BAB VI

KESIMPULAN DAN SARAN

6.1. Kesimpulan

Berdasarkan pada bab-bab sebelumnya maka dapat penulis simpulkan sebagai berikut :

a. Berdasarkan dari hasil uji coba empiris yang penulis lakukan, untuk proses kegiatan Enkripsi *file* teks (.txt) dengan ukuran sebesar 500 KB algoritma *IDEA* mempunyai kelebihan dari segi pemakaian *CPU*, *Memory* dan waktu dibandingkan algoritma *AES* dan *DES*. Algoritma *IDEA* hanya membutuhkan *CPU* 68 %, *Memory* 0.0405 %, waktu 367.0 ms. Sementara dari proses kegiatan Dekripsi *file* teks (.txt) dengan ukuran sebesar 2.188 KB, algoritma *DES* mempunyai kelebihan dari segi pemakain *CPU*, *Memory* dan waktu dibandingkan algoritma *AES* dan *IDEA*. Algortima *DES* hanya membutuhkan *CPU* 92 %, *Memory* 0.0136 %, waktu 783.0 ms.
b. Pada penelitian ini telah berhasil dirancang sebuah aplikasi bantu untuk membandingkan proses kinerja algoritma kriptografi *AES*, *DES* dan *IDEA* pada perangkat *mobile* berbasis sistem operasi *android* yang dapat berjalan pada *android* v2.3 *(gingerbread)* dan versi diatasnya.

6.2 Saran

Saran dari penulis untuk pengembangan aplikasi JAID ini lebih lanjut adalah aplikasi ini dapat dikembangkan dengan menggunakan algoritma simetris yang lain selain *AES*, *DES* dan *IDEA* dan menggunakan algoritma asimetris. Untuk kegiatan Enkripsi dan Dekripsi *file* teks (.txt) dengan ukuran *file* sebesar 500 – 2188 KB gunakan algoritma *AES* karena tidak banyak memutuhkan *resources smartphone* yang banyak.

DAFTAR PUSTAKA

Abd Elminaam Diaa Salama., Hatem Mohamed Abdual Kader., Mohiy Mohamed Hadhoud, May 2010, *Evaluating the Performance of Symmetric Encryption Algortithms,* International Journal of Network Security, Volume No : 10, PP No : 216-222.

Abd Elminaam Diaa Salama., Hatem Mohamed Abdual Kader., Mohiy Mohamed Hadhoud, Ocktober 2009, *Perfromance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices*, International Journal of Computer Theory and Engineering, Volume No : 1, ISSN : 1793-8201.

Ariyus Dony, Juni 2008, *Pengantar Ilmu Kriptografi,* Penerbit Andi, Yogyakarta.

Brahme Manoj V.., 2011, *Sms Based Secure Mobile Banking*, International Journal of Engineering and Technology, Volume No : 3(6), ISSN : 0975-4024.

Engeles Derick., July 2011, *Analysis of Chiper Text Size Produced by Various Encryption Algorithms,* International Journal of Engineering Science and Technology, Volume : 3, ISSN : 0975-5462.

Foelyati Rika., M. Ary Murti., Asep Mulyana, Juni 2009, *Analisis Perbandingan Unjuk Kerja Algoritma Lorentz, Julia Set dan Tent Function Sebagai Algoritma Chaotic*, Seminar Nasional Aplikasi Teknologi Informasi, ISSN : 1907-5022.

Goud V. Rajesham., Md. Hameed Pasha, 2011, *Textual Encryption Using Conventional Encryption Algorithm,* International Journal of Computer Trends and Technology, Volume No : 2, ISSN : 2231-2803.

Kumar G.Ramana., K.Suresh., B.Swati., Januari – februari 2012, *An Area-Efficient Universal Cryptography Processor for Smart Cards*, Journal of Engineering Research and Applications, Volume No : 2, ISSN : 2248-9622.

Kitsos Paris., Odysseas Koufopavlou, Januari 2004, *Configurable Hardware Implementations of Bulk Encryption Units for Wireless Communications*, The International Arab Journal of Information Technology, Volume : 1.

Kolhekar Megha., Anita Jadhav., July 2011, *Implementation of Elliptic Curve Cryptography On Text and Image,* International Journal of Enterprise Computing and Business System, Volume No : 1, ISSN : 2230-8849.

Mukherjee Swarnendu., Debashis Ganguly., Somnath Naskar, August 2009, *A New Generation Cryptographic Technique*, International Journal of Computer Theory and Engineering, Volume No : 1, ISSN : 1793-8201.

Nath Joyshree., Asoke Nath., March 2011, *Advanced Steganography Algorithm using Encrypted Secret Message*, International Journal of Advanced Computer Science and Applications, Volume No : 2, ISSN :

O. Alanazi Hamdan .., B.B. Zaidan., A.A. Zaidan., Hamid A. Jalab., M. Shabbir., Y. Al-Nabhani, March 2010, New Comparative Study Between DES, 3DES and AES within Nine Factors, Journal of Computing, Volume No : 2, ISSN : 2151-9617.

P.Saranya.., Varalakshmi L.M., March 2011, H.*264 based Selective Video Encryption for Mobile Applications*, International Journal of Computer Applications, Volume No : 4, ISSN : 0975-8887.

Qhobosheane Sehlabaka., Mokakatlela Mokakatlela., Makhamisa Senekane., May 2011, *Design and Implementation of a Encryption Mobile Objects Protocol (EMOP) for J2ME, J2SE, and J2EE Applications*, International Journal of Computer Science and Network Security, Volume No : 5, ISSN :

Reddy.P.V.G.D Prasad., K.R. Sudha., P. Sanyasi Naidu., 2010, *A Modified Location-Dependent Image Encryption for Mobile Information System, International Journal of Engineering Science and Technology*, Volume No : 2(5), ISSN : 0975-5462.

Rakheja Pankaj., July 2011, *Integrating DNA Computing in International Data Encryption Algortihm (IDEA)*, International Journal of Computer Application, Volume No : 26(3), ISSN : 0975-8887.

S. Navale Getta., Swati S. Joshi., Aarhadhana A. Deshmukh., Januari 2010, *M-Banking Security-a Futuristic Improved Security Approach*, International Journal of Computer Science Issues, Volume No : 7, ISSN : 1694-0814.

Saxena Kshitiz., 2010, *The Analyses of Wireless Encryption Protocol-Proposed Enhancement to Handshake Mechanism in WPA*, International Journal of Engineering and Technology, Volume No : 2(8) ISSN : 3657-3661.

Settia Neetu, December 2010, *Cryptanalysis od Modern Cryptographic Algorithms*, International Journal of Computer Science and Technology, Volume No : 1, ISSN : 2229-4333.

Thulasimani L.., M.Madheswaran., 2010., *Design and Implementation of Reconfigurable Rijndael Encryption Algorithms for Reconfigurable Mobile Terminals*, International Journal on Computer Science and Engineering, Volume No : 2, ISSN : 0975-3397.

LAMPIRAN

SKPL

SPESIFIKASI KEBUTUHAN PERANGKAT LUNAK

JAID

(Analisis Perbandingan Algoritma Kriptografi AES, DES DAN IDEA yang Tepat untuk Perangkat Mobile)

Untuk :

Kepentingan Penelitian

Dipersiapkan Oleh :

BUDY / 115301627

Program Studi Magister Teknik Informatika

Universitas Atma Jaya Yogyakarta

DAFTAR PERUBAHAN

Revisi	Deskripsi
A	
B	
C	
D	
E	
F	

INDEX TGL	-	A	B	C	D	E	F
Ditulis oleh							
Diperiksa oleh							
Disetujui oleh							

DAFTAR HALAMAN PERUBAHAN

Halaman	Revisi	Halaman	Revisi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

A. Pendahuluan

1. Tujuan

Dokumen Spesifikasi Kebutuhan Perangkat Lunak (SKPL) ini merupakan dokumen spesifikasi kebutuhan perangkat lunak JAID (Analisis Perbandingan Algoritma Kriptografi *AES*, *DES* dan *IDEA* yang tepat untuk Perangkat *Mobile*) untuk mendefinisikan kebutuhan perangkat lunak yang meliputi antarmuka, (antarmuka antara perangkat lunak dengan *user*) dan atribut (*feature-feature* tambahan yang dimiliki sistem), serta mendefinisikan fungsi-fungsi perangkat lunak.

2. Ruang Lingkup

Perangkat Lunak JAID dikembangkan dengan tujuan untuk :

a. Menganalisis algoritma-algoritma (*AES*, *DES* dan *IDEA*) yang telah ditentukan, untuk proses enkripsi dan dekripsi guna mengetahui kinerja dari masing-masing algoritma tersebut.

3. Definisi dan Akronim

Tabel 1 berikut ini berisi daftar definisi akronim dan singkatan.

Tabel 1. Daftar Definisi Akronim dan Singkatan

Keyword/phrase	Definisi
SKPL	Adalah spesifikasi kebutuhan dari perangkat lunak JAID yang akan dikembangkan.
SKPL-JAID-xxx	Kode yang merepresentasikan kebutuhan pada JAID dimana xxx merupakan nomor fungsi produk.
JAID	Perangkat lunak berbasis *android* yang berfungsi sebagai *tool* pembantu untuk membandingkan algoritma *AES*, *DES* dan *IDEA* untuk proses enkripsi dan dekripsi.
Algoritma	Adalah kumpulan urutan perintah yang menentukan operasi-operasi tertentu yang diperlukan untuk menyelesaikan suatu masalah atau mengerjakan suatu tugas tertentu.
Android	Adalah sistem operasi untuk perangkat *mobile* yang berbasis linux.
Android SDK	Adalah *tools API* (*Applications Programming Interface*) yang diperlukan untuk memulai mengembangkan aplikasi pada *platform android* menggunakan bahasa pemrograman java.
ADT	*ADT* (*android development tools*) adalah plugin yang didesain untuk *IDE eclipse*.
AES	*Advanced Encryption Standart* merupakan algoritma *block cipher* yang menggunakan sistem permutasi dan subsitusi (*P-Box* dan *S-Box*) bukan dengan jaringan *Feistel* sebagaimana *block chiper* pada umumnya.

DES	*Data Encryption Standart* merupakan algoritma yang beroperasi pada ukuran blok 64 bit. *DES* mengenkripsikan 64 bit teks asli menjadi 64 bit teks kode dengan menggunakan 56 bit kunci internal.
IDEA	*Internationa Data Encryption Standart* merupakan algoritma beroperasi pada sebuah blok teks-asli yang panjangnya 64 bit dan kunci 128 bit.

4. Referensi

Referensi yang digunakan dalam pembuatan SKPL ini adalah sebagai berikut :

a. Pressman Rogeer S., Software Engineering Seventh Edition, McGraw-Hill International Companies, 2010.
b. Emmanuel Safirman Bata, Pengembangan Sistem Pakar Berbasis Mobile untuk Membantu Mendiagnosis Penyakit Akibat Gigitan Nyamuk, 2012.
c. FX. Yudho Prasojo, Pembangunan Layanan Berbasis Lokasi untuk *User* Trans Jogja di Platform Android, 2012.
d. Felix Cahya Suryana, Implementasi Kriptografi dengan Algoritma 3-DES dan RSA pada Sistem Informasi Rekam Medik Berbasis WEB, 2008.

5. Deskripsi Umum (*Overview*)

Secara umum dokumen SKPL ini terbagi atas tiga bagian utama. Bagian pertama berisi penjelasan mengenai

dokumen SKPL yang mencakup tujuan pembuatan SKPL, ruang lingkup masalah dalam perancangan perangkat lunak JAID, definisi, akronim dan singkatan-singkatan yang digunakan dalam pembuatan SKPL, referensi dan deskripsi umum tentang dokumen SKPL.

Bagian kedua berisi penjelasan umum tentang perangkat lunak JAID yang akan dirancang, mencakup perspektif produk yang akan dikembangkan, fungsi perangkat lunak karakteristik *user*, batasan dalam *user*an perangkat lunak dan asumsi yang dipakai dalam perancangan perangkat lunak JAID yang akan dirancang.

B. Deskripsi Kebutuhan

1. Perspektif Produk

Aplikasi pembanding algoritma *AES, DES* dan *IDEA* pada perangkat *mobile* (JAID*)* yang berbasis sistem operasi *andorid* ini dirancang untuk membantu penulis menguji kinerja algoritma-algoritma sesuai dengan spesifikasi *smartphone* yang digunakan. Sehingga penulis dapat memperoleh hasil yang nanti dijadikan data untuk dianalisis agar bisa tercapai kesimpulan sesuai dengan bukti empiris pada saat uji coba. Harapan selanjutnya ditujukan pada para pengembang aplikasi kriptografi pada perngakat *mobile*, agar dapat menentukan algoritma yang tepat untuk merancang sebuah aplikasi kriptografi

pada perangkat *mobile* sesuai dengan spesifikasi *smartphone* tersebut. Aplikasi ini tidak digunakan secara umum pada kalangan pengguana perangkat *mobile* khususnya yang berbasis sistem operasi *android*. Pengujian waktu proses enkripsi dan dekripsi dilakukakan dengan memasukkan *file* teks (*.txt)* sesuai dengan ukuran *file* yang telah ditentukan.

JAID berjalan pada *platform android* dan dibuat mengguanakan bahasa pemrograman *android*, *editor Eclipse Galileo. User* JAID adalah *user* biasa yang akan berinteraksi langsung dengan sistem melalui *GUI (Graphical User Interface).* Untuk bisa menjalankan *feature-feature* yang terdapat pada aplikasi JAID, *user* bisa menggunakan *trackpad* yang telah disediakan pada perangkat *mobile*. Selain itu *user* juga bisa mengakses melalui *touch screen* atau langsung pada layar sentuh, dan pada umumnya *smartphone* yang menggunakan sistem operasi *android* sudah mendukung teknologi *touch screen.*

2. Fungsi Produk

a. Fungsi Mengenkripsi

Fungsi mengenkripsi merupakan fungsi awal yang digunakan untuk mengenkripsi *file* teks *(.txt)* atau

plaintext yang hendak di enkripsi dengan menggunakan algoritma yaitu *DES*, *AES* dan *IDEA*.

b. Fungsi Mendekripsi

Fungsi mendekripsi merupakan fungsi kedua setelah *file* teks (.txt) yang sudah dienkripsi atau *chipertext*. Fungsi ini digunakan untuk mendeskripsi *file teks (.txt)* yang telah di enkripsi sebelumnya.

3. Karakteristik *User*

Karakteristik dari *user* perangkat lunak JAID yaitu :

a. *User*

1)Memahami perangkat lunak yang digunakan.

2)Memahami pengoprasian perangkat *mobile* dengan *platform android.*

4. Batasan-batasan

Batasan-batasan dalam perancangan perangkat lunak JAID tersebut adalah :

a. Kebijakan Umum

Berpedoman pada tujuan dari perancangan perangkat lunak JAID.

b. Keterbatasan Perangkat Keras

Dapat diketahui kemudian setelah sistem ini berjalan (sesuai kebutuhan).

5. Asusmsi dan Ketergantungan

Asumsi yang digunakan dalam perancangan perangkat lunak JAID yaitu sebagai berikut :

a. Perangakat *mobile* berbasis *android* minimal versi 2.3 *Gingerbread*.
b. Data yang di enkripsi maunpun dekripsi harus sesuai (*file* teks *.txt*).

C. Kebutuhan Khusus

1. Kebutuhan Antarmuka Eksternal

Kebutuhan antarmuka eksternal pada perangkat lunak JAID meliputi kebutuhan antarmuka pemakai, antarmuka perangkat keras, antarmuka perangkat lunak.

a. Antarmuka Pemakai

User berinteraksi dengan antarmuka yang ditampilkan dalam bentuk *form-form.*

b. Antarmuna perangkat keras

Perangkat keras yang digunakan untuk menjalankan perangkat lunak JAID adalah sebagai berikut :

1) Perangkat *mobile* atau *smartphone* minimal berbasis *android* 2.3 *Gingerbread*.

c. Antarmuka perangkat lunak

Perangkat lunak yang dibutuhkan untuk mengoprasikan perangkat lunak JAID adalah sebagai berikut :

b) Nama : *Google Android v2.3 Gingerbread*

Sumber : *Google*

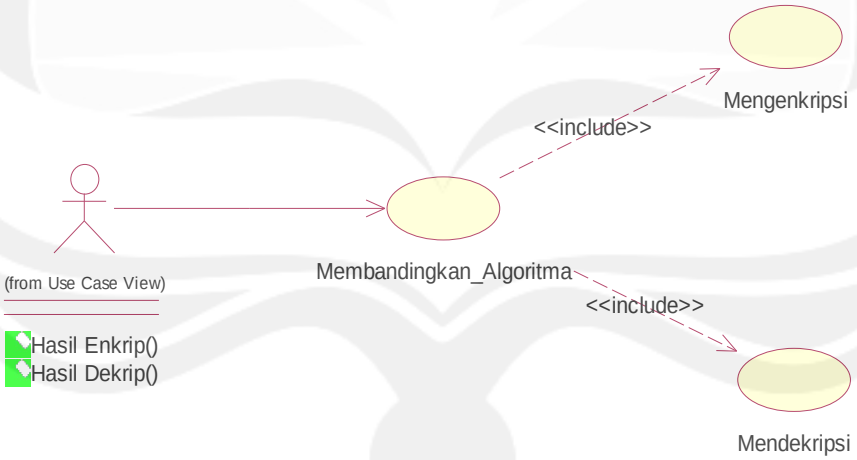
Fungsi : Sebagai sistem operasi yang digunakan pada *mobile device*.

2) Nama : *DalvikVM* (*dalvik* virtual mesin)

Sumber : *Apache*

Fungsi : Merupakan *interpreter* yang mengeksekusi *file* kedalam format *dalvik executable* (*.*dex*).

2. Kebutuhan Fungsionalitas Perangkat Lunak



Gambar 1. *Use Case* Diagram JAID

Use case pada gamabar diatas menunjukkan satu aktor yang berhubungan langsung dengan sistem yaitu *user*. *User* berfungsi untuk menjalankan aplikasi,

penjelasan secara rinci dapat dilihat pada *Use Case Spesification* berikut ini.

D. Spesifikasi Rinci Kebutuhan

1. Spesifikasi *use case* : Mengenkripsi

Tabel 2. Spesifikasi *use case* : Enkripsi

Use case name	Mengenkripsi
Brief description	*Use case* ini digunakan *user* untuk melakukan enkripsi *file teks* (.txt) menggunakan algoritma yang tersedia yaitu *AES*, *DES* dan *IDEA*.
Actor	*User*.
Basic Flow	1. *Use case* ini dimulai ketika *user* hendak melakukan enkripsi. 2. *User* memasukkan *plainttext* berupa *file* berekstensi teks (*.txt)*. 3. *User* memasukkan kunci (22 karakter). 4. *User* melakukan *read file*. 5. Sistem melakukan enkripsi *file* teks(.txt). 6. Sistem menampilkan informasi penggunaan *resources* untuk proses enkripsi tersebut. 7. *Use case* selesai.
Altirnative flow	*None*
Error flow	E-1 : *User* belum *read file* plaintext yang akan dienkripsi. 1. Sistem memberikan peringatan bahwa *user* belum melakukan *read file*.

	2. Kembali ke *basic flow* langkah keempat. E-2 : *User* memasukkan kunci lebih atau kurang dari 22 karakter. 1. Sistem memberikan peringatan bahwa *user* memasukkan kunci lebih atau kurang dari 22 karakter. 2. Kembali ke *basic flow* langkah ketiga.
Pre conditions	None
Post conditions	Proses enkripsi dijalankan.

2. Spesifikasi use case : Mendekripsi

Tabel 3. Spesifikasi *use case* : Dekripsi

Use case name	Mendekripsi
Brief description	*Use case* ini digunakan *user* untuk melakukan dekripsi *file teks* (.txt) yang sudah dienkripsi sebelumnya.
Actor	*User*.
Basic Flow	*1. Use case* ini dimulai ketika *user* hendak melakukan dekripsi. *2. User* memasukkan *chipertext* berupa *file* teks (*.txt)*. *3. User* memasukkan kunci (22 karakter). *4. User* melakukan *read file*. *5.* Sistem melakukan dekripsi *file* teks(.txt). *6.* Sistem menampilkan informasi

	penggunaan *resources* untuk proses enkripsi tersebut. 7. *Use case* selesai.
Altirnative flow	*None*
Error flow	E-1 : *User* belum *read file chipertext* yang akan dienkripsi. 1. Sistem memberikan peringatan bahwa *user* belum melakukan *read file*. 2. Kembali ke *basic flow* langkah keempat. E-2 : *User* memasukkan kunci lebih atau kurang dari 22 karakter. 1. Sistem memberikan peringatan bahwa *user* memasukkan kunci lebih atau kurang dari 22 karakter. 2. Kembali ke *basic flow* langkah ketiga.
Pre conditions	*Use case enkripsi* telah dilakukan.
Post conditions	Proses dekripsi dijalankan.

DPPL

DESKRIPSI PERANCANGAN PERANGKAT LUNAK

JAID

(Analisis Perbandingan Algoritma Kriptografi AES, DES DAN IDEA yang Tepat untuk Perangkat Mobile)

Untuk :

Kepentingan Penelitian

Dipersiapkan Oleh :

BUDY / 115301627

Program Studi Magister Teknik Informatika

Universitas Atma Jaya Yogyakarta

DAFTAR PERUBAHAN

Revisi	Deskripsi
A	
B	
C	
D	
E	
F	

INDEX TGL	-	A	B	C	D	E	F
Ditulis oleh							
Diperiksa oleh							
Disetujui oleh							

DAFTAR HALAMAN PERUBAHAN

Halaman	Revisi	Halaman	Revisi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

A. Pendahuluan

1. Tujuan

Dokumen Deskripsi Perancangan Perangkat Lunak (DPPL) ini merupakan dokumen Deskripsi Perancangan Perangkat lunak JAID (Analisis Perbandingan Algoritma Kriptografi *AES*, *DES* dan *IDEA* yang tepat untuk Perangkat *Mobile*). Dokumen DPPL tersebut digunakan oleh pengembang perangkat lunak sebagai acuan untuk implementasi pada tahap selanjutnya.

2. Ruang Lingkup

Perangkat Lunak JAID dikembangkan dengan tujuan untuk :

b. Menganalisis algoritma-algoritma (*AES*, *DES* dan *IDEA*) yang telah ditentukan, untuk proses enkripsi dan dekripsi guna mengetahui kinerja dari masing-masing algoritma tersebut pada setiap *smartphone*.

3. Definisi dan Akronim

Tabel 1 berikut ini berisi daftar definisi akronim dan singkatan.

Tabel 1. Daftar Definisi Akronim dan Singkatan

Keyword/phrase	Definisi
DPPL	Deskripsi Perancangan Perangkat Lunak atau disebut juga *Software Design Description* (SDD) merupakan deskripsi dari perancangan produk/perangkat lunak yang akan dikembangkan.
JAID	Perangkat lunak berbasis *android* yang berfungsi sebagai *tool* pembantu untuk membandingkan algoritma *AES*, *DES* dan *IDEA* untuk proses enkripsi dan dekripsi.
Algoritma	Adalah kumpulan urutan perintah yang menentukan operasi-operasi tertentu yang diperlukan untuk menyelesaikan suatu masalah atau mengerjakan suatu tugas tertentu.
Android	Adalah sistem operasi untuk perangkat *mobile* yang berbasis *linux*.
Android SDK	Adalah *tools API* (*Applications Programming Interface*) yang diperlukan untuk memulai mengembangkan aplikasi pada *platform android* menggunakan bahasa pemrograman *java*.
ADT	*ADT* (*android development tools*) adalah *plugin* yang didesain untuk *IDE eclipse*.
AES	*Advanced Encryption Standart* merupakan algoritma *block cipher* yang menggunakan sistem permutasi dan subsitusi (*P-Box* dan *S-Box*) bukan dengan jaringan *Feistel* sebagaimana *block chiper*

	pada umumnya.
DES	*Data Encryption Standart* merupakan algoritma yang beroperasi pada ukuran blok 64 bit. *DES* mengenkripsikan 64 bit teks asli menjadi 64 bit teks kode dengan menggunakan 56 bit kunci internal.
IDEA	*Internationa Data Encryption Standart* merupakan algoritma beroperasi pada sebuah blok teks-asli yang panjangnya 64 bit dan kunci 128 bit.

4. Referensi

Referensi yang digunakan dalam pembuatan SKPL ini adalah sebagai berikut :

e. Pressman Rogeer S., Software Engineering Seventh Edition, McGraw-Hill International Companies, 2010.

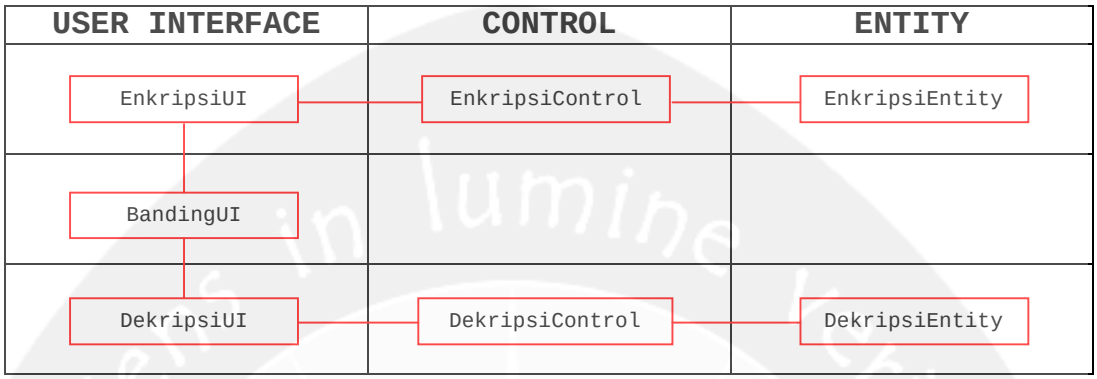
f. Emmanuel Safirman Bata, Pengembangan Sistem Pakar Berbasis Mobile untuk Membantu Mendiagnosis Penyakit Akibat Gigitan Nyamuk, 2012.

g. FX. Yudho Prasojo, Pembangunan Layanan Berbasis Lokasi untuk Pengguna Trans Jogja di Platform Android, 2012.

h. Felix Cahya Suryana, Implementasi Kriptografi dengan Algoritma 3-DES dan RSA pada Sistem Informasi Rekam Medik Berbasis WEB, 2008.

B. Perancangan Sistem

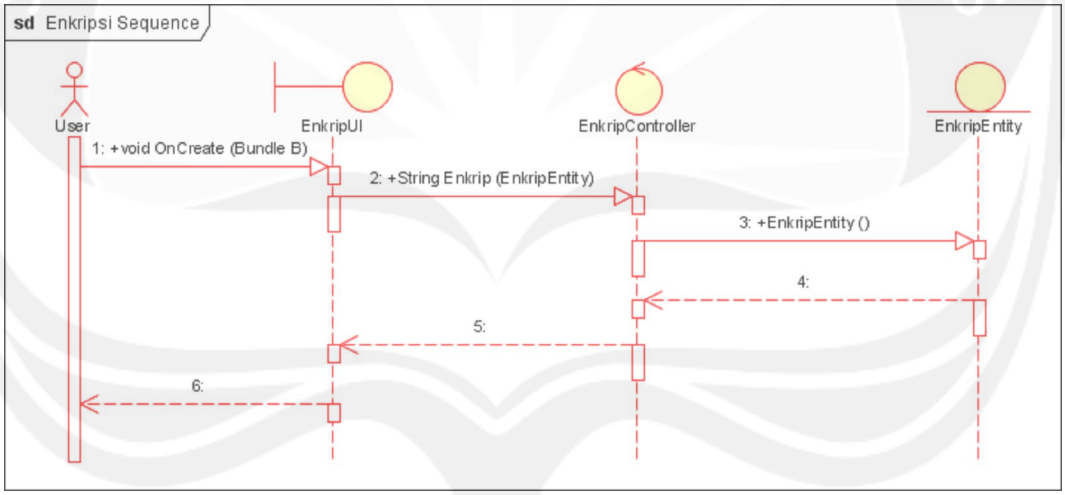
1. Perancangan Arsitektur



Gambar 1. Perancangan Arsitektur

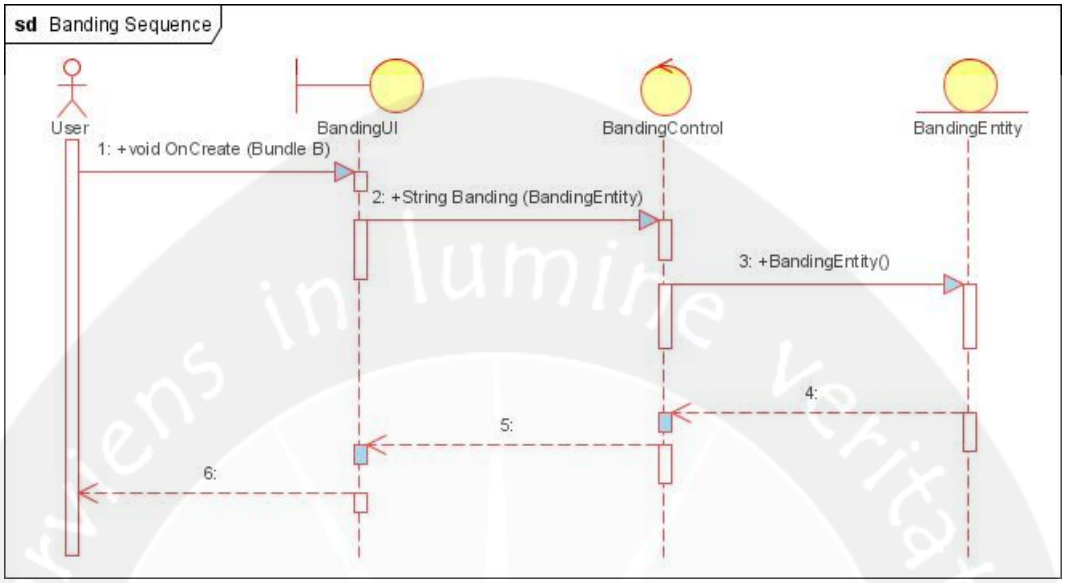
2. Perancangan Rinci

a. Enkripsi



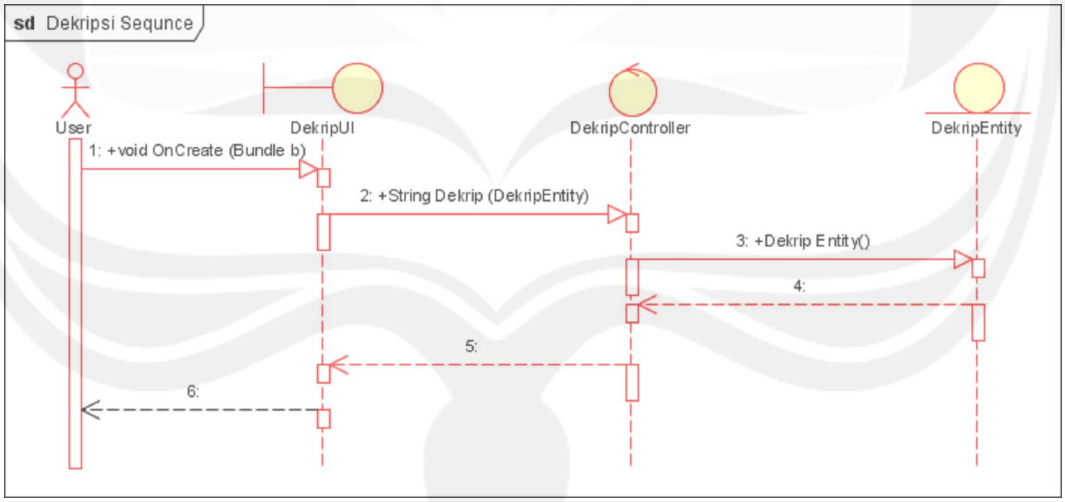
Gambar 2. Perancangan Rinci Enkripsi

b. Banding



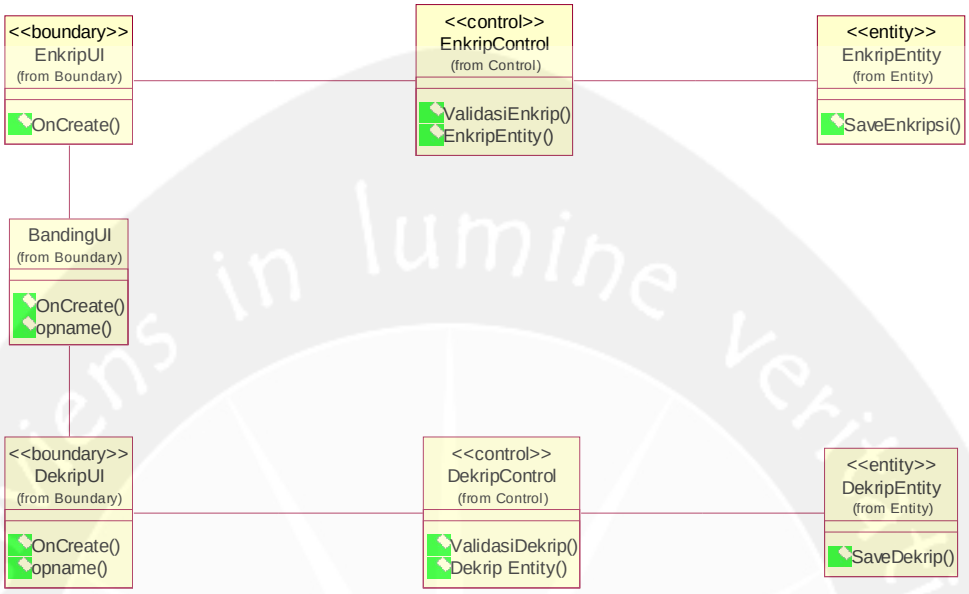
Gambar 3. Perancangan Rinci Banding

c. Dekripsi



Gambar 3. Perancangan Rinci Dekripsi

3. Class Diagram



Gambar 4. *Class* Diagram

4. Deskripsi Kelas

a. *Specific Design Class* EnkripsiUI

Tabel 2. *Specific Design Class* EnkripsiUI

EnkripsiUI	**<<boundary>>**
+void onCreate(Bundle b) *Construktor*, ini digunakan untuk menginisialisasi semua atribut dari kelas ini. +Enkripsi ():String Variabel ini digunakan untukmasuk ke dalam Menu Enkripsi yang berfungsi mengenkripsi *file teks teks teks (.txt)*.	

b. *Specific Design Class* BandingUI

Tabel 3. *Specific Design Class* EnkripsiUI

BandingUI	**<<boundary>>**
+void onCreate(Bundle b) *Construktor*, ini digunakan untuk menginisialisasi semua atribut dari kelas ini. +Banding ():String Variabel ini digunakan untuk masuk ke dalam Menu Banding	

yang berfungsi membanding algoritma.

c. *Specific Design Class* DekripsiUI

Tabel 4. *Specific Design Class* DekripsiUI

DekripsiUI	**<<boundary>>**
+void onCreate(Bundle b) *Construktor*, ini digunakan untuk menginisialisasi semua atribut dari kelas ini. +Dekripsi ():String Variabel ini digunakan untuk masuk ke dalam Menu Dekripsi yang berfungsi mendekripsi *file teks (.txt)*.	

C. Perancangan Antarmuka

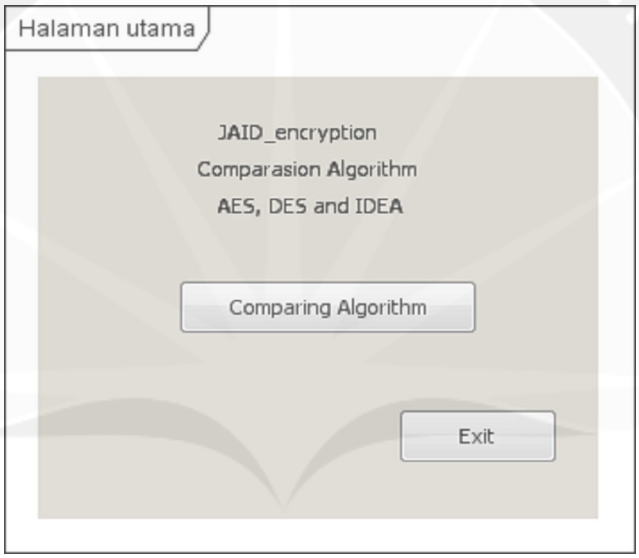
1. *Splash Screen*

Splash Screen merupakan tampilan pertama program JAID sebelum masuk ke menu utama. Rancangan *Splash Screen* dapat dilihat pada gambar 5 berikut ini.

Gambar 5. *Splash Screen* JAID

2. Halaman Utama

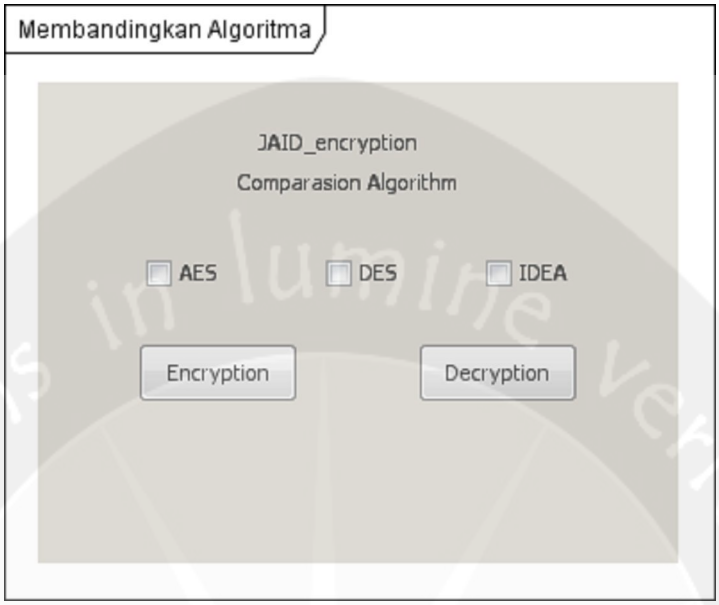
Halaman utama merupakan merupakan antarmuka yang berfungsi sebagai menu utama yang terdapat menu *comparing algorithm* dan *exit.* Menu *comparing algorithm* digunakan untuk kegiatan membandingkan algoritma sedangkan menu *exit* untuk keluar dari aplikasi JAID. Halaman utama dapat dilihat pada gambar 6 berikut ini.



Gambar 6. Halaman Utama JAID

3. Halaman *Comparing Algorithm*

Halaman *comparing algorithm* merupakan antarmuka yang digunakan oleh *user* untuk melakukan proses enkripsi dan dekripsi. Didalam halaman ini terdapat menu pilihan *encryption* dan *decryption* yang digunakan untuk enkripsi dan dekripsi. Halaman *comparing algorithm* dapat dilihat pada gambar 7 berikut ini.



Gambar 7. Halaman *comparing algorithm*

4. Halaman *Encryption*

Halaman *encryption* pada gambar 8 merupakan halaman antarmuka yang digunakan oleh *user* untuk proses enkripsi sesuai dengan algoritma yang sudah ditentukan. Pada halaman ini terdapat menu *read file* untuk membaca *file teks (.txt)* yang diinputkan dan *encryption* untuk proses enkripsi. Rancangan antarmuka halaman *encryption* dapat dilihat pada gambar 8 berikut ini.

Gambar 8. Halaman *encryption* JAID

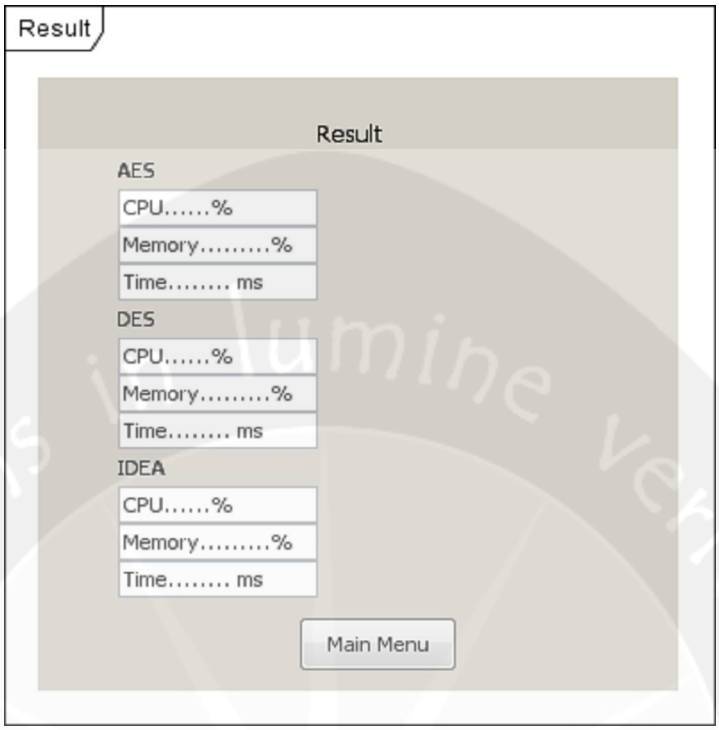
5. Halaman *Decryption*

Halaman *decryption* pada gambar 9 merupakan halaman antarmuka yang digunakan oleh *user* untuk melakukan proses dekripsi sesuai dengan algoritma yang digunakan pada proses enkripsi sebelumnya. Pada halaman ini terdapat menu *read file* untuk membaca *file teks (.txt)* yang hendak didekripsi dan menu *decryption* untuk proses dekripsi. Rancangan antarmuka halaman *decryption* dapat dilihat pada gambar 9 berikut ini.

Gambar 9. Halaman *decryption* JAID

6. Halaman *Result*

Halaman *Result* pada gamabar 10 merupakan halaman antarmuka yang digunakan oleh *user* untuk melihat informasi *resources* dan algoritma yang digunakan oleh sistem ketika proses yang terdiri dari informasi *CPU*, *Memory* dan *Time* pada saat sistem melakukan proses enkripsi dan dekripsi sesuai dengan algoritma yang digunakan pada proses enkripsi sebelumnya. Rancangan antarmuka halaman *result* dapat dilihat pada gambar 10 berikut ini.



Gambar 10. Halaman *Result* JAID