



**IMPLEMENTASI KEAMANAN DATA DENGAN ALGORITME
RIVEST SHAMIR ADLEMAN TERHADAP DATA KEGIATAN
PERUSAHAAN: STUDI KASUS KEMENTERIAN
LINGKUNGAN HIDUP DAN KEHUTANAN**

SKRIPSI

FIRMANSYAH MAULANA

1110511028

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2015**



**IMPLEMENTASI KEAMANAN DATA DENGAN ALGORITME
RIVEST SHAMIR ADLEMAN TERHADAP DATA KEGIATAN
PERUSAHAAN: STUDI KASUS KEMENTERIAN
LINGKUNGAN HIDUP DAN KEHUTANAN**

SKRIPSI

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

FIRMANSYAH MAULANA

1110511028

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2015**

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Firmansyah Maulana
NRP : 1110511028
Tanggal : 30 Juli 2015

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 30 Juli 2015
Yang Menyatakan,



(Firmansyah Maulana)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Firmansyah Maulana
NRP : 1110511028
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non Eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Implementasi Keamanan Data Dengan Algoritme Rivest Shamir Adleman Terhadap Data Kegiatan Perusahaan: Studi Kasus Kementerian Lingkungan Hidup Dan Kehutanan

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 30 Juli 2015

Yang menyatakan,



(Firmansyah Maulana)

PENGESAHAN

Skripsi diajukan oleh:

Nama : Firmansyah Maulana
NRP : 1110511028
Program Studi : Teknik Informatika
Judul Skripsi : Implementasi Keamanan Data Dengan Algoritme Rivest Shamir Adleman Terhadap Data Kegiatan Perusahaan: Studi Kasus Kementerian Lingkungan Hidup Dan Kehutanan

Telah berhasil dipertahankan di hadapan Tim Pengaji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Yuni Widiastiwi, S.Kom., M.Si.

Ketua Pengaji

Anita Muliawati, S.Kom., M.T.I.

Pengaji I



Dr. Nidjo Sandjojo, M.Sc.

Dekan

Bambang Wasuta, S.Kom., M.T.I.

Pengaji II (Pembimbing)

Yuni Widiastiwi, S.Kom., M.Si.

Ka. prodi

Ditetapkan di: Jakarta

Tanggal Ujian: 30 Juli 2015

**IMPLEMENTASI KEAMANAN DATA DENGAN ALGORITME
RIVEST SHAMIR ADLEMAN TERHADAP DATA KEGIATAN
PERUSAHAAN: STUDI KASUS KEMENTERIAN
LINGKUNGAN HIDUP DAN KEHUTANAN**

Firmansyah Maulana

Abstrak

Penelitian ini dilakukan untuk menambahkan keamanan data pada aplikasi yang digunakan perusahaan untuk melaporkan data kegiatannya ke Kementerian Lingkungan Hidup dan Kehutanan (KLHK). Data kegiatan tersebut nantinya diperiksa oleh KLHK melalui bidang Pengelolaan Limbah Bahan Berbahaya dan Beracun (PLB3). Aplikasi yang digunakan perusahaan tersebut adalah aplikasi Pelaporan PLB3, yang mana data yang dihasilkan oleh aplikasi tersebut dapat menimbulkan kerawanan untuk dicuri, disadap, ataupun diubah oleh pihak yang tidak bertanggung jawab atau dilakukan peretasan. Sehingga penelitian ini melakukan pengamanan data dengan algoritme *Rivest Shamir Adleman* (RSA). Hasil pengujian yang telah dilakukan pada penelitian ini bahwa untuk pengecekan data terhadap enkripsi dan dekripsi data kegiatan perusahaan dapat berjalan dengan baik. Kemudian, untuk pengujian terhadap waktu proses pengamanan data menghasilkan waktu yang bervariasi menyesuaikan dengan ukuran datanya. Sehingga dapat disimpulkan bahwa pengamanan data kegiatan perusahaan dengan menggunakan algoritme RSA dapat berhasil dengan melihat ukuran data yang ada, bila semakin besar data untuk melakukan enkripsi dan dekripsi maka dibutuhkan waktu untuk proses yang cukup lama pula.

Kata Kunci: Keamanan Data, RSA, KLHK, PLB3.

THE IMPLEMENTATION OF SECURITY DATA USING ALGORITHM RIVEST SHAMIR ADLEMAN TOWARD COMPANY ACTIVITY DATA: CASE STUDY IN THE MINISTRY OF ENVIRONMENT AND FORESTRY

Firmansyah Maulana

Abstract

The research is purposed to increase data security on the used company application for reporting their activity data to Ministry of Environment and Forestry, *Kementrian Lingkungan Hidup dan Kehutanan* (KLHK). The data will be checked by KLHK through the Management of Hazardous and Toxic Waste, *Pengelolaan Limbah Bahan Berbahaya dan Beracun* (PLB3), in which the result of data that produced by the application will be insecure to be stolen, tapped, or changed by the irresponsible one or hacker. That is why this research used security data with algorithm Rivest Shamir Adleman (RSA). The result from this research; for checking data toward encryption and decryption company activity data, it is running well. Then, for examination towards timing of security data process, the result is own the various timing based on the size of data. Therefore, it can be concluded that security company activity data using Algorithm RSA is success based on the result of size data. If the data is bigger to encrypt and decrypt, it takes quite time.

Keyword: Security Data, RSA, KLHK, PLB3.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT atas segala karunia-Nya sehingga Skripsi ini berhasil diselesaikan. Judul yang dipilih dalam penelitian ini yang dilaksanakan sejak Februari 2015 ini adalah Implementasi Keamanan Data Dengan Algoritme *Rivest Shamir Adleman* Terhadap Data Kegiatan Perusahaan: Studi Kasus Kementerian Lingkungan Hidup Dan Kehutanan. Terima kasih penulis ucapkan kepada Bapak Bambang Warsuta, S.Kom., M.T.I., selaku dosen pembimbing yang telah banyak memberikan saran yang sangat bermanfaat.

Disamping itu, ucapan terima kasih juga disampaikan kepada Ayahanda (Alm.) H. Yosman, ayahanda Linggo Busono, ibunda Elfi Hendriani dan kedua saudari penulis Viona Rosalina, S.Pd., dan Ardyana Amaraluhita serta seluruh keluarga yang tidak henti-hentinya memberikan penulis semangat dan doa. Penulis juga sampaikan terimakasih kepada Bapak Sigit Es Teget, S.E. yang telah membantu dalam penelitian ini dan tidak lupa penulis ucapkan terima kasih kepada teman-teman jurusan Teknik Informatika lokal A, B, C, dan khususnya lokal G angkatan 2010 sampai 2011 dan tim bimbingan Bapak Bambang Warsuta. Kemudian seluruh pihak yang terlibat dalam kelancaran Skripsi ini, yang belum disebutkan penulis ucapkan terima kasih.

Penulis menyadari bahwa masih banyak kekurangan dari Skripsi ini. Oleh karena itu, penulis mengharapkan saran dan kritik yang bersifat konstruktif dari semua pihak. Semoga Skripsi ini dapat memberikan kontribusi positif serta bermanfaat. Aamiin.

Jakarta, 30 Juli 2015

Firmansyah Maulana

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI	iii
PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN.....	xii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Ruang Lingkup Penelitian	2
I.4 Tujuan Penelitian	3
I.5 Manfaat Penelitian	3
I.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
II.1 Keamanan Data	5
II.2 Kriptografi	6
II.3 Algoritme Kunci Publik	8
II.4 <i>Unified Modeling Language (UML)</i>	23
II.5 Penelitian Terkait	24
BAB III METODOLOGI PENELITIAN	27
III.1 Tahapan Penelitian	27
III.2 Teknik Pengumpulan Data	28
III.3 Lokasi dan Waktu	29
III.4 Alat Bantu Penelitian	29
BAB IV HASIL DAN PEMBAHASAN	31
IV.1 Analisis Kebutuhan	31
IV.2 Analisis Algoritme RSA	32
IV.3 Perancangan Sistem	37
IV.4 Pembuatan Sistem	54
IV.5 Pengujian Sistem	62
BAB V PENUTUP	65
V.1 Kesimpulan	65
V.2 Saran	66

DAFTAR PUSTAKA	67
RIWAYAT HIDUP	
LAMPIRAN	

DAFTAR TABEL

Tabel 1 Hasil Perbandingan Algoritme	19
Tabel 2 Penelitian Terkait	24
Tabel 3 <i>Method Extended Euclidean</i>	36
Tabel 4 Hasil Pengujian Aplikasi	64

DAFTAR GAMBAR

Gambar 1 Algoritme Kunci Publik Untuk Kerahasiaan	10
Gambar 2 Algoritme Kunci Publik Untuk Otentikasi	10
Gambar 3 Algoritme Kunci Publik Untuk Kerahasiaan dan Otentikasi	11
Gambar 4 Tahapan Penelitian	27
Gambar 5 Secara Umum Penggunaan Algoritme RSA	33
Gambar 6 Pembangkitan Kunci Algoritme RSA	34
Gambar 7 Enkripsi Algoritme RSA	35
Gambar 8 Dekripsi Algoritme RSA	35
Gambar 9 Interaksi Aplikasi Secara Umum Kondisi Saat Ini	37
Gambar 10 Pengembangan Interaksi Aplikasi Secara Umum	38
Gambar 11 Manajemen Kunci Aplikasi Portal PLB3	39
Gambar 12 Manajemen Kunci Aplikasi Pelaporan PLB3	40
Gambar 13 Distribusi Kunci	41
Gambar 14 Proses Enkripsi	42
Gambar 15 Proses Dekripsi	43
Gambar 16 <i>Use Case Diagram</i> Aplikasi Pelaporan PLB3	44
Gambar 17 <i>Use Case Diagram</i> Aplikasi Portal PLB3	45
Gambar 18 <i>State Chart Diagram</i> Aplikasi Pelaporan PLB3	46
Gambar 19 <i>State Chart Diagram</i> Aplikasi Portal PLB3	46
Gambar 20 <i>Class Diagram</i> Aplikasi Pelaporan PLB3	47
Gambar 21 <i>Class Diagram</i> Aplikasi Portal PLB3	48
Gambar 22 <i>Activity Diagram</i> Aplikasi Pelaporan PLB3	49
Gambar 23 <i>Activity Diagram</i> Aplikasi Portal PLB3	50
Gambar 24 <i>Sequence Diagram</i> Aplikasi Pelaporan PLB3	51
Gambar 25 <i>Sequence Diagram</i> Aplikasi Portal PLB3	52
Gambar 26 Manajemen Kunci Aplikasi Portal PLB3	53
Gambar 27 Manajemen Kunci Aplikasi Pelaporan PLB3	53
Gambar 28 Formulir Ubah Kunci Publik	54
Gambar 29 Koding Mendapatkan Nilai p, q, n dan $\phi(n)$	55
Gambar 30 Koding Mendapatkan Nilai e	56
Gambar 31 Koding Mendapatkan Nilai d	57
Gambar 32 Koding Enkripsi	58
Gambar 33 Koding Dekripsi	59
Gambar 34 Manajemen Kunci Aplikasi Portal PLB3	60
Gambar 35 Manajemen Kunci Aplikasi Pelaporan PLB3	61
Gambar 36 Ubah Kunci Aplikasi Pelaporan PLB3	62
Gambar 37 Hasil Enkripsi Data Kegiatan Perusahaan	63
Gambar 38 Hasil Dekripsi Data Kegiatan Perusahaan	63

DAFTAR LAMPIRAN

Lampiran 1 Hasil Wawancara

Lampiran 2 Peraturan Pemerintah dan Undang-undang

Lampiran 3 Hasil Wawancara