

**MODEL IMPLEMENTASI ALGORITMA RC4 PADA HALAMAN
KRITIK DAN SARAN MAHASISWA (STUDI KASUS: WEBSITE
MAHASISWA STMIK ATMA LUHUR PANGKALPINANG)**

SKRIPSI



**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2019**

**MODEL IMPLEMENTASI ALGORITMA RC4 PADA HALAMAN
KRITIK DAN SARAN MAHASISWA (STUDI KASUS: WEBSITE
MAHASISWA STMIK ATMA LUHUR PANGKALPINANG)**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



Oleh:

SHIFA HATIMA

1411500053

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2019**

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 1411500053
Nama : SHIFA HATIMA
Judul Skripsi : MODEL IMPLEMENTASI ALGORITMA RC4 PADA
HALAMAN KRITIK DAN SARAN MAHASISWA
(STUDI KASUS: WEBSITE MAHASISWA S'TMIK
ATMA LUHUR PANGKALPINANG)

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, Juni 2019



(SHIFA HATIMA)

LEMBAR PENGESAHAN SKRIPSI

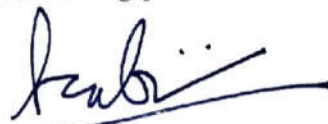
**MODEL IMPLEMENTASI ALGORITMA RC4 PADA HALAMAN
KRITIK DAN SARAN MAHASISWA (STUDI KASUS: WEBSITE
MAHASISWA STMIK ATMA LUHUR PANGKALPINANG)**

Yang dipersiapkan dan disusun oleh

**SHIFA HATIMA
1411500053**

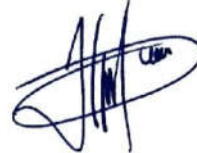
Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 01 Juli 2019

**Susunan Dewan Penguji
Dosen Penguji II**



**Eza Budi Perkasa, M.Kom
NIDN. 0201089201**

Dosen Pembimbing



**Yohanes Setiawan Japriadi, M.Kom
NIDN. 0219068501**

Kaprodi Teknik Informatika



**R. Burham Santanto F., S.Si, M.Kom
NIDN. 0224048003**

Dosen Penguji I



**Ari Amir Alkodri, M.Kom
NIDN. 0201038601**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 01 Juli 2019

KETUA STMIK ATMA LUHUR PANGKALPINANG



Dr. Husni Teja Sukmana, S.T., M.Sc

KATA PENGANTAR

Puji syukur Alhamdulillah kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada program studi Teknik Informatika di STMIK Atma Luhur.

Dengan segala keterbasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ibuku tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Husni Teja Sukmana, S.T., M.Sc, Ph.D, selaku Ketua STMIK Atma Luhur.
5. Bapak R.Burham Isnanto Farid, S.Si., M.Kom selaku Kaprodi Teknik Informatika.
6. Bapak Yohanes Setiawan, M.Kom. selaku pembimbing teori serta pembimbing sistem.
7. Bapak Ari Amir Alkodri, M.Kom selaku penguji I sidang.
8. Bapak Eza Budi Perkasa, M.Kom selaku penguji II sidang.
9. Adikku Cabella Salsabella dan Abilla Assyifa yang selalu menjadi penyemangatku.
10. Untuk sahabat sahabat ku Kiki Hardianty, Desty Satriany, Vanny Agustiani, Teddy Wahyudin, Hardini Kartika dan lainnya.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya Amin.

Pangkalpinang, Juni 2019

Penulis



ABSTRACT

Critics and suggestions are natural thing conveyed to an educational institution. STMIK Atma Luhur's students can provide criticism and suggestions for the progress of the campus using the student website. Unfortunately, the criticism data and suggestions are not secured by the encryption process, so that the privacy of the students becomes disturbed. This certainly makes students reluctant to express their criticisms and suggestions. This study aims to maintain the confidentiality of criticism and suggestions that have been filled by students. In maintaining information on criticism and suggestions, cryptography is needed. In cryptography there are two main processes, namely encryption and decryption. Encryption is converting the original text (plain text) into crypted text (chiper text), while decryption is the process of returning from cryped text (chiper text) to the original text (plain text). We uses the Rivest Code 4 algorithm (RC4) because it is one algorithm whose cipher text results have the same length of character as the original text. This method consists of three main stages, namely KSA (Key Schedulling Algorithm), PRGA (Pseudo Random Generation Algorithm), and XOR process. This research uses the RAD model, OOP method, and UML modeling tools. From the results of the tests conducted, the success rate of encryption and decryption using the RC4 algorithm against the data of criticism and suggestions submitted by students amounted to 73.33%.

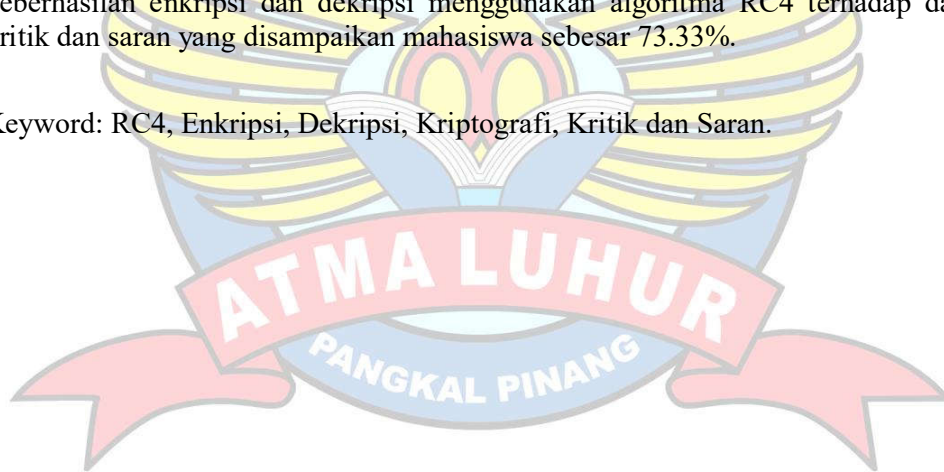
Keyword: RC4, Encryption, Decryption, Cryptography, Criticism and Suggestions.



ABSTRAK

Kritik dan saran merupakan hal yang wajar disampaikan pada suatu institusi, tidak terkecuali institusi pendidikan. Mahasiswa STMIK Atma Luhur dapat memberikan kritik dan sarannya demi kemajuan kampus menggunakan website mahasiswa. Sayangnya, data kritik dan saran tidak diamankan dengan proses enkripsi, sehingga privasi dari mahasiswa menjadi terganggu. Hal ini tentunya membuat mahasiswa segan mengutarakan kritik dan sarannya. Penelitian ini bertujuan untuk menjaga kerahasiaan kritik dan saran yang telah diisi mahasiswa. Dalam menjaga informasi kritik dan saran tersebut, diperlukan penerapan kriptografi. Di dalam kriptografi terdapat dua proses utama yaitu enkripsi dan dekripsi. Enkripsi merupakan mengubah teks asli menjadi teks sandi, sedangkan dekripsi adalah proses pengembalian dari teks sandi ke teks aslinya. Penulis menggunakan algoritma Rivest Code 4 (RC4) karena merupakan salah satu algoritma yang hasil penyandiannya (*ciphertext*) memiliki ukuran panjang karakter yang sama dengan teks aslinya (*plaintext*). Metode ini terdiri dari tiga tahap utama, yaitu KSA (*Key Scheduling Algorithm*), PRGA (*Pseudo Random Generation Algorithm*) dan proses XOR. Penelitian ini menggunakan model RAD, metode OOP, dan alat bantu pemodelan UML. Dari hasil pengujian yang dilakukan, tingkat keberhasilan enkripsi dan dekripsi menggunakan algoritma RC4 terhadap data kritik dan saran yang disampaikan mahasiswa sebesar 73.33%.

Keyword: RC4, Enkripsi, Dekripsi, Kriptografi, Kritik dan Saran.

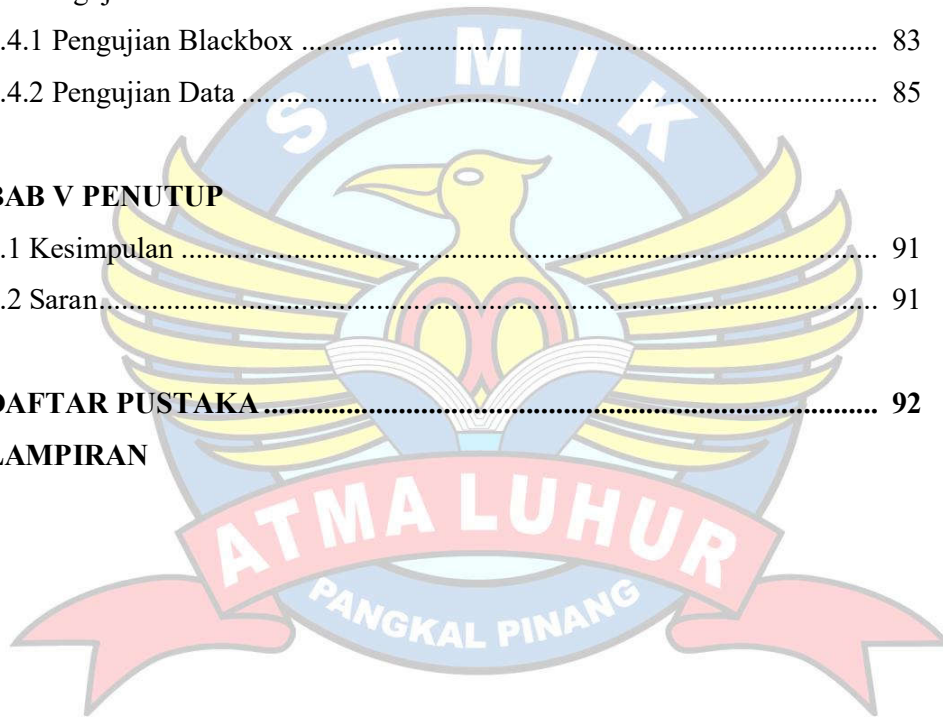


DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR.....	iii
ABSTRACK.....	v
ABSTRAK	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xii
DAFTAR SIMBOL	xiv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat Penelitian	3
1.6 Sistematika Penelitian	3
BAB II LANDASAN TEORI	
2.1 Rapid Application Development (RAD).....	5
2.1.1 Fase dan Tahapan Pengembangan Sistem.....	6
2.1.2 Kelebihan dan Kekurangan RAD.....	6
2.2 Definisi Metode Pengembangan Perangkat Lunak	7
2.2.1 Metode Object Oriented Programming (OOP)	7
2.2.2 Konsep dasar dari Pemrograman Berorientasi Obyek	8
2.3 Definisi Alat Bantu Pengembangan Perangkat Lunak.....	9
2.3.1 UML (Unified Modelling Language).....	9
2.4 Teori Pendukung	10
2.4.1 Pengamanan Data.....	10

2.4.2 Kriptografi.....	10
2.4.3 Algoritma Kriptografi	12
2.4.4 Jenis Algoritma Kriptografi	13
2.5 Rivest Code (RC4)	15
2.5.1 Sejarah Rivest Code 4 (RC4).....	15
2.5.2 Deskripsi Algoritma RC4.....	16
2.5.3 Key-Scheduling Algoritma (KSA).....	17
2.5.4 Pseudo-Rando Generation Algoritim	17
2.5.5 Implementasi dari Algoritma RC4	18
2.5.6 Tentang Keamanan dari Algoritma RC4.....	20
2.5.7 Kelebihan Algoritma RC4.....	20
2.5.8 Kekurangan Algoritma RC4	21
2.6 Kode ASCII.....	21
2.6.1 Kode Standard ASCII	21
2.6.2 Kode <i>Extended</i> ASCII.....	22
2.7 Definisi Basisdata.....	23
2.8 Tinjauan Perangkat Lunak	24
2.9 Penelitian Terdahulu	28
 BAB III METODOLOGI PENELITIAN	
3.1 Model Pengembangan Perangkat Lunak.....	31
3.2 Metode Pengembangan Perangkat Lunak.....	32
3.3 Alat Bantu Perkembangan Perangkat Lunak	32
3.4 Simulasi Penerapan Algoritma RC4 Untuk Proses Enkripsi dan Dekripsi Kritik dan Saran Mahasiswa	33
 BAB IV HASIL DAN PEMBAHASAN	
4.1 Analisa Masalah	39
4.1.1 Analisa Sistem Berjalan	39
4.1.2 Analisa Kebutuhan	39
4.2 Perancangan Sistem	42

4.2.1 Identifikasi Sistem Usulan	42
4.2.2 Activity Diagram.....	42
4.2.3 Use Case Diagram.....	49
4.2.4 Rancangan Layar.....	55
4.2.5 Sequence Diagram	62
4.2.6 Class Diagram	70
4.2.7 Spesifikasi Basis data.....	71
4.3 Implementasi.....	75
4.4 Pengujian.....	83
4.4.1 Pengujian Blackbox	83
4.4.2 Pengujian Data	85
BAB V PENUTUP	
5.1 Kesimpulan	91
5.2 Saran.....	91
DAFTAR PUSTAKA.....	92
LAMPIRAN	



DAFTAR GAMBAR

	Halaman
Gambar 2.1 RAD (Rapid Application Development).....	5
Gambar 2.2 Algoritma Simetris	14
Gambar 2.3 Algoritma Asimetris.....	15
Gambar 2.4 Tahap pencarian dari Rc4 Byte ouput diplih dengan mencari nilai S[i] dan S[j], menambahkannya dengan modulo 256, dan mencari hasil penjumlahannya si S	18
Gambar 2.5 Tabel ASCII Teks.....	22
Gambar 2.6 Tabel ASCII Simbol.....	23
Gambar 4.1 Activity Diagram Login	43
Gambar 4.2 Activity Diagram Beranda	44
Gambar 4.3 Activity Diagram Data Akademik.....	45
Gambar 4.4 Activity Diagram Jadwal Kuliah.....	46
Gambar 4.5 Activity Diagram Kartu Hasil Studi.....	46
Gambar 4.6 Activity Diagram Hasil Studi Kumulatif	47
Gambar 4.7 Activity Diagram Kritik dan Saran	48
Gambar 4.8 Activity Diagram BPM	49
Gambar 4.9 Use Case Diagram Mahasiswa	50
Gambar 4.10 Use Case Diagram BPM	54
Gambar 4.11 Rancangan Layar Halaman Login.....	56
Gambar 4.12 Rancangan Layar Halaman Beranda	56
Gambar 4.13 Rancangan Layar Halaman Data Akademik	57
Gambar 4.14 Rancangan Layar Tahun Ajaran dan Semester untuk Jadwal Kuliah.....	57
Gambar 4.15 Rancangan Layar Halaman Jadwal Kuliah	58
Gambar 4.16 Rancangan Layar Tahun Ajaran dan Semester untuk Kartu Hasil Studi.....	58
Gambar 4.17 Rancangan Layar Halaman Kartu Hasil Studi	59
Gambar 4.18 Rancangan Layar Halaman Hasil Studi Kumulatif.....	60

Gambar 4.19 Rancangan Layar Tahun Ajaran dan Semetser untuk Kritik dan Saran.....	60
Gambar 4.20 Rancangan Layar Isi Kritik dan Saran	61
Gambar 4.21 Rancangan Layar BPM	61
Gambar 4.22 Rancangan Layar Data Kritik dan Saran Mahasiswa.....	62
Gambar 4.23 Sequence Diagram Login	63
Gambar 4.24 Sequence Diagram Beranda	64
Gambar 4.25 Sequence Diagram Data Akademik	65
Gambar 4.26 Sequence Diagram Jadwal Kuliah.....	66
Gambar 4.27 Sequence Diagram Kartu Hasil Studi.....	66
Gambar 4.28 Sequence Diagram Hasil Studi Kumulatif	67
Gambar 4.29 Sequence Diagram Kritik dan Saran	68
Gambar 4.30 Sequence Diagram Login SPMI.....	69
Gambar 4.31 Sequence Diagram Kritik dan Saran SPMI.....	70
Gambar 4.32 Class Diagram	71
Gambar 4.33 Tampilan Layar Login.....	76
Gambar 4.34 Tampilan Layar Beranda.....	76
Gambar 4.35 Tampilan Layar Data Akademik.....	77
Gambar 4.36 Tampilan Layar Pemilihan Tahun Ajaran dan Semester Jadwal Kuliah.....	77
Gambar 4.37 Tampilan Layar Jadwal Kuliah	78
Gambar 4.38 Tampilan Layar Pemilihan Tahun Ajaran dan Semester Kartu Hasil Studi.....	78
Gambar 4.39 Tampilan Layar Kartu Hasil Studi	79
Gambar 4.40 Tampilan Layar HSK Online	79
Gambar 4.41 Tampilan Layar Pemilihan Tahun Ajaran dan Semester Kritik dan Saran.....	80
Gambar 4.42 Tampilan Layar Mengisi Kritik dan Saran.....	80
Gambar 4.43 Tampilan Layar Login SPMI	81
Gambar 4.44 Tampilan Layar Kritik dan Saran SPMI	82

DAFTAR TABEL

	Halaman
Tabel 2.1 Penelitian Terdahulu	27
Tabel 3.1 Jadwal Kerja.....	31
Tabel 3.2 Array Kunci Awal.....	33
Tabel 3.3 Nilai Array S.....	34
Tabel 3.4 Nilai Array T.....	35
Tabel 3.5 Nilai Permutasi Array S.....	35
Tabel 3.6 Percobaan Enkripsi.....	38
Tabel 3.7 Percobaan Key Salah.....	38
Tabel 3.8 Percobaan Key Benar.....	38
Tabel 4.1 Kebutuhan Fungsional Mahasiswa.....	40
Tabel 4.2 Kebutuhan Fungsional BPM.....	41
Tabel 4.3 Kebutuhan Perangkat Keras.....	41
Tabel 4.4 Kebutuhan Perangkat Lunak.....	41
Tabel 4.5 Deskripsi Use Case Login.....	50
Tabel 4.6 Deskripsi Use Case Melihat Beranda.....	50
Tabel 4.7 Deskripsi Use Case Melihat Data Akademik.....	51
Tabel 4.8 Deskripsi Use Case Melihat Jadwal Kuliah.....	52
Tabel 4.9 Deskripsi Use Case Melihat Kartu Hasil Studi.....	52
Tabel 4.10 Deskripsi Use Case Melihat Hasil Studi Kumulatif.....	53
Tabel 4.11 Deskripsi Use Case Mengisi Kritik dan Saran.....	53
Tabel 4.12 Deskripsi Use Case Logout.....	54
Tabel 4.13 Deskripsi Use Case Login BPM.....	55
Tabel 4.14 Deskripsi Use Case Melihat Kritik dan Saran.....	55
Tabel 4.15 Spesifikasi Basis Data jadwal.....	71
Tabel 4.16 Spesifikasi Basis Data khs.....	72
Tabel 4.17 Spesifikasi Basis Data kritik.....	74
Tabel 4.18 Spesifikasi Basis Data mahasiswa.....	74

Tabel 4.19 Spesifikasi Basis Data nilai	75
Tabel 4.20 Spesifikasi Basis Data user	75
Tabel 4.21 Pernyataan untuk Kuesioner Pengujian Sistem Mahasiswa	83
Tabel 4.22 Pernyataan untuk Kuesioner Pengujian Sistem BPM	84
Tabel 4.23 Rekap Hasil Pengujian Fungsional	85
Tabel 4.24 Rekap Pengujian Data	85
Tabel 4.25 Hasil Pengujian Data	86



DAFTAR SIMBOL

1. Simbol Use Case Diagram

Aktor



Menggambarkan orang atau sistem yang menyediakan atau menerima informasi dari sistem yang dibuat atau bisa disebut dengan pengguna aplikasi.

Association



Menggambarkan hubungan aktor dengan *use case*.

Use Case



Menggambarkan fungsionalitas dari suatu sistem sehingga pengguna sistem paham dan mengerti kegunaan sistem yang akan dibangun.

2. Simbol Activity Diagram

Start State



Menggambarkan awal dari aktivitas.

End State



Menggambarkan akhir aktivitas.

Transition



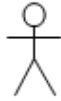
Menggambarkan perpindahan kontrol antar *state*.

Activity State



Menggambarkan proses bisnis.

3. Sequence Diagram



Aktor

Pengguna aplikasi atau biasa disebut *user*.



Pesan Tipe Send

Menggambarkan suatu obyek mengirim data masuk.



Garis Hidup

Menggambarkan kehidupan suatu obyek.



Waktu Aktif

Menggambarkan objek dalam keadaan aktif dan berinteraksi. Semua yang berhubungan dengan waktu aktif adalah sebuah tahap yang dilakukan di dalamnya.



Keluaran

Menggambarkan sebuah keluaran yang didapatkan setelah melalui beberapa tahapan.

