PENERAPAN DIGITAL SIGNATURE PADA TRANSKRIP NILAI SEBAGAI OTENTIKASI DATA

Ibnu Berliyanto G.A[1], Amir Hamzah[2], Suwanto Raharjo[2]
[1]Teknik Informatika, FTI, IST AKPRIND, guntur_arya1@yahoo.co.id
[2]Teknik Informatika, FTI, IST AKPRIND, miramzah@yahoo.co.id
[3]Teknik Informatika, FTI, IST AKPRIND, wa2n@akprind.ac.id

ABSTRACT

Along with the rapid development of information technology especially which is related to computers and internet, data security is a complex issue, one of the problem is data manipulation. One way to prevent this is to create a data security system that can prevent data manipulation activities and ensure that the data is authentic. In this case, data security technology using a digital signature is a quite right effort .

The application of digital signature methods on transcripts with a web-based application is one of the solutions in the application of data security systems. The application is built using a digital signature with function of CRC32 hash algorithm that will generate a CRC value based on certain bits within the file, and then combined with a unique value for the variable then integrated with database and included on the transcript as evidence of authentic data.

The results of this application is a security data system which show the transcripts using digital signature, as data authentication attempts. With the digital signature application hopefully can help to reduce any data manipulation activities, especially academic data which is one of the manipulated data is sensitive and too risky to be manipulated.

Keywords : Transcript, digital signatures, hash function, CRC32, authentic.

INTISARI

Seiring dengan pesatnya perkembangan teknologi informasi khususnya yang berkaitan dengan komputer dan internet, keamanan data merupakan salah satu permasalahan yang kompleks, salah satunya adalah manipulasi data. Salah satu cara mencegahnya adalah dengan membuat suatu sistem keamanan data yang bisa mencegah kegiatan manipulasi data dan menjamin bahwa data tersebut otentik. Dalam hal ini, teknologi keamanan data menggunakan metode *digital signature* merupakan upaya yang cukup tepat.

Penerapan metode *digital signature* pada transkrip nilai dengan aplikasi berbasis web merupakan salah satu solusi dalam pengaplikasian sistem keamanan data. Aplikasi ini dibangun menggunakan *digital signature* dengan fungsi *hash* algoritma CRC32 yang akan menghasilkan nilai CRC berdasarkan file dalam hitungan bit tertentu, kemudian dikombinasikan dengan nilai variabel unik untuk selanjutnya diintegrasikan dengan database dan disertakan pada transkrip sebagai bukti data tersebut otentik.

Hasil dari aplikasi ini adalah suatu sistem keamanan data yang menampilkan transkrip dengan *digital* signature, sebagai upaya otentikasi data. Dengan adanya aplikasi *digital signature* ini diharapkan dapat membantu mengurangi adanya kegiatan manipulasi data, khususnya data akademik yang merupakan salah satu data sensitif dan terlalu beresiko untuk dimanipulasi.

Kata kunci : Transkrip, *digital signature*, fungsi hash, CRC32, otentik.

PENDAHULUAN

Pada masa kini, komputer dan internet sudah menjadi kebutuhan utama. Hampir semua orang menggunakan komputer maupun internet dalam kehidupan mereka sehari-hari, baik untuk keperluan pendidikan, bisnis, hiburan, dan lain-lain. Namun, seiring dengan pesatnya perkembangan teknologi informasi khususnya dalam hal yang berkaitan dengan komputer dan internet, masalah keamanan data juga semakin kompleks.

Beberapa masalah keamanan tersebut adalah pencurian serta pemalsuan data dan dokumen cetak maupun digital. Data-data yang terdistribusi dalam internet dan *database*, ataupun yang sudah dicetak dapat dengan mudah dimanipulasi oleh pihak yang tidak bertanggung jawab. Salah satu cara untuk mencegahnya adalah dengan membuat suatu tanda khusus yang memastikan bahwa data tersebut adalah data benar dan otentik serta mempunyai syarat integritas data. Untuk itu dapat digunakan salah satu teknologi keamanan data yang disebut dengan *digital signature*.

Salah satu alasan penerapan *digital signature* pada transkrip nilai mahasiswa adalah dikarenakan semakin pesatnya kecanggihan teknologi pada saat ini yang dapat dengan mudahnya siapapun memanipulasi data dan dokumen dari yang semestinya menjadi tidak valid sebagai cara untuk memperoleh keuntungan pihak tertentu. Dengan maraknya pemalsuan transkrip, manipulasi data nilai akademik, dan lain sebagainya yang terkait dengan bukti akademik yang bisa mengakibatkan kerugian terhadap pihak tertentu, maka penulis semakin terdorong untuk mencoba menciptakan suatu sistem keamanan data khususnya transkrip nilai sebagai upaya untuk mencegah pemalsuan data dan meningkatkan nilai integritas sebuah data.

Berdasarkan latar belakang masalah yang ada, maka didapat rumusan masalah bagaimana merancang suatu aplikasi *digital signature* berbasis web sebagai media otentikasi keaslian data atau dokumen menggunakan fungsi hash. Dimana fungsi hash tersebut akan menghasilkan nilai hash *(hash-value)* atau pesan ringkas *(message digest)* melalui proses hashing dari data atau dokumen. Fungsi *hash* mengkompresi sembarang pesan yang berukuran berapa saja menjadi *message digest* yang ukurannya selalu tetap (dan lebih dari panjang pesan semula) sesuai dengan algoritma yang digunakan. Kemudian nilai hash tersebut dapat digunakan sebagai kode verifikasi yang disertakan pada pesan, dokumen,ataupun arsip salinan guna memastikan keaslian data yang sesuai dengan data yang tersimpan di dalam sebuah *database* terpusat.

TINJAUAN PUSTAKA

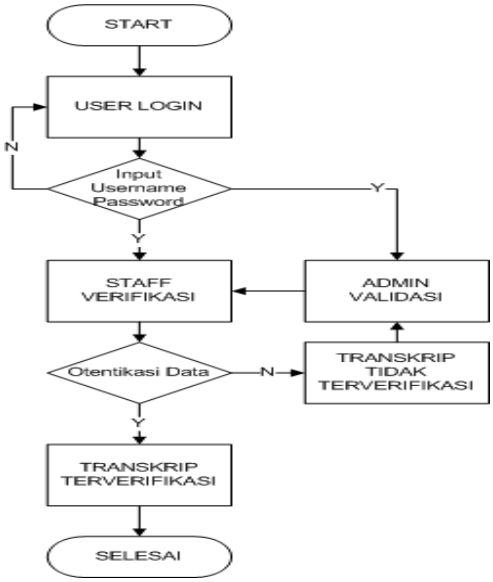
Penelitian yang membahas mengenai sistem informasi layanan administrasi surat pada Fakultas Teknologi Informasi Universitas Kanjuruhan Malang, dimana akan di uji cobakan cara pemberian kode digital pada pesan yang dikirimkan secara elektronik dengan tujuan untuk mengurangi penumpukan berkas yang berlebihan ketika staf memerlukan pengesahan dari dekan (Dwanoko, 2012).

Di dalam skripsi yang membahas tentang sistem keamanan data teks yang sifatnya terbuka dimana isinya dapat dibaca dan diubah dengan mudah. Kebanyakan sistem yang digunakan dalam permasalahan ini adalah dengan mengenkripsi pesan menjadi cipherteks yang tidak dapat dibaca lagi, kemudian memerlukan proses dekripsi agar pesan dapat dibaca kembali. Hal ini dirasa akan mempersulit penerima pesan karena harus mengolahnya terlebih dahulu (Siregar, 2011).

Pada skripsi yang membahas tentang pengembangan perangkat lunak untuk simulasi *Schnorr authentication* dan *digital signature* scheme dan perangkat lunak yang juga dapat digunakan sebagai fasilitas pendukung dalam proses belajar-mengajar mencakup input variabel-variabel, kunci privat, kunci publik, pesan, pembentukan *digital signature*, proses verifikasi dan proses dekripsi (Jusmail, 2011).

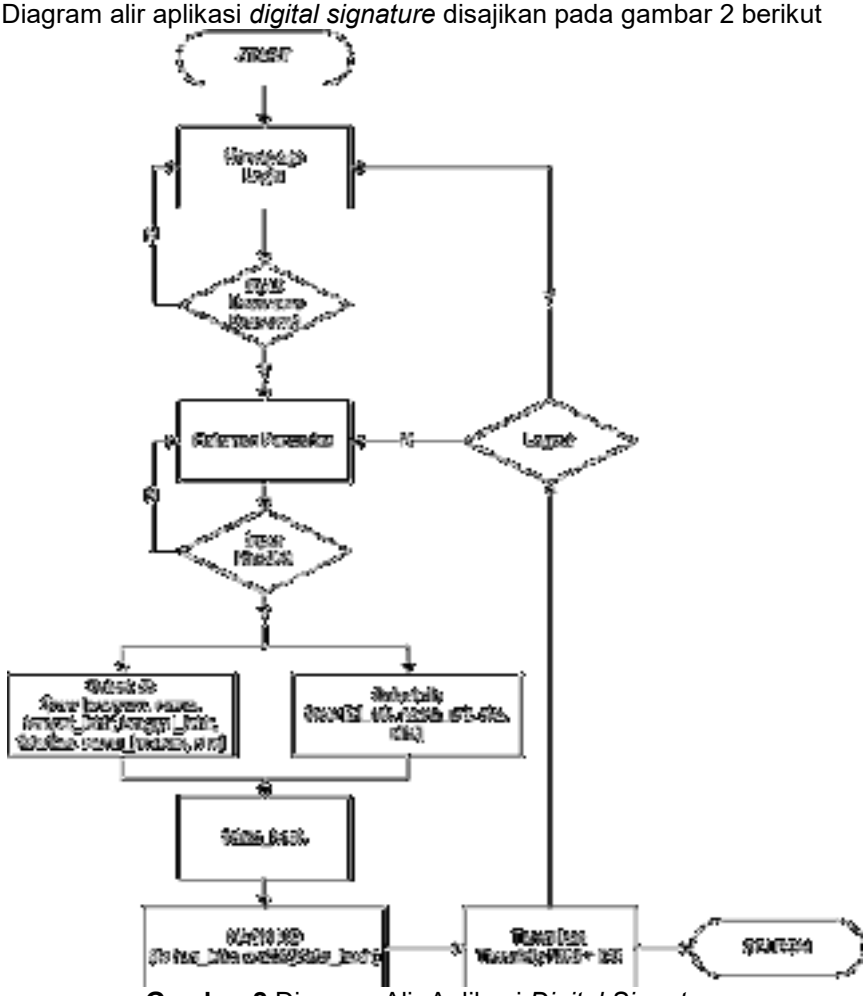
METODOLOGI PENELITIAN

Diagram alir user aplikasi ditampilkan pada gambar 1 berikut :



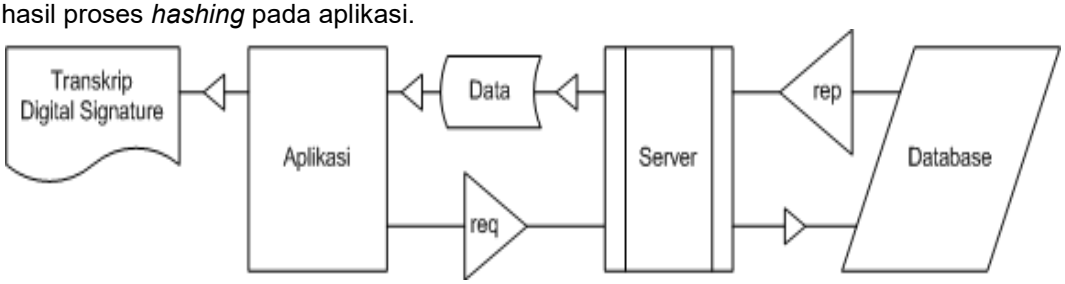
Gambar 1 Diagram Alir User Aplikasi

Diagram alir aplikasi *digital signature* disajikan pada gambar 2 berikut



Gambar 2 Diagram Alir Aplikasi *Digital Signature*

Gambar 3 merupakan proses hashing transkrip nilai pada aplikasi yang akan dirancang. Pada gambar menjelaskan bahwa aplikasi mengirim request data ke server untuk kemudian memanggil data yang dibutuhkan ke database, kemudian data tersebut diproses oleh server. Kemudian server mengirimkan data hasil dari request aplikasi untuk di *hash* pada aplikasi kemudian ditampilkan dalam bentuk transkrip beserta nilai *hash* dari hasil proses *hashing* pada aplikasi.



Gambar 3 Proses *Hashing* pada Aplikasi

PEMBAHASAN

Pemikiran awal pembuatan aplikasi ini yaitu membangun sebuah aplikasi *digital signature* untuk membangkitkan nilai *hash (hash value)* yang akan menjadi kode *digital signature* pada transkrip mahasiswa menggunakan metode *hashing* dengan algoritma CRC32, sehingga pada setiap transkrip tersebut akan memiliki kode yang berbeda-beda yang dihasilkan atas dasar data mahasiswa dan perolehan nilai prestasi akademik masing-masing mahasiswa sebagai upaya untuk menciptakan suatu transkrip yang disertai dengan identitas yang unik dengan tujuan untuk mengamankan data dari upaya pemalsuan maupun manipulasi data transkrip.

Dengan mempertimbangkan tingkat keamanan data agar aplikasi dapat menjadi sebuah sistem yang sesuai tujuannya, aplikasi *digital signature* ini dibuat dengan memperhatikan beberapa skema dari *digital signature* yaitu proses pemberian tanda tangan dengan proses hashing dan proses validasi untuk memastikan *digital signature* benar-benar terintegrasi dengan data transkrip pada database sebagai pendukung integritas data. Sehingga tingkat keamanan data bisa dijamin karena proses pengolahan transkrip *digital signature* harus melalui beberapa prosedur yang ketat.

Validasi hanya dapat diproses dan dilakukan pada level administrator sebagai proses integrasi kode *digital signature* transkrip yang telah dihasilkan dari proses *hashing* dengan database transkrip mahasiswa yang bersangkutan agar dalam proses otentikasi bisa dipastikan bahwa data tersebut otentik. Bukti validasi akan disertakan pada transkrip dari hasil pencarian di halaman pencarian dan ditampilkan pada "*DS Stored"*. Sedangkan level user hanya mempunyai hak akses pada halaman pencarian.

Pada setiap proses pencarian, data transkrip yang akan ditampilkan selalu menyertakan proses *hashing* yang nilainya akan ditampilkan pada "*DS Processed"*, sehingga dapat diketahui apabila transkrip tersebut otentik atau tidak. Dapat dipastikan data otentik apabila nilai *digital signature* pada *DS processed* sama dengan nilai pada *DS Stored*. Tampilan pada proses ini dapat dilihat pada gambar 4

INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA

INSTITUTE OF SCIENCE & TECHNOLOGY AKPRIND YOGYAKARTA

JALAN KALISAHAK 28 KOMPLEK BALAPAN YOGYAKARTA 55222, INDONESIA

P.O. BOX 45, TELP. (0274) 563029, FAX. (0274) 563847

Nama :Anto
Tempat/Tanggal lahir :Solo, 01 Jul 1990
Fakultas :Teknologi Industri
Jurusan :Teknik Informatika
Program :Strata 1
Nomor Mahasiswa :07052811

No	Kode	Mata Kuliah	Kredit	Nilai
1	TIFS1001	Basis Data	3	A
2	TIFS1002	Pemrograman Dasar	3	B
3	TIFS1003	Sistem Informasi	3	B
4	TIFS1004	Logika Informatika	3	B
			12	39

IP Kumulatif : 3.25

DS Stored	:	20130073034379
DS Processed	:	20130073034379

VERIFIED

Gambar 4. Tampilan Transkrip Otentik

Apabila nilai pada *DS Processed* tidak sama dengan nilai pada *DS Stored* atau nilai *DS Stored* tidak ditampilkan, ada kemungkinan manipulasi data atau kemungkinan data belum divalidasi. Maka data transkrip tersebut dinyatakan tidak otentik. Tampilan dapat dilihat seperti pada gambar 5

INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA

INSTITUTE OF SCIENCE & TECHNOLOGY AKPRIND YOGYAKARTA

JALAN KALISAHAK 28 KOMPLEK BALAPAN YOGYAKARTA 55222, INDONESIA

P.O. BOX 45, TELP. (0274) 563029, FAX. (0274) 563847

Nama Andi
Tempat/Tanggal lahir Solo, 01 Jul 1990
Fakultas Teknologi Industri
Jurusan Teknik Informatika
Program Strata 1
Nomor Mahasiswa 07052810

no	Kode	Mata Kuliah	Kredit	Nilai
1	TIFS1002	Pemrograman Dasar	3	B
2	TIFS1003	Sistem Informasi	3	B
3	TIFS1001	Basis Data	3	C
4	TIFS1004	Logika Informatika	3	C
			12	30

IP Kumulatif : 2.50

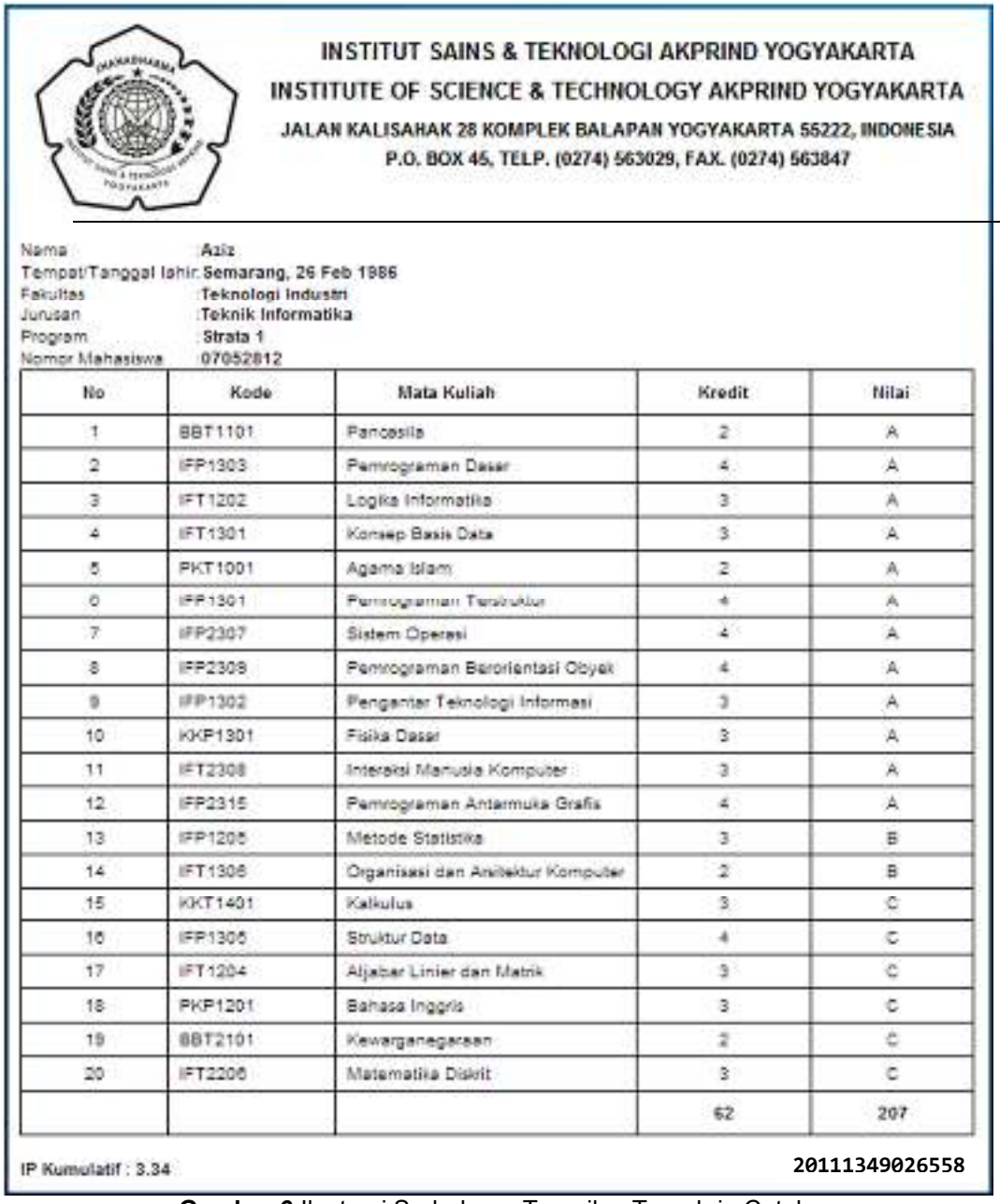
DS Stored	:	
DS Processed	:	20130534424814

NOT VERIFIED! Please contact administrator

Gambar 5 Tampilan Transkrip Tidak Otentik

Dalam aplikasi *digital signature* ini, satu perubahan karakter atau *digit* data saja pada database akan merubah nilai *digital signature*. Maka dari itu dalam aplikasi ini

administrator merupakan faktor utama pendukung keamanan aplikasi *digital signature* ini sehingga harus menjadi perhatian utama dan diperlukan prosedur yang ketat dan terjamin agar aplikasi bisa tetap berfungsi sebagaimana mestinya. Selanjutnya, gambar 6 menampilkan ilustrasi sederhana transkrip cetak dengan *digital signature.*



INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA
INSTITUTE OF SCIENCE & TECHNOLOGY AKPRIND YOGYAKARTA
JALAN KALISAHAK 28 KOMPLEK BALAPAN YOGYAKARTA 55222, INDONESIA
P.O. BOX 45, TELP. (0274) 563029, FAX. (0274) 563847

Nama : Aziz
Tempat/Tanggal lahir : Semarang, 26 Feb 1986
Fakultas : Teknologi Industri
Jurusan : Teknik Informatika
Program : Strata 1
Nomor Mahasiswa : 07052812

No	Kode	Mata Kuliah	Kredit	Nilai
1	BBT1101	Pancasila	2	A
2	IFP1303	Pemrograman Dasar	4	A
3	IFT1202	Logika Informatika	3	A
4	IFT1301	Konsep Basis Data	3	A
5	PKT1001	Agama Islam	2	A
6	IFP1301	Pemrograman Terstruktur	4	A
7	IFP2307	Sistem Operasi	4	A
8	IFP2309	Pemrograman Berorientasi Obyek	4	A
9	IFP1302	Pengantar Teknologi Informasi	3	A
10	KKP1301	Fisika Dasar	3	A
11	IFT2308	Interaksi Manusia Komputer	3	A
12	IFP2315	Pemrograman Antarmuka Grafis	4	A
13	IFP1205	Metode Statistika	3	B
14	IFT1306	Organisasi dan Arsitektur Komputer	2	B
15	KKT1401	Kalkulus	3	C
16	IFP1305	Struktur Data	4	C
17	IFT1204	Aljabar Linier dan Matrik	3	C
18	PKP1201	Bahasa Inggris	3	C
19	BBT2101	Kewarganegaraan	2	C
20	IFT2206	Matematika Diskrit	3	C
			62	207

IP Kumulatif : 3.34 20111349026558

Gambar 6 Ilustrasi Sederhana Tampilan Transkrip Cetak

Dari gambar diatas dapat dilihat di bagian kanan bawah pada gambar bahwa *digital signature* disertakan pada transkrip dan dicetak dengan kode ”20111349026558”.

Uji Coba Program

Sebelum program dapat digunakan maka program harus di uji terlebih dahulu apakah program telah bebas dari kesalahan-kesalahan atau masih ada yang perlu diperbaiki lagi. Program di test terlebih dahulu untuk melakukan pengecekan apakah validasi pada input dan output aplikasi sudah sesuai dengan harapan atau belum.

Pengujian ini dilakukan agar kemungkinan kesalahan yang terjadi dapat diidentifikasi sejak awal. Pengujian ini dilakukan menggunakan komputer dengan sistem operasi windows 7. Pada tabel 1 ditampilkan hasil pengujian perubahan *digital signature*.

Tabel 1 Tabel Perubahan *Digital Signature*

NO.	Data	Digital Signature (DS)	Keterangan
1	Anton	*20111578303266*	DS awal sebelum dilakukan perubahan data
2	Antonius	*20111678800342*	DS setelah dilakukan penambahan huruf (**-ius**) pada nama Anton
3	Anto	*20110073034379*	DS setelah dilakukan pengurangan huruf (**n**) pada nama Anton
4	A → B	*20111051652332*	DS setelah dilakukan penggantian nilai dari **A** menjadi **B** pada satu matakuliah
5	~~A~~ → B & B → A	*20110516112886*	DS setelah dilakukan pertukaran nilai dari dua matakukuliah yang berbeda dimana matakuliah dengan nilai **A** dirubah nilainya menjadi **B**, sedangkan matakuliah dengan nilai **B** dirubah nilainya menjadi **A**.

Dari tabel diatas dapat dijelaskan bahwa sampel data pengujian diambil dari salah satu data mahasiswa bernama Anton. Dapat dilihat bahwa perubahan dengan penambahan, pengurangan, pergantian, dan pemindahan yang terdiri dari satu atau beberapa karakter yang relatif sedikitpun akan menghasilkan perubahan *Digital Signature* yang sangat signifikan.

Evaluasi Sistem

Aplikasi ini masih bersifat simulasi dan belum diterapkan dalam sistem sesungguhnya, sehingga data-data yang ditampilkan seperti nama mahasiswa, nomer induk mahasiswa, nilai mahasiswa, dan data lainnya yang ditampilkan pada aplikasi ini hanya bersifat mewakili. Kelemahan dari sistem ini salah satunya adalah bahwa fungsi utama aplikasi yaitu algoritma fungsi hash CRC32 tidak disusun sendiri atau diciptakan oleh penulis akan tetapi hanya menggunakan pemanggilan fungsi hash CRC32 yang telah disediakan oleh skrip PHP, sehingga penulis tidak membahas mengenai parameter-parameter algoritma.

KESIMPULAN

Hasil dari penelitian pada aplikasi digital signature berbasis web ini dapat disimpulkan antara lain :

1. Digital signature dengan metode hashing bisa menjadi salah satu solusi metode keamanan data karena mempunyai tingkat keakuratan nilai yang cukup tinggi terhadap perubahan suatu data.
2. Aplikasi dari penelitian ini masih bersifat simulasi karena masih menggunakan database lokal dengan data-data yang bersifat mewakili.
3. Dengan aplikasi digital signature ini diharapkan dapat membantu meningkatkan sistem keamanan data dan mempermudah dalam proses otentikasi data.
4. Dari pengujian aplikasi, algoritma CRC32 yang digunakan dalam sistem mempunyai panjang *message digest* 32 bit telah menghasilkan 10 digit kode digital signature dalam bilangan decimal yang berbeda-beda pada setiap data transkrip. Akan tetapi tidak dilakukan perbandingan hasil dengan menggunakan algoritma lain seperti

MD5, SHA1, maupun SHA256 yang masing-masing memiliki panjang *message digest* 128 bit, 160 bit, dan 256 bit yang memungkinkan hasil bilangan *hexadecimal* dengan panjang digit yang berbeda-beda.

DAFTAR PUSTAKA

Andi. (2003). *Memahami Model Enkripsi dan Security Data.* Yogyakarta: Andi Offset.

Dewa. (2012, September 9). *Pengertian Database*. Retrieved Mei 22, 2013, from Sumber Ilmu: http://dewa-sumberilmu.blogspot.com

Dwanoko, Y. S. (2012). *Model Otentifikasi E-Surat Menggunakan Metode Digital Signature Dengan Algoritma MD5.* Malang: Universitas Kanjuruhan.

Hakim, Z. (2013, Februari 12). *Pengertian Digital Signature*. Retrieved Mei 22, 2013, from Zainalhakim: http://www.zainalhakim.web.id

Jusmail. (2011). *Pengembangan Perangkat Lunak Untuk Simulasi Shcnorr Authentication Dan Digital Signature Scheme.* Yogyakarta: UIN Sunan Kalijaga.

Luqman. (2012, Desember 25). *Lukman Hakim*. Retrieved Mei 22, 2013, from Pengertian Hash: http://luqmanh-fst10.web.unair.ac.id

Munir, R. (2006). *Kriptografi.* Bandung: Informatika Bandung.

Pratiwi, S. A. (2010). *Algoritma Perhitungan Langsung pada Cyclic Redundancy Code 32.* Jakarta: Universitas Gunadarma.

Pribadi, N. C. (2011). *Penerapan Digital Signature Pada Dunia Internet.* Bandung: Institut Teknologi Bandung.

Ranuyoga. (2012, September 16). *Pengertian Web Server*. Retrieved Juli 5, 2013, from Open Source: http://ranoeyoga.blogspot.com

Rusli, A. (2010). *Mahir Manipulasi Fungsi String PHP 5.* Jakarta: PT Elex Media Komputindo.

Siregar, N. (2011). *Strategi Otentikasi Pesan Menggunakan Digital Signature dengan Metode DSA (Digital Standard Algorithm).* Medan: Universitas Sumatera Utara.

Syafril. (2010, Juni 11). *Syafril*. Retrieved Mei 22, 2013, from Web Based Applications: http://syafrilchairiansyah1972.wordpress.com