

**PENERAPAN KRIPTOGRAFI PADA RFID DENGAN
ALGORITMA MD5 DAN ALGORITMA RC4**

SKRIPSI



disusun oleh

Muhammad Ilyas

13.11.6794

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

**PENERAPAN KRIPTOGRAFI PADA RFID DENGAN
ALGORITMA MD5 DAN ALGORITMA RC4**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muhammad Ilyas

13.11.6794

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

PERSETUJUAN

SKRIPSI

**PENERAPAN KRIPTOGRAFI PADA RFID DENGAN
ALGORITMA MD5 DAN ALGORITMA RC4**

yang dipersiapkan dan disusun oleh

Muhammad Ilyas

13.11.6794

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 09 Agustus 2017

Dosen Pembimbing,



Ferry Wahyu Wibowo, S.Si, M.Cs.
NIK. 190302235

PENGESAHAN

SKRIPSI

**PENERAPAN KRIPTOGRAFI PADA RFID DENGAN
ALGORITMA MD5 DAN ALGORITMA RC4**

yang dipersiapkan dan disusun oleh

Muhammad Ilyas

13.11.6794

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Agustus 2017

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ahlihi Masruro, M.Kom.
NIK. 190302148



Akhmad Dahlan, M.Kom.
NIK. 190302174



Ferry Wahyu Wibowo, S.Si, M.Cs.
NIK. 190302235



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 30 Agustus 2017

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, 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.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 30 Agustus 2017



Muhammad Ilyas
NIM. 13.11.6794

MOTTO

“Barang siapa yang keluar dalam menuntut ilmu maka ia adalah seperti berperang di jalan Allah hingga pulang.”

(H.R. Tirmidzi)

“Waktu itu bagaikan pedang, jika kamu tidak memanfaatkannya menggunakan untuk memotong, ia akan memotongmu (menggilasmu)”

(H.R. Muslim)



PERSEMBAHAN

Sebagai ucapan syukur dan terimakasih atas terselesainya skripsi ini saya persembahkan kepada :

1. Kedua orang tua, bapak saya Ir. Metsu Koan, ibu saya Sukaenah, serta adik saya Tirta Buana Choir dan Ilham Fauzan yang telah memberikan dukungan moril dan materi serta motivasi dalam pengerjaan skripsi ini.
2. Bapak Ferry Wahyu Wibowo, S.Si, M.cs sebagai dosen pembimbing yang telah membimbing dalam pembuatan skripsi dari awal hingga akhir.
3. Bapak Agus Purwanto, M. Kom., Bapak M.Fairul Filza, M.Kom., Thofa, Rahmat, Mahda, Qonitah, Nara, Ifa, Indra, Akbar , Irfan, serta Rizal yang telah membantu dan memberikan masukan dalam penyelesaian skripsi.
4. Keluarga besar yang berada di Medan dan Kebumen yang telah memberikan dukungan selama ini.
5. Teman-teman yang tidak dapat disebutkan satu per satu yang juga turut membantu proses penyelesaian skripsi ini.

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Alhamdulillahirobbilalamin, puji dan syukur senantiasa penulis haturkan pada kehadiran Allah SWT. Karena berkat limpahan nikmat dan rahmat-Nya maka penulis dapat menyelesaikan karya ilmiah atau skripsi yang berjudul “Penerapan Kriptografi pada RFID dengan Algoritma MD5 dan Algoritma RC4”.

Maksud dan tujuan skripsi ini adalah untuk melengkapi dan memenuhi syarat yang telah ditentukan oleh Universitas Amikom Yogyakarta untuk menyelesaikan program Strata 1 (Satu). Dalam pembuatan skripsi ini tidak terlepas dari berbagai pihak yang telah membantu baik dari segi material dan spiritual. Atas segala bimbingan, dukungan dan bantuan yang secara langsung maupun tidak langsung yang telah diberikan. Penulis menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Sudarmawan, M.T. selaku Ketua Prodi Teknik Informatika di Universitas Amikom Yogyakarta.
3. Bapak Ferry Wahyu Wibowo, S.Si., M.Cs. selaku dosen pembimbing yang telah memberi arahan baik kritik maupun saran dalam penyusunan skripsi ini.
4. Bapak Ahlihi Masruro, M.Kom. selaku penguji I, Bapak Akhmad Dahlan, M.Kom. selaku penguji II, dan Bapak Ferry Wahyu Wibowo, S.Si., M.Cs. selaku penguji III, serta semua dosen Jurusan Teknik Informatika Universitas Amikom Yogyakarta, terima kasih atas semua jasa Bapak dan Ibu Dosen.
5. Kedua Orang Tua, adik dan segenap keluarga yang telah memberikan dukungan moril serta materil dengan tulus, ikhlas dan penuh kasih sayang.
6. Sahabat-sahabat yang telah memberikan semangat, motivasi, dan membantu dalam pengerjaan skripsi ini.
7. Seluruh staf dan karyawan Universitas Amikom Yogyakarta yang banyak membantu kelancaran segala aktivitas penulisan skripsi ini.

8. Semua pihak yang telah membantu sampai terselesaikannya penyusunan skripsi ini. Semoga Allah SWT. Senantiasa memberikan rahmat dan karunia-Nya pada penulis dan rekan-rekan semuanya.

Penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan terutama dalam penyajian materi. Oleh karena itu, penulis memohon saran dan kritik yang membangun dari pembaca. Selain itu, penulis berharap bahwa skripsi ini dapat bermanfaat bagi masyarakat khususnya dalam memberikan solusi bagi permasalahan teknologi yang ada.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 30 Agustus 2017

Muhammad Ilyas

DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN	Error! Bookmark not defined.
MOTTO	vi
PERSEMBAHAN.....	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
INTISARI.....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Maksud Penelitian.....	2
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	3
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI.....	6
2.1 Kajian Pusaka.....	6
2.2 Konsep Dasar Sistem	6
2.3 Pengertian Kriptografi.....	8

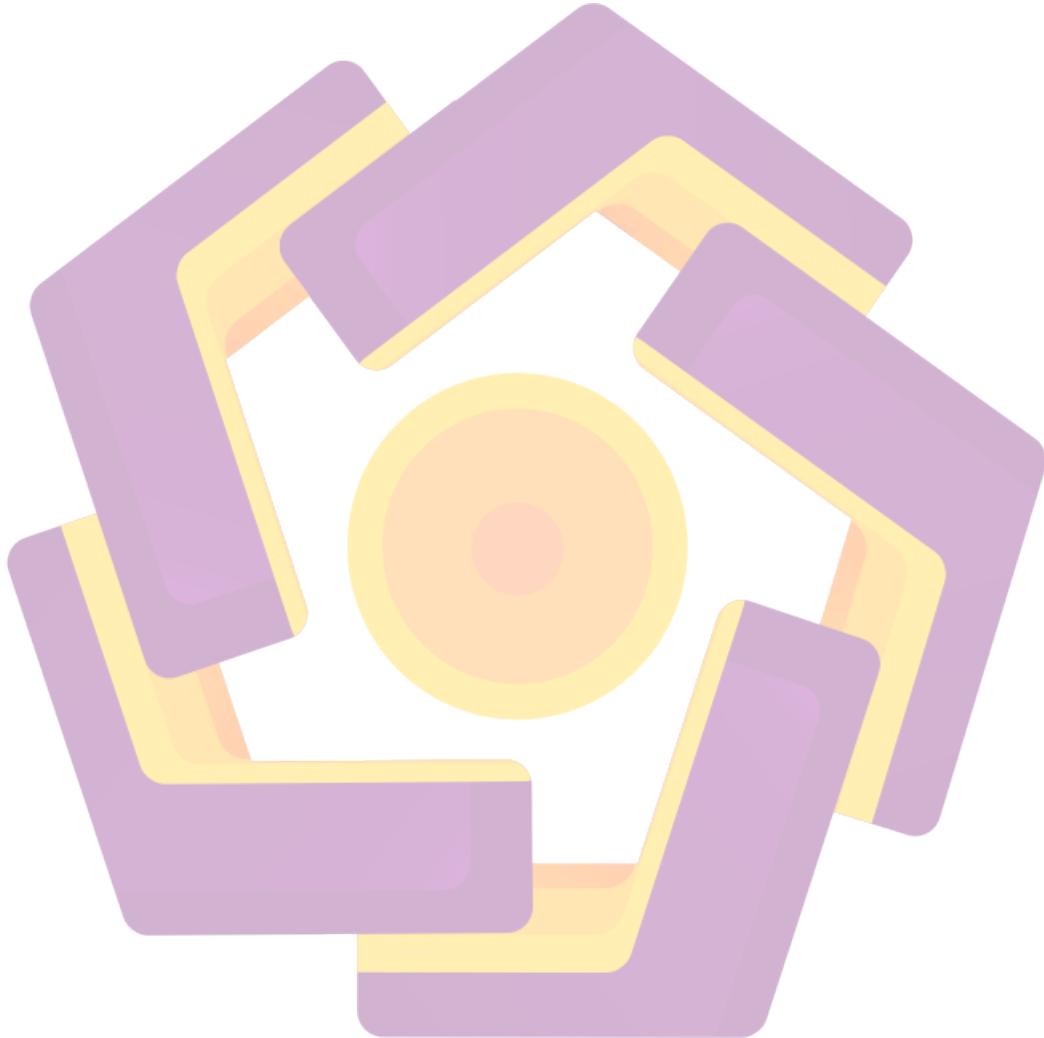
2.3.1	Sistem Kriptografi.....	8
2.4	MD5	9
2.5	RC4	10
2.6	Pengujian Sistem.....	12
2.7	Perangkat Keras yang Digunakan	13
2.7.1	<i>Radio Frequency Identification (RFID)</i>	13
2.8	Perangkat Lunak dan Bahasa Pemograman Yang Digunakan.....	16
2.8.1	C#	16
2.8.2	Visual Studio.....	16
2.8.3	SQL Server.....	17
BAB III ANALISA DAN PERANCANGAN		18
3.1	Konsep Aplikasi	18
3.2	Analisa SWOT	18
3.2.1	Analisa Kekuatan (<i>Strength</i>).....	18
3.2.2	Analisa Kelemahan (<i>Weakness</i>)	19
3.2.3	Analisa Peluang (<i>Opportunity</i>)	19
3.2.4	Analisa Ancaman (<i>Threats</i>)	19
3.3	Analisis Kebutuhan Sistem	19
3.3.1	Kebutuhan Fungsional	20
3.3.2	Kebutuhan Non-Fungsional	20
3.4	Perancangan Sistem	21
3.5	Perancangan Interface	22
BAB IV IMPLEMENTASI DAN PEMBAHASAN		23
4.1	Implementasi Algoritma.....	23
4.1.1	Implementasi Algoritma MD5	23
4.2.2	Implementasi Algoritma RC4	25
4.1	Hasil Akhir Produk	27
4.2	Pengujian Sistem.....	28
BAB V PENUTUP.....		30

5.1 Kesimpulan	30
5.2 Saran.....	30
DAFTAR PUSTAKA	31
LAMPIRAN	



DAFTAR TABEL

Tabel 2.1 Perbedaan RFID dengan Barcode.....	13
Tabel 4.1. Hasil Black-Box Testing.....	29



DAFTAR GAMBAR

Gambar 2.1. RFID Reader	14
Gambar 2.2. Bentuk Fisik RFID Card	15
Gambar 3.1 Alur Kerja Aplikasi	21
Gambar 3.2 Tampilan Utama Aplikasi	22
Gambar 4.1 Pseudo Code Transformation	24
Gambar 4.2 Pseudo Code Padder Buffer	24
Gambar 4.3 Flowchart MD5	25
Gambar 4.4 Pseudo Code KSA	26
Gambar 4.5 Pseudo Code PRGA	26
Gambar 4.6 Flowchart RC4	27
Gambar 4.7 Hasil Akhir aplikasi.....	27
Gambar 4.8 Data Di Database.....	28
Gambar 4.9 Data tidak ditemukan di database.....	29

INTISARI

Teknologi RFID sudah digunakan di sebagian kalangan masyarakat. Teknologi RFID sudah digunakan sebagai alat presensi dan juga pembayaran. Di dalam RFID terdapat data yang bersifat privasi dari masing-masing pemiliknya. Keamanan yang dimiliki RFID terbilang masih kurang bahkan tidak ada. Kriptografi adalah ilmu untuk mengamankan data dengan metode tertentu. Untuk menjaga data yang ada pada RFID maka menggunakan 2 algoritma yang dikombinasikan untuk memperkuat sistem keamanan pada RFID. Dua algoritma itu ialah Algoritma MD5 dan Algoritma RC4 dimana algoritma tersebut dapat memperkuat sistem keamanan pada RFID. Algoritma MD5 dan RC4 merupakan salah satu kriptografi yang hingga saat ini masih digunakan karena memiliki keunggulan masing-masing. Sehingga dapat mencegah pencurian data yang ada di RFID agar tidak disalahgunakan oleh orang lain. Jika data yang ada di dalam RFID dicuri oleh orang lain maka data informasi pribadi ada ditangan orang yang tidak seharusnya.

Kata Kunci : Kriptografi, MD5, RC4, RFID

ABSTRACT

RFID technology is already used in most societies. RFID technology is already being used for presensi and also payments. Data in RFID which contain privacy from each RFID card's owner. Security in RFID have relatively still less did not even exist. Cryptography is a method of securing data with certain methods. To keep the existing data on the RFID uses two algorithms that combine to strengthen the security of the RFID system. The two algorithms are algorithms MD5 and RC4 algorithm where the algorithm can strengthen the security of the RFID system. The algorithms MD5 and RC4 cryptographic is one which to this day is still used because it has the benefits of each. So as to prevent the theft of data in RFID from being misused by others.

Keyword : Cryptography, MD5, RC4, RFID