

**IMPLEMENTASI ALGORITMA RC6 UNTUK KEAMANAN WEB
LOGIN**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Christanto T Munthe

15.11.8893

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA RC-6 UNTUK KEAMANAN WEB LOGIN

yang dipersiapkan dan disusun oleh

Christanto Triputra Munthe

15.11.8893

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 April 2019

Dosen Pembimbing,



Nila Feby Puspitasari, S.Kom, M.Cs.

NIK. 190302161

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA RC-6 UNTUK KEAMANAN WEB LOGIN

yang dipersiapkan dan disusun oleh

Christanto Triputra Munthe

15.11.8893

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Oktober 2019

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Agung Nugroho, M.Kom.
NIK. 190302242

Acihmah Sidauruk, M.Kom.
NIK. 190302238

Nila Febv Puspitasari, S.Kom, M.Cs.
NIK. 190302161



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Oktober 2019



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, 28 Oktober 2019



Christanto Triputra Munthe
NIM. 15.11.8893

MOTTO

“Barangsiapa setia dalam perkara-perkara kecil, ia setia juga dalam perkara-perkara besar. Dan barangsiapa tidak benar dalam perkara-perkara kecil, ia tidak benar juga dalam perkara-perkara besar. Jadi, jikalau kamu tidak setia dalam hal yang tidak jujur, siapakah yang akan mempercayakan kepadamu harta yang sesungguhnya?”

(Lukas 16:10-11)

“Janganlah hendaknya kamu kuatir tentang apa pun juga, tetapi nyatakanlah dalam segala hal keinginanmu kepada Allah dalam doa dan permohonan dengan ucapan syukur”

(Filipi 4:6)

“Never expect GOD to do for you what you don't do to others”

(Bob Marley)

“Do what you can, with what you have, where you are”

(Theodore Roosevelt)

PERSEMBAHAN

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esayang telah memberikan rahmat sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Penulis juga sangat berterima kasih kepada semua pihak yang terlibat secara langsung maupun tidak langsung dalam proses pembuatan skripsi ini hingga selesai. Oleh karena itu, penulis persembahkan skripsi ini kepada :

1. Bapak Nomensen Munthe dan Ibu Nurliana Br Barus, selaku orang tua tercinta yang selalu mendoakan, memberikan semangat dan memberikan semua fasilitas yang dibutuhkan untuk penunjang kuliah.
2. Kakak Tigor Novrianta Munthe dan kakak Baginta Munthe yang selalu mendoakan, memberi nasehat dan juga memberikan motivasi.
3. Ibu Nila Feby Puspitasari, S.Kom, M.Cs. yang telah membimbing dari awal hingga akhir proses pembuatan skripsi dan juga ketika ujian pendadaran.
4. Dosen-dosen di Universitas Amikom Yogyakarta yang telah memberikan dan mengajarkan banyak ilmu selama masa perkuliahan.
5. Teman-Teman kelas 15 IF 06 dan 7 sekawan yang telah menemani masa perkuliahan dari awal kuliah hingga selesai. Semoga kita semua sukses dunia akhirat dan menjadi pribadi yang lebih baik lagi.

Moses Asi Oktavianus, Richo Misere Sarwom, dan semua teman yang telah memberikan masukan dan semangat dalam proses pengerjaan skripsi.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esayang telah memberikan rahmat sehingga penulis dapat menyelesaikan skripsi yang berjudul Implentasi Algoritma RC6 Untuk Keamanan Web Login.

Skripsi ini penulis buat guna menyelesaikan studi jenjang Strata Satu (S1) pada program studi Informatika fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program strata 1 dan untuk memperoleh gelar Sarjana Komputer.

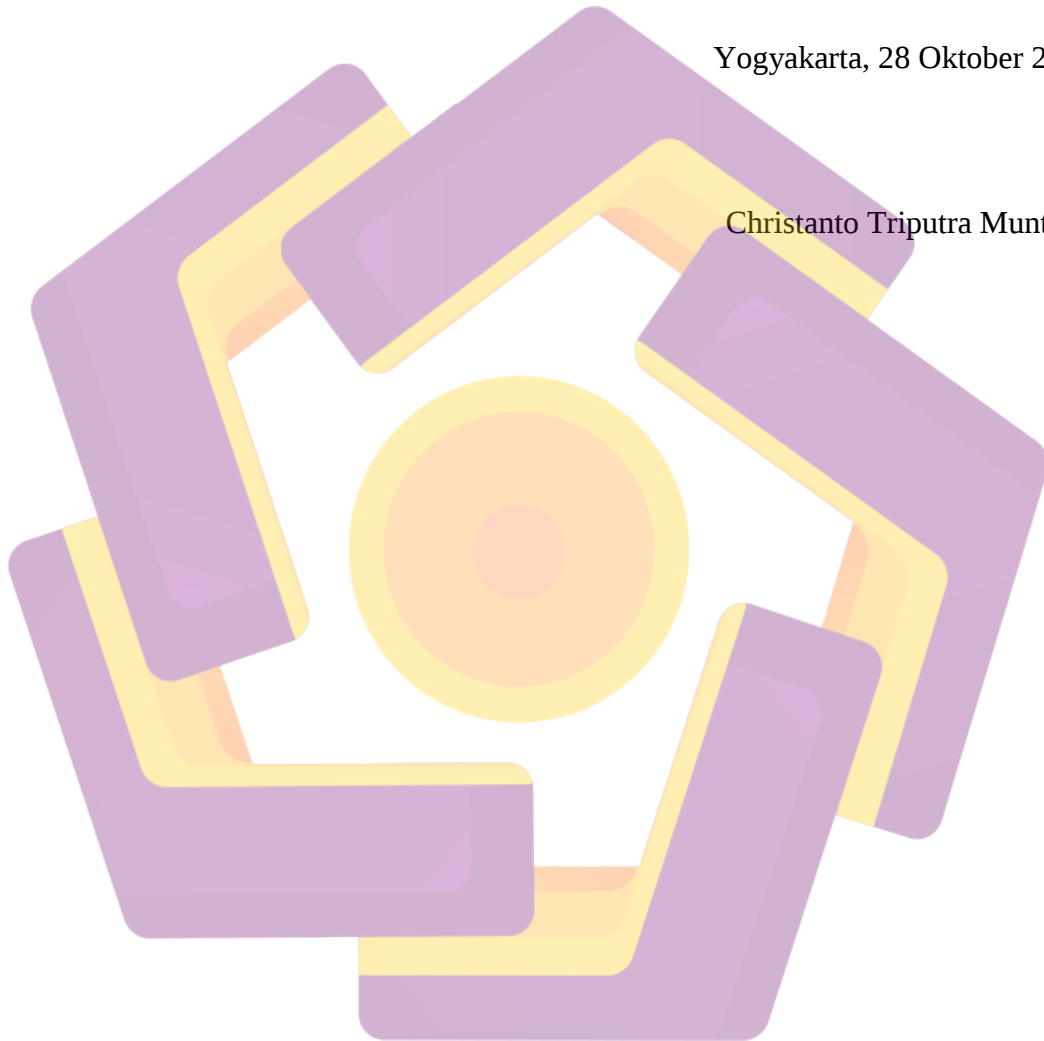
Dengan selesainya skripsi ini, maka pada kesempatan ini penulis mengucapkan terimakasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Nila Feby Puspitasari, S.Kom, M.Cs. selaku Dosen Pembimbing yang selalu bijaksana memberikan bimbingan, nasehat serta waktunya selama penulisan skripsi ini.
4. Erik Hadi Saputra, S.Kom, M.Eng. selaku Dosen Wali yang telah memberikan dukungan pengarahan selama masa perkuliahan.
5. Dosen Penguji dan segenap Dosen Universitas Amikom Yogyakarta yang telah berbagi ilmu dan pengalamannya.
6. Kedua orang tua beserta kakak dan adik yang selalu mendoakan, memberikan semangat dan dukungan moril.
7. Teman-teman 7 Sekawan yang telah menemani dari awal kuliah sampai selesai. Semoga kita semua sukses dan menjadi pribadi yang lebih baik lagi.
8. Semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu memberikan dukungan.

Semoga Tuhan Yang Maha Esa memberikan balasan yang lebih kepada semua yang telah ikut membantu penulis dalam menyelesaikan skripsi ini. Demi perbaikan selanjutnya, saran dan kritik yang membangun akan penulis terima dengan senang hati dan rasa terima kasih. Semoga skripsi ini dapat bermanfaat bagi penulis, pembaca dan mendorong penelitian-penelitian selanjutnya.

Yogyakarta, 28 Oktober 2019

Christanto Triputra Munthe



DAFTAR ISI

LEMBAR JUDUL	I
PERSETUJUAN	II
PENGESAHAN	III
PERNYATAAN	IV
MOTTO	V
PERSEMBAHAN	VI
KATA PENGANTAR	VII
DAFTAR ISI	IX
DAFTAR TABEL	XII
DAFTAR GAMBAR	XIII
INTISARI	XIV
ABSTRACT	XV
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Maksud Penelitian	3
1.5 Manfaat Penelitian	4
1.5.1 Bagi Peneliti	4
1.5.2 Bagi Universitas	4
1.5.3 Bagi Pembaca	4
1.6 Metode Penelitian	5
1.6.1 Metode Pengumpulan Data	5
1.6.2 Metodologi Pengembangan Aplikasi	5
1.7 Sistematika Penulisan	7

BAB II LANDASAN TEORI.....	9
2.1 Tinjauan Pustaka.....	9
2.2 Dasar Teori.....	16
2.2.1 Keamanan Web	16
2.2.1.1 Celah Keamanan Web	16
2.2.2 Login	21
2.2.3 Password	22
2.3 Kriptografi.....	22
2.3.1 Komponen – Komponen Kriptografi	23
2.3.2 Tujuan Kriptografi	25
2.3.3 Algoritma Kriptografi	26
2.4 Algoritma RC-6	26
2.4.1 Key Expansion Algorithm.....	27
2.5 Algoritma Enskripsi RC-6	28
2.6 Algoritma Deskripsi RC-6	30
2.7 ASCII (<i>American Standard Code for Information Interchange</i>).....	31
2.8 Perangkat Lunak yang Digunakan	32
2.8.1 Web Editor	32
2.8.2 Web Server	32
2.8.3 Xampp.....	33
2.9 Bahasa Pemrograman.....	33
2.9.1 PHP <i>Hypertext Preprocessor</i> (PHP).....	33
2.9.2 CSS	34
2.10 Alat Kelengkapan Sistem.....	34
2.10.1 Flowchart (Bagan Alir).....	34
2.10.1.1 Flowchart Sistem	34
2.10.1.2 Flowchart Program	35
2.10.2 Use Case Diagram	36
2.11 SQL Injection.....	37
BAB III ANALISIS DAN PERANCANGAN	39

3.1 Analisis Kebutuhan Sistem	39
3.1.1 Analisis Kebutuhan	39
3.1.1.1 Kebutuhan Fungsional	40
3.1.1.2 Kebutuhan Nonfungsional	40
3.1.2 Analisis Data	41
3.2 Perancangan Sistem	47
3.2.1 Permodelan Sistem	47
3.2.1.1 <i>Flowchart Login</i>	48
3.2.1.2 <i>Flowchart</i> algoritma RC6 proses Enkripsi	49
3.2.1.3 <i>Flowchart</i> algoritma RC6 proses Deskripsi	51
3.3 Perancangan Permodelan Antar Muka (<i>Interface</i>)	52
3.3.1 Perancangan <i>Interface login</i>	52
3.3.2 Perancangan <i>Interface Register</i>	53
BAB IV IMPLEMENTASI DAN HASIL	54
4.1 Implementasi Program	54
4.1.1 Implementasi <i>Interface</i>	54
4.1.2 Implementasi Prosedural	55
4.1.2.1 Pembangkitan Kunci RC6	56
4.1.2.2 Enkripsi RC6	57
4.1.2.3 Deskripsi Algoritma RC6	59
4.1.2.4 <i>Login</i> dengan Algoritma RC6	60
4.2 Pengujian sistem	61
4.2.1 Pengujian Tanpa Menggunakan Algoritma RC6	61
4.2.2 Pengujian Serangan pada <i>Web Login</i> dengan Algoritma RC6	63
4.3 Analisa Hasil Pengujian	64
BAB V PENUTUP	66
5.1 Kesimpulan	66
5.2 Saran	66
DAFTAR PUSTAKA	68

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian	12
Tabel 2.2 Simbol <i>Flowchart System</i>	35
Tabel 2.3 Simbol <i>Flowchart Program</i>	36
Tabel 2.4 Simbol <i>Use Case</i>	37
Tabel 3.1 Perangkat Keras/Hardware	41
Tabel 3.2 Perangkat Lunak/Software	41
Tabel 3.3 Contoh <i>Plaintext</i> dan Kunci	42
Tabel 3.4 Blok <i>Plaintext</i>	42
Tabel 3.5 Hasil Konversi <i>Text</i> ke Desimal	42
Tabel 3.6 Hasil Konversi Biner	43
Tabel 3.7 Penggabungan Bilangan Biner	44
Tabel 3.8 Hasil Iterasi Pertama	45
Tabel 3.9 Konversi Hasil Iterasi ke Biner	46
Tabel 3.10 Konversi Biner ke Karakter ASCII	47
Tabel 4.1 Pengujian query <i>SQL Injection</i> Tanpa Algoritma RC6	62
Tabel 4.2 Pengujian query <i>SQL Injection</i> dengan Algoritma RC6	63

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Deskripsi	25
Gambar 2.2 Formula Pembangkitan Kunci Algoritma RC6.....	28
Gambar 2.3 Formula Algoritma Enkripsi RC6.....	29
Gambar 2.4 Formula Algoritma Deskripsi RC6	31
Gambar 2.5 Bilangan Biner Hasil Konversi ASCII.....	32
Gambar 3.1 Proses <i>Whitening</i> Awal	44
Gambar 3.2 Aturan <i>Iterasi</i> RC6	45
Gambar 3.3 <i>Flowchart</i> Proses <i>Login</i>	48
Gambar 3.4 Algoritma Enkripsi RC6.....	49
Gambar 3.5 Algoritma Deskripsi RC6.....	51
Gambar 3.6 Perancangan Antar Muka Halaman <i>Login</i>	52
Gambar 3.7 Perancangan Antar Muka <i>Create User</i> Atau <i>Registrasi</i>	53
Gambar 4.1 Tampilan Halaman saat <i>Login</i> Sukses	55
Gambar 4.2 Tampilan Halaman saat <i>Login</i> Gagal.....	55
Gambar 4.3 <i>Source Code</i> Pembangkitan Kunci	56
Gambar 4.4 Halaman saat Pembuatan Akun Baru.....	57
Gambar 4.5 <i>Password</i> yang telah di Enkripsi	57
Gambar 4.6 <i>Source Code</i> Enkripsi <i>Password</i>	58
Gambar 4.7 Perhitungan Enkripsi Algoritma RC6.....	58
Gambar 4.9 Perhitungan Deskripsi Algoritma RC6	59
Gambar 4.8 <i>Source Code Login</i> Algoritma RC6	60
Gambar 4.10 Tampilan <i>Login</i> Sukses Pengujian <i>Query SQL</i>	61
Gambar 4.11 Tampilan <i>Login</i> Gagal Pengujian <i>Query SQL Injection</i>	63

INTISARI

Saat ini salah satu sarana yang paling banyak digunakan untuk mengakses halaman *web* adalah dengan memakai *user-id* dan *password* yang dimasukkan pada *formlogin*. Namun format standar dari *form login* akan mengirimkan *user-id* dan *password* dari *client* ke *server* dalam format *plaintext* atau teks asli. Dalam format ini, sangat mudah untuk mendapatkan data *user-id* dan *password* yang valid dan dapat digunakan pada *form login*.

Untuk itu diberikan alternatif pengamanan dengan melakukan enkripsi *user-id* dan *password* pada *form login web*. Algoritma yang digunakan dalam proses enkripsi adalah algoritma simetri RC-6, dirancang dengan menggunakan bahasa pemrograman PHP.

Proses penelitian dilakukan dengan mengikuti aturan algoritma simetri RC-6. Langkah awal penelitian dengan membuat *script* pembangkitan kunci untuk proses enkripsi, kemudian proses enkripsi RC-6 dengan PHP dan perancangan *form login web* yang sudah menggunakan enkripsi. Dengan menggunakan *query SQL Injection*, terlihat bahwa *query* berhasil menembus sistem *login* yang tidak menggunakan enkripsi. Sementara dalam *form login* halaman *web* yang sudah menggunakan enkripsi, *query SQL Injection* gagal menembus sistem *login*.

Kata Kunci: Web, Login, Enkripsi, Deskripsi, RC-6, PHP, SQL Injection

ABSTRACT

Currently, one of the most widely used tools to access web pages is to use the user-id and password entered in the login form. However, the standard format of the login form will send user-id and password from the client to the server in plaintext or original text format. In this format, it is very easy to get a valid user-id and password data and can be used on the login form.

For that reason, an alternative security is provided by encrypting the user-id and password on the web login form. The algorithm used in the encryption process is the RC-6 symmetry algorithm, designed using the PHP programming language.

The research process is carried out by following the rules of the RC-6 symmetry algorithm. The initial step of the research is to create a key generation script for the encryption process, then the RC-6 encryption process with PHP and the design of a web login form that already uses encryption. By using SQL Injection queries, it appears that the query has penetrated the login system that does not use encryption. While in the web page login form that already uses encryption, the SQL Injection query fails to penetrate the login system.

Keyword: Web, Login, Encryption, Description, RC-6, PHP, SQL Injection