PERANCANGAN SISTEM PENGESAHAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITME RSA

Hardiansyah [1], Ichsan Ramdhani [2], Mukhamad Khotib Arifai [3]
Program Studi Teknik Informatika, Universitas Pamulang
Jl. Raya Puspitek Serpong No. 10, Tangerang Selatan
E-mail : hardi113@gmail.com, dosen02110@unpam.ac.id, dosen01995@unpam.ac.id

ABSTRAK--- Penggunaan aplikasi wordprosesor dalam membuat suatu surat-menyurat pada masa ini sudah sangat terbiasa digunakan oleh masyarakat baik secara individu maupun kelembagaan. Dari surat resmi yang dicetak maupun berupa digital dokumen surat selalu memberikan pengesahaan biasa berupa tanda tangan dan pembubuhan stempel, dan biasanya surat resmi terdapat suatu format atau template dalam pembuatannya. Apabila kita membuat aplikasi wordprosesor agar bisa ditinjau oleh beberapa orang diperlukan pengiriman dokumen tersebut secara daring, hal tersebut tidak efisien, atau menggunakan wordprosesor berbasis web yang tidak dapat dikontrol secara ketat pada penggunaannya. Hal tersebut menimbukan kebocoran informasi yang dapat merugikan perusahaan baik secara sadar maupun tidak sadar. Pada era pandemi covid-19 perusahan-perusahan sudah terbiasa dalam menggunakan dokumen surat-menyurat dalam bentuk digital. Namun pengesahannya biasanya hanya meletakan gambar tanda-tangan maupun stempel. Hal tersebut menimbulkan kerawanan untuk dipalsukan, karena penggunaan gambar digital sangat rentan untuk dipalsukan. Tujuan dari penelitian ini adalah (1) untuk membuat suatu aplikasi yang dapat dengan mudah digunakan untuk membuat surat resmi agar bisa di akses dan di koreksi secara bersama-sama, (2) pembubuhan pengesahan secara bertingkat dan aman dengan algoritma RSA, dan (3) pengarsipan surat secara digital dalam memudahkan pencarian. Metode pengembangan perangkat lunak yang digunakan dalam penelitian ini adalah waterfall. Walaupun memang termasuk pengembangan clasic, namun menekankan fase-fase yang berurutan dan sistematis. Secara teoritis hasil penelitian ini akan menambah khasanah ilmu pengetahuan khususnya dalam bidang pengembangan perangkat lunak

Kata Kunci : RSA, waterfall, surat, Sistem Informasi Manajeman.

1. PENDAHULUAN

Penggunaan Aplikasi wordprosesor dalam membuat suatu surat-menyurat pada masa ini sudah sangat terbiasa digunakan oleh masyarakat baik secara individu maupun kelembagaan. Dari surat resmi yang dicetak maupun berupa digital dokumen surat selalu memberikan pengesahaan biasa berupa tanda tangan dan pembubuhan stempel, dan biasanya surat resmi terdapat suatu format atau template dalam pembuatannya. Pada era pandemi covid-19 perusahan-perusahan sudah terbiasa dalam menggunakan dokumen surat-menyurat dalam bentuk digital. Namun pengesahannya biasanya hanya meletakan gambar tanda-tangan maupun stempel. Hal tersebut menimbulkan kerawanan untuk dipalsukan, karena penggunaan gambar digital sangat rentan untuk dipalsukan.

Pengamanan data tidak hanya sebatas data tersebut tidak dapat dibaca orang lain, tetapi juga bagaimana agar data tersebut tidak dapat diubah dan dapat dipastikan dikirim oleh orang yang benar. Selama berabad-abad lamanya tanda tangan telah digunakan untuk membuktikan keabsahan dokumen. Oleh karena itu, data yang dikirim perlu diberi suatu tanda bahwa data tersebut sah. Dari pemikiran tersebut, munculah ide untuk membuat tandatangan digital. Salah satu cara untuk membuat sidik tandatangan adalah dengan menggunakan fungsi algoritma RSA.

Salah satu media komunikasi di dalam website adalah form, dimana form ini digunakan oleh user untuk berinteraksi dengan server. Pada zaman teknologi informasi sekarang ini, dapat dipublikasikan melalui internet dengan media website. Hal tersebut dapat mempermudah dalam hal kolaborasi dalam pembuatan surat dan memudahkan format yang seragam dalam pembuatan surat.

Pengarsipan sangat diperlukan dalam surat-menyurat. Pengarsipan adalah sebuah proses dan cara dimana informasi dalam bentuk dokumen disimpan dengan aman dalam jangka waktu tertentu yang ditentukan oleh hukum. Dokumen dapat diarsipkan dalam berbagai format dan di berbagai perangkat. Meskipun suatu dokumen berstatus tidak aktif, namun dokumen itu dapat diaktifkan kembali. Database menempati posisi penting dalam masyarakat berbasis informasi dan pengetahuan. Dapat dikatakan bahwa database

merupakan pokok penunjang perkembangan teknologi informasi, serta merupakan kerangka utama beroperasinya sistem berbasis komputer.

Setiap aplikasi pada Sistem Informasi Manajeman memerlukan media dokumentasi tercetak baik yang menggunakan kertas (paper) maupun tidak menggunakan kertas (paperless) atau biasa juga dikenal dengan istilah e-paper. Penggunaan e-paper atau lembaran/dokumen digital yang digunakan untuk setiap lembar naskah yang dicetak dari SIM baik oleh staf administrasi maupun pihak lainnya rentan terhadap pemalsuan dan pembajakan oleh pihak-pihak yang tidak bertanggungjawab.

Berbagai pengamanan terhadap berkas elektronik (e-paper) telah banyak dilakukan, seperti pengamanan berkas dengan watermarking (Chao-Yong Hsu: 2005). Pengamanan lain pada berkas elektronik seperti dengan memberikan tanda tangan elektronik atau digital signature untuk e-voting (ÃLukasz Nitschke: 2008). Pengamanan secara konvensional seperti yang dilakukan dengan melegalisasi setiap lembaran yang telah dicetak dan ditanda tangani oleh pejabat yang berwenang serta distempel. Beberapa jenis pengamanan ini masih rentan terhadap pemalsuan dan kurang efektif dengan jenis aplikasi SIM yang banyak diimplementasikan di berbagai Perusahaan.

Pengamanan surat tidak hanya sebatas surat tersebut tidak dapat dibaca orang lain, tetapi juga bagaimana agar surat tersebut tidak dapat diubah dan dapat dipastikan dikirim oleh orang yang benar. Selama berabad-abad lamanya tanda tangan telah digunakan untuk membuktikan keabsahan dokumen. Oleh karena itu, surat yang dikirim perlu diberi suatu tanda bahwa surat tersebut sah. Dari pemikiran tersebut, munculah ide untuk membuat sidik dijital (digital signature). Menurut Munir (2004), sidik dijital bukanlah tanda tangan yang didijitasi dengan alat scanner, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen).

Sidik dijital dapat dibuat dengan mengubah data menjadi message digest oleh fungsi hash tertentu. Kemudian dari message digest tersebut dibuat sidik dijital dengan algoritma kriptografi. Pada tahun 1991, Ronald Rivest memperkenalkan fungsi hash MD5 (Message Digest Algorithm 5). MD5 adalah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standar internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file. Sebelumnya, pada tahun 1977 Rivest bersama Shamir dan Adleman membuat sebuah algoritma untuk teori penomoran pada sebuah public-key cryptosystem, algoritma ini dikenal dengan RSA cryptosystem. Algoritma RSA (Rivest Shamir Adleman) menggunakan kunci asimetris yang menggunakan dua kunci dalam proses enkripsi dekripsi, sehingga mempunyai tingkat keamanan lebih tinggi dibandingkan algortima yang menggunakan kunci simetris. Menurut Munir (2004) untuk membuat sidik dijital, algoritma yang cocok digunakan hanyalah algoritma kunci publik. Dengan fungsi hash MD5 dan algoritma RSA, diharapkan dapat menghasilkan sidik dijital yang mampu menjamin keabsahan surat.Banyaknya jenis surat dan laporan yang dibuat seperti surat tugas, surat tagihan ataupun laporan pertanggung jawaban oleh karyawan perusahaan yang bersifat antar departeman atau bersifat internal maupun surat yang bersifat external menjadikan surat-surat resmi tidak terarsipkan dengan baik, dikarenakan dibuat dan disimpan pada perangkat kerja karyawan masing-masing. Apabila membutuhkan suatu persetujuan biasanya surat-surat tersebut dikirimkan dengan media online yang menyebabkan redudancy pada berkas dan akan sulit melacak versi dari surat-surat tersebut. Apabila pembuatan surat-surat dapat dibuat menggunakan satu aplikasi yang dapat digunakan secara bersama-sama, maka pelacakan kerasipan untuk menverifikasi kebenaran isi surat lebih mudah.

2. TINJAUAN PUSTAKA

Menurut Deddy Ackbar Rianto, Dkk (2015 : 296) “Perancangan dapat diartikan perencanaan dari pembuatan suatu sistem yang menyangkut berbagai komponen sehingga akan menghasilkan sistem yang sesuai dengan hasil dari tahap analisa sistem”.

Menurut Berto Nadeak, Dkk (2016 : 54) mendefinisikan :

“Perancangan adalah langkah pertama dalam fase pengembangan rekayasa produk atau sistem. Perancangan itu adalah proses penerapan berbagai teknik dan prinsip yang bertujuan untuk mendefinisikan sebuah peralatan, satu proses atau satu sistem secara detail yang membolehkan dilakukan realisasi fisik”.

Menurut Adi Nugroho (2016: 77), adalah “strategi untuk memecahkan masalah dan mengembangkan solusi terbaik permasalahan itu. Perancangan juga dapat diartikan sebagai suatu kegiatan didalam menciptakan suatu kondisi baru solusi yang didasari atas evaluasi dari konspesi yang serasi serta bentuk permasalahan atau kasus yang ada”.

Perancangan suatu sistem merupakan suatu proses atau tahap implementasi pengembangan suatu aplikasi atau perangkat lunak berupa proses pengubahan spesifikasi sistem menjadi sistem yang dapat dijalankan.Perancangan aplikasi merupakan deksripsi struktur aplikasi yang di implementasikan, data yang merupakan bagian sistem dan kadang-kadang algoritma yang digunakan.

Algoritma kriptografi asimetrik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (public key algorithm) karena kunci untuk enkripsi dibuat umum (public key) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (private key). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA.

RSA merupakan singkatan dari penemunya yakni Rivest, Shamir dan Adlemen.(Dony Ariyus:2008). Algorima RSA melibatkan seleksi digit angka prima dan mengalikan secara bersama-sama untuk mendapatkan jumlah , yaitu n. Angka-angka ini dilewati algoritma matematis untuk menentukan kunci publik KU ={e,n} dan kunci pribadi KR={d,n} yang secara matematis berhubungan ini merupakan hal yang sulit untuk menentukan e dan d diberi n. (Harun Mukhtar, 2018). Surat merupakan salah satu bentuk alat komunikasi berupa komunikasi tertulis untuk menyampaikan pesan dari seseorang atau lembaga kepada orang lain atau lembaga lain (Sri Dinanta dan Bambang Nur: 2019). Tanda tangan digital (Digital Signature) adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas. Yang dimaksud dengan tanda tangan digital menurut Rinaldi Munir (2005) “bukanlah tanda tangan yang di-digitalisasi dengan alat scanner, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan”.

3. METODE PENELITIAN

Pada penelitian ini peneliti akan membangun suatu sistem pengamanan dokumen elektronik pada Sistem Informasi Akademik (SIA) menggunakan digital signature dengan algoritma kurva eliptik yang terdiri dari modifikasi perangkat lunak yang telah ada dan membuat baru perangkat lunak pembaca keabsahan tanda tangan Algoritma kurva eliptik yang digunakan merupakan algoritma pengembangan dari algoritma tanda tangan digital sebelumnya, seperti RSA, DSA. Digunakannya algoritma kurva eliptik pada penelitian tesis ini dikarenakan tingkat kesulitan yang tinggi untuk lebar bit yang rendah. Seperti yang telah di bahas pada bab 2 bahwa algoritma kurva eliptik hanya membutuhkan 160 bit untuk tingkat keamanan yang sama pada algoritma RSA yang membutuhkan panjang bit sebesar 1024 (perbandingan di http://www.rsa.com/rsalabs/node.asp?id=2013).

Proses pembuatan tanda tangan, enkripsi, hingga pengujian keabsahan tanda tangan dengan algoritma kurva eliptik menurut aturan standar (certicom, 2000) dalam aturan pada prosedur algoritma kurva elipstik dari proses pembentukan tanda tangan dan pengujian keabsahan tanda tangan berikut:

Prosedur penentuan kunci.Setiap pengguna SIA pada saat melakukan transaksi (mencetak dokumen SIA) akanmenghasilkan public key dan private key yang akan digunakan juga pada proses pembacaankeabsahan tanda tangan. Langkah-langkah proses pembuatan kedua kunci ini adalah:

Menentukan sebuah bilangan bulat random dA, yang nilainya diantara [1,n-1]

Menghitung QA = dA* G □ G[(x1, y1)] dengan y2 = x3 + ax + b (mod p).

Kunci rahasia = dA , dan kunci publik = QA

Prosedur pembangkitan tanda tangan (Signing):

Langkah-langkah yang dilakukan pada proses signing atau pembentukan tanda tangan adalah sebagai berikut:

Memilih sebuah bilangan bulat random k, yang nilainya diantara [1, n-1]

Menghitung QA = k * G = (x1,y1) dan r = x1 mod n, jika r = 0 maka kembali ke langkah 1

Menghitung k-1 mod n

Menghitung e = HASH(m)

Menghitung s = k-1 {e+dA * r} mod n

Tanda tangan untuk massage m adalah (r, s)

Prosedur verifikasi keabsahan tanda tangan (Verifing)

Setelah tanda tangan dihasilkan (proses signing), Algoritma selanjutnya yang diperlukan adalah pengujian keabsahan tanda tangan (verifying). Algoritma verifying adalah sebagai berikut:

Memverifikasi bahwa r dan s adalah bilangan bulat antara [1, n-1]

Menghitung e = HASH(m)

Menghitung w = s-1 mod n

Menghitung u1 = ew mod n dan u2 = rw mod n

Menghitung u1 * G + u2 * QA = (x1, y1)

Menghitung v = x1 mod n Jika v = r, maka tanda tangan adalah sah

4. HASIL DAN PEMBAHASAN

Hasil penelitian berupa pengimplementasian dari desain yang telah dibuat pada bagian sebelumnya. Hasil pengimplementasian terdiri dari implementasi interface yang merupakan hasil dari rancangan antarmuka dan implementasi perangkat lunak yang merupakan hasil dari desain perangkat lunak.

Sedangkan untuk bagian pembahasan akan dibahas mengenai tahap pengujian sistem, hasil pengujian sistem dan analisis hasil pengujian sistem. Pada saat dilakukan enkripsi bersamaan pula dilakukan proses *hashing* pada *file* data tersebut. Proses *hashing* berfungsi sebagai autentikasi terhadap data untuk memastikan data tersebut masih utuh atau tidak. Hasil dari proses enkripsi adalah data yang terenkripsi dan *message digest* dari proses *hashing*.

Gambar 15 *Interface Menu Encryption*

Gambar 16 menunjukkan jendela *menu decryption* yang berfungsi untuk melakukan proses dekripsi. Sebagai masukan pada proses dekripsi adalah *file* data yang terenkripsi dan kunci pribadi. Setelah ditentukan *file* data yang terenkripsi dan kunci pribadi yang diambil dari lokasi penyimpanan, langkah selanjutnya dilakukan proses dekripsi untuk mendekripsi *file* data tersebut sehingga kembali menjadi bentuk yang normal (tidak tersandikan).

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka dapat disimpulkan bahwa:

Sistem dapat melakukan proses enkripsi dan dekripsi pada file dengan baik dan benar dikarenakan dapat memenuhi konsep kriptosistem, sehingga diketahui bahwa metode enkripsi dan dekripsi RSA serta fungsi hash SHA-512 dapat digunakan secara bersamaan;

Semakin panjang kunci yang digunakan maka semakin lama waktu yang dibutuhkan untuk menemukan kunci yang digunakan dalam kriptosistem;

Sistem dapat mengidentifikasi ada tidaknya perubahan file sehingga dapat disimpulkan bahwa sistem dapat menverifikasi keaslian dari file; Pemberian nama kunci yang berbeda untuk kunci publik dan kunci pribadi tidak mempengaruhi ukuran file yang akan dienkripsi maupun didekripsi; Peningkatan ukuran file dipengaruhi oleh nama file, delimiter, nilai hash dan ukuran panjang bytes hasil enkripsi dengan algoritma RSA; dan Waktu yang diperlukan untuk proses dekripsi lebih lama dari waktu untuk proses enkripsi.

5.2 Saran

Saran pengembangan dari penelitian ini adalah: (1) Penelitian yang dilakukan masih bersifat umum sehingga untuk ke depannya, penelitian ini bisa dilanjutkan dan difokuskan ke masalah-masalah yang lebih khusus dengan suatu studi kasus tertentu; (2) Pengembangan yang perlu diperhatikan untuk ke depannya dengan memberikan fungsi untuk mengkompresi ukuran file menjadi lebih kecil sehingga membantu mempercepat proses enkripsi dan dekripsi pada file..

DAFTAR PUSTAKA

[1]. Munir, Rinaldi, 2006, Kriptografi, Bandung: Informatika.

[2]. Saipul, 2010, Implementasi Tanda Tangan Digital Menggunakan Fungsi Hash Algoritma SHA-256 dan RSA dalam Proses Otentikasi Data, Yogyakarta: Universitas Ahmad Dahlan.

[3]. Fernando, Ricky, 2009, Studi dan Implementasi Tanda Tangan Digital dengan Menggunakan Algoritma Elgamal, http://www.informatika.org/~rinaldi/Kriptografi/2008-2009/Makalah2/MakalahIF3058-2009-b014.pdf. Diakses tanggal 1 April 2011.

[4]. Wahyuni, Ana, 2011, Aplikasi Kriptografi Untuk Pengamanan E-Dokumen dengan Metode Hybrid: Biometrik Tandatangan dan DSA (Digital Signature Algorithm), Semarang: Universitas Diponegoro.

[5]. Setiawan, Febrianto, 2007, Penerapan Metode Enkripsi Rijndael, Enkripsi RSA, dan Hash SHA-512 untuk Keamanan Transfer File Elektronik, Surabaya: Universitas Kristen Petra.

[6]. Suprapti, Iswanti, 2003, Studi Sistem Keamanan Data dengan Metode Public Key Cryptography, Bandung: Institut Teknologi Bandung.

[7]. Kurniawan, Yusuf, 2004, Kriptografi: Keamanan Internet dan Jaringan Komunikasi, Bandung: Informatika.

[8]. Burrows, James, 2005, Securer Hash Standard, USA: US National Institute and Technology.

[9]. Piper, Frederick Charles, Sean Murphy, 2002, Cryptography: A Very Short Introduction, New York: Oxford University Press Inc.