IMPLEMENTASI DIGITAL *SIGNATURE* PADA *APPROVAL* DOKUMEN PDF DENGAN METODE RSA

PROPOSAL TUGAS AKHIR

Oleh:

Ahmad Daud Laia

4311701037

Disusun untuk pengajuan proposal Tugas Akhir Program Diploma IV

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

BATAM

2020

HALAMAN PENGESAHAN PROPOSAL

IMPLEMENTASI DIGITAL *SIGNATURE* PADA APPROVAL DOKUMEN PDF DENGAN METODE RSA

Oleh:

AHMAD DAUD LAIA 4311701037

Proposal ini telah dikonsultasikan dengan dosen pembimbing
sebagai persyaratan untuk melaksanakan sidang proposal
di

PROGRAM DIPLOMA IV
PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA
POLITEKNIK NEGERI BATAM

Batam, November 2020
Disetujui oleh:
Pembimbing I,

Supardianto, S.ST., M.Eng.

Digitally signed by Supardianto, S.ST., M.Eng.
DN: cn=Supardianto, S.ST., M.Eng. gn=Supardianto, S.ST., M.Eng. c=Indonesia l=ID ou=113105
Reason: I am the author of this document
Location:
Date: 2020-11-13 10:09+07:00

Supardianto, S.ST., M. Eng.

NIK. 113105

1. Latar Belakang

Tanda tangan dijadikan untuk identifikasi asli atau tidak nya sebuah dokumen yang sudah di tanda tangani. Selain itu, digunakan menjadi sebuah bukti orang yang menandatangani mengetahui dan menyetujui isi dari dokumen yang telah di tanda tangani nya. Tanda tangan digital adalah sebuah teknik dalam kriptografi yang dapat digunakan untuk menandatangani dokumen digital. Teknologi Informasi yang begitu berkembang pesat, membuat keamanan data termasuk tanda tangan digital menjadi rawan untuk dimanipulasi oleh orang yang tidak bertanggung jawab. Sama seperti tanda tangan konvensional, tanda tangan digital sebagai bukti keabsahan sebuah dokumen sehingga pembuat dokumen tidak bisa menyangkal bahwa dia yang membuat dokumen tersebut begitu juga sebalik nya.

Pada penelitian kali ini membahas tentang pengamanan dokumen berbasis digital *signature*. Dengan menggunakan metode-metode yang ada pada kriptografi. Penelitian kali ini menggunakan metode RSA. Metode RSA termasuk ke dalam jenis algoritma asimetris. Proses enkripsi dokumen dilakukan pada saat dokumen tersebut dikirim untuk mengamankan file agar tidak dapat terbaca oleh orang yang tidak berhak mengakses file tersebut . RSA yang mempunyai dua kunci yang berbeda, disebut pasangan kunci (key pair) untuk proses enkripsi dan dekripsi. Kunci-kunci yang ada pada pasangan kunci mempunyai hubungan secara matematis, tetapi tidak dapat dilihat secara komputasi untuk mendeduksi kunci yang satu ke pasangannya. Algoritma ini disebut kunci publik, karena kunci enkripsi tidak bersifat rahasia. Orang-orang dapat menggunakan kunci publik ini, tapi hanya orang yang mempunyai kunci privat sajalah yang bisa mendekripsi data tersebut

Pengujian pada pengamanan dokumen yang berformat menggunakan metode RSA. Pengujian sistem dilakukan untuk mengetahui apakah penelitian ini telah memenuhi tujuan untuk mengamankan tanda tangan sebuah dokumen menggunakan metode RSA . Pengujian sistem secara menyeluruh yaitu pengujian implementasi digital signature yang akan digunakan oleh admin/dosen/mahasiswa, dari segi tampilan dan segi proses yang terjadi di setiap halaman dan selanjutnya melakukan proses enkripsi dan dekripsi file dengan menerapkan algoritma

kriptografi RSA. Metode yang digunakan untuk pengumpulan data adalah Kuisioner.

2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka yang menjadi rumusan masalah pada penulisan tugas akhir ini adalah:

1. Cara kerja algoritma kriptografi RSA dalam tanda tangan digital disebuah dokumen atau berkas dengan format PDF
2. Bagaimana merancang dan membangun aplikasi digital *signature* untuk implementasi algoritma kriptografi RSA.
3. Proses penyandian serta implementasi algoritma kriptografi RSA dalam sebuah program komputer yang sederhana.

3. Batasan Masalah

Batasan masalah dalam hasil dalam Penelitian ini adalah:

1. Aplikasi yang dirancang memakai bahasa pemrograman PHP.
2. Data yang dikelola adalah format PDF.

4. Tujuan

Adapun tujuan pada tugas akhir ini adalah.

1. Merancang dan membangun aplikasi digital *signature*.
2. Mengaplikasikan algoritma kriptografi RSA.

5. Manfaat

Manfaat dari penelitian ini adalah sebagai berikut :

1. Tanda tangan yang tersimpan didalam dokumen format PDF lebih aman dengan adanya algoritma kriptografi RSA.
2. Mencegah terjadinya pemalsuan berkas atau dokumen.
3. Mengamankan duplikasi tanda tangan digital.

6. Landasan Teori

6.1 Algoritma Kriptografi

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

a) Enkripsi, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut Plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enskripsi bisa diartikan dengan Cipher atau kode

b) Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (tesk-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma untuk enkripsi.

c) Kunci, yang dimaksud adalah kunci yang dipakai untu melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

6.2 Kriptografi

Cryptography berasal dari dua kata Yunani, yaitu *crypto* yang berarti rahasia dan grapho yang berarti menulis. Secara umum *cryptography* dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya disebutenkripsi, dan membentuk suatu bidang keilmuan yang disebut Kriptografi.

6.3 Kriptografi RSA

Sandi RSA merupakan algoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi

dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA masih dipercaya dan digunakan secara luas di internet. (Kriptografi Kunci Publik:Sandi RSA, 2008).

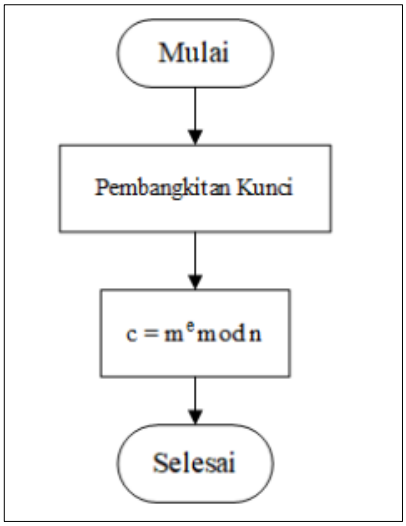
7. Metode Penelitian

7.1 Pengumpulan Data

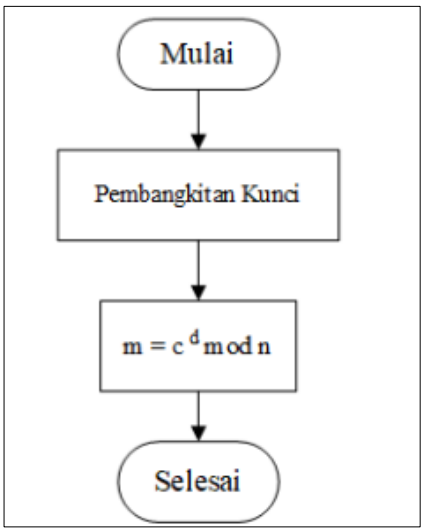
Melakukan pengumpulan data yang berkaitan dengan sumber perancangan system. Pengumpulan data menggunakan kuisioner sebagai metode pengumpulan data.

7.2 Perancangan Perangkat Lunak

Melakukan perancangan kebutuhan perangkat lunak dan tahapan-tahapan proses implementasi algoritma kriptografi RSA pada tanda tangan digital untuk menjalankan proses enkripsi, digunakan kunci public yang telah dibentuk sebelumnya, yaitu kunci publik (n, e). Sedangkan dalam proses dekripsi RSA digunakan kunci rahasia yang sudah ditentukan sejak awal perhitungan. Pasangan kunci rahasia (n, d). Flow chart enkripsi algoritma kriptografi RSA dan flow chart dekripsi algoritma kriptografi RSA dapat dilihat pada gambar dibawah ini.



Flow chart enkripsi algoritma kriptografi RSA.



Flow chart dekripsi algoritma kriptografi RSA.

7.3 Pembuatan Perangkat Lunak

Tahapan yang harus dipersiapkan dalam melakukan pembuatan aplikasi diantaranya : persiapan software yang digunakan, membuat desain interface, dan fungsi menu aplikasi.

Berikut ini adalah desain fungsi dari aplikasi yang akan dirancang :

1. Halaman Login

   Digunakan untuk masuk ke aplikasi dengan memasukkan username dan password yang sesuai pada form. Halaman ini juga agar mencegah pengguna untuk menyalahgunakan aplikasi.
2. Halaman Enkripsi

   Halaman enkripsi bertujuan untuk melakukan pembentukan kunci dan proses enkripsi menggunakan algoritma kriptografi RSA sekaligus pembuatan tanda tangan digital yang diterapkan pada dokumen berformat PDF.
3. Halaman Dekripsi

   Halaman dekripsi bertujuan untuk melakukan proses dekripsi pada ciphertext sekaligus proses verifikasi tanda tangan digital pada sebuah dokumen text apakah dokumen tersebut masih asli atau telah dimodifikasi.

4. Halaman Kunci

   Halaman kunci bertujuan untuk menyimpan nilai n, kunci e dan kunci d, yang telah digunakan pada saat proses enkripsi. Pada halaman ini, admin dapat melakukan pengiriman file dokumen beserta kunci kepada penerima dokumen,

7.4 Pengujian Perangkat Lunak

Pada tahap ini dilakukan pengujian perangkat lunak secara menyeluruh untuk memastikan fungsi menu aplikasi ini berjalan dengan baik sesuai yang diharapkan dengan memastikan tidak ada *bug* ataupun *logic error* pada aplikasi tanda tangan digital. Kemudian algortima RSA diuji melalui pembangkitan kunci publik dan kunci privat ini bertujuan agar nilai $p \neq q$ karena apabila nilai $p = q$, maka $n=p2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n. Selanjutnya pengujian proses enkripsi, dekripsi dan proses verifikasi pada tahap terakhir.

8. Rencana Pelaksanaan

No	Kegiatan	2020												
		November				December				Januari				
		I	II	III	IV	I	II	III	IV	I	II	III	IV	V
1	Pengajuan Judul													
2	Pengumpulan Data													
3	Pembuatan Proposal													
4	Sidang Proposal													
5	Perancangan													
6	Revisi Proposal													

7	Sidang TA1													
8	Perancangan Produk dan Tugas Akhir													
9	Evaluasi dan Revisi													
10	Sidang TA 2													

9. Daftar Pustaka

A. Yudo Husodo, "Penerapan Metode Digital Signature dalam Legalisasi Ijazah dan Transkrip Nilai Mahasiswa," Bandung, 2010.

Z. Arifin, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," Inform. Mulawarman, vol. 4, no. 3, hal. 7–14, 2009.

R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtainingdigital signatures and public-key cryptosystems", Communications ofthe ACM, vol. 21, pp. 120-126, 1978

C. Romine, "Digital Signature Standard (DSS)", Federal InformationProcessing Standards Publication, Information Technology LaboratoryNational Institute of Standards and Technology, Jul. 2013.

Pahrizal, Pahrizal & Pratama, David. (2016). IMPLEMENTASI ALGORITMA RSA UNTUK PENGAMANAN DATA BERBENTUK TEKS. Pseudocode. 3.44-49. 10.33369/pseudocode.3.1.44-49.

Munir, Rinaldi. (2005). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak.

Basri. 2016. Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi, Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, Universitas Al Asyairah Mandar, Sulawesi Barat.

Ginting, A., Isnanto, R.R., & Windasari, I.P. 2015. Implementasi Algoritma Kriptografi RSAUntuk Enkripsi dan Dekripsi Email, Jurnal Program Studi Sistem Komputer, Universitas Diponegoro, Semarang.