

**APLIKASI PELAYANAN KRITIK DAN SARAN MENGGUNAKAN ALGORITMA
RSA DI FAKULTAS TEKNIK UNIVERSITAS BANGKA BELITUNG BERBASIS
WEB**

SKRIPSI

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



OLEH :

ARPIAN YOGI PRATAMA

1611520008

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMALUHUR
PANGKALPINANG
2018/2019**

**APLIKASI PELAYANAN KRITIK DAN SARAN MENGGUNAKAN ALGORITMA
RSA DI FAKULTAS TEKNIK UNIVERSITAS BANGKA BELITUNG BERBASIS
WEB**

SKRIPSI



OLEH :

ARPIAN YOGI PRATAMA

1611520008

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

LEMBAR PERNYATAAN

Yang bertandatangan di bawah ini :

NIM : 1611520008

Nama : Arpian Yogi Pratama

Judul Skripsi : APLIKASI PELAYANAN KRITIK DAN SARAN
MENGUNAKAN ALGORITMA RSA DI
FAKULTAS TEKNIK UNIVERSITAS BANGKA
BELITUNG BERBASIS WEB

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

Pangkalpinang, 04 Juli 2019



Arpian Yogi Pratama

LEMBAR PERSETUJUAN SIDANG

NIM : 1611520008
Nama : Arpian Yogi Pratama
Judul Skripsi : APLIKASI PELAYANAN KRITIK DAN SARAN
MENGUNAKAN ALGORITMA RSA DI
FAKULTAS TEKNIK UNIVERSITAS BANGKA
BELITUNG BERBASIS WEB

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

Pangkalpinang, 04 Juli 2019



Dwi Yuni Sylfania, M.Kom

Dosen Pembimbing

LEMBAR PENGESAHAN SKRIPSI

**APLIKASI PELAYANAN KRITIK DAN SARAN MENGGUNAKAN
ALGORITMA RSA DI FAKULTAS TEKNIK UNIVERSITAS BANGKA
BELITUNG BERBASIS WEB**

Yang dipersiapkan dan disusun oleh

**Arpian Yogi Pratama
1611520008**

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 04 Juli 2019

Dosen Penguji II



**Ade Septryanti, S.Kom., M.T.
NIDN : 0216099002**

Dosen Pembimbing



**Dwi Yuny Sylfania, M.Kom
NIDN : 0207069301**

Kaprodi Teknik Informatika



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

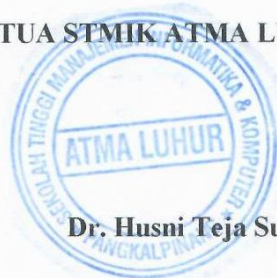
Dosen Penguji I



**Delpiah Wahyuningsih, M.Kom
NIDN : 0008128901**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 04 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 karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika STMIK Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, 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. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur .
4. Bapak Dr. Husni Teja Sukmana, ST., M.Sc selaku Ketua STMIK Atma Luhur.
5. Bapak R.Burham Isnanto Farid, S.Si., M. Kom Selaku Kaprodi Teknik Informatika.
6. Ibu Dwi Yuny Sylfania, M. Kom selaku dosen pembimbing.
7. Dekan Fakultas Teknik, dosen – dosen dan seluruh tenaga kependidikan di Fakultas Teknik Universitas Bangka Belitung yang telah memberi saya dukungan dalam menyelesaikan skripsi ini.
8. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2015 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik Nya, Amin.

Pangkalpinang, Juli 2019

Penulis



ABSTRAK

Telah dilakukan penelitian menggunakan algoritma kriptografi *Rhivest Shamir Adleman*. Penelitian ini diterapkan dalam sebuah aplikasi pelayanan kritik dan saran berbasis web di fakultas teknik universitas bangka Belitung. Aplikasi ini dibuat karena kotak saran dan kritik di fakultas teknik sering kosong yang dikarenakan kekhawatiran mahasiswa apabila pesan mereka disadap oleh orang yang tidak berhak. Untuk Proses yang digunakan pada aplikasi ini adalah enkripsi, dekripsi dan pembangkitan kunci. Metode untuk pengembangan aplikasi menggunakan metode *waterfall* dan tools pengembangan sistem menggunakan *activity diagram*, *use case diagram*, dan *sequence diagram*. Dengan adanya aplikasi ini, tentunya akan mempermudah mahasiswa untuk mengamankan pesan yang disampaikan dan proses pengiriman pesan akan lebih efektif dan efisien.

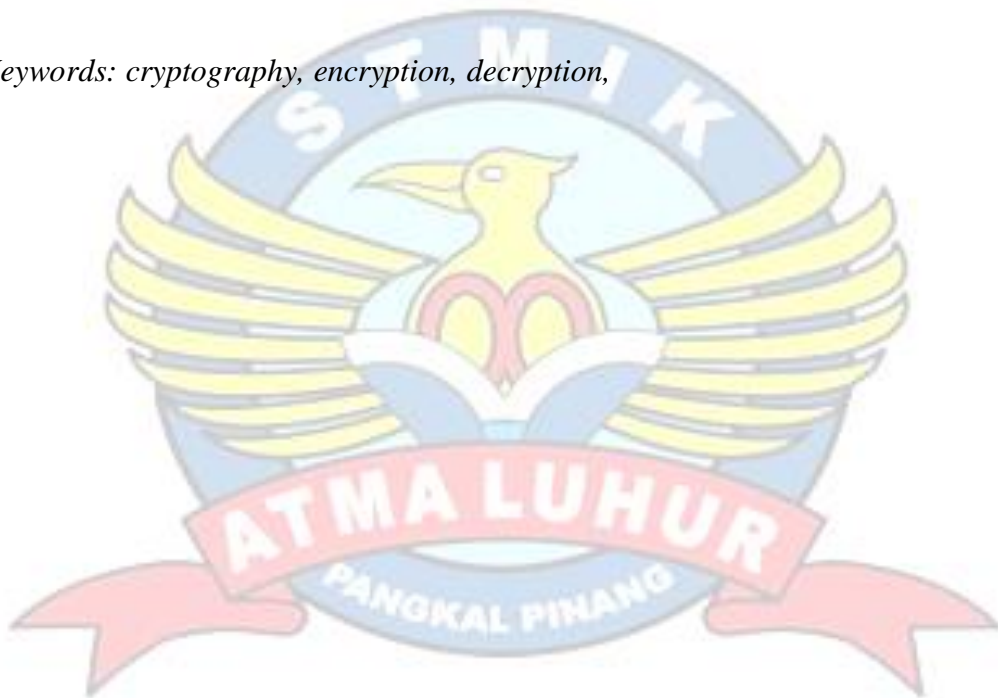
Kata Kunci : kriptografi, enkripsi, dekripsi,



ABSTRACT

Research has been conducted using the Rivest Shamir Adleman cryptographic algorithm. This research was applied in a web-based application of criticism and advice services at the engineering faculty of the Bangka Belitung University. This application is made because the suggestion and criticism boxes in the engineering faculty are often empty due to student concerns when their messages are tapped by unauthorized people. The processes used in this application are encryption, decryption and key generation. Methods for application development use the waterfall method and system development tools using activity diagrams, use case diagrams, and sequence diagrams. With this application, absolutely that it will facilitate students of this application to secure the messages delivered and the process of sending messages will be more effective and efficient.

Keywords: cryptography, encryption, decryption,



DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN SKRIPSI	iii
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
DAFTAR SIMBOL	xiv
BAB I PENDAHULUAN	
1.1. Latar Belakang	1
1.2. Rumusan Masalah.	3
1.3. Tujuan dan Manfaat Penelitian	3
1.4. Batasan Masalah	3
1.5. Sistematika Penulisan.....	3
BAB II LANDASAN TEORI	
2.1. <i>Web</i>	5
2.2. Bahasa Pemrograman PHP.....	5
2.3. MySQL.....	6
2.3.1. Keunggulan MySQL	
2.3.2. Tipe Data di MySQL.....	6
2.4. Definisi Keamanan	9
2.5. Kriptografi.....	9
2.5.1. Tujuan Kriptografi	11
2.6. Pesan, <i>Plaintext</i> , dan <i>Ciphertext</i>	11
2.7. Enkripsi dan Dekripsi	12
2.8. Kriptanalisis dan Kriptologi.....	12

2.9. ASCII	12
2.10. Model Pengembangan <i>Waterfall</i>	13
2.11. <i>Unified Modeling Language</i> (UML).....	15
2.12. Algoritma RSA	15
2.13. Penelitian Terdahulu	20

BAB III METODOLOGI PENELITIAN

3.1. Model Pengembangan Perangkat Lunak	23
3.1.1. Pengumpulan Data	23
3.1.2. Analisis	23
3.1.3. Desain	24
3.1.4. Implementasi.....	24
3.1.5. Pengujian	25
3.2. Metode Pengembangan Perangkat lunak	25
3.3. Alat Bantu Pengembangan Sistem	25

BAB IV PEMBAHASAN DAN HASIL

4.1. Sejarah Universitas	26
4.1.1. Struktur Organisasi Fakultas Teknik.....	26
4.1.2. Visi dan Misi.....	27
4.2. Analisa Masalah	28
4.2.1. Analisa Sistem Berjalan	28
4.2.2. Analisa Kebutuhan Sistem.....	29
4.3. Perancangan	30
4.3.1. <i>Use case</i> Diagram	30
4.3.2. Perancangan <i>Database</i>	33
4.3.3. <i>Class</i> Diagram.....	35
4.3.4. <i>Sequence</i> Diagram.....	35
4.3.4. Interface	37
4.4. Implementasi	41
4.4.1. Tampilan Layar <i>Login</i>	41

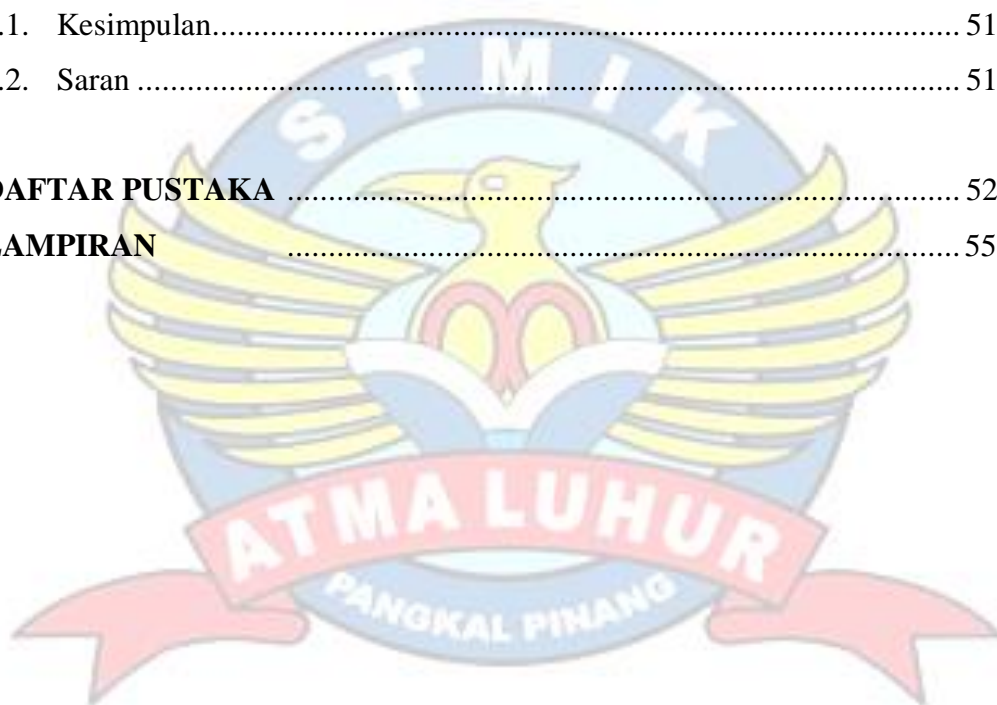
4.4.2. Tampilan Layar <i>User</i>	43
4.4.3. Tampilan Layar Admin	44
4.5. Pengujian.....	46
4.5.1. Pengujian Box <i>Login</i>	47
4.5.2. Pengujian Box <i>User</i>	47
4.5.3. Pengujian Box Admin	48
4.5.4. Pengujian Hasil Kueisioner	49

BAB V PENUTUP

5.1. Kesimpulan.....	51
5.2. Saran	51

DAFTAR PUSTAKA	52
-----------------------------	----

LAMPIRAN	55
-----------------------	----



DAFTAR GAMBAR

2.1. Proses Enkripsi dan Dekripsi Algoritma Simetris	10
2.2. Proses Enkripsi dan Dekripsi Algoritma Asimetris	10
2.3. Metode Pengembangan <i>Waterfall</i>	14
3.1. Metode <i>Waterfall</i>	23
4.1. Struktur Organisasi Fakultas Teknik.....	26
4.2. <i>Activity Diagram</i> Proses Pelayanan Kritik Dan Saran Manual.....	29
4.3. <i>Use case Diagram User</i>	31
4.4. <i>Use case Diagram Admin</i>	31
4.5. <i>Class Diagram</i>	35
4.6. <i>Sequence Diagram Login</i>	35
4.7. <i>Sequence Diagram</i> Enkripsi	36
4.8. <i>Sequence Diagram</i> Dekripsi	36
4.9. <i>Sequence Diagram Generate Key</i>	37
4.10. Rancangan Layar <i>Login</i>	37
4.11. Rancangan Layar Profil Kampus	38
4.12. Rancangan Layar Profil Pengembang	38
4.13. Rancangan Layar <i>User</i> Untuk Mengirimkan <i>Chipertext</i>	39
4.14. Rancangan Layar <i>User</i> Untuk Mendapatkan <i>Chipertext</i>	39
4.15. Rancangan Layar Untuk Mendekripsikan Pesan	40
4.16. Rancangan Layar Untuk Mendapatkan <i>Plaintext</i>	40
4.17. Rancangan Layar Kotak Masuk.....	41
4.18. Tampilan Layar <i>Login</i>	41
4.19. Tampilan Layar Profil Universitas	42
4.20. Tampilan Layar Pengembang	42
4.21. Tampilan <i>User</i> untuk mengirimkan <i>ciphertext</i>	43
4.22. Tampilan <i>User</i> untuk meng-enkrip pesan	43
4.23. Tampilan <i>User</i> untuk mendapatkan <i>ciphertext</i>	44
4.24. Tampilan Layar Admin	44
4.25. Tampilan Layar <i>Generate key</i>	45

4.26. Tampilan Layar Kotak Masuk	45
4.27. Tampilan Layar Mendekripsikan Pesan	46
4.28. Tampilan Layar Menampilkan Pesan.....	46
4.29. Diagram Hasil Pengujian Dari Kueisioner	50






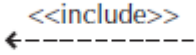
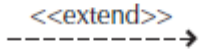
DAFTAR TABEL

2.1. Tipe Data Numerik Beserta Fungsinya	7
2.2. Tipe Data <i>Date & Time</i> Beserta Fungsinya.....	8
2.3. Tipe Data <i>String</i> Beserta Fungsinya	8
2.4. Karakter ASCII.....	13
2.5. Parameter Algoritma RSA.....	15
2.6. Daftar Penelitian Terkait Terdahulu.....	20
4.1. Tabel <i>Login</i>	34
4.2. Tabel <i>User</i>	34
4.3. Pengujian Black Box Login.....	47
4.4. Pengujian Black Box User.....	47
4.5. Pengujian Black Box Admin	48
4.6. Pengujian Hasil Kueisioner	49



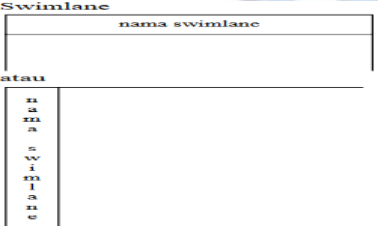
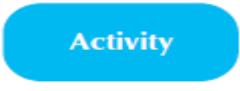
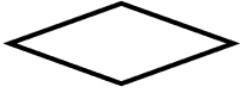


DAFTAR SIMBOL

1. Simbol *Use case* Diagram

No	Simbol	Keterangan
1		<i>Use case</i> Gambaran fungsional dari suatu sistem, sehingga pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun.
2		Aktor Sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu
3		<i>Association</i> Merupakan abstraksi berupa garis tanpa panah yang menghubungkan antara aktor dan <i>use case</i> atau <i>use case</i> dengan <i>use case</i>
4		<i>Include</i> Menunjukkan bahwa suatu <i>use case</i> seluruhnya merupakan fungsionalitas dari <i>use case</i> lainnya
5		<i>Extend</i> Merupakan perpanjangan kasus penggunaan untuk memasukkan perilaku opsional. Memiliki panah yang diambil dari penggunaan ekstensi kasus ke kasus penggunaan dasar

2. Simbol *Activity* Diagram

No	Simbol	Keterangan
1	<p>Status Awal</p> 	<p>Initial Node</p> <p>Merupakan simbol untuk memulai <i>Activity</i> diagram</p>
2	<p>Status akhir</p> 	<p><i>Activity</i> Final Node</p> <p>Merupakan simbol untuk mengakhiri <i>Activity</i> diagram</p>
3	<p>Swimlane</p> 	<p>Swimline</p> <p>Merupakan simbol untuk mengakhiri <i>activity</i> Diagram</p>
4		<p><i>Activity</i></p> <p><i>Activity</i> juga merupakan proses komputasi atau perubahan kondisi yang bisa berupa kata kerja atau ekspresi</p>
5	<p>Percabangan / <i>decision</i></p> 	<p>Decision</p> <p>Merupakan cara untuk menggabungkan ketika ada lebih dari 1 transisi yang masuk atau pilihan untuk mengambil keputusan</p>

3. Simbol *Sequence Diagram*

No	Simbol	Keterangan
1		Aktor Menggambarkan orang yang berinteraksi dengan sistem
2		<i>Entity Class</i> Menggambarkan hubungan kegiatan yang akan dilakukan
3		<i>Boundary Class</i> Menggambarkan sebuah penggambaran dari <i>form</i>
4		<i>Control Class</i> Menggambarkan penghubung antara <i>boundary</i> dengan tabel
5		<i>Life Line</i> Menggambarkan tempat mulai dan berakhir sebuah pesan
6		<i>Line Message</i> Menggambarkan pengiriman pesan