android. Imlementasi antarmuka tiap-tiap menu dan diujicobakan pada tahap pengujian. Berikut ini adalah implementasi antarmuka dari aplikasi Enkripsi Vigenere Cipher.

Tampilan Menu Utama (Main Menu)

Gambar 4.10 Main Menu

Pada tampilan berikutnya yaitu Main Menu. Pada Main Menu terdapat 5 pilihan yang dapat diklik yaitu Enkripsi Teks, Dekripsi Teks, Tentang Aplikasi, Help / Bantuan, Exit / Keluar.

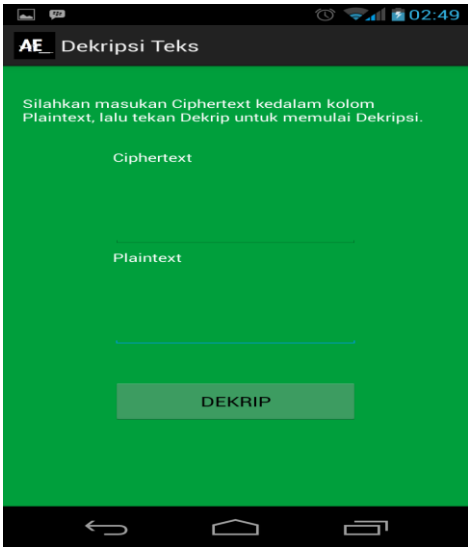


Gambar 4.11. Enkripsi Teks

Enkripsi Teks

Pada tampilan Enkripsi Teks ini adalah proses untuk mengenkripsi teks dari Plaintext ke Ciphertext. Pada form ini terdapat 2 kolom yaitu kolom Plaintext untuk memasukan teks yang akan dienkripsi dan kolom Ciphertext untuk melihat hasil dari enkripsi teks tersebut.

Tampilan Dekripsi Teks



Gambar 4.12 Dekripsi Teks

Pada tampilan Enkripsi Teks ini adalah proses untuk mengenkripsi teks dari Ciphertext ke Plaintext. Pada form ini terdapat 2 kolom, yaitu kolom Ciphertext untuk memasukan teks yang akan didekripsi dan kolom Plaintext untuk melihat hasil dari dekripsi teks tersebut.

Pengujian Aplikasi menggunakan Black Box Testing

Pengujian merupakan metode yang dilakukan untuk mejelaskan mengenai penoperasian perangkat lunak yang terdiri dari perangkat pengujian, metode pengujian dan pelaksanaan pengujian.

Pengujian program ini menggunakan metode Black Box. Pengujian Black Box merupakan pengujian program bedasarkan fungsi dari program. Tujuan dari metode Black Box ini adalah untuk menemukan kesalahan fungsi pada program. Pengujian dengan metode Blackbox dilakukan dengan cara memberikan sejumlah input pada program aplikasi yang kemudian diproses sesuai dengan kebutuhan fungsionalnya untuk melihat apakah program aplikasi menghasilkan keluaran yang diinginkan dan sesuai dengan fungsi dari program tersebut.

Berikut ini adalah tabel pengujian aplikasi untuk pengecekan menu-menu yang ada di dalam aplikasi.

Tabel 4.3 Pengujian pada Aplikasi

No.	Kasus/diuji	Skenario uji	Hasil yang diharapkan	Jenis Pengujian
1	Tampilan Awal	Memilih launcher icon Aplikasi untuk masuk ke Splash Screen lalu masuk Menu Utama	Ketika icon diklik / disentuh maka aplikasi berjalan dan masuk ke splash screen	☑ Berhasil ☐ Tidak Berhasil
2	Enkripsi Teks	Menampilkan form Enkripsi teks dan mengenkripsikan teks	Ketika button dekrip di klik / di sentuh maka akan menampilkan hasil enkripsi teks	☑ Berhasil ☐ Tidak Berhasil
3	Dekripsi Teks	Menampilkan form Dekripsi teks dan mengdekripsikan teks.	Ketika button enkrip di klik / di sentuh maka akan menampilkan hasil dekripsi teks	☑ Berhasil ☐ Tidak Berhasil
4	Tentang Aplikasi	Akan menampilkan penjelasan tentang nama pembuat Aplikasi.	Ketika menu Tentang Aplikasi di klik / di sentuh maka akan menampilkan	☑ Berhasil ☐ Tidak Berhasil

			penjelasan tentang nama pembuat Aplikasi	
5	Bantuan	Akan menampilkan penjelasan tentang Aplikasi.	Ketika menu Bantuan di klik / di sentuh maka akan menampilkan penjelasan tentang Aplikasi	☑ Berhasil ☐ Tidak Berhasil
6	Keluar	Akan keluar dari aplikasi tersebut.	Ketika menu Exit di klik / di sentuh maka akan keluar dari aplikasi tersebut.	☑ Berhasil ☐ Tidak Berhasil

Kesimpulan Hasil Pengujian

Bedasarkan pengujian yang telah dilakukan yaitu dengan pengujian Black Box Testing, dapat ditentukan kesimpulan bahwa aplikasi Android Enkripsi dan Dekripsi dapat berjalan dengan baik, namun tidak menutup kemungkinan aplikasi ini tidak berjalan dengan baik.

PENUTUP

Kesimpulan

Bedasarkan pengujian yang telah dilakukan oleh penlulis mengenai Aplikasi Enkripsi dan Dekripsi Dengan Metode Vigenere Cipher Berbasis Android, maka dapat diambil kesimpulan sebagai berikut:

1. Pembuatan Aplikasi Enkripsi dan Dekripsi Dengan Metode Vigenere Cipher Berbasis Android telah berhasil dilakukan dengan baik.
2. Dari hasil pengujiian pada aplikasi diperoleh kesimpulan bahwa fungsi – fungsi yang terdapat berjalan dengan baik dan seusai dengan yang diharapkan, sehingga layak digunakan oleh pengguna atau end user.
3. Aplikasi Enkripsi dan Dekripsi Dengan Metode Vigenere Cipher Berbasis Android ini dapat melakukan enkripsi teks dan dekripsi teks dengan sempurna.
4. Aplikasi Enkripsi dan Dekripsi Dengan Metode Vigenere Cipher Berbasis Android ini dapet diakses dimana saja dan kapan saja dengan syarat harus menggunakan mobile device berbasis Android berversi 4.2 Jelly Bean.

Saran

Aplikasi yang telah dibuat oleh penulis ini masih bersifat prototype sehingga tidak lepas dari kekurangan dan kelemahan. Dengan demikian diperlukan pengembangan sistem dan aplikasi yang lebih lanjut dengan memperhatikan hal-hal sebagai berikut :

1. Bagi yang ingin mengembangkan aplikasi ini disarankan agar mengembangkan aplikasi tidak hanya untuk keamanan pesan teks saja, melainkan dapat memberikan keamanan gambar (image) juga.
2. Aplikasi ini hanya dapat memberikan keamanan pesan dalam bentuk teks sehingga penulis berharap dapat dikembangkan untuk keamanan image seperti : png, jpg dll.

DAFTAR PUSTAKA

Anisyah, 2016, *Pedoman pembinaan pendidikan kependudukan dan lingkungan hhidup di sekolah. Jakarta:* Depdiknas.

Ariyus, Dony. 2014. *Pengantar Ilmu Kriptografi*. Yogyakarta: Andi offset.

Buyens, Jim. 2001. *Web Database Development.* Elex Media Komputindo. Jakarta

DeCoster, J. 2012. *Advances OpenJDK Project with New Code, NetBeans Integration Governance Board and Availability of Compability Test.*

Dhanta, Rizky. 2009. *Kamus Istilah Komputer Grafis & Internet*. Surabaya: Indah Post, (1999)

Fatimah, Wina Noviani, 2011. *Pengenalan Eclipse*.

Nazarudin Safaat Harahap, 2012. *Pemograman Aplikasi Mobile Smartphone*

Rinaldi Munir, 2015. *Belajar Ilmu Kriptografi.* Penerbit Andi.

Sadikin, Rifki, 2012. *Kriptografi Untuk Keamana Jaringan.*