



**PENGUNAAN DIGITAL SIGNATURE & ENKRIPSI UNTUK
MENINGKATKAN OTENTIKASI, INTEGRITAS, KEAMANAN DAN
NON-REPUDIASI DATA**

**Studi Kasus Proses Pengiriman Data/Informasi Melalui *Email*
PT. Dimension Data Indonesia**

**UNIVERSITAS
MERCU BUANA**

Rhema Riesaputra

41507110109

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2014**

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NIM : 41507110109
Nama : Rhema Riesaputra
Judul Skripsi : PENGGUNAAN DIGITAL SIGNATURE & ENKRIPSI
UNTUK MENINGKATKAN OTENTIKASI, INTEGRITAS,
KEAMANAN DAN NON-REPUDIASI DATA

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiarisme, maka saya siap untuk mendapatkan sanksi akademis yang terkait dengan hal tersebut.

Jakarta, Juni 2014



Rhema Riesaputra

UNIVERSITAS
MERCU BUANA

LEMBAR PENGESAHAN

NIM : 41507110109
NAMA : Rhema Riesaputra
Judul Skripsi : PENGGUNAAN DIGITAL SIGNATURE & ENKRIPSI
UNTUK MENINGKATKAN OTENTIKASI, INTEGRITAS,
KEAMANAN DAN NON-REPUDIASI DATA

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, JUNI 2014



Sabar Rudiarto, S.Kom., M.Kom

Koordinator Tugas Akhir

Tri Daryanto, S.Kom., MT

Kaprodi Teknik Infomatika

KATA PENGANTAR

Segala puji syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa yang telah memberikan segala nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan skripsi ini.

Laporan skripsi yang berjudul “PENGUNAAN DIGITAL SIGNATURE & ENKRIPSI UNTUK MENINGKATKAN OTENTIKASI, INTEGRITAS, KEAMANAN DAN NON-REPUDIASI DATA” ini di buat untuk melengkapi salah satu syarat memperoleh gelar Sarjana Strata 1 (S1) pada Program Studi Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa penulisan laporan skripsi ini tidak terlepas dari dukungan, bantuan serta sumbangan pikiran dari berbagai pihak. Oleh karena itu dalam kesempatan ini penulis ingin memberikan ucapan terimakasih kepada:

1. Ida Nurhaida, S.T., MT., selaku pembimbing dalam menyelesaikan skripsi, terima kasih banyak atas bimbingan dan dukungannya.
2. Dr. Bambang Hariyanto, MT., selaku Dekan Fakultas Ilmu Komputer.
3. Tri Daryanto, S.Kom., MT., selaku Ketua Program Studi Teknik Informatika, Universitas Mercu Buana .
4. Sabar Rudiarto, S.Kom., M.Kom., selaku Koordinator Tugas Akhir Jurusan Teknik Informatika.
5. Seluruh dosen dan staff akademis program Strata-1 Universitas Mercu Buana.
6. Adeodatus Darrell Riesaputra, dan Istri tercinta yang tidak ada hentinya dalam memberikan doa dan dukungan, serta kasih sayang kepada penulis.
7. Bapak, ibu, kakak, dan adik tercinta yang tidak ada hentinya dalam memberikan doa dan dukungan, serta kasih sayang kepada penulis.
8. Frandinata Halim, S.T., M.M., selaku penasihat konsep dan sebagai penyedia fasilitas yang memberikan izin dalam pengerjaan studi kasus untuk menyelesaikan skripsi.

9. Djoni Djitrahadi, selaku motivator dan sebagai penyedia fasilitas yang memberikan izin dan pembiayaan untuk mendukung penulis agar dapat terus melanjutkan perkuliahan di Universitas Mercu Buana.
10. Rusdi Rachim, S.Kom., M.TI., selaku motivator dan yang memberikan izin dalam pengerjaan studi kasus untuk menyelesaikan skripsi.
11. Teman-teman dari Universitas Mercu Buana Teknik Informatika angkatan serta rekan-rekan lain yang tidak bisa disebutkan satu persatu, yang selalu membantu penulis dalam setiap waktu dan kesempatan.

Akhir kata dengan segala kerendahan hati penulis memohon maaf yang sebesar-besarnya atas segala kekurangan dan keterbatasan dalam penulisan laporan skripsi ini. Semoga laporan akhir ini dapat memberikan manfaat bagi pihak-pihak yang berkepentingan.



Jakarta, Juni 2014

Rhema Riesaputra

UNIVERSITAS
MERCU BUANA

DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
ABSTRACT	vi
ABSTRAK	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
BAB I PENDAHULUAN	
1.1. Latar Belakang	1
1.2. Perumusan Masalah.....	2
1.3. Ruang Lingkup.....	2
1.4. Batasan Masalah.....	3
1.5. Tujuan dan Manfaat Penelitian	3
1.5.1. Tujuan Penelitian.....	3
1.5.2. Manfaat Penelitian.....	4
1.6. Sistematika Penulisan.....	4
1.7. Metodologi Penelitian	6
BAB II LANDASAN TEORI	
2.1. Jaringan Komputer	8
2.2. Kriptografi.....	8
2.2.1. Sejarah Kriptografi.....	8
2.2.2. Kunci Simentris.....	11
2.2.3. Contoh Penerapan Kunci Simentris	11
2.2.4. Kunci Asimentris.....	13
2.2.5. Contoh Penerapan Kunci Asimentris	14
2.3 Fungsi Hash.....	15

2.3.1.	Konsep Dasar Fungsi Hash	16
2.3.1.	Sifat-Sifat Fungsi Hash	16
2.4.	<i>Digital Signature</i>	17
2.4.1.	Fungsi <i>Digital Signature</i>	17
2.4.2.	Contoh Penerapan Fungsi <i>Digital Signature</i>	18
2.5.	Fungsi Enkripsi Pada Proses Pengiriman Data	21
2.5.1	Contoh Penerapan Enkripsi Pada Proses Pengiriman Data	22
2.6.	Konsep Dasar dan Komponen <i>Email</i>	24
2.7.	SMTP Protokol	26
2.8.	IMAP Protokol	26
 BAB III ANALISA DAN PERANCANGAN		
3.1.	Profil Perusahaan.....	28
3.1.1.	PT. Dimension Data Indonesia.....	28
3.1.2.	Pengakuan Industri Secara Global	29
3.1.3.	Bidang Usaha	30
3.1.4.	Sejarah Perusahaan.....	31
3.2.	Analisa Masalah	31
3.3.	Alternatif Solusi	34
3.4.	Topologi Rancangan Implementasi dan Pengujian.....	34
 BAB IV IMPLEMENTASI DAN PENGUJIAN		
4.1.	Lingkungan Pengujian.....	37
4.2.	Sistem Operasi.....	38
4.3.	Spesifikasi Perangkat Lunak (<i>Software</i>)	38
4.4.	Spesifikasi Perangkat Keras (<i>Hardware</i>).....	39
4.5.	Persiapan Implementasi.....	39
4.6.	Implementasi dan Pengujian Fungsi	62
4.7.	Analisa Hasil Pengujian	64
4.7.1	Tabel Hasil Analisa dan Pengujian	70
 BAB V PENUTUP		
5.1	Kesimpulan.....	71

5.2	Saran	72
DAFTAR PUSTAKA		74



DAFTAR GAMBAR

Gambar 1.1. Kerangka Berfikir.....	6
Gambar 2.1. Hieroglyphics	9
Gambar 2.2. Skema Atbash Enkripsi	10
Gambar 2.3. Spartans Selinder.....	10
Gambar 2.4. Julius Caesar <i>Shifting Alphabet</i>	10
Gambar 2.5. Kunci Simetris.....	11
Gambar 2.6. Tabel Vigenere	12
Gambar 2.7. Kunci Asimetris.....	14
Gambar 2.8. Fungsi Hash.....	16
Gambar 2.9. Proses Pertukaran Kunci Publik.....	19
Gambar 2.10. Proses Digital Signature	21
Gambar 2.11. Proses Pengiriman Data Menggunakan Digital Signature	21
Gambar 2.12. Proses Enkripsi dan Dekripsi	23
Gambar 2.13. Proses Transmisi Data Melalui <i>Email</i>	25
Gambar 3.1. Gartner Magic Quadrant.....	29
Gambar 3.2. Bidang Usaha	30
Gambar 3.3. Terminologi Pengiriman <i>Email</i>	33
Gambar 3.4. Topologi Implementasi	35
Gambar 4.1. Pembuatan Akun <i>Email</i> Baru.....	40
Gambar 4.2. Pengisian Data Pada Akun <i>Email</i> Baru.....	41
Gambar 4.3. Pengisian Nomor Handpone Untuk Pengiriman Kode Verifikasi .	42
Gambar 4.4. Pengisian Kode Verifikasi.....	42
Gambar 4.5. Konfigurasi IMAP Sebagai MDA.....	42
Gambar 4.6. Konfigurasi Account Setup Pada MUA	43
Gambar 4.7. Konfigurasi IMAP Pada MUA.....	44
Gambar 4.8. Pemilihan Menu Thunderbird Add-ons Manager	44
Gambar 4.9. Proses Instalasi Thunderbird Add-ons	45
Gambar 4.10. Pemilihan Sumber Aplikasi Thunderbird Add-ons Manager.....	45
Gambar 4.11. Key Management User A	46

Gambar 4.12. Pembuatan Certificate Key Pair Baru User A.....	46
Gambar 4.13. Pembuatan Certificate Key Pair Baru User A.....	47
Gambar 4.14. Pembuatan Certificate Key Pair Baru User A.....	47
Gambar 4.15. Pembuatan Certificate Key Pair Baru User A.....	48
Gambar 4.16. Penyimpanan Certificate Key Pair Baru User A.....	48
Gambar 4.17. Key Management User B	49
Gambar 4.18. Pembuatan Certificate Key Pair Baru User B	49
Gambar 4.19. Pembuatan Certificate Key Pair Baru User B	50
Gambar 4.20. Pembuatan Certificate Key Pair Baru User B	50
Gambar 4.21. Pembuatan Certificate Key Pair Baru User B	51
Gambar 4.22. Penyimpanan Certificate Key Pair Baru User B	51
Gambar 4.23. Proses Pengiriman Public Key User A.....	52
Gambar 4.24. Proses Pengiriman Public Key User A.....	52
Gambar 4.25. Proses Pengiriman Public Key User B.....	53
Gambar 4.26. Proses Pengiriman Public Key User B.....	53
Gambar 4.27. Proses Penerimaan Public Key User A	54
Gambar 4.28. Proses Penerimaan Public Key User A	54
Gambar 4.29. Proses Penyimpanan Public Key User A	55
Gambar 4.30. Proses Import Public Key User A	55
Gambar 4.31. Proses Import Public Key User A.....	56
Gambar 4.32. Proses Import Public Key User A.....	56
Gambar 4.33. Proses Import Public Key User A.....	57
Gambar 4.34. Proses Penerimaan Public Key User B	57
Gambar 4.35. Proses Penyimpanan Public Key User B.....	58
Gambar 4.36. Proses Penyimpanan Public Key User B.....	58
Gambar 4.37. Proses Import Public Key User B	59
Gambar 4.38. Proses Import Public Key User B	59
Gambar 4.39. Proses Import Public Key User B	60
Gambar 4.40. Proses Import Public Key User B	60
Gambar 4.41. Proses Pengiriman <i>Email</i> Host X Menuju Host B	61
Gambar 4.42. Proses Pengiriman <i>Email</i> Host A Menuju Host C	62
Gambar 4.43. Proses Pengiriman <i>Email</i> Host A Menuju Host C	62

Gambar 4.44. Proses Pengiriman <i>Email</i> Host A Menuju Host B	63
Gambar 4.44. Proses Pengiriman <i>Email</i> Host A Menuju Host B	64
Gambar 4.45. Hasil Penerimaan <i>Email</i> Host X Menuju Host B.....	65
Gambar 4.46. Hasil Penerimaan <i>Email</i> Host X Menuju Host B.....	65
Gambar 4.47. Hasil Penerimaan <i>Email</i> Host A Menuju Host C.....	66
Gambar 4.48. Hasil Penerimaan <i>Email</i> Host A Menuju Host C.....	66
Gambar 4.49. Hasil Penerimaan <i>Email</i> Host A Menuju Host C.....	67
Gambar 4.50. Hasil Penerimaan <i>Email</i> Host.A Menuju Host B.....	68
Gambar 4.51. Proses Verifikasi <i>Email</i> Host.A Menuju Host B.....	68
Gambar 4.52. Data/Informasi <i>Email</i> Host.A Menuju Host B.....	69



DAFTAR TABEL

Tabel 2.1. Perbandingan Metode Enkripsi	15
Tabel 2.2. Ukuran Nilai Hash	15
Tabel 4.3. Tabel Hasil Analisa Dan Pengujian	70

