

**PERANCANGAN APLIKASI DIARY MENGGUNAKAN
ALGORITMA KRIPTOGRAFI RC6
BERBASIS ANDROID**

SKRIPSI



Disusun oleh

AEDHOH SALIM ASSAIDI

12.11.5806

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA**

2015

**PERANCANGAN APLIKASI DIARY MENGGUNAKAN
ALGORITMA KRIPTOGRAFI RC6
BERBASIS ANDROID**

SKRIPSI

Untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



Disusun oleh

AEDHOH SALIM ASSAIDI

12.11.5806

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA**

2015

PERSETUJUAN

SKRIPSI

**PERANCANGAN APLIKASI DIARY MENGGUNAKAN
ALGORITMA KRIPTOGRAFI RC6
BERBASIS ANDROID**

Yang dipersiapkan dan disusun oleh

Aedhoh Salim Assaidi

12.11.5806

Telah disetujui oleh Dosen Pembimbing Skripsi

Pada tanggal 11 Maret 2015

Dosen Pembimbing,

Armadyah Amborowati, S.Kom, M.Eng.

NIK. 190302063

PENGESAHAN

SKRIPSI

**PERANCANGAN APLIKASI DIARY MENGGUNAKAN
ALGORITMA KRIPTOGRAFI RC6
BERBASIS ANDROID**

Yang disusun oleh

Aedhoh Salim Assaidi

12.11.5806

Telah dipertahankan di depan Dewan Penguji

Pada tanggal 15 Oktober 2015

Susunan Dewan Penguji

Nama Penguji

Barka Satva, M.Kom.
NIK. 190302126

Yuli Astuti, M.Kom.
NIK. 190302146

Armadyah Amborowati, S.Kom, M.Eng.
NIK. 190302063

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 10 November 2015



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa, Skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam Skripsi ini tidak terdapat karya yang pernah diajukan orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

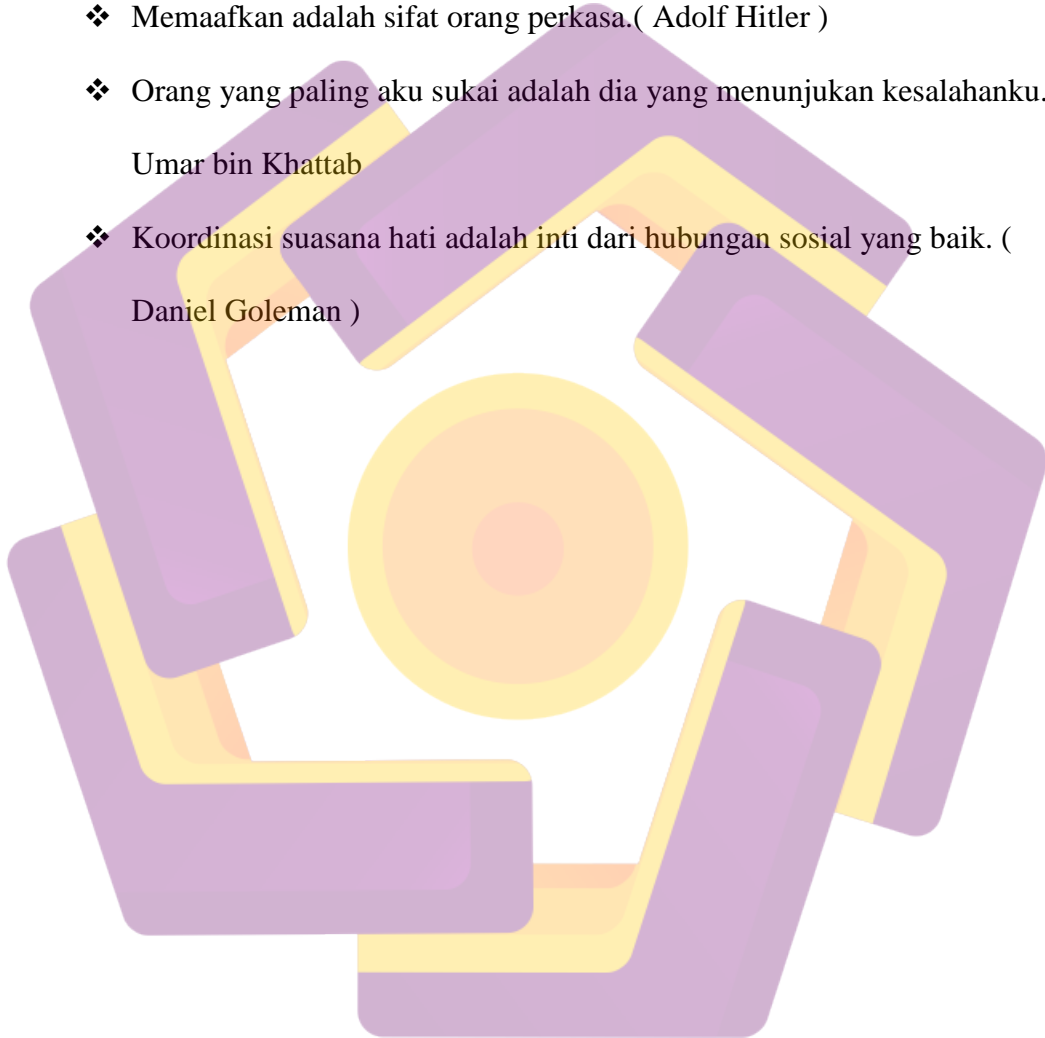
Yogyakarta, 10 November 2015



Aedhoh Salim Assaidi
12.11.5806

MOTTO

- ❖ Jadilah bagian dari perubahan yang ingin kamu saksikan di dunia ini. (Adolf Hitler)
- ❖ Memaafkan adalah sifat orang perkasa.(Adolf Hitler)
- ❖ Orang yang paling aku sukai adalah dia yang menunjukkan kesalahanku. (Umar bin Khattab
- ❖ Koordinasi suasana hati adalah inti dari hubungan sosial yang baik. (Daniel Goleman)



PERSEMBAHAN

Skripsi ini bukanlah hasil terbaik, namun penulis berusaha sebaik mungkin untuk mempersembahkan karya ini kepada :

1. Umi Afiah Muhasin, Abi Salim Assaidi yang terus mendukung dan mendoakan kelancaran dan kemudahan.
2. Chal Faris Muhasin, Kakak Adik Latif Assaidi, Adik-adik Chaifah Assaidi dan Muhammad Assaidi yang mendukung dan mendoakan.
3. Teman-teman saya Sugeng Andreassusilo, Julian Damas Suryawan , Rizki Samudra, Wikan Setya L.P , Afi Muhammad Furqoni, dan yang tidak dapat disebutkan satu persatu, yang telah membantu serta mendukung dalam penyusunan Skripsi ini.
4. Rekan-rekan Seperjuangan Himpunan Mahasiswa Jurusan Teknik Informatika (HMJTI) STMIK AMIKOM Yogyakarta, yang telah memberi banyak pengalaman dan wawasan berorganisasi terutama Intan Meydian Sari, yang juga memberi banyak referensi penulisan dan masukan.
5. Rekan-rekan Kelas 12 S1 TI 02 yang banyak memberi pengalaman dan keceriaan selama perkuliahan baik di kelas maupun di luar kelas.

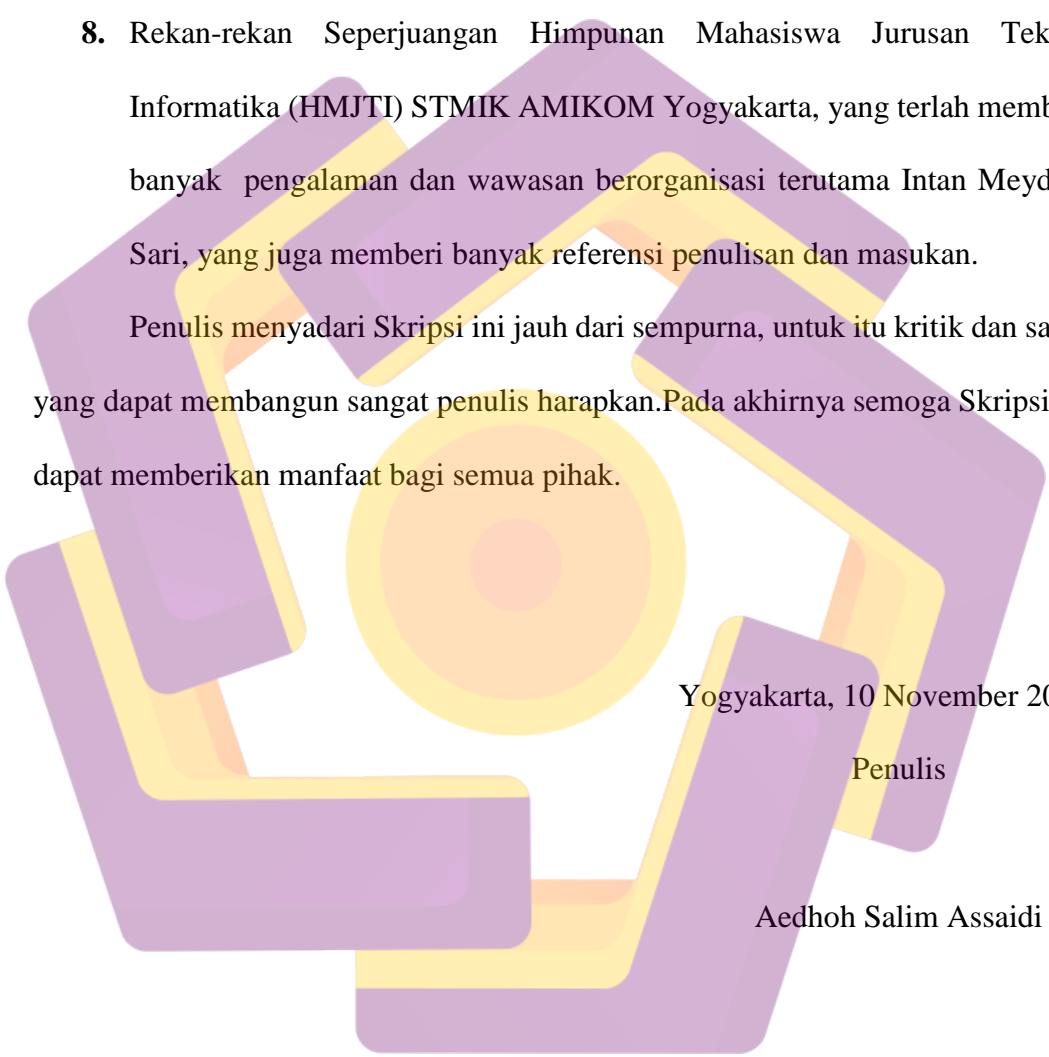
KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillahirobil'amin. Puji syukur terpanjat kehadirat Allah SWT, yang telah melimpahkan rahmat dan hidayah-Nya, sehingga Skripsi berjudul **“PERANCANGAN APLIKASI DIARY MENGGUNAKAN ALGORITMA KRIPTOGRAFI RC6 BERBASIS ANDROID”** dapat terselesaikan dengan baik, lancar dan tepat waktu. Salawat serta salam semoga tetap dilimpahkan kepada Nabi Muhammad SAW beserta keluarga dan sahabat-sahabatnya.

Skripsi ini disusun sebagai syarat memperoleh gelar Strata-1. Keberhasilan dalam penyusunan Skripsi ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, terima kasih penulis ucapkan kepada :

1. Kedua Orang tua tercinta Umi Afiah Muhasin dan Abi Salim Assaidi yang terus mendukung dan mendoakan kelancaran dan kemudahan.
2. Paman Chal Faris Muhasin, Kakak Adik Latif Assaidi, Adik-adik Chaifah Assaidi dan Muhammad Assaidi yang mendukung dan mendoakan.
3. Bapak Prof.M. Suyanto MM, selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer “ AMIKOM” Yogyakarta.
4. Ibu Armadyah Amborowati, S,Kom, M.Eng , selaku dosen pembimbing
5. Bapak Sudarmawan, M.T, selaku Ketua Jurusan S1 Teknik Informatika
6. Segenap staff dan dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya selama perkuliahan serta semua pihak yang tidak dapat saya sebutkan satu per satu

- 
7. Teman-teman saya Sugeng Andreassusilo, Julian Damas Suryawan , Rizki Samudra, Wikan Setya L.P , Afi Muhammad Furqoni, dan yang tidak dapat disebutkan satu persatu, yang telah membantu serta mendukung dalam penyusunan Skripsi ini.
 8. Rekan-rekan Seperjuangan Himpunan Mahasiswa Jurusan Teknik Informatika (HMJTI) STMIK AMIKOM Yogyakarta, yang telah memberi banyak pengalaman dan wawasan berorganisasi terutama Intan Meydian Sari, yang juga memberi banyak referensi penulisan dan masukan.
Penulis menyadari Skripsi ini jauh dari sempurna, untuk itu kritik dan saran yang dapat membangun sangat penulis harapkan. Pada akhirnya semoga Skripsi ini dapat memberikan manfaat bagi semua pihak.

Yogyakarta, 10 November 2015

Penulis

Aedhoh Salim Assaidi

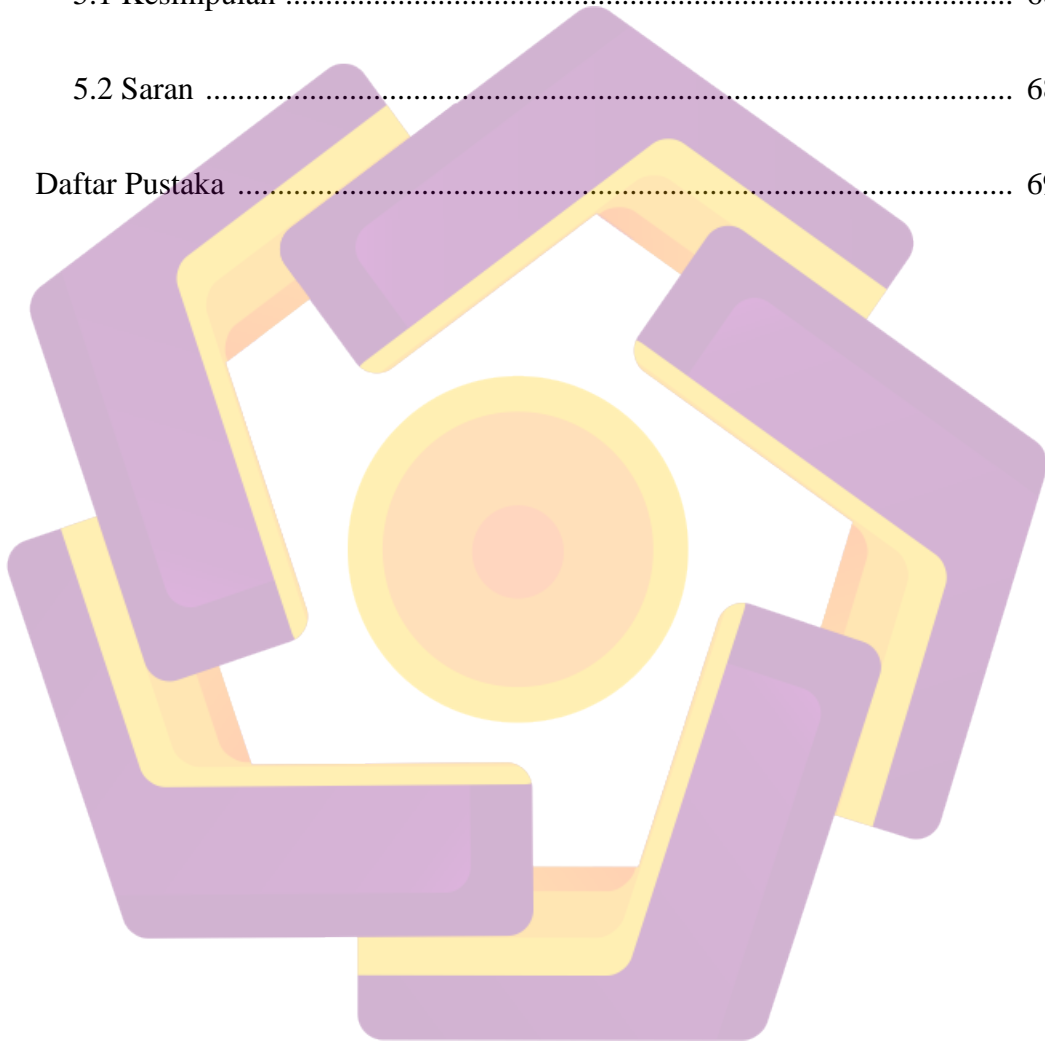
Daftar Isi

HALAMAN JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvi
<i>ABSTRACT</i>	xvii
BAB I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Metode Penelitian	3
1.6 Sistematika Penulisan	4
BAB II Landasan Teori	6
2.1 Tinjauan Pustaka	6
2.2 Dasar Teori	8

2.2.1 <i>Diary</i>	8
2.2.2 Kriptografi	8
2.2.2.1 Algoritma Kriptografi	9
2.2.2.2 Rivest Cipher 6 (RC6)	10
2.2.3 <i>Systems Development Life Cycle (SDLC)</i>	14
2.2.4 Analisis Kebutuhan Sistem	15
2.2.5 <i>Unified Modeling Language (UML)</i>	17
2.2.5.1 <i>Use case</i> Diagram	17
2.2.5.2 <i>Activity</i> Diagram	19
2.2.5.3 <i>Class</i> Diagram	19
2.2.5.4 <i>Sequence</i> Diagram	20
2.2.6 Pengujian Sistem	21
2.2.6.1 <i>White-box</i> Testing	21
2.2.6.2 <i>Black-box</i> Testing	22
BAB III Analisi dan Perancangan	23
3.1 Gambaran Umum Sistem	23
3.2 Analisis Kebutuhan Sistem	23
3.2.1 Kebutuhan Fungsional	23
3.2.2 Kebutuhan Non Fungsional	24
3.2.2.1 Kebutuhan Perangkat Keras	24
3.2.2.2 Kebutuhan Perangkat Lunak	25
3.3 Perancangan UML	25

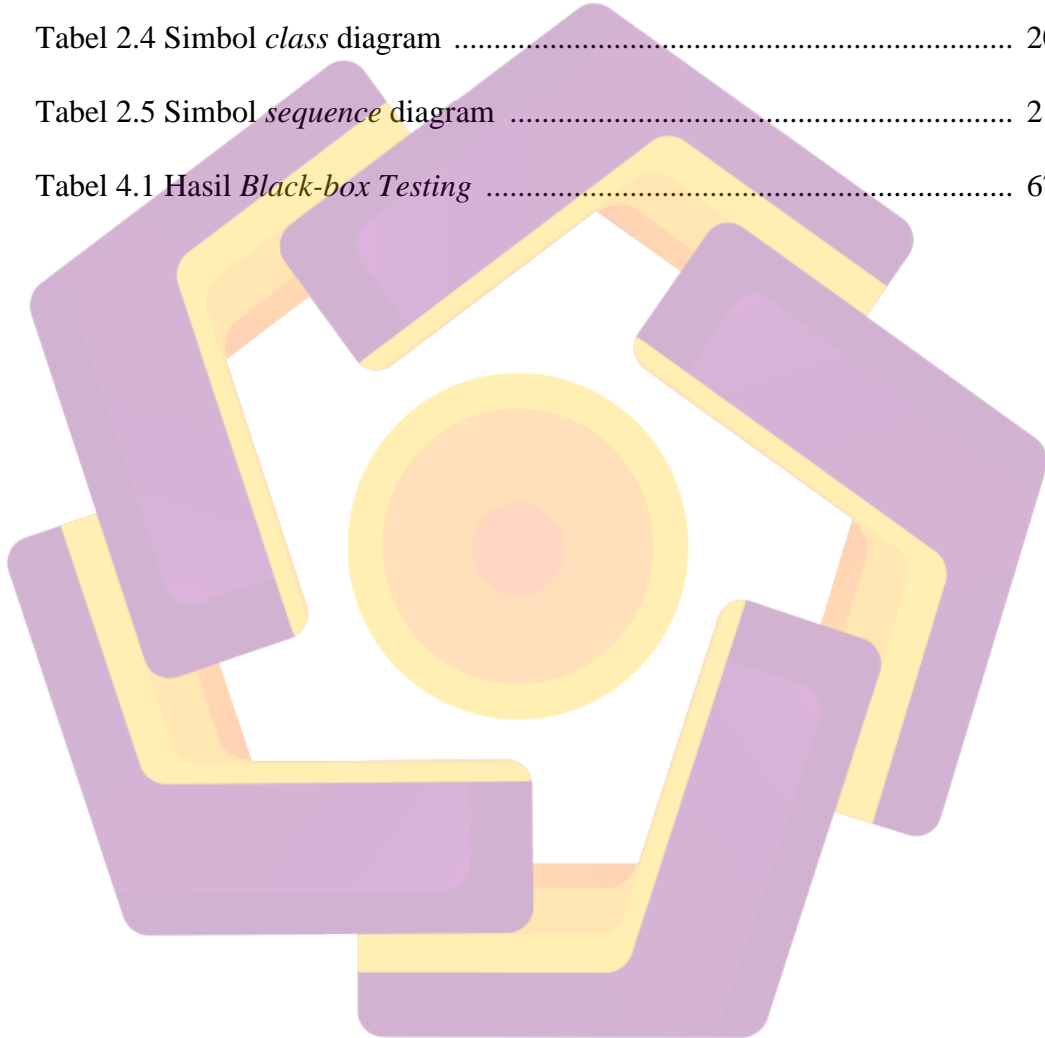
3.3.1 <i>Use case</i> Diagram	25
3.3.2 <i>Activity</i> Diagram	26
3.3.3 <i>Class</i> Diagram	32
3.3.4 <i>Sequence</i> Diagram	32
3.3.5 Rancangan Antar Muka	35
BAB IV Implementasi dan Pembahasan	38
4.1 Implementasi Kode Program	38
4.1.1 Algoritma Kriptografi RC6	38
4.1.2 Menu Tambah <i>Diary</i>	46
4.1.3 Menu <i>Edit Diary</i>	48
4.1.4 <i>Data Base Diary</i>	50
4.2 Implementasi Antar Muka	52
4.2.1 <i>Splash Screen</i>	52
4.2.2 Menu <i>Login</i>	53
4.2.3 Menu Utama	54
4.2.4 Tambah <i>Diary</i>	55
4.2.5 <i>Edit Diary</i>	56
4.2.6 Menu Bantuan	57
4.3 Implementasi Program Pada <i>Smartphone</i>	58
4.3.1 Spesifikasi <i>Smartphone</i>	58
4.3.2 Membuat Program Menjadi <i>File .apk</i>	59
4.3.3 Instalasi pada <i>Smartphone</i>	62
4.4 Pengujian Program	65

4.4.1	<i>White-box</i> Testing	65
4.4.2	<i>Black-box</i> Testing	67
BAB V Penutup		68
5.1	Kesimpulan	68
5.2	Saran	68
Daftar Pustaka		69



Daftar Tabel

Tabel 2.1 Tinjauan Pustaka	7
Tabel 2.2 Simbol <i>use case</i> diagram	18
Tabel 2.3 Simbol <i>activity</i> diagram	19
Tabel 2.4 Simbol <i>class</i> diagram	20
Tabel 2.5 Simbol <i>sequence</i> diagram	21
Tabel 4.1 Hasil <i>Black-box Testing</i>	67



Daftar Gambar

Gambar 2.1 Proses Enkripsi RC6.....	12
Gambar 2.2 <i>Systems Development Life Cycle</i>	15
Gambar 3.1 <i>Use case Diagram</i> Aplikasi <i>Diary</i> Kriptografi RC6	26
Gambar 3.2 <i>Activity Diagram</i> Menu Registrasi	27
Gambar 3.3 <i>Activity Diagram</i> Menu <i>Login</i>	28
Gambar 3.4 <i>Activity Diagram</i> Tulis <i>Diary</i>	29
Gambar 3.5 <i>Activity Diagram</i> <i>Edit Diary</i>	30
Gambar 3.6 <i>Activity Diagram</i> <i>Delete Diary</i>	31
Gambar 3.7 <i>Class Diagram</i> Aplikasi <i>Diary</i> Kriptografi RC6.....	32
Gambar 3.8 <i>Sequence Diagram</i> Menu Registrasi	33
Gambar 3.9 <i>Sequence Diagram</i> Menu <i>Login</i>	33
Gambar 3.10 <i>Sequence Diagram</i> Tulis <i>Diary</i>	34
Gambar 3.11 <i>Sequence Diagram</i> <i>Edit Diary</i>	34
Gambar 3.12 <i>Sequence Diagram</i> Hapus <i>Diary</i>	35
Gambar 3.13 Rancangan <i>Splash Screen</i>	35
Gambar 3.14 Rancangan Menu Utama	36
Gambar 3.15 Rancangan Tambah <i>Diary</i>	36
Gambar 3.16 Rancangan Lihat <i>Diary</i>	37
Gambar 4.1 Deklarasi dan Konversi RC6.....	39
Gambar 4.2 Penjadwalan Kunci.....	40
Gambar 4.3 Pergeseran Bit	40
Gambar 4.4 Pemecahan Blok Cipertext.....	41
Gambar 4.5 Pemecahan Blok Plaintext.....	42
Gambar 4.6 Penambahan <i>Padding</i>	43
Gambar 4.7 Enkripsi	44
Gambar 4.8 Dekripsi	45
Gambar 4.9 Penghilangan <i>Padding</i>	45
Gambar 4.10 Tambah <i>Diary</i>	46
Gambar 4.11 Enkripsi di Menu Tambah <i>Diary</i>	47
Gambar 4.12 Proses Simpan	48

Gambar 4.13 Dekripsi pada Menu <i>Edit Diary</i>	49
Gambar 4.14 Hapus <i>Diary</i>	50
Gambar 4.15 <i>Create Tabel</i>	51
Gambar 4.16 <i>List View Diary</i>	51
Gambar 4.17 Antar Muka <i>Splash Screen</i>	52
Gambar 4.18 Antar Muka Menu <i>Login</i>	53
Gambar 4.19 Antar Muka Menu Utama	54
Gambar 4.20 Antar Muka Tambah <i>Diary</i>	55
Gambar 4.21 Antar Muka Menu <i>Edit</i>	56
Gambar 4.22 Antar Muka Menu Bantuan.....	57
Gambar 4.22 Proses <i>Export</i>	59
Gambar 4.23 <i>Export</i> Android.....	60
Gambar 4.24 <i>File Export</i>	60
Gambar 4.25 Pilih Lokasi Penempatan <i>File</i>	61
Gambar 4.26 <i>Password Account</i>	61
Gambar 4.27 Proses selesai.....	62
Gambar 4.28 Lokasi <i>File .apk</i>	63
Gambar 4.29 Persetujuan Instalasi	63
Gambar 4.30 Proses <i>Install</i>	64
Gambar 4.31 Selseai Instalasi	64

INTISARI

Buku harian adalah catatan mengenai kejadian yang dialami oleh penulis. Perkembangan teknologi informasi berpengaruh besar pada banyaknya perubahan aktifitas manusia, tak terkecuali menulis buku harian.

Kini banyak orang yang menulis kejadian-kejadian yang dialaminya tidak hanya pada sebuah buku lalu disimpan ditempat tertentu agar isi dari buku tersebut tidak diketahui orang lain, namun pada *smartphone* mereka. Namun kebanyakan isi catatan harian yang ditulis di *smartphone* hanya disimpan tanpa pengamanan. Jadi orang lain dapat dengan mudah membaca catatan harian yang harusnya bersifat pribadi. Dengan Algoritma kriptografi kita dapat mengamankan tulisan dengan proses enkripsi data.

Proses Enkripsi adalah proses mengubah susunan tulisan bahkan merubah karakter hurufnya secara acak dengan metode tertentu sehingga tulisan tidak dapat dibaca tanpa kunci tertentu untuk merapikan kembali tulisan tersebut. Hal ini mendorong saya untuk mendesain aplikasi Diary atau buku harian dengan algoritma kriptografi sehingga kerahasiaan dari isi diary yang ditulis tetap terjaga.

Kata kunci : RC6, Diary, RC6 Diary

ABSTRACT

Diary is a note about daily life. Development in information and technology changes every aspect of humans life including making a diary.

Now days people not only writing their dialy life on diary books but also on their gadget or smartphone in order to maintain their privacy. Usually diary notes are saved using plaint text so everybody can see and read everything on that diary. With cryptogrophy algorytm diary are not save in plaint text but in chiper text.

chiper text are writen with shuffling and changing the plain text using encryption method. Keys are used to lock the encryption so that only the right key can open the chiper text. This problem make me want to developt a diary application program for better security and privacy for user

Keyword : RC6, Diary, RC6 Diary