



**KRIPTOGRAFI PENGIRIMAN SURAT MENGGUNAKAN ALGORITMA  
*BLOWFISH DAN BASE64***



**VANDY RAMER SAPUTRA**

**41512010028**

UNIVERSITAS  
MERCU BUANA

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS MERCU BUANA**

**JAKARTA**

**2016**



UNIVERSITAS  
**MERCU BUANA**

**KRIPTOGRAFI PENGIRIMAN SURAT MENGGUNAKAN ALGORITMA  
*BLOWFISH DAN BASE64***

*Laporan Tugas Akhir*

Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer

U VANDY RAMER SAPUTRA S

41512010028

MERCU BUANA

PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA

2016

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41512010028  
Nama : VANDY RAMER SAPUTRA  
Judul Tugas Akhir : **KRIPTOGRAFI PENGIRIMAN SURAT  
MENGGUNAKAN ALGORITMA *BLOWFISH* DAN  
*BASE64***

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 18 Agustus 2016



VANDY RAMER SAPUTRA

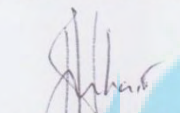
UNIVERSITAS  
MERCU BUANA

**LEMBAR PENGESAHAN**

NIM : 41512010028  
Nama : Vandy Ramer Saputra  
Program Studi : Informatika  
Fakultas : Ilmu Komputer  
Judul Tugas Akhir : Kriptografi Pengiriman Surat Menggunakan Algoritma  
*Blowfish Dan Base64*

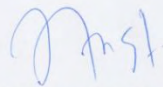
Jakarta, 18 Agustus 2016

Disetujui dan diterima oleh,



Dr. Ida Nurhaida, MT

Dosen Pembimbing



Desi Ramayanti, S.Kom, MT

Koordinator Tugas Akhir  
Informatika



Dr. Yaya Sudarya Triana, M.Kom

Ketua Program Studi  
Informatika

UNIVERSITAS  
MERCU BUANA

## KATA PENGANTAR

Alhamdulillahirabbil'alamin, Puji serta syukur atas kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, dan berkat kesempatan yang diberikannya juga penulis dapat menyelesaikan program studi strata satu (S1) pada jurusan teknik Informatika Universitas Mercu Buana Jakarta.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan dan kekurangan penulis menyadari laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan dan dorongan dari pihak lain. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada :

1. Ibu Dr. Ida Nurhaida. M.T, selaku Pembimbing Tugas Akhir yang telah mengarahkan dan membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Bapak Dr, Yaya Sudarya Triana. M.Kom, selaku Kaprodi Informatika Universitas Mercu Buana.
3. Ibu Desi Ramayanti, S.Kom, MT, selaku Koordinator Tugas Akhir Informatika Universitas Mercu Buana.
4. Seluruh Dosen Informatika Universitas Mercu Buana yang telah mendukung penulis baik doa maupun materi.
5. Kedua Orang Tua dan Saudara-saudara tercinta yang telah memberikan dorongan moril dan do'anya untuk kesuksesan penulis cinta kasih yang begitu besar, sehingga memungkinkan penulis menyelesaikan Laporan Tugas Akhir ini tepat pada waktunya.
6. Beserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Semoga Allah SWT membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua, Aamiin.

Akhir kata penulis mengharapkan tulisan ini dapat memberi manfaat bagi penulis khususnya pembaca pada umumnya. Penulis menyadari bahwa tulisan ini tidak lepas dari kekurangan. Atas saran dan kritik yang membangun penulis mengucapkan terima kasih.

Jakarta, 18 Agustus 2016

Vandy Ramer Saputra



## ABSTRACT

*The development of the computer when it's already going fast. In today's era of information technology in digital messaging and security in information storage letter is important and can not be ignored. With technology growing so rapidly, the exchange of information into a very easy thing to simply rely on the Internet as a medium of exchange. But one of them a negative impact on the development of information technology is the theft of data. With the data theft, the security aspects of mail delivery and data storage are considered important. In this thesis Mailer made in secret and officially order the letter to its goal. For the letter to be sent securely, hence the need for securing a mail file, so that the letter can not be stolen by those who menginkan file this letter. To facilitate the authors in the design application system was built in the development of cryptographic algorithms using blowfish and base64 with PHP and using MySQL database, which can secure or hide file documents by way of decrypting and mengdekripsikan letter file and digital science, so that others who menginkan document this bias is not stolen with ease. Meaning of letters will be up to the party bosses safely without changing in the slightest. The file received will be immediately seen and verified for endorsement letter.*

*Keyword: PHP and MySQL*

UNIVERSITAS  
MERCU BUANA

## ABSTRAKSI

Perkembangan komputer saat ini memang sudah berjalan dengan cepat. Di era teknologi informasi sekarang ini pengiriman pesan secara digital dan keamanan dalam penyimpanan informasi surat adalah hal yang penting dan tidak dapat diabaikan. Dengan makin berkembangnya teknologi yang begitu pesat maka pertukaran informasi menjadi hal yang sangat mudah dengan hanya mengandalkan internet sebagai media pertukaran. Tetapi salah satunya dampak negatif dalam perkembangan teknologi informasi adalah adanya pencurian data. Dengan adanya pencurian data maka aspek keamanan dalam pengiriman surat serta penyimpanan data dianggap penting. Dalam tugas akhir ini dibuatlah Aplikasi pengiriman surat secara rahasia dan resmi agar surat tersebut sampai di tujuannya. Agar surat dikirim secara aman, oleh karena itu perlu adanya pengamanan suatu file surat, supaya surat tersebut tidak bisa dicuri oleh pihak yang menginginkan file surat ini. Untuk memudahkan penulis dalam perancangan system aplikasi ini dibangun dalam pengembangan kriptografi menggunakan algoritma *blowfish* dan *base64* dengan program PHP dan menggunakan basis data *MySQL*, yang dapat mengamankan atau merahasiakan file dokumen dengan cara menenkripsi dan mendekripsikan file surat dan digital sains, agar pihak lain yang menginginkan dokumen ini tidak bias dicuri dengan mudah. Maka surat akan sampai kepada pihak atasan secara aman tanpa berubah sedikit pun. File yang akan diterima akan segera dilihat dan diverifikasi untuk pengesahan surat.

Kata Kunci : PHP dan *MySQL*



## DAFTAR ISI

	Hal
HALAMAN JUDUL .....	ii
LEMBAR PERNYATAAN.....	iii
LEMBAR PENGESAHAN .....	iv
KATA PENGANTAR .....	v
ABSTRACT.....	vii
ABSTRAK.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiv
1. PENDAHULUAN .....	1
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penulisan.....	2
1.5 Metode Penelitian .....	3
1.6 Sistematika Penulisan .....	3
2. LANDASAN TEORI.....	5
2.1 Definisi Kriptografi.....	5
2.2 Sejarah Kriptografi.....	6
2.3 Tujuan Kriptografi .....	7
2.4 Algoritma Kriptografi .....	8
2.5 Algoritma Blowfish .....	10
2.6 Algoritma Base64 .....	12
2.7 PHP .....	14
2.7.1 Pengertian Php .....	14
2.7.2 Kelebihan Php .....	14
2.7.3 <i>Script</i> Php.....	14
2.8 XAMPP.....	15
2.8.1 Pengertian Xampp.....	15

2.9	MySQL .....	15
2.9.1	Keunggulan My SQL.....	15
3.	ANALISA PERANCANGAN SISTEM .....	17
3.1	Analisa Sistem Berjalan.....	17
3.2	<i>Use Case</i> Diagram Sistem Berjalan.....	17
3.3	<i>Activity</i> Diagram Membuat Surat.....	19
3.4	Analisa Sistem Usulan .....	22
3.5	<i>Use Case</i> Diagram Sistem Usulan .....	22
3.6	<i>Activity</i> Diagram <i>Login</i> .....	27
3.7	<i>Sequence</i> Diagram Usulan .....	33
3.8	<i>Class</i> Diagram.....	40
3.9	Struktur Basis Data .....	41
3.10	Perancangan Tampilan.....	45
3.11	Algoritma Blowfish.....	48
3.11.1	Proses Enkripsi Dan Deskripsi Surat.....	48
3.12	Algoritma Base64 .....	51
3.12.1	Proses Enkripsi Dan Deskripsi Tanda Tangan.....	51
4.	IMPLEMENTASI DAN PENGUJIAN.....	54
4.1	Implementasi.....	54
4.2	Implementasi Basis Data.....	55
4.3	Implementasi Dan Pengujian Program.....	60
4.4	Metode Pengujian .....	72
4.5	Skenario Pengujian .....	72
4.6	Kasus Dan Hasil Pengujian.....	74
4.7	Analisa Hasil Pengujian.....	78
5.	PENUTUP.....	79
5.1	Kesimpulan .....	79
5.2	Saran .....	79
	DAFTAR PUSTAKA .....	80

## DAFTAR GAMBAR

	Halaman
Gambar 1.1 Metode Waterfall .....	4
Gambar 2.1 Proses Kriptografi Secara Umum(Lusiana n.d) .....	5
Gambar 2.2 Scytale (Lusiana n.d) .....	7
Gambar 2.3 Algoritma Simetris (Prakoso n.d).....	10
Gambar 2.4 Algoritma Asimetris (P& Dessyanto n.d) .....	11
Gambar 3.1 <i>Use Case</i> Diagram Sistem Berjalan.....	15
Gambar 3.2 <i>Activity</i> Diagram Membuat Surat.....	17
Gambar 3.3 <i>Activity</i> Diagram Memberikan Surat.....	18
Gambar 3.4 <i>Activity</i> Diagram Menerima Surat.....	19
Gambar 3.5 <i>Use Case</i> Diagram Sistem Usulan.....	20
Gambar 3.6 <i>Activity</i> Diagram <i>Login</i> .....	25
Gambar 3.7 <i>Activity</i> Diagram Mengelola Data <i>User</i> .....	26
Gambar 3.8 <i>Activity</i> Diagram Mengelola Fakultas.....	27
Gambar 3.9 <i>Activity</i> Diagram Mengelola Data Prodi .....	28
Gambar 3.10 <i>Activity</i> Diagram Mengelola Data Surat.....	30
Gambar 3.11 <i>Sequence</i> Diagram <i>Login</i> .....	31
Gambar 3.12 <i>Sequence</i> Diagram Mengelola Data <i>User</i> .....	32
Gambar 3.13 <i>Sequence</i> Diagram Mengelola Data Fakultas .....	33
Gambar 3.14 <i>Sequence</i> Diagram Mengelola Data Prodi .....	34
Gambar 3.15 <i>Sequence</i> Diagram Mengelola Data Surat .....	35
Gambar 3.16 <i>Sequence</i> Diagram Mengelola Data Tanda Tangan .....	36
Gambar 3.17 <i>Sequence</i> Diagram Mengelola Data Verifikasi.....	37
Gambar 3.18 <i>Class</i> Diagram.....	38
Gambar 3.19 Rancangan Tampilan Layar <i>Login</i> .....	43
Gambar 3.20 Rancangan Menu Home/ Utama .....	44
Gambar 3.21 Rancangan Tampilan Kelola Surat .....	44
Gambar 3.22 Rancangan Tampilan Surat Verifikasi .....	45
Gambar 3.23 Rancangan Layar Menu Verifikasi Tanda Tangan .....	45
Gambar 3.24 Rancangan Layar Menu Cetak Surat .....	46
Gambar 3.25 <i>Flowchart</i> Surat .....	50
Gambar 3.26 <i>Flowchart</i> Tanda Tangan.....	53
Gambar 4.1 Database Vandy .....	55

Gambar 4.2	Tabel Admin .....	55
Gambar 4.3	Tabel Dekan .....	56
Gambar 4.4	Tabel DPM.....	56
Gambar 4.5	Tabel Fakultas .....	57
Gambar 4.6	Tabel Ketua Prodi .....	57
Gambar 4.7	Tabel Mahasiswa .....	58
Gambar 4.8	Tabel Prodi.....	58
Gambar 4.9	Tabel Surat .....	59
Gambar 4.10	Tabel Wadek .....	59
Gambar 4.11	Tampilan <i>Login</i> Admin.....	60
Gambar 4.12	Potongan Koding Tampil <i>Login</i> .....	60
Gambar 4.13	Tampilan Utama Admin Setelah <i>Login</i> .....	62
Gambar 4.14	Tampilan <i>Login</i> Mahasiswa.....	62
Gambar 4.15	Tampilan Utama Mahasiswa Setelah <i>Login</i> .....	63
Gambar 4.16	Tampilan <i>Login</i> DPM .....	63
Gambar 4.17	Tampilan UtamanDPM Setelah <i>Login</i> .....	64
Gambar 4.18	Tampilan <i>Login</i> Kaprodi.....	64
Gambar 4.19	Tampilan Utama Kaprodi Setelah <i>Login</i> .....	65
Gambar 4.20	Tampilan <i>Login</i> Wakil Dekan.....	65
Gambar 4.21	Tampilan Utama Wakil Dekan Setelah <i>Login</i> .....	66
Gambar 4.22	Tampilan <i>Login</i> Dekan.....	66
Gambar 4.23	Tampilan Utama Dekan Setelah <i>Login</i> .....	67
Gambar 4.24	Tampilan Mahasiswa Mengirim Surat.....	67
Gambar 4.25	Tampilan Verifikasi DPM.....	68
Gambar 4.26	Tampilan Verifikasi Kaprodi .....	68
Gambar 4.27	Tampilan Verifikasi Wakil Dekan .....	69
Gambar 4.28	Tampilan Verifikasi Dekan.....	69
Gambar 4.29	Tampilan Surat Sudah Verifikasi .....	70
Gambar 4.30	Tampilan Surat Yang Akan Dicitak .....	70
Gambar 4.31	Tampilan Admin Mengelola Surat.....	71

## DAFTAR TABEL

		Halaman
Tabel3.1	Skenario <i>Use Case</i> Diagram Membuat Surat.....	16
Tabel3.2	Skenario <i>Use Case</i> Diagram Memberikan Surat.....	16
Tabel3.3	Skenario <i>Use Case</i> Diagram Menerima Surat.....	16
Tabel3.4	<i>Activity</i> Diagram Membuat Surat .....	17
Tabel 3.5	<i>Activity</i> Diagram Memberikan Surat.....	18
Tabel3.6	<i>Activity</i> Diagram Menerima Surat.....	19
Tabel3.7	Deskripsi <i>Use Case</i> Diagram Kelola Data <i>User</i> .....	21
Tabel3.8	Deskripsi <i>Use Case</i> Diagram Kelola Data Fakultas.....	21
Tabel3.9	Deskripsi <i>Use Case</i> Diagram Kelola Data Akun.....	22
Tabel3.10	Deskripsi <i>Use Case</i> Diagram Ganti Password .....	22
Tabel3.11	Deskripsi <i>Use Case</i> Diagram Kelola Program Studi.....	22
Tabel3.12	Deskripsi <i>Use Case</i> Diagram Kelola Surat.....	23
Tabel3.13	Deskripsi <i>Use Case</i> Diagram Kelola Tanda Tangan.....	23
Tabel 3.14	Deskripsi <i>Use Case</i> Diagram Cetak Surat.....	24
Tabel 3.15	Deskripsi <i>Use Case</i> Diagram Verifikasi .....	24
Tabel 3.16	<i>Activity</i> Diagram <i>Login</i> .....	25
Tabel 3.17	<i>Activity</i> Diagram Mengelola Data <i>User</i> .....	26
Tabel3.18	<i>Activity</i> Diagram Mengelola Data Fakultas.....	28
Tabel3.19	<i>Activity</i> Diagram Mengelola Data Prodi .....	29
Tabel3.20	<i>Activity</i> Diagram Mengelola Data Surat.....	30
Tabel3.21	Keterangan <i>Sequence</i> Diagram <i>Login</i> .....	31
Tabel3.22	Keterangan <i>Sequence</i> Diagram MengelolaData <i>User</i> .....	32
Tabel3.23	Keterangan <i>Sequence</i> Diagram Mengelola Data Fakultas .....	33
Tabel 3.24	Keterangan <i>Sequence</i> Diagram Mengelola Data Prodi .....	34
Tabel 3.25	Keterangan <i>Sequence</i> Diagram Mengelola Data Surat .....	35
Tabel 3.26	Keterangan <i>Sequence</i> Diagram Mengelola Data Tanda Tangan .....	36
Tabel 3.27	Keterangan <i>Sequence</i> Diagram Mengelola Data Verifikasi.....	37
Tabel 3.28	Struktur Basis Data Admin.....	39
Tabel3.29	Struktur Basis Data Mahasiswa.....	39
Tabel3.30	Struktur Basis Data DPM .....	40

Tabel3.31	Struktur Basis Data Ketua Prodi .....	40
Tabel3.32	Struktur Basis Data Wakil Dekan (Wadek) .....	41
Tabel3.33	Struktur Basis Data Dekan .....	41
Tabel3.34	Struktur Basis Data Surat .....	42
Tabel 3.35	<i>Activity</i> Diagram Memberikan Surat.....	18
Tabel3.36	<i>Activity</i> Diagram Menerima Surat.....	19
Tabel3.37	Deskripsi <i>Use Case</i> Diagram Kelola Data <i>User</i> .....	21
Tabel3.38	Deskripsi <i>Use Case</i> Diagram Kelola Data Fakultas.....	21
Tabel 3.39	Deskripsi <i>Use Case</i> Diagram Kelola Data Akun.....	22
Tabel 3.10	Deskripsi <i>Use Case</i> Diagram Ganti Password .....	22
Tabel 3.11	Deskripsi <i>Use Case</i> Diagram Kelola Program Studi.....	22
Tabel 3.12	Deskripsi <i>Use Case</i> Diagram Kelola Surat.....	23
Tabel 3.13	Deskripsi <i>Use Case</i> Diagram Kelola Tanda Tangan.....	23
Tabel 3.14	Deskripsi <i>Use Case</i> Diagram Cetak Surat.....	24
Tabel 3.15	Deskripsi <i>Use Case</i> Diagram Verifikasi .....	24
Tabel 3.16	<i>Activity</i> Diagram <i>Login</i> .....	25
Tabel 3.17	<i>Activity</i> Diagram Mengelola Data <i>User</i> .....	26
Tabel4.1	Rancangan Pengujian Halaman Admin.....	75
Tabel4.2	Pengujian <i>Login</i> User .....	76
Tabel4.3	Pengujian Mengelola Data User.....	76
Tabel4.4	Pengujian Mengelola Data Surat.....	78
Tabel 4.5	Pengujian Mengelola Data Tanda Tangan.....	79
Tabel4.6	Pengujian Mengelola Data Fakultas.....	80
Tabel4.7	Pengujian Mengelola Data Prodi.....	81
Tabel4.8	Pengujian Mengelola Data Verifikasi .....	81