



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**RANCANG BANGUN APLIKASI NOTES
TERENKRIPSI DENGAN MENGGUNAKAN
ALGORITMA AES-256 BERBASIS ANDROID**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer (S.Kom.)**



**Aswin Darma Saputra
13110110003**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2017**

LEMBAR PENGESAHAN SKRIPSI

RANCANG BANGUN APLIKASI NOTES TERENKRIPSI DENGAN MENGGUNAKAN ALGORITMA AES-256 BERBASIS ANDROID

Oleh

Nama : Aswin Darma Saputra

NIM : 13110110003

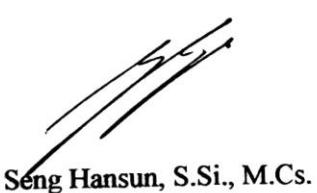
Program Studi : Teknik Informatika

Fakultas : Teknik dan Informatika

Tangerang, 13 November 2017

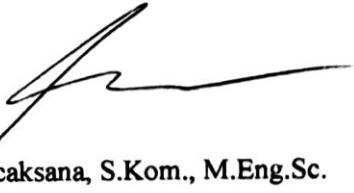
Menyetujui,

Ketua Sidang



Seng Hansun, S.Si., M.Cs.

Dosen Penguji



Arya Wicaksana, S.Kom., M.Eng.Sc.

Dosen Pembimbing I,



Hargyo Tri N. I., S.Kom., M.Sc.

Dosen Pembimbing II,



Ni Made Satvika Iswari, S.T., M.T.

Mengetahui,

Ketua Program Studi



Maria Irmina Prasetyowati, S.Kom., M.T.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Aswin Darma Saputra

NIM : 13110110003

Program Studi : Teknik Informatika

Fakultas : Teknik dan Informatika

menyatakan bahwa skripsi yang berjudul "**Rancang Bangun Aplikasi Notes Terenkripsi dengan Menggunakan Algoritma AES-256 Berbasis Android**" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan / penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 13 November 2017



Aswin Darma Saputra

N U S A N T A R A

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, skripsi dengan judul “Rancang Bangun Aplikasi Notes Terenkripsi dengan Menggunakan Algoritma AES-256 Berbasis Android” ini dapat terselesaikan dengan baik. Laporan ini dibuat sebagai salah satu syarat kelulusan mata kuliah skripsi pada Program Studi Teknik Informatika, Fakultas Teknik dan Informatika.

Skripsi ini dapat diselesaikan karena dukungan dan keterlibatan dari beberapa pihak. Oleh karena itu, ucapan terima kasih layak diucapkan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara yang memberi inspirasi bagi penulis untuk berprestasi.
2. Maria Irmina Prasetyowati, S.Kom., M.T., selaku Ketua Program Studi Teknik Informatika Universitas Multimedia Nusantara, telah menerima penulis dengan baik untuk berkonsultasi dan telah banyak mengajarkan banyak hal mengenai perancangan program yang baik selama saya berkuliah di UMN.
3. Hargyo Tri N. I., S.Kom., M.Sc., selaku dosen pembimbing skripsi yang telah memberikan banyak ilmu pengetahuan tentang hal-hal yang berkaitan dengan enkripsi untuk penulis agar dapat menyelesaikan skripsi dengan baik.
4. Ni Made Satvika Iswari, S.T., M.T., selaku dosen pembimbing skripsi yang telah memberikan ilmu pengetahuan tentang tata cara penulisan karya ilmiah untuk penulis agar dapat menyelesaikan laporan skripsi dengan baik.
5. Keluarga penulis yang telah mendukung penulisan dan penyelesaian skripsi.

6. Arthur Bachtiar Gunawan, Dausan Djaja, Orville Lambert, Fernandre Kurniawan, Hans Rafael, Richard Firdaus, dan teman-teman angkatan 2013 yang telah belajar bersama dan berbagi ilmu selama 4 tahun ini.
7. Louis, Derin, Johanes Harvei, dkk. yang telah menyemangati penulis dalam menyelesaikan skripsi.
8. Pihak-pihak lain yang turut membantu dalam menyelesaikan penyusunan skripsi ini yang tidak dapat disebutkan satu per satu.

Semoga skripsi ini dapat bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi bagi para pembaca, terutama mahasiswa Universitas Multimedia Nusantara.

Tangerang, 2017

Aswin Darma Saputra

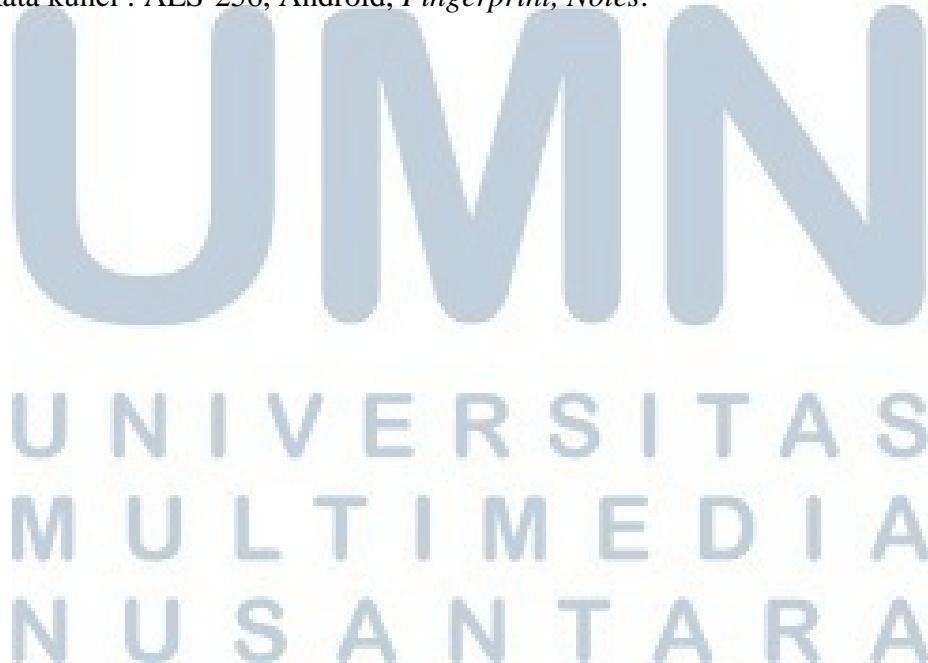


RANCANG BANGUN APLIKASI NOTES TERENKRIPSI DENGAN MENGGUNAKAN ALGORITMA AES-256 BERBASIS ANDROID

ABSTRAK

Android merupakan sistem operasi *smartphone* yang paling banyak digunakan. Dengan meningkatnya kasus pencurian data yang dilakukan oleh *hackers* membuat orang menjadi lebih waspada dengan keamanan pada data penting mereka. Oleh karena itu, metode keamanan yang bisa memberikan keamanan tambahan kepada *files* di dalam *smartphone* dibutuhkan. Salah satu cara untuk mengamankan data penting adalah dengan menyimpannya melalui aplikasi *notes* yang terlindungi dengan sistem *authentication* dan telah dienkripsi sebelumnya. Teknik *fingerprint authentication* sangat populer karena keunikannya. Berdasarkan fakta tersebut, sebuah aplikasi *notes* terenkripsi dibangun menggunakan algoritma AES-256 dengan *fingerprint authentication* untuk membantu pengguna mengamankan data mereka. Aplikasi ini dibangun menggunakan Android Studio, SQLite Database, dan bahasa pemrograman Java. Kesimpulan dari penelitian adalah aplikasi ini menuntut tingkat *attention* pengguna lebih rendah, lebih cepat dibandingkan dengan *password authentication*, dan lebih dipilih oleh *user* untuk mengamankan data penting mereka.

Kata kunci : AES-256, Android, *Fingerprint*, *Notes*.



DESIGN AND DEVELOPMENT ENCRYPTED NOTES APPLICATION

USING AES-256 ALGORITHM BASED ON ANDROID

ABSTRACT

Android is the most widely used smartphone operating system. The increasing numbers of data theft committed by hackers makes people become more aware about the security of their important data. Therefore, security methods that can provide additional security to the data inside the smartphone are needed. One way to secure an important data is by securely keep it in a notes application with authentication system that previously encrypt the data prior to storing it. The fingerprint authentication technique is very popular due to its uniqueness. Base on those facts, a notes-encryption application is created using AES-256 algorithm with fingerprint authentication to help users secure their data. This application is developed using Android Studio, SQLite Database, and Java programming language. The conclusions from the experiment are that the application demands lower user attention, faster than password-authentication, and more preferable by users for securing their critical data.

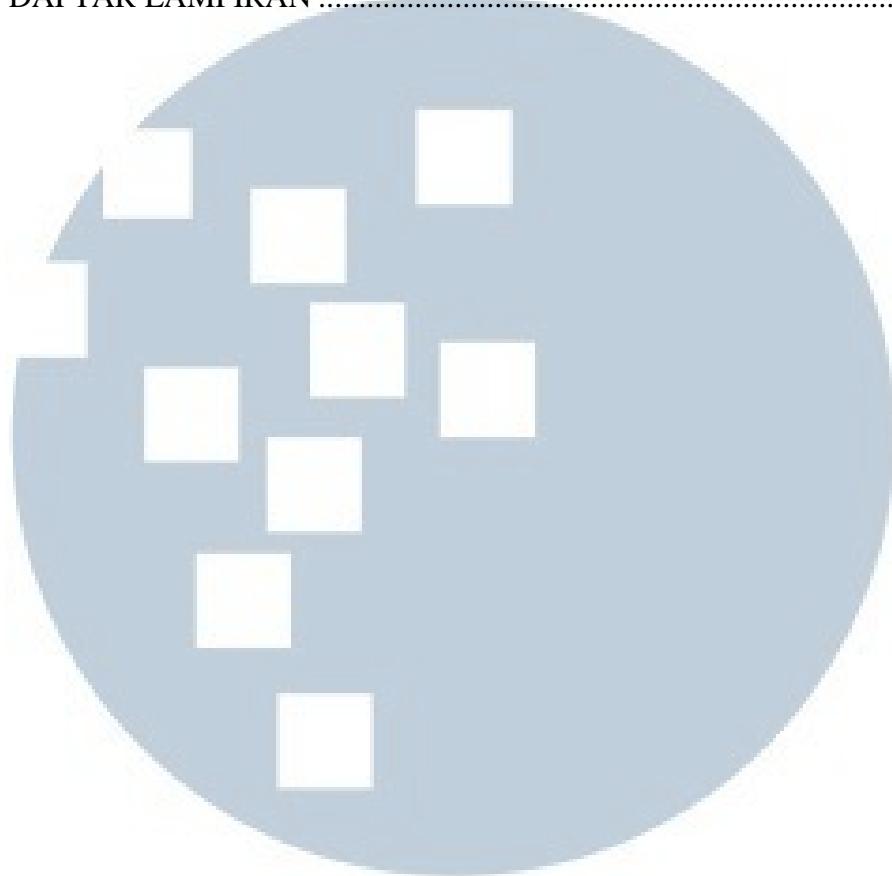
Keywords : AES-256, Android, Fingerprint, Notes.



DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI	Error! Bookmark not defined.
PERNYATAAN TIDAK MELAKUKAN PLAGIA	Error! Bookmark not defined.
KATA PENGANTAR	iv
ABSTRAK.....	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
DAFTAR RUMUS	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
2.1 Notes	6
2.2 Algoritma Enkripsi	6
2.3 Algoritma Enkripsi AES.....	6
2.4 Cipher Block Chaining (CBC).....	13
2.5 Android Keystore.....	13
2.6 Fingerprint	14
2.7 Usability and Security Testing.....	17
BAB III METODOLOGI DAN PERANCANGAN SISTEM	21
3.1 Metodologi Penelitian.....	21
3.2 Perancangan Aplikasi	22
3.2.1 Data Flow Diagram	23
3.2.2 Flowchart	29
3.2.3 Struktur Tabel.....	45
3.2.4 Rancangan Tampilan Antarmuka	46
BAB IV IMPLEMENTASI DAN UJI COBA	52
4.1 Spesifikasi Perangkat.....	52
4.2 Implementasi.....	53
4.2.1 Implementasi Metode	53
4.2.2 Implementasi Tampilan	59
4.3 Skenario Uji Coba Aplikasi.....	69
4.3.1 Uji Coba Usability	69
4.3.2 Analisis Hasil Uji Coba Usability	74
4.3.3 Uji Faktor Keamanan	77
4.3.4 Analisis Hasil Uji Faktor Keamanan	87
BAB V SIMPULAN DAN SARAN	91
5.1 Simpulan	91
5.2 Saran	91

DAFTAR PUSTAKA.....	93
DAFTAR LAMPIRAN	95



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR GAMBAR

Gambar 1.1 Statistik Sistem Operasi Smarphone di Pasaran.....	1
Gambar 1.2 Detail Statistik Sistem Operasi Smarphone di Pasaran	2
Gambar 2.1 S-box	7
Gambar 2.2 Ilustrasi ShiftRows()	8
Gambar 2.3 Ilustrasi MixColumns()	11
Gambar 2.4 Ilustrasi AddRoundKey()	12
Gambar 2.5 Pseudocode Algoritma AES	13
Gambar 2.6 Tipe fingerprint menurut Henry Classification System	14
Gambar 2.7 Proses Authentication pada Android OS.....	16
Gambar 2.8 Kurva Usability Testing	20
Gambar 3.1 DFD Context Diagram Aplikasi Notes	23
Gambar 3.2 DFD Level 1 Aplikasi Notes	24
Gambar 3.3 DFD Level 2 Proses Fingerprint Activity	27
Gambar 3.4 DFD Level 2 Proses Backup Password.....	28
Gambar 3.5 Flowchart Notes Application	29
Gambar 3.6 Flowchart Fingerprint Activity.....	30
Gambar 3.7 Flowchart Generate Encryption Key.....	31
Gambar 3.8 Flowchart Initialize Crypto Object.....	32
Gambar 3.9 Flowchart Fingerprint Handler.....	33
Gambar 3.10 Flowchart Backup Password	34
Gambar 3.11 Flowchart Register Backup Password Activity.....	35
Gambar 3.12 Flowchart Hash Password	36
Gambar 3.13 Flowchart Enter Backup Password Activity	37
Gambar 3.14 Flowchart Home Activity	38
Gambar 3.15 Flowchart Create Note Activity	39
Gambar 3.16 Flowchart Android Encryption	40
Gambar 3.17 Flowchart Android Decryption	41
Gambar 3.18 Flowchart Search Notes	42
Gambar 3.19 Flowchart Read Note Activity	43
Gambar 3.20 Flowchart Edit Note Activity	44
Gambar 3.21 Rancangan Antarmuka Fingerprint Activity	46
Gambar 3.22 Rancangan Antarmuka Register Backup Password Activity	47
Gambar 3.23 Rancangan Antarmuka Enter Backup Password Activity.....	48
Gambar 3.24 Rancangan Antarmuka Home Activity	49
Gambar 3.25 Rancangan Antarmuka Create Note Activity	49
Gambar 3.26 Rancangan Antarmuka Read Note Activity	50
Gambar 3.27 Rancangan Antarmuka Edit Note Activity.....	51
Gambar 4.1 Potongan Kode Fungsi generateKey()	53
Gambar 4.2 Potongan Kode Variabel yang Digunakan	54
Gambar 4.3 Potongan Kode Fungsi initCipher()	55
Gambar 4.4 Potongan Kode Fungsi initKeystore().....	55
Gambar 4.5 Potongan Kode Fungsi check()	56
Gambar 4.6 Potongan Kode Fungsi getSecretKey()	56
Gambar 4.7 Potongan Kode Fungsi encrypt().....	57
Gambar 4.8 Potongan Kode Fungsi decrypt().....	58

Gambar 4.9 Tampilan Halaman Fingerprint Activity Tanpa Backup Password ..	59
Gambar 4.10 Tampilan Halaman Register Backup Password Activity	60
Gambar 4.11 Tampilan Halaman Fingerprint Activity dengan Backup Password	61
Gambar 4.12 Tampilan Halaman Enter Backup Password Activity.....	62
Gambar 4.13 Tampilan Halaman Home Activity	63
Gambar 4.14 Tampilan Halaman Home Activity Saat Melakukan Search	64
Gambar 4.15 Tampilan Halaman Create Note Activity.....	65
Gambar 4.16 Tampilan Halaman Read Note Activity	66
Gambar 4.17 Tampilan Halaman Read Note Activity dengan Delete Confirmation	67
Gambar 4.18 Tampilan Halaman Edit Note Activity.....	68
Gambar 4.19 Aplikasi yang Sudah Dimasukkan Data.....	71



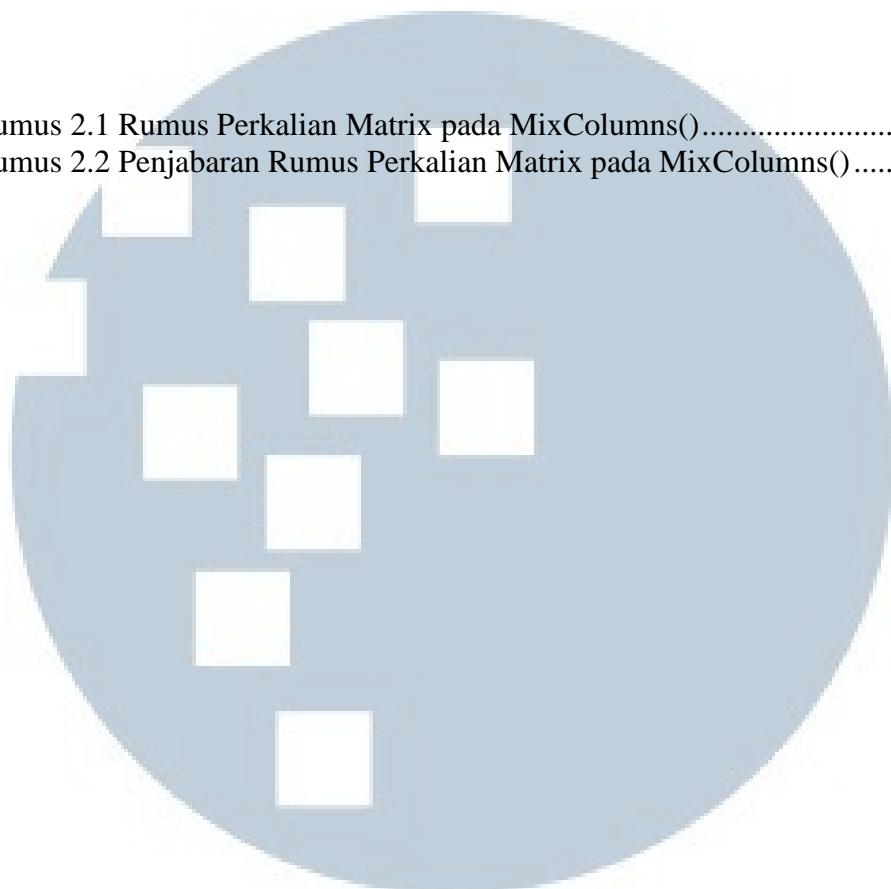
DAFTAR TABEL

Tabel 2.1 Measurable Usability Metrics (Kainda dkk., 2010).....	17
Tabel 2.2 Measurable Security Metrics (Kainda dkk. 2010)	19
Tabel 3.1 Struktur Tabel Password	45
Tabel 3.2 Struktur Tabel Notes	45
Tabel 3.3 Struktur Tabel Keystore	46
Tabel 4.1 Hasil Observasi Uji Coba Usability Aplikasi	71
Tabel 4.2 Daftar Pertanyaan Kuesioner Uji Usability	73
Tabel 4.3 Daftar Jawaban Kuesioner Uji Usability	74
Tabel 4.4 Hasil Observasi Keberhasilan Menggunakan Security System	78
Tabel 4.5 Hasil Observasi Keberhasilan Mengingat Data	85
Tabel 4.6 Daftar Pertanyaan Kuesioner Uji Faktor Keamanan	85
Tabel 4.7 Daftar Jawaban Kuesioner Uji Faktor Keamanan.....	86



DAFTAR RUMUS

Rumus 2.1 Rumus Perkalian Matrix pada MixColumns().....	8
Rumus 2.2 Penjabaran Rumus Perkalian Matrix pada MixColumns()	8



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA