APLIKASI PENERAPAN ALGORITMA RC6 PADA GAMBAR BERBASIS ANDROID

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Teknik
pada Jurusan Teknik Informatika

Oleh :

IMAM WIBISONO
10751000173

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2014

LEMBAR PENGESAHAN

APLIKASI PENERAPAN ALGORITMA RC6 PADA GAMBAR BERBASIS ANDROID

TUGAS AKHIR

Oleh :

IMAM WIBISONO
10751000151

Telah dipertahankan di depan sidang dewan penguji
Sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
Di Pekanbaru, pada tanggal, 18 Februari 2014

Pekanbaru, 18 Februari 2014
Mengesahkan,

Dekan

Dra. Hj. Yenita Morena, M.Si
NIP. 19601125 198503 2 002

Ketua Jurusan

Elin Haerani, ST, M.Kom
NIP. 19810523 200710 2 003

DEWAN PENGUJI

Ketua	:	M. Safrizal, ST., M.Cs
Sekretaris I	:	M. Safrizal, ST., M.Cs
Anggota I	:	Nazruddin Safaat, ST., M.T
Anggota II	:	Iwan Iskandar, ST., M.T

APLIKASI PENERAPAN ALGORITMA RC6 PADA GAMBAR BERBASIS ANDROID

IMAM WIBISONO
10751000173

Tanggal Sidang : 18 Februari 2014
Periode Wisuda : Juni 2014

Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Gambar merupakan salah satu media yang dapat memberikan informasi yang lebih banyak dari pada informasi yang disajikan dalam bentuk tulisan. Oleh karena itu maka diperlukan sebuah aplikasi untuk mengamankan sebuah gambar sehingga gambar tidak dapat dilihat oleh orang yang tidak berhak melihat. Salah satu aplikasi pengamanan tersebut ialah menggunakan kriptografi dengan metode RC6. Metode ini merupakan pengamanan simetris dimana kunci enkipsi dan dekripsi sama. Algoritma RC6 dispesifikasikan dengan notasi RC6-w/r/b. Dimana W adalah ukuran dari word dalam bit, karena pada RC6 menggunakan 4 buah register maka word adalah ukuran blok dibagi 4. R adalah jumlah iterasi, dimana R tidak boleh negatif, dan B adalah panjang kunci dalam bytes. Metode ini memiliki tahapan dalam melakukan enkipsi dan dekripsi seperti whitening awal, transpormasi. mixing, swap register, dan whitening akhir. Aplikasi ini berjalan pada Android dalam pengamanan gambar dengan menggunakan Agoritma RC6. Pengujian aplikasi blackbox, fungsional semua fungsi sesuai dengan yang diinginkan. Pengujian serangan exhausitive attack digunakan untuk mengungkap *plainteks* atau kunci dengan mencoba semua kemungkinan, kunci dilakukan sebanyak enam kali dengan hasil gagal.

Kata kunci : Android, Blackbox, Exhaustive Attack, Gambar, RC6.

RC6 ALGORITHM APPLICATION ON THE IMAGES ANDROID BASED

IMAM WIBISONO
10751000173

Date of Final Exam : 18 February 2014
Graduation Ceremony Period : June 2014

Informatics Engineering Departement
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau

ABSTRACT

Image is one of the means that can provide more information than presented in letter. Therefore, it would an application to secure an image so the image cannot be viewed by people who are not entitled to see. One of the security applications are the use of cryptographic security with RC6 methods. This method is a symmetric security which encryption and decryption keys are the same. RC6 algorithm specified by the notation RC6-w/r/b. W is the size of a word in bits, because the RC6 uses 4 registers so word is the block size divided by 4. R is the number of iterations, where R cannot be negative, and B is the length key in bytes. This method has stages in performing encryption and decryption as the first whitening, transformation, mixing, swap registers, and whitening the end. Security application on Android for images using the RC6 algorithm Blackbox applications testing, functional testing applications, functional all functions in accordance with thedesired. and examination of exhaustive offensive attack used to uncover of plainteks or key with try all possible it is done six times as failed results.

Keywords : *Android, Blackbox, Exhaustive Attack, Images, RC6.*

KATA PENGANTAR

Assalamu ’alaikum wa rahmatullahi wa barakatuh.

Alhamdulillah, puji dan syukur senantiasa diucapkan ke hadirat Allah SWT, atas segala limpahan anugerah dan petunjuk-Nya, Tugas Akhir dengan judul "**APLIKASI PENERAPAN ALGORITMA RC6 PADA GAMBAR BERBASIS ANDROID**" ini dapat diselesaikan, sebagai salah satu syarat kelulusan dalam menyelesaikan studi di Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau.

Banyak sekali pihak yang telah membantu dalam penyelesaian Tugas Akhir ini, baik secara moril maupun materil. Untuk itu, terima kasih dihaturkan kepada:

1. Prof. DR. H. M. Nazir, selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Dra. HJ. Yennita Morena, M.Si, selaku Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Elin Haerani, M.Kom, selaku Ketua Jurusan Teknik Informatika, Fakultas Sains dan Teknologi.
4. Muhammad Safrizal, ST, Mcs selaku Pembimbing Tugas Akhir dan Penasehat Akademis yang telah memberikan masukan yang bermanfaat kepada penulis.
5. Nazruddin Safaat H, MT selaku Penguji I Tugas Akhir yang telah memberikan masukan yang bermanfaat kepada penulis.
6. Iwan Iskandar, M.T selaku Penguji II Tugas Akhir yang telah memberikan masukan yang bermanfaat kepada penulis.
7. Muhammad Affandes, MT selaku Koordinator Tugas Akhir.
8. Seluruh dosen dan karyawan Fakultas Sains dan Teknologi, khususnya Jurusan Teknik Informatika.

9. Kedua orang tua, mbak dan mas yang telah memberikan do'a dan motivasi kepada penulis sehingga Tugas Akhir ini dapat terselesaikan sesuai dengan yang diiinginkan.
10. Kusmiati siregar, Hendra Arifin Siregar, Syahrial Ramadhan Siregar, Nur Ika Dewi dan Mas Heri terima kasih atas dukungan, saran, kritik dan diskusinya untuk kesempuranaan penyusunan Tugas Akhir ini.
11. Teman-teman Jurusan Teknik Informatika khususnya angkatan 2007, terima kasih atas dukungan, saran, kritik dan diskusinya untuk kesempuranaan penyusunan Tugas Akhir ini.
12. Semua pihak yang tidak bisa disebutkan satu persatu yang telah banyak membantu selama ini.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, kritik serta saran yang membangun dari rekan-rekan pembaca sangat dibutuhkan agar dapat membuat Tugas Akhir ini lebih baik. Akhir kata penulis berharap agar Tugas Akhir ini bisa memberikan manfaat bagi pembaca dan semua pihak yang berkepentingan. Terima kasih.

Pekanbaru, 27 january 2014

Penulis

DAFTAR ISI

Halaman

LEMBAR PERSETUJUAN ii
LEMBAR PENGESAHAN iii
LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL iv
LEMBAR PERNYATAAN v
LEMBAR PERSEMBAHAN vi
ABSTRAK vii
ABSTRACT viii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR GAMBAR xiv
DAFTAR TABEL xvi
DAFTAR SIMBOL xviii
DAFTAR LAMPIRAN xxi
BAB I PENDAHULUAN I-1
1.1 Latar Belakang I-1
1.2 Rumusan Masalah I-2
1.3 Batasan Masalah I-3
1.4 Tujuan I-3
1.5 Sistematika Penulisan I-3
BAB II LANDASAN TEORI II-1
2.1 Kriptografi II-1
2.1.1 Pengertian Kriptografi II-1
2.2 Block Chipper II-3
2.3 Citra Digital II-6
2.4 Algoritma RC6 ..... II-7
2.4.1 Pembentukan Kunci Internal II-8
2.4.1.1 Konvensi Kunci Rahasia dari Byetes ke Word II-9
2.4.1.2 Inisialisasi Array S. II-9
2.4.1.3 Mencampurkan L dan S II-9

2.4.2 Proses Enkripsi dan Dekripsi II-10
2.5.Pengertian Android II-15
2.5.1 Versi Android II-15
2.5.2 Fitur – Fitur Android II-16
2.5.3 Arsitektur Android II-16
2.5.4 Perangkat Android II-18
2.5.5 Market Android II-18
2.6 *Unified Modeling Language* UML..... II-19
2.6.1 Use Case Diagram II-19
2.6.2 Class Diagram II-20
2.6.3 Sequen Diagram II-21
BAB III METODOLOGI PENELITIAN..... III-1
3.1. Tahapan Penelitian III-1
3.2. Pengumpulan Data..... III-2
3.3. Analisa dan Perancangan..... III-2
3.4. Implementasi dan Pengujian..... III-2
3.5. Kesimpulan dan Saran..... III-3
BAB IV ANALISIS DAN PERANCANGAN.....IV-1
4.1.Deskripsi Umum Sistem IV-1
4.2.Analisa Sistem IV-2
4.2.1. Analisa Pengguna IV-2
4.2.2. Analisa Fitur dan Isi.....IV-2
4.3. Analisa Fungsional IV-2
4.3.1. Model Use Case IV-3
4.3.2. Class Diagram IV-4
4.3.3. Sequence Diagram IV-6
4.3.4. Activy Diagram IV-9
4.3.5. Deploy Diagram IV-13
4.4. Analisa Perhitungan Manual Algoritma rc6 .....IV-14
4.5. Perancangan Menu IV-19
4.6. Perancangan Data Base IV-22
4.7. Perancangan Interface IV-23

BAB V IMPLEMENTASI DAN PENGUJIAN V-1
5.1 Implementasi Perangkat Lunak V-1
5.2 Batasan Implementasi V-1
5.3 Lingkungan Implementasi V-1
5. 4 Implementasi Kelas V-2
5.5 Impelementasi Interface V-4
5.6. Pengujian V-8
5.6.1. Pengujian Kirim Gambar V-9
5.6.2. Pengujian Dekripsi V-10
5.6.3. Pengujian Ukuran File V-11
5.5.4.Pengujian Keamanan Kunci V-11
5.7. Kesimpulan Pengujian V-12
BAB VI PENUTUP VI-1
6.1 Kesimpulan VI-1
6.2 Saran VI-1
DAFTAR PUSTAKA
LAMPIRAN
DAFTAR RIWAYAT HIDUP