IMPLEMENTASI ALGORITMA ENKRIPSI RC6 PADA KARTU MIFARE CLASSIC BERBASIS TEKNOLOGI *NEAR FIELD COMMUNICATION* DALAM SISTEM OPERASI ANDROID

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
pada Jurusan Ilmu Komputer / Informatika

Disusun oleh:

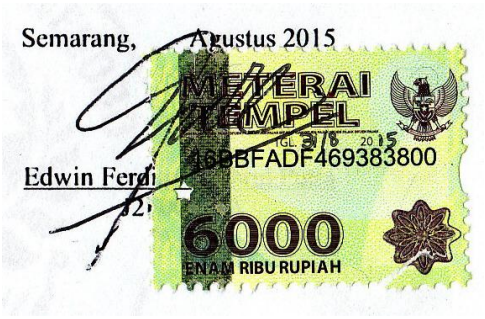
Edwin Ferdian Syahrul Putra

J2F 008 022

JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.



HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Enkripsi RC6 Pada Kartu MIFARE Classic Berbasis Teknologi Near Field Communication Dalam Sistem Operasi Android

Nama : Edwin Ferdian Syahrul Putra

NIM : J2F008022

Telah diujikan pada sidang tugas akhir pada tanggal 31 Agustus 2015 dan dinyatakan lulus pada tanggal 31 Agustus 2015.

Semarang, Agustus 2015

Mengetahui,
Ketua Jurusan Ilmu Komputer/ Informatika
FSM UNDIP

Agus Buhtiar, S.Si., MT
NIP. 19690720 200312 1 002

Panitia Penguji Tugas Akhir
Ketua,

Drs. Eko Adi Sarwoko, M.Kom.
NIP. 1965 1107 1992 03 1 003

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Enkripsi RC6 Pada Kartu MIFARE Classic Berbasis Teknologi Near Field Communication Dalam Sistem Operasi Android

Nama : Edwin Ferdian Syahrul Putra

NIM : J2F008022

Telah diujikan pada sidang tugas akhir pada tanggal 31 Agustus 2015.

Semarang, Agustus 2015

Pembimbing,

Aris Sugiharto, S.Si., M.Kom

NIP. 19710811 199702 1 004

ABSTRAK

Near Field Communication (NFC) merupakan jenis teknologi baru pengembangan dari RFID. Aplikasi NFC pada zaman sekarang telah cukup merata di berbagai lini kehidupan, contohnya dalam pembayaran tiket *commuterline*, pembayaran tiket tol, dan sebagainya. NFC sendiri menggunakan chip khusus yang dibenamkan ke dalam media kartu, salah satunya MIFARE Classic. MIFARE Classic merupakan jenis chip tertua dan yang paling banyak digunakan. Seiring dengan perkembangannya, MIFARE Classic tidaklah seaman seperti ketika pertamakali dikembangkan. Data yang terisi di dalamnya, dapat dengan mudah dicuri, sehingga pada akhirnya terkompromikan keamanannya. Dengan menambahkan satu layer enkripsi, dapatlah ditingkatkan level keamanan pada kartu MIFARE Classic. Penggunaan algoritma RC6 sebagai enkripsi dan dekripsi, didasarkan pada tingkat keamanan RC6 yang pernah menjadi kandidat kriptografi AES. Pembuatan aplikasi enkripsi dan dekripsi sendiri dilakukan dalam platform Android dengan bahasa pemrograman Java. Pemilihan Android sebagai platform pengembangan adalah karena dalam Android, implementasi NFC sangatlah lengkap. Dengan algoritma RC6 sebagai enkripsi dan dekripsi, kunci yang digunakan bersifat simetris. Sehingga dihasilkan enkripsi yang sangat mencukupi untuk teks yang akan dimasukkan ke dalam chip MIFARE Classic tersebut.

Kata kunci: Kriptografi, NFC, Enkripsi, Dekripsi, RC6, Teks, Android.

ABSTRACT

Near Field Communication (NFC) is a new technology which is developed from RFID. Nowadays NFC applications are very common on everyday life, such as on commuterline ticketing payment, toll road ticket payment, and so forth. NFC itself uses special chip which is integrated in card media, one example is MIFARE Classic. MIFARE Classic is the oldest chip and the most widely used NFC chip. As the development continues, MIFARE Classic is not as safe as it were invented. The data which is contained on MIFARE Classic chip can be easily hacked or stolen, so it is compromising its safety. With adding a new encryption layer, it improves security level on MIFARE Classic. The use of RC6 algorithm is based on security level it has, on RC6 which also one of AES cryptography candidates. Application development itself is done on Android platform with Java language. The choice of Android as development platform is because Android has comprehensive NFC implementation and library. With the use of RC6 algorithm as encryption and decryption algorithm, the key used is symmetric. Therefore the result is an encryption which is very sufficient for text that will be encrypted on MIFARE Classic chip itself..

Keywords: Cryptography, NFC, Encryption, Decryption, RC6, Text, Android.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan berkat dan karunia-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "Implementasi Algoritma Enkripsi RC6 Pada Kartu MIFARE Classic Berbasis Teknologi *Near Field Communication* Dalam Sistem Operasi Android". Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer / Informatika Fakultas Sains Dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada:

1. Ibu Prof. Dr. Widowati, S.Si, M.Si selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T selaku Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
3. Bapak Indra Waspada, S.T, M.TI selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
4. Bapak Aris Sugiharto, S.Si, M.Kom selaku pembimbing I yang telah membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
5. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Allah SWT membalas segala kebaikan yang telah Anda berikan kepada penulis.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca. Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan, khususnya pada bidang Informatika.

Semarang, Agustus 2015

Penulis

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Bab pendahuluan menyajikan mengenai latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup pelaksanaan dan penulisan tugas akhir mengenai implementasi algoritma enkripsi RC6 pada kartu MIFARE Classic berbasis teknologi *Near Field Communication* (NFC) dalam sistem operasi Android.

1.1. Latar Belakang

Di zaman modern ini, teknologi *wireless* dan teknologi *mobile* sangatlah pesat berkembang, guna mempermudah aktivitas dan gaya hidup manusia. Dalam teknologi *wireless* atau nirkabel, dikenal beberapa teknologi, antara lain, Wi-Fi, WiMAX, LTE, 4G, RFID, *Bluetooth* LE, dan NFC. Khusus untuk NFC, teknologi ini mengalami perkembangan dan implementasi yang sangat cepat akhir-akhir ini, terutama dalam bidang *e-ticketing* dan *e-payment* (Husni & Purwantoro, 2012). Penerapan teknologi-teknologi tersebut sangatlah masif dan sudah menjadi kelaziman di sekitar kita. Pada umumnya, penerapan teknologi *wireless* ini, dipadukan dengan teknologi *mobile,* selain karena keduanya saling mendukung, juga karena teknologi *mobile* memang diciptakan untuk beroperasi secara *wireless* atau nirkabel. Salah satu contoh teknologi *mobile* yang berkembang pesat akhir-akhir ini adalah teknologi sistem operasi *mobile* Android OS yang dikembangkan oleh Google tahun 2008 (Safaat, 2011).

Android OS diciptakan sebagai sistem operasi *mobile* yang dapat digunakan pada *smartphone*/tablet berbasis layar sentuh (*touchscreen*) (Safaat, 2011). Sistem operasi ini bersifat *open-source*, yang berarti semua pihak dapat menggunakan serta memodifikasinya dengan tanpa biaya, sesuai dengan kebutuhannya. Mekanisme ini menjadikan Android OS sebagai salah satu sistem operasi *mobile* yang memiliki tingkat adopsi paling cepat di masyarakat. Selain itu, Android OS dilihat dari segi fitur, selalu mengimplementasikan teknologi-teknologi terbaru, salah satunya NFC. Teknologi NFC dalam Android OS digunakan sebagai media transfer data, metode pembayaran, serta otomasi tugas (*task automation*) (Aksay et. al., 2012). Dengan demikian NFC telah sangat terintegrasi dalam Android OS, juga karena para

developer dapat menciptakan aplikasi-aplikasi yang menggunakan *class-class* NFC yang telah disediakan oleh Android OS.

NFC merupakan akronim dari *Near Field Communication*, atau Komunikasi Medan Dekat. NFC merupakan teknologi pertukaran data berbasis gelombang radio (RFID) yang hanya beroperasi pada jarak yang sangat dekat (< 10 cm) (Coskun, et. al., 2012). Teknologi ini banyak diimplementasikan kedalam *e-ticketing* dan *e-payment*. Dalam penerapan di kedua bidang tersebut, NFC membutuhkan chip yang dipasangkan dalam suatu media, yang umumnya berupa kartu. Pada umumnya, para produsen menjual hanya chipnya saja, untuk kemudian oleh pihak pengguna dipasangkan atau dibenamkan ke dalam kartu yang terkustomisasi bentuk atau tampilannya. Beberapa jenis chip NFC, antara lain MIFARE, FeliCa, Calypso (Coskun, et. al., 2012). Yang paling umum digunakan adalah jenis MIFARE Classic, tipe ini lazim digunakan untuk *e-ticketing* di beberapa Sistem Kereta *Commuter Line*, salah satunya di Indonesia. Untuk membaca kartu NFC diperlukan suatu *receiver*, yang dapat berupa *dedicated receiver* maupun *receiver* yang diintegrasikan ke dalam *smartphone*/tablet.

Salah satu jenis chip NFC yang umum digunakan di kartu-kartu NFC yang beredar adalah MIFARE Classic. Chip ini dikembangkan oleh NXP *Semiconductors* sebagai alternatif penyimpanan data berbasis teknologi NFC. Chip ini dikenal dengan biaya produksi dan harga jual yang sangat murah, walaupun kapasitas data yang dapat disimpan hanya sedikit, tapi sangat mencukupi untuk data-data *e-payment* dan *e-ticketing*. Namun demikian, MIFARE Classic memiliki beberapa kelemahan, terutama dalam aspek keamanan (Haselsteiner, 2005). Mengingat tidak ada penerapan digital *signature* (tandatangan digital) pada chip ini. Oleh karena itu dibutuhkan suatu mekanisme enkripsi-dekripsi terhadap data-data yang tersimpan agar lebih terjaga keamanannya.

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: “cryptós” artinya “secret” (rahasia), sedangkan “gráphein” artinya “writing” (tulisan) (Munir, 2006). Jadi, kriptografi berarti “secret writing” (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudiation*. Kata "seni" di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata "*graphy*" didalam "*cryptography*" itu sendiri sudah menyiratkan sebuah seni). Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Dalam kriptografi modern dikenal beberapa algoritma, salah satunya adalah Algoritma RC6 (ARCSIX) yang dirancang oleh Ronald L. Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin. Algoritma RC6 merupakan salah satu algoritma yang menggunakan mode *Cipher Block Chaining* (Prayudi, 2005). Algoritma ini adalah salah satu kandidat *Advanced Encryption Standard* (AES) yang diajukan oleh RSA Laboratories kepada U.S. National Institue of Standards and Technology (NIST). Algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST.

Pemilihan Algoritma RC6 didasari pada penggunaan iterasi yang cukup banyak, hingga 20 iterasi (Prayudi, 2005), sehingga keamaanan data lebih terjamin dibandingkan algoritma lain, misalnya RSA atau RC5. Pencipta RC6 memberikan *security margin* yang besar, sebanyak 12 *round*, yang menghasilkan perlindungan keamanan tinggi. Selain itu, penjadwalan kunci yang ada pada RC6 menjamin semua kunci yang digunakan tidak memiliki kunci lemah. Semua kunci yang ada mempunyai kekuatan yang sama.

Dengan menerapkan algoritma RC6 sebagai salah satu solusi enkripsi-dekripsi untuk kartu MIFARE Classic berbasis NFC di dalam mobile OS Android, diharapkan tingkat keamanan kartu MIFARE Classic akan lebih meningkat, sehingga adopsi teknologi NFC akan lebih umum, dan keamanannya dapat lebih terjaga dan tidak mudah diretas oleh pihak-pihak yang tidak bertanggung-jawab.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana merancang dan menghasilkan suatu perangkat lunak yang dapat memberikan keamanan sebuah data yang tersimpan di dalam kartu atau chip NFC yang bersifat penting, dan memberikan kemudahan dalam mengamankan data yang disimpan di dalam kartu atau chip NFC.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah menghasilkan suatu perangkat lunak yang dapat memberikan keamanan sebuah data yang tersimpan di dalam kartu atau chip NFC yang bersifat penting, dan memberikan kemudahan dalam mengamankan data yang disimpan di dalam kartu atau chip NFC.

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah sebagai berikut:

1. Bagi mahasiswa:
   a. Mengimplementasikan ilmu yang didapat selama perkuliahan ke dunia nyata dengan merancang dan mengembangkan algoritma RC6 ke dalam teknologi NFC.
   b. Menambah bekal pengetahuan yang dapat dipergunakan untuk persiapan dalam rangka menghadapi dunia kerja di masa yang akan datang.
2. Bagi pihak terkait yang membutuhkan pengamanan data:
   a. Memudahkan dalam mengamankan data yang disimpan dalam chip NFC dan meminimalisir gangguan yang dapat dilakukan oleh penyadap.
   b. Mengurangi rasa khawatir pengirim akan tersampaikannya data rahasia tersebut ke pihak penerima dengan keamanan yang tetap terjaga.

1.4. Ruang Lingkup

Ruang lingkup pada Implementasi Algoritma RC6 pada kartu MIFARE Classic berbasis sistem operasi Android adalah sebagai berikut:

1. Aplikasi ini dibuat dengan model proses *Unified Process*.
2. *Input* berupa teks yang disimpan ke dalam kartu MIFARE Classic dan kunci yang kemudian dienkripsi dengan algoritma RC6 hingga menghasilkan *ciphertext*.
3. *Output* berupa *ciphertext* yang telah terenkripsi dan siap untuk ditulis kedalam kartu MIFARE Classic.

4. Pengembangan menggunakan IDE (*Integrated Development Environment*) Android Studio dengan bahasa pemrograman Java.
5. Bentuk implementasi menggunakan *devices* Android.
6. Menggunakan algoritma RC6 sebagai algoritma enkripsi dan dekripsi.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam laporan tugas akhir ini terbagi menjadi beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

berisi uraian tentang latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI

berisi penjelasan singkat konsep–konsep yang mendukung pengembangan aplikasi, meliputi konsep Kriptografi, Algoritma *Cipher Block Chaining*, Algoritma RC6, *Unified Process*, *Unified Modeling Language*, *Near Field Communication*, Sistem Operasi Android, dan Android Studio.

BAB III ANALISIS DAN PERANCANGAN

membahas proses pengembangan sistem pada tahap definisi kebutuhan, analisis dan perancangan aplikasi dengan hasil berupa desain dan rancangan sistem yang akan dikembangkan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

membahas tentang implementasi dan pengujian sistem. Implementasi kriptografi dilakukan berdasarkan rancangan yang telah dibuat pada bab sebelumnya. Dilanjutkan dengan proses berikutnya yaitu pengujian sistem, dimana proses pengujian dilakukan dengan menguji *class* dan menguji secara diagnosis.

BAB V PENUTUP

berisi kesimpulan yang diambil dari aplikasi yang dibangun dan saran untuk pengembangan lebih lanjut.