ANALISA PENGGUNAAN DIGITAL SIGNATURE DALAM MENINGKATKAN AUTENTIKASI DAN INTEGRITAS DOKUMEN PADA PT XYZ

MAHAYUDA

41509010013

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2013

ANALISA PENGGUNAAN DIGITAL SIGNATURE DALAM MENINGKATKAN AUTENTIKASI DAN INTEGRITAS DOKUMEN PADA PT XYZ

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

MAHAYUDA

41509010013

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2013

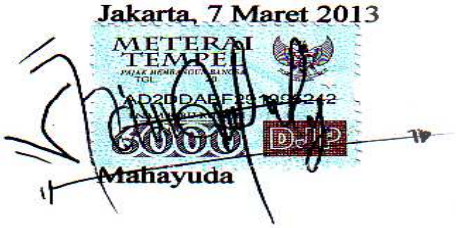
LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM	:	41509010013
Nama	:	Mahayuda
Judul Skripsi	:	Analisa Penggunaan *Digital Signature* Dalam Meningkatkan Autentikasi Dan Integritas Dokumen Pada PT XYZ

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

Jakarta, 7 Maret 2013



Mahayuda

LEMBAR PENGESAHAN

Yang bertanda tangan dibawah ini menyatakan bahwa Laporan Tugas Akhir ini dari mahasiswa berikut ini

Nama	:	Mahayuda
NIM	:	41509010013
Jurusan	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul Skripsi	:	Analisa Penggunaan *Digital Signature* Dalam Meningkatkan Autentikasi Dan Integritas Dokumen Pada PT XYZ.

Skripsi ini telah diperiksa dan disetujui.

Jakarta, Maret 2013

Ida Nurhaida, S.T., M.T.
Pembimbing Tugas Akhir

Sabar Rudiarto, S.Kom., M.Kom.
Koord. Tugas Akhir Teknik Informatika

Tri Daryanto, S.Kom., M.T.
Kaprodi Teknik Informatika

KATA PENGANTAR

Puji syukur alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

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

1. Ibu Ida Nurhaida, S.T., M.T. selaku Pembimbing Tugas Akhir pada jurusan Teknik Informatika Universitas Mercu Buana.
2. Bapak Tri Daryanto, S.kom., M.T. selaku Kepala Program Studi pada Jurusan Teknik Informatika Universitas Mercu Buana.
3. Bapak Sabar Rudiarto, M.kom. selaku Koordinator Tugas Akhir pada Jurusan Teknik Informatika Universitas Mercu Buana.
4. Untuk seluruh dosen dan staff jurusan Teknik Informatika
5. Bapak Andi selaku General Manager PT Hyundai Mobil
6. Bapak Teddy selaku Network Manager & Hardware Indonesia yang telah memberikan ide maupun pendapat.
7. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
8. Saudara dan sahabat-sahabat yang telah memberikan dukungan moral untuk terus menyelesaikan tugas akhir ini.
9. Teman-teman dari Forum JRC Teknik Informatika khususnya untuk Rachman Hakim, Ihsan Firdaus, Reeval Suheri, Agus Sarjuni, yang telah memberikan dukungan moral untuk terus menyelesaikan tugas akhir ini.

Akhir kata saya mengucapkan banyak terima kasih, karena tanpa kalian Tugas Akhir ini tidak dapat diselesaikan dengan baik. Semoga semua yang telah membantu mendapat balasan dari Allah SWT (amien).

Wassalamu ‘alaikum

Jakarta, Maret 2013

Mahayuda

DAFTAR ISI

Halaman

JUDUL i

LEMBAR PERNYATAAN ii

LEMBAR PERSETUJUAN iii

KATA PENGANTAR iv

ABSTRACT vi

ABSTRAK vii

DAFTAR ISI viii

DAFTAR GAMBAR xii

DAFTAR TABEL xiv

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Perumusan Masalah 2

1.3 Batasan Masalah 2

1.4 Tujuan dan Manfaat 2

1.5 Metode Penelitian 3

1.6 Sistematika Penulisan Laporan 4

BAB II LANDASAN TEORI

2.1 Kriptografi dan Sistem Informasi 6

2.2 Mekanisme Kriptografi 7

2.3 Kriptografi Simetris dan Asimetris 9

2.3.1 Kriptografi Simetris 9

2.3.2 Kriptografi Asimetris 11

2.3.3 Kriptografi Gabungan 12

2.4 Keamanan Sistem Kriptografi 13
2.5 DES (Data Encryption Standard) 13
2.5.1 Permutasi Awal 16
2.5.2 Pembangkitan Kunci Internal 17
2.5.3 Enciphering 21
2.5.4 Permutasi Terakhir 25
2.5.5 Dekripsi 26
2.6 Fungsi Hash 27
2.6.1 Fungsi Hash Satu Arah 28
2.7 Digital Signature 30
2.7.1 Otentikasi 32
2.7.2 Integritas 32
2.7.3 Non-repudiation 33
2.8 System Development Life Cycle (SDLC Model Waterfall) 33
BAB III ANALISA DAN PERANCANGAN
3.1 Profil Perusahaan 36
3.1.1 Visi dan Misi PT XYZ 37
3.1.2 Kebijakan Perusahaan 37
3.1.3 Jenis Produk yang Dihasilkan 38
3.2 Manajemen dan Struktur Organisasi 39
3.2.1 Profil IT PT XYZ 40
3.3 Analisa Sistem yang Sedang Berjalan 41
3.4 Analisa Solusi 43
3.5 Metode Analisa 46
3.6 Analisa Cara Kerja Sistem 47
3.7 Metode Perancangan 48

3.8 Hasil Perancangan 48
3.9 Perancangan Sistem 49
3.10 Diagram Use Case 49
3.11 Diagram Aktivitas 50
3.12 Diagram Sekuensial 52
3.13 Perancangan Program 53
3.13.1 Perancangan Form 53
3.13.2 Perancangan Struktur Program 56
3.13.3 Perancangan Flowchart 57
BAB IV IMPLEMENTASI DAN PENGUJIAN
4.1 Spesifikasi Kebutuhan Sistem 61
4.1.1 Perangkat Keras (Hardware) 61
4.1.2 Perngkat Lunak (Software) 61
4.2 Implementasi 61
4.3 Pengujian 65
4.3.1 Skenario Pengujian 65
4.3.2 Hasil Pengujian 68
4.3.3 Analisa Hasil Pengujian 70
BAB V KESIMPULAN DAN SARAN
5.1 Kesimpulan 72
5.2 Saran 73
DAFTAR PUSTAKA 74

DAFTAR GAMBAR

Halaman

1. Gambar 2.1 Mekanisme kriptografi 8
2. Gambar 2.2 Kriptografi berbasis kunci 9
3. Gambar 2.3 Mekanisme kriptografi simetris 10
4. Gambar 2.4 Mekanisme kriptografi asimetris 11
5. Gambar 2.5 Skema global algoritma DES 14
6. Gambar 2.6 Jaringan feitsel untuk satu putaran DES 15
7. Gambar 2.7 Algoritma Enkripsi DES 16
8. Gambar 2.8 Proses pembangkitan kunci-kunci internal DES 21
9. Gambar 2.9 Diagram komputasi fungsi *f* 22
10. Gambar 2.10 Skema perolehan R_i 25
11. Gambar 2.11 Contoh hashing beberapa buah pesan dengan panjang berbeda 28
12. Gambar 2.12 Skema fungsi hash satu arah 29
13. Gambar 2.13 Konsep digital signature 33
14. Gambar 2.14 Gambar diagram waterfall model 34
15. Gambar 3.1 Struktur organisasi PT XYZ 40
16. Gambar 3.2 Topologi yang sedang berjalan pada PT XYZ 43
17. Gambar 3.3 Diagram aliran data untuk sistem yang diusulkan pada jaringan lokal 44
18. Gambar 3.4 Diagram aliran data untuk sistem yang diusulkan pada jaringan global 45
19. Gambar 3.5 Analisa cara kerja sistem 47
20. Gambar 3.6 Diagram use case pada sisi pengirim 49
21. Gambar 3.7 Diagram use case pada sisi penerima 50
22. Gambar 3.8 Diagram aktivitas pada sisi pengirim 51
23. Gambar 3.9 Diagram aktivitas pada sisi penerima 51

24. Gambar 3.10 Diagram sekuensial untuk use case pada sisi pengirim 52
25. Gambar 3.11 Diagram sekuensial untuk use case pada sisi penerima 53
26. Gambar 3.12 Perancangan form menu Panduan 53
27. Gambar 3.13 Perancangan form menu Hash Function 54
28. Gambar 3.14 Perancangan form menu Digital Signature 55
29. Gambar 3.15 Perancangan form menu Validasi 55
30. Gambar 3.16 Struktur program aplikasi 56
31. Gambar 3.17 Struktur menu Hash Function 56
32. Gambar 3.18 Struktur menu Digital Signature 57
33. Gambar 3.19 Struktur menu Validasi 57
34. Gambar 3.20 Flowchart pada sisi pengirim 57
35. Gambar 3.21 Flowchart pada sisi penerima 59
36. Gambar 4.1 Tampilan menu hash function 62
37. Gambar 4.2 Tampilan server 1 63
38. Gambar 4.3 Tampilan server 2 63
39. Gambar 4.4 Tampilan pemanggilan program 64
40. Gambar 4.5 Tampilan kalkulator hash 64

DAFTAR TABEL

Halaman

1. Tabel (a) Matriks Masukan 17
2. Tabel (b) Matriks inisial permutasi (IP) 17
3. Tabel (c) Kunci eksternal 64-bit 18
4. Tabel (d) Matriks permutasi kompresi PC-1 18
5. Tabel (e) Jumlah pergeseran-bit pada tiap putaran 19
6. Tabel (f) Matriks permutasi kompresi-2 (PC-2) 19
7. Tabel (g) Matriks permutasi ekspansi 22
8. Tabel (h) P.box 24
9. Tabel (i) Matriks invers inisial permutasi (IP^{-1}) 26
10. Tabel 2.1 Beberapa macam fungsi hash 30
11. Tabel 4.1 Skenario pengujian 66
12. Tabel 4.2 Hasil Pengujian 68