

**PEMBUATAN *CERTIFICATE HYPERTEXT TRANSPORT  
PROTOCOL SECURE (HTTPS)***

**Tugas Akhir**



Angga Febrianto

05.01.1884

**DIPLOMA III**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
"AMIKOM"  
YOGYAKARTA  
2008**

**PEMBUATAN *CERTIFICATE HYPERTEXT TRANSPORT*  
*PROTOCOL SECURE (HTTPS)***

**TUGAS AKHIR**

Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Ahli Madya Komputer  
Pada Jurusan Teknik Informatika



**Disusun Oleh :**  
**Angga Febrianto**  
**05.01.1884**

**JURUSAN TEKNIK INFORMATIKA**  
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**  
**"AMIKOM"**  
**YOGYAKARTA**  
**2008**

**HALAMAN PERSETUJUAN**

**PEMBUATAN *CERTIFICATE HYPERTEXT TRANSPORT  
PROTOCOL SECURE (HTTPS)***

**TUGAS AKHIR**

Disusun guna memenuhi persyaratan untuk menyelesaikan mata kuliah

Tugas Akhir pada jurusan Teknik Informatika

Sekolah Tinggi Manajemen Informatika dan Komputer

"AMIKOM" Yogyakarta

Disahkan dan disetujui oleh :

Mengetahui,

Ketua STMIK AMIKOM Yogyakarta

Dosen Pembimbing

(Prof. Dr. M. Suyanto, MM)

(Sudarmawan, MT)

## HALAMAN PENGESAHAN

### PEMBUATAN *CERTIFICATE HYPERTEXT TRANSPORT PROTOCOL SECURE (HTTPS)*

#### TUGAS AKHIR

Telah diuji dan disyahkan dihadapan tim penguji Sekolah Tinggi Manajemen  
Informatika dan Komputer "AMIKOM" Yogyakarta, pada :

Hari : Kamis  
Tanggal : 07 Agustus 2008  
Pukul : 13:00  
Tempat : Stack

Tim Penguji

Penguji I : Dr. Abidarin Rosidi, MMA

Penguji II : Andi Sunyoto, M.Kom

Penguji III : Sudarmawan, MT

## HALAMAN MOTO



“.....Allah meninggikan orang yang beriman diantara kamu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah maha mengetahui apa yang kamu kerjakan  
(QS. Al-Mujaadalah :11)

**Ibnu Rajab** berkata, “Barang siapa yang memelihara ketaatan kepada Allah di masa muda dan masa kuatnya, maka Allah akan memelihara kekuatannya disaat tua dan saat kekuatannya melemah. Ia akan tetap diberi kekuatan pendengaran, penglihatan, kemampuan berpikir dan kekuatan akal.”

## KATA PENGANTAR

Puji syukur kepada Allah SWT yang telah melimpahkan rahmat, taufik dan hidayah-NYA sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul **Pembuatan *Certificate Hypertext Transport Protocol Secure (HTTPS)***.

Penyusunan Tugas Akhir ini bertujuan untuk menambah wawasan dan pengetahuan penulis khususnya di bidang teknik informatika dan telekomunikasi serta sebagai salah satu syarat kelulusan untuk memperoleh gelar Ahli Madya Komputer pada jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Pembuatan laporan ini juga tidak lepas dari bantuan berbagai pihak. Untuk itu pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada :

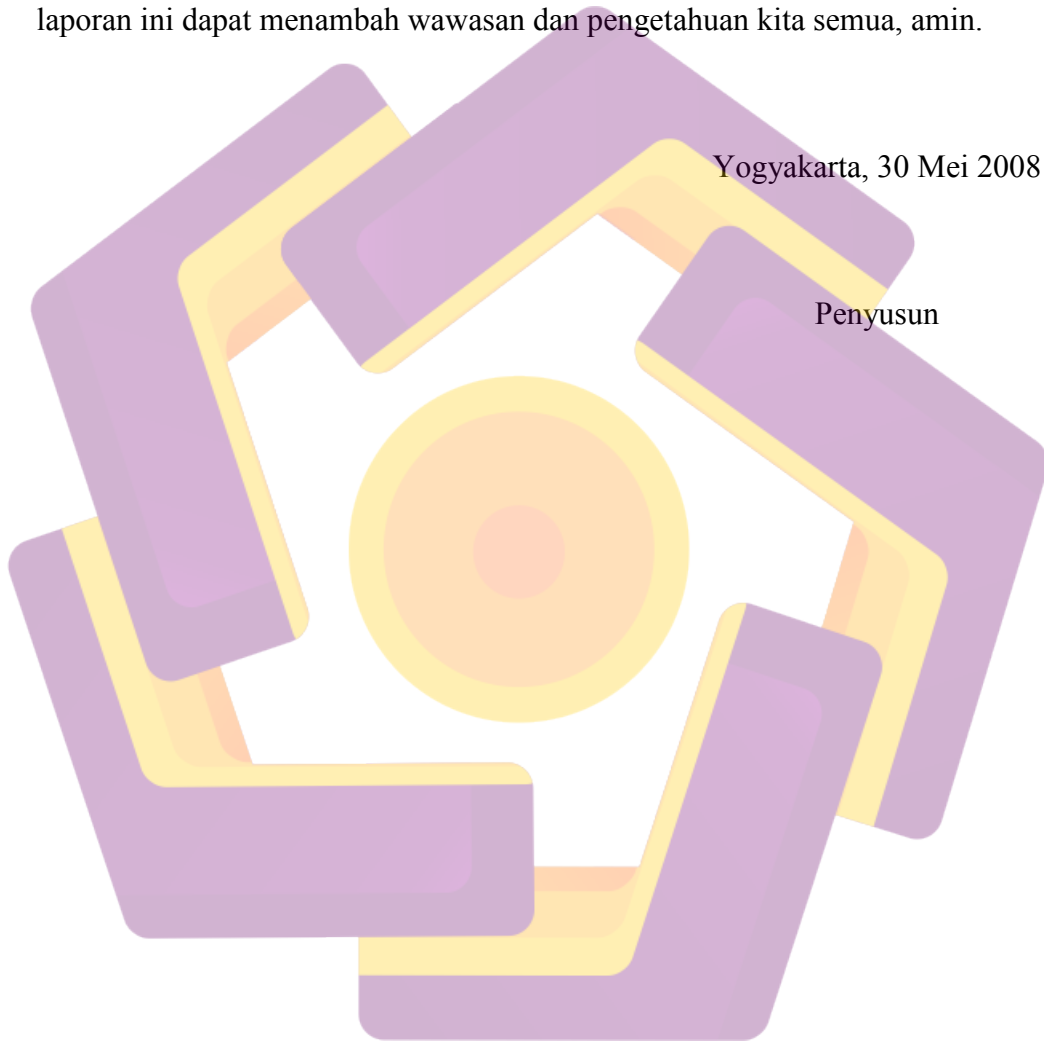
1. Bapak M. Suyanto, DR, MM. selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku dosen pembimbing yang telah memberikan arahan dan masukan.
3. Bapak Abidarin Rosidi, DRS, DR, MM selaku dosen metodologi penelitian yang telah memberikan masukan dalam format penulisan laporan.
4. Seluruh staff dan karyawan STMIK AMIKOM Yogyakarta.

Seperti kata pepatah, *tiada gading yang tak retak*, kami menyadari sepenuhnya bahwa penulisan laporan ini masih memiliki banyak kekurangan. Untuk itu kami mengharap kritik dan saran yang bersifat membangun.

Akhir kata kami berharap semoga apa yang telah kami tuangkan dalam laporan ini dapat menambah wawasan dan pengetahuan kita semua, amin.

Yogyakarta, 30 Mei 2008

Penyusun



## DAFTAR ISI

	Halaman
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN MOTO.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LISTING.....	xv
INTISARI.....	xvi
<b>BAB I. PENDAHULUAN</b>	
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah.....	5
1.3. Batasan Masalah.....	6
1.4. Maksud dan Tujuan Penelitian.....	6
1.5. Manfaat Penelitian.....	7
1.6. Metodologi.....	8
1.7. Sistematika Penulisan.....	8
1.8. Jadwal Penelitian.....	9
<b>BAB II. LANDASAN TEORI</b>	



2.1. Tinjauan Pustaka .....	10
2.2. Komunikasi Data.....	12
2.3. Model Komunikasi Data .....	14
2.3.1. <i>OSI Model</i> .....	14
a. <i>Physical</i> .....	15
b. <i>Data Link</i> .....	15
c. <i>Network</i> .....	16
d. <i>Transport</i> .....	16
e. <i>Session</i> .....	16
f. <i>Presentation</i> .....	16
g. <i>Application</i> .....	17
2.4. TCP/IP Model .....	17
2.5. Dasar-Dasar Sistem Keamanan Data .....	20
2.6. Kriptografi.....	22
2.6.1. Pengertian Kriptografi.....	22
2.6.2. Algoritma Kriptografi Klasik.....	24
2.6.3. Algoritma Kriptografi Modern.....	24
a. <i>Symmetric Algorithms</i> .....	24
b. <i>Assymmetric Algorithms</i> .....	25
2.6.4. Algoritma Kriptografi RSA .....	25
2.6.5. <i>Web Server</i> .....	26
2.6.6. <i>Web Server Apache</i> .....	27
2.6.7. <i>Secure Socket Layer</i> .....	27

2.6.8. <i>Mod_SSL</i> .....	28
2.6.9. Model Arsitektur .....	29
2.6.10. Teknik Kriptografi SSL.....	30
2.6.11. Ringkasan Pesan ( <i>Message Digests</i> ).....	30
2.6.12. Tanda Tangan Digital ( <i>Digital Signature</i> ).....	31
2.6.13. Sertifikasi Digital .....	32
2.6.14. Isi Sertifikat ( <i>Certificate Content</i> ) .....	32
2.6.15. Otoritas Sertifikat.....	35
2.6.16. Rantai Sertifikat ( <i>Certificate Chains</i> ) .....	36
2.6.17. <i>Root-Level CA</i> .....	36
2.6.18. Manajemen Sertifikat .....	37
2.6.19. Cara Kerja SSL .....	38
2.6.19.1. Pembentukan <i>Session</i> .....	38
2.6.19.2. Metode Pertukaran Kunci .....	40
2.6.19.3. Kerahasiaan Dalam Pertukaran Data .....	41
2.6.19.4. Fungsi <i>Digest</i> .....	42
2.6.19.5. <i>Protokol Handshake Sequence</i> .....	42
2.6.19.6. Pengiriman Data.....	43
2.7. Ettercap .....	44

### **BAB III. GAMBARAN UMUM OBJEK PENELITIAN**

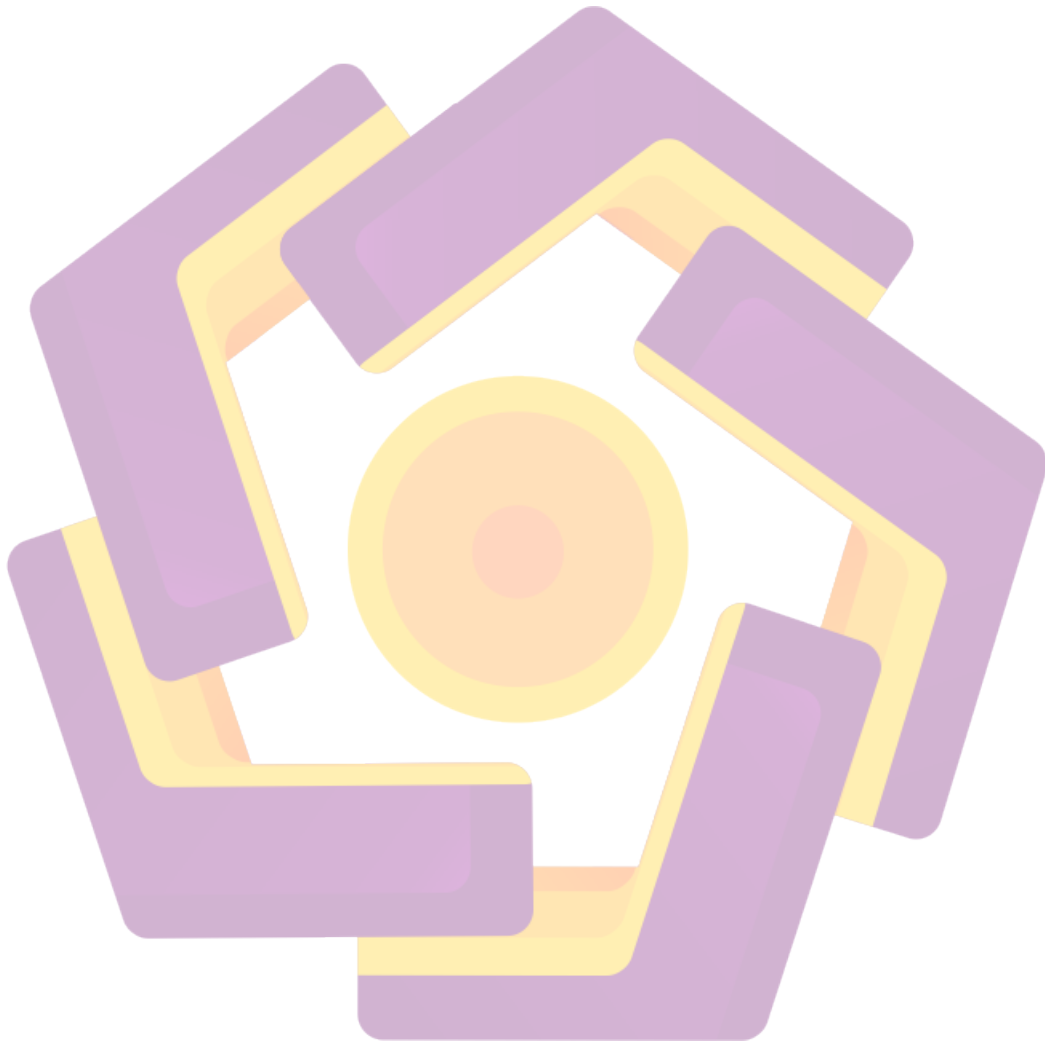
3.1. <i>Spesifikasi Sistem</i> .....	46
3.2. Perancangan serta Pemodelan implementasi <i>SSL</i> pada <i>web server Apache</i> .....	47
3.3. Pembuatan Sertifikat Digital .....	48
3.4. Pembuatan <i>Certificate Authority</i> .....	48
3.5. Implementasi model <i>web server</i> menggunakan <i>SSL</i> .....	49
3.6. Pengujian sistem .....	51
<b>BAB IV. PEMBAHASAN</b>	
4.1. Ancaman Transaksi Data .....	52
4.1.1. <i>Sniffing</i> pada ISP langsung .....	53
4.1.2. <i>Sniffing</i> pada Jalur <i>Internet Backbone</i> .....	54
4.2. Cara Kerja <i>HTTP</i> menggunakan <i>SSL</i> .....	55
4.3. Pemakaian Domain Untuk Sertifikat Digital .....	57
4.4. Desain Arsitektur .....	60
4.5. Spesifikasi Sistem .....	61
4.6. Instalasi <i>SSL</i> pada <i>Web server Apache</i> .....	62
4.7. Pemodelan Implementasi <i>SSL</i> pada <i>Web server Apache</i> .....	63
4.8. Contoh isi <i>Certificate Authority</i> dan sertifikat digital.....	64
4.9. Pembuatan Sertifikat Digital .....	66
4.10. Pembuatan <i>Certificate Authority</i> .....	73
4.11. Implementasi model <i>Web server</i> menggunakan <i>SSL</i> .....	76
4.12. Perancangan Pengujian .....	86

**BAB V. PENUTUP**

5.1. Kesimpulan .....	95
5.2. Saran.....	96

**DAFTAR PUSTAKA**

**LAMPIRAN**



## DAFTAR TABEL

	Halaman
Tabel 1.1. Jadwal Penelitian.....	9
Tabel 2.1. Informasi <i>Certificate</i> .....	33
Tabel 2.2. Informasi <i>Distinguished Name</i> .....	33
Tabel 4.1. Standar pengaksesan <i>SSL</i> .....	57
Tabel 4.2. Penggunaan sertifikat <i>SSL</i> pada standar NON <i>wild card</i> sertifikat ...	59
Tabel 4.3. Contoh <i>CA</i> dari <i>URL</i> <i>usu.ac.id</i> .....	64
Tabel 4.4. Contoh <i>CA</i> dari <i>URL</i> <i>gamatechno.net</i> .....	64
Tabel 4.5. Contoh sertifikat digital untuk subdomian <i>login.gamatechno.net</i> .....	65
Tabel 4.6. Contoh sertifikat digital untuk subdomain <i>portal.usu.ac.id</i> .....	65

## DAFTAR GAMBAR

	Halaman
Gambar 2.1. <i>OSI model</i> .....	15
Gambar 2.2. <i>Layer TCP/IP</i> .....	18
Gambar 2.3. Proses Enkripsi/Dekripsi Sederhana .....	23
Gambar 2.4. Versi <i>Protokol SSL</i> .....	28
Gambar 2.5. Arsitektur modul .....	29
Gambar 2.6. Contoh dari sebuah <i>PEM-encoded certificate</i> .....	35
Gambar 2.7. Cara kerja <i>SSL Urutan Handshake</i> .....	39
Gambar 2.8. Susunan <i>Protokol</i> .....	43
Gambar 2.9. <i>SSL Record Protokol</i> .....	44
Gambar 4.1. Ancaman pada sistem informasi berbasis internet .....	53
Gambar 4.2. Proses Pengaksesan Sertifikat oleh Browser .....	56
Gambar 4.3. Arsitektur <i>Web server</i> Menggunakan <i>SSL</i> .....	61
Gambar 4.4. <i>RSA Private Key</i> yang <i>Secure</i> .....	68
Gambar 4.5. <i>RSA Private Key</i> yang <i>UnSecure</i> .....	69
Gambar 4.6. Keterangan isi dari <i>Certificate Authority</i> .....	74
Gambar 4.7. <i>HTTP</i> dan <i>HTTPS</i> dalam satu <i>Apache server</i> .....	76
Gambar 4.8. Address bar pada saat request <i>HTTP</i> .....	79
Gambar 4.9. Pesan Peringatan <i>CA</i> yang tidak mempunyai otorisasi "USU" .....	80
Gambar 4.10. Address bar pada saat <i>HTTP</i> telah diredirect ke <i>HTTPS</i> .....	81

Gambar 4.11. Gambar <i>window</i> keseluruhan	
setelah aplikasi selesai loading “USU” .....	81
Gambar 4.12. Sertifikat Digital untuk domain “portal.usu.ac.id” .....	82
Gambar 4.13. <i>HTTP</i> dan <i>HTTPS</i> pada Apache <i>server</i> yang berbeda .....	83
Gambar 4.14. Skenario <i>forwarding sniffing</i> .....	86
Gambar 4.15. Pengisian netmask jaringan.....	88
Gambar 4.16. Menu <i>bridged sniffing</i> .....	88
Gambar 4.17. Pengisian interfacace jaringan.....	89
Gambar 4.18. Menu memulai <i>sniffing</i> .....	89
Gambar 4.19. Proses <i>sniffing</i> dimulai .....	89
Gambar 4.20. Hasil <i>sniffing</i> .....	90
Gambar 4.21. Hasil <i>sniffing</i> <a href="http://friendster.com">http://friendster.com</a> .....	92
Gambar 4.22. Hasil <i>sniffing</i> <a href="http://fotografer.net">http://fotografer.net</a> .....	93
Gambar 4.23. Hasil <i>sniffing</i> <a href="https://ib.bankmandiri.co.id">https://ib.bankmandiri.co.id</a> .....	93
Gambar 4.24. Hasil <i>sniffing</i> <a href="https://sikeu.usu.ac.id">https://sikeu.usu.ac.id</a> .....	94

## DAFTAR LISTING

	Halaman
Listing 4.1. Perintah Penginstallan <i>Library</i> .....	62
Listing 4.2. Perintah Installasi Apache, Modssl dan Openssl .....	63
Listing 4.3. Perintah pembuatan kunci private <i>RSA</i> .....	67
Listing 4.4. Perintah melihat isi dari kunci <i>private</i> .....	67
Listing 4.5. Perintah membuat dekripsi PEM dari kunci <i>private</i> .....	68
Listing 4.6. Perintah membuat <i>Certificate Signing Request</i> .....	70
Listing 4.7. Perintah melihat isi <i>CSR</i> .....	71
Listing 4.8. deskripsi file <i>gamatechno.csr</i> .....	71
Listing 4.9. Perintah untuk membuat kunci private <i>RSA</i> untuk <i>CA</i> .....	73
Listing 4.10. Perintah Mensign <i>Certificate Authority (CA)</i> .....	74
Listing 4.11. Perintah pengesahan <i>CSR</i> oleh <i>CA</i> .....	75
Listing 4.12. Konfigurasi <i>httpd.conf</i> .....	78
Listing 4.13. Perintah menjalankan Apache menggunakan <i>SSL</i> .....	79
Listing 4.14. Konfigurasi <i>httpd.conf</i> untuk <i>Web server HTTP</i> .....	85
Listing 4.15. Konfigurasi <i>httpd.conf</i> untuk <i>Web server HTTPS</i> .....	85
Listing 4.16. Perintah men- <i>sniffing</i> paket menuju 209.11.168.242 .....	92



## INTISARI

### PEMBUATAN *CERTIFICATE* *HYPERTEXT TRANSPORT PROTOKOL SECURE* (*HTTPS*)

Keamanan komputer saat ini telah menjadi perhatian tersendiri dalam pembuatan berbagai jenis aplikasi *website*, terutama saat terjadinya pertukaran data atau informasi *HTTP* yang penting, dan rahasia, contoh *web*, *e-mail*, *milis*, *newsgroup*, dan sebagainya. Seiring berkembangnya ilmu dan teknologi tersebut maka banyak masalah terjadi diantaranya pembobolan *user* dan *password* ketika menggunakan *protokol HTTP*.

Dari permasalahan di atas maka terdapat beberapa cara untuk mengamankan dalam pengiriman *user* dan *password* dalam aplikasi tersebut diantaranya cara menggunakan *HTTPS (HyperText Transport Protocol Secure)* dan kriptografi kunci publik (*Public Key Cryptography*). Dalam perkembangan teknologi yang di dukung oleh *Secure Socket Layer* dimana *protokol* tersebut bekerja tepat di bawah sebuah aplikasi jaringan komputer. *Protokol HTTPS* ini memberikan keamanan dengan metode otentifikasi terhadap *server* yang dihubungi.

Penelitian ini menghasilkan agar administrator dapat membuat *webserver* yang menggunakan *HTTP* lebih mengerti tentang kebocoran yang ada di *protokol* tersebut dan mengganti dengan *HTTPS* serta bisa melakukan instalasi dan mengimplementasikan dalam dunia informasi dan lebih jeli terhadap kewanaman pertukaran data intranet maupun internet. Dari hasil pengujian maka di dapat *protokol HTTPS* lebih aman dari pada *protokol HTTP*.

Keyword : *HTTPS, HTTP, Webserver, Kriptografi, Kunci Publik*