Jurnal CyberTech

Vol.1. No.1, April 2018, pp. 109~119
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Penerapan Kriptografi Berbasis *Digital Signature* Menggunakan Algoritma RSA Pada SPT di Sekretariat Daerah Kota Medan

Dinda Utari[**], Faisal Taufik[**], Rico Imanta Ginting[**]
[*]Program Studi Sistem Informasi, STMIK Triguna Dharma
[**]Program Studi Sistem Komputer Dan Sistem Informasi Dosen Pembimbing, STMIK Triguna Dharma

Article Info

Article history:
Received April 12th, 2018
Revised April 20th, 2018
Accepted April 26th, 2018

Keyword:
Kriptografi
Digital Signature
RSA
SPT

ABSTRACT

Di kantor Sekretariat Daerah Kota Medan terdapat sebuah dokumen instansi berupa surat dinas yang sering disebut dengan Surat Perintah Tugas (SPT). SPT adalah surat resmi yang dibuat dan dikeluarkan oleh seorang pejabat yang berwewenang di instansi atau lembaga tertentu dimana isinya menugaskan seorang pegawai untuk melakukan suatu pekerjaan. Pada SPT biasa dilampirkan stempel dan tanda tangan para pejabat yang berwewenang, namun cara tersebut masih memiliki kekurangan yang harusnya bisa diantisipasi agar tetap terjaga keasliannya, karena stempel dan tanda tangan dapat dengan mudahnya ditiru.

Saat ini penggunaan SPT sudah dalam bentuk file digital, penggunaan file digital rentan dengan adanya perubahan data yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab sehingga memunculkan terbentuknya surat palsu. Oleh karena itu perlu adanya suatu sarana yang dapat memberikan layanan untuk memverifikasi keaslian suatu dokumen dan keutuhan data pada SPT dengan cepat dan mudah. Sistem kriptografi dan digital singnature dapat digunakan untuk memverifikasi keaslian suatu dokumen.

Kriptografi dan digital signature memiliki fasilitas keamanan, yaitu kerahasiaan pesan, kebenaran pengirim, otentitas pesan dan anti penyangkalan. Dengan adanya kedua aspek ini penerima pesan akan percaya bahwa pesan yang dikirim masih otentik dari pengerim aslinya dan dapat membantu staf dan pegawai dalam memverifikasi keaslian pada SPT. Dalam menyelesaikan masalah ini menggunakan algortima RSA (Rivest Shamir Adleman).

First Author
Nama : Dinda Utari
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : miss.dindautari@gmail.com

1. PENDAHULUAN

Teknologi jaringan komputer pada saat ini dapat menghubungkan antara komputer satu dengan komputer lainnya, untuk saling bertukar informasi [1]. Dengan adanya perkembangan teknologi digital hal yang perlu diperhatikan adalah keamanan dan perlindungan data [2]. Dengan segala kecanggihan yang ada terdapat beberapa hal yang jarang diperhatikan oleh pemilik informasi, yaitu keamanan informasi. Dengan adanya keamanan pada informasi pihak yang tidak berkepentingan tidak dapat mengakses informasi tersebut.

Di kantor Sekretariat Daerah Kota Medan terdapat sebuah dokumen instansi berupa surat dinas yang diberikan kepada pegawai untuk melaksanakan suatu tugas beserta fungsinya, yang sering disebut dengan Surat Perintah Tugas (SPT). SPT adalah surat resmi yang dibuat dan dikeluarkan oleh seorang pejabat yang berwewenang di instansi atau lembaga tertentu dimana isinya menugaskan seorang pegawai untuk melakukan suatu pekerjaan.

SPT biasa dilampirkan beserta stempel instansi tersebut dan tanda tangan para petinggi yang berwewenang, cara tersebut masih memiliki kekurangan yang harusnya bisa diantisipasi agar tetap terjaga keaslian isi surat tersebut. Karena stempel dan tanda tangan dapat dengan mudahnya ditiru. Saat ini penggunaan SPT sudah dalam bentuk *file*

digital, penggunaan *file* digital rentan dengan adanya perubahan data yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab sehingga memunculkan kekhawatiran terbentuknya surat palsu.

Oleh karena itu perlu adanya suatu sarana yang dapat memberikan layanan untuk memverifikasi keaslian suatu dokumen dan keutuhan data pada SPT dengan cepat dan mudah [3]. Sistem kriptografi dapat digunakan memverifikasi keaslian suatu dokumen [4]. Kriptografi memiliki fasilitas keamanan yaitu, kerahasiaan pesan, kebenaran pengirim, otentitas pesan dan anti penyangkalan. Untuk memperkuat keaslian dari SPT tersebut, maka dikembangkanlah *digital signature*. *Digital signature* dapat digunakan untuk melakukan suatu pembuktian seacara matematis bahwa pesan tidak mengalami perubahan secara ilegal, sehingga dapat digunakan untuk memverifikasi [5]. Dengan adanya tanda tangan digital penerima pesan akan percaya bahwa pesan yang dikirim masi otentik dari pengirim aslinya. Kedua aspek keamanan informasi diatas merupakan layanan yang disediakan oleh kriptografi. Pada masalah ini algortima yang digunakan adalah algoritma RSA (Rivest Shamir Adleman).

2. KAJIAN PUSTAKA

2.1 Surat Perintah Tugas (SPT)

SPT merupakan dokumen dinas dari atasan yang ditujukan untuk pegawai agar melaksanakan pekerjaan sesuai dengan tugas serta fungsinya. SPT dibuat berdasarkan peraturan daerah. SPT dibuat setelah perjalanan dinas selesai dilaksanakan yang berfungsi sebagai bahan pertanggung jawaban pegawai yang telah melakukan kegiatan pengawasan terhadap instansi pemerintah.

2.2 Kriptografi

Kriptografi berawal dari bahasa Yunani, kripto yang berarti rahasia dan graphia yang berarti catatan atau tulisan. Sedangkan berdasarkan dari istilahnya, kriptografi yakni ilmu dan seni untuk mengamankan pesan pada saat dikirim dari satu tempat ketempat yang lain [6]. Kata "seni" tersebut berawal dari kenyataan sejarah yaitu pada masa-masa awal mula sejarah kriptografi ada setiap orang mungkin mempunyai cara yang berbeda dan unik dalam melindungi pesannya'.

Kriptografi adalah suatu bidang kelimuan atau seni untuk menjaga keamanan sebuah pesan data yang dikirim dari satu tempat ke tempat lain [7].

2.3 *Digital Signature*

Digital Signature merupakan sutau teknologi digital yang dapat disisipkan pada suatu dokumen untuk menjaga otentifikasinya. Cara kerja dan fungsi *digital signature* hampir sama dengan tanda tangan versi nyata, yaitu memberikan kepastian, keaslian dan persetujuan dokumen oleh penanda tangan. Fungsi *digital signature* yaitu untuk melakukan pengesahan terhadap data yang akan dikirim. Fungsi utamanya adalah anti penyangkalan.

Pengertian tanda tangan elektronik berdasarkan pasal 1 ayat (12) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah "Tanda tangan yang terdiri atas informasi elektronik yang dikaitkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

2.4 Algoritma RSA (Rivest Shamir Adleman)

Rivest, Shamir dan Adleman atau disingkat RSA adalah sebuah *public key cipher* yang dibuat oleh tiga orang peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1978. *Cipher* ini memiliki dua kunci, yaitu kunci publik dan kunci privat atau rahasia. Keamanan *cipher* RSA ini terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat *up to date*.

2.4.1 Proses Pembangkit Kunci RSA

Untuk menggunakan RSA terlebih dahulu pendeskripsi membangkitkan sepasang kunci yaitu kunci publik dan kunci privat. Hal pertama yang dilakukan algoritma pembangkit kunci adalah membangkitkan dua bilangan prima. Pembangkitan bilangan prima menggunakan algoritma pengujian bilangan prima misalnya algoritma Miller –Rabin. Untuk lebih jelasnya dalam membangkitkan kunci algoritma RSA dapat dilihat pada penjelasan di bawah ini:

a. Menentukan dua bilangan prima, dengan nama :
   p dan *q*

b. Menhitung nilai modulus (n):
$n = p \times q$

c. Menghitung nilai totient $\phi(n)$:
$\phi(n) = (p\text{-}1) \times (q\text{-}1)$

d. Menghitung nilai e dengan syarat (*greator common divisor*) $gcd(e, \phi(n)) = 1$, dimana e = bilangan prima dan $1 < e < \phi(n)$.

e. Mencari nilai *deciphering exponent* (d):
$d = (1 + (k \times \phi(n)) / e$

2.4.2 Proses Enkripsi

Setelah kunci publik dibangkitkan maka proses selanjutnya yang dilakukan adalah proses enkripsi. Enkripsi adalah sebuah proses mengubah *plaintext* menjadi *ciphertext*. Enkripsi dapat dilakukan dengan rumus $C = P^e \ mod \ n$.

2.4.3 Proses Dekripsi

Jika pendekripsi mendapatkan teks sandi yang dienkripsi dengan kunci publik, maka pendekripsi dapat menggunakan kunci privatnya untuk mengembalikan teks asli. Jadi dekripsi adalah suatu proses pengembalian *ciphertext* ke *plaintext*. Dekripsi dapat dilakukan dengan rumus $P = C^d \ mod \ n$.

3. ANALISA DAN HASIL

3.1 Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah-langkah dalam penyelesaian masalah dalam perancangan sistem kriptogafi berbasis *digital signature* dengan menggunakan algoritma RSA.

3.3.1 Proses Pembangkit Kunci RSA

Pada tahap ini yang pertama dilakukan adalah membangkitkan kunci terlebih dahulu dengan nama p dan q. Beriku ini proses pembangkit kunci dengan algoritma RSA yaitu:

a. Menentukan dua bilangan prima, dengan nama :
$p = 11$
$q = 17$

b. Menhitung nilai modulus (n):
$n = p \times q$
$= 11 \times 17$
$= 187$

c. Menghitung nilai totient $\phi(n)$:
$\phi(n) = (p\text{-}1) \times (q\text{-}1)$
$= (11\text{-}1) \times (17\text{-}1)$
$= 10 \times 16$
$= 160$

d. Menghitung nilai e dengan syarat (*greator common divisor*) $gcd(e, \phi(n)) = 1$, dimana e = bilangan prima dan $1 < e < \phi(n)$.
$gcd(3,160) = 1$

e. Mencari nilai *deciphering exponent* (d):
$d = (1 + (k \times \phi(n)) / e$
$= (1 + (2 \times 160)) / 3$
$= 321 / 3$
$= 107$

3.3.2 Proses Enkripsi

Sebelum *plaintext* dienkripsi, *plaintext* tersebut harus diubah terlebih dahulu ke dalam bentuk kode ASCII (*American Standart Code for Information*) desimal. Yang akan menjadi *plaintext* yaitu (094/1004708-11-2019).

Tabel 3.1 Kode ASCII

Karakter	Hex	Desimal	Karakter	Hex	Desimal	Karakter	Hex	Desimal	Karakter	Hex	Desimal
NUL (null)	0	0	Space	20	32	@	40	64	`	60	96
Start Heading	1	1	!	21	33	A	41	65	a	61	97
Start Text	2	2	"	22	34	B	42	66	b	62	98
End Text	3	3	#	23	35	C	43	67	c	63	99
End Transmit.	4	4	$	24	36	D	44	68	d	64	100
Enquiry	5	5	%	25	37	E	45	69	e	65	101
Acknowlege	6	6	&	26	38	F	46	70	f	66	102
Bell	7	7	`	27	39	G	47	71	g	67	103
Backspace	8	8	(	28	40	H	48	72	h	68	104
Horiz. Tab	9	9	)	29	41	I	49	73	i	69	105
Line Feed	A	10	*	2A	42	J	4A	74	j	6A	106
Vert. Tab	B	11	+	2B	43	K	4B	75	k	6B	107
Form Feed	C	12	,	2C	44	L	4C	76	l	6C	108
Carriage Return	D	13	-	2D	45	M	4D	77	m	6D	109
Shift Out	E	14	.	2E	46	N	4E	78	n	6E	110
Shift In	F	15	/	2F	47	O	4F	79	o	6F	111
Data Link Esc	10	16	0	30	48	P	50	80	p	70	112
Direct Control 1	11	17	1	31	49	Q	51	81	q	71	113
Direct Control 2	12	18	2	32	50	R	52	82	r	72	114
Direct Control 3	13	19	3	33	51	S	53	83	s	73	115
Direct Control 4	14	20	4	34	52	T	54	84	t	74	116
Negative ACK	15	21	5	35	53	U	55	85	u	75	117
Synch Idle	16	22	6	36	54	V	56	86	v	76	118
End Trans Block	17	23	7	37	55	W	57	87	w	77	119
Cancel	18	24	8	38	56	X	58	88	x	78	120
End of Medium	19	25	9	39	57	Y	59	89	y	79	121
Substitue	1A	26	:	3A	58	Z	5A	90	z	7A	122
Escape	1B	27	;	3B	59	[	5B	91	{	7B	123
Form separator	1C	28	<	3C	60	\	5C	92	|	7C	124
Group separator	1D	29	=	3D	61	]	5D	93	}	7D	125
Record Separator	1E	30	>	3E	62	^	5E	94	~	7E	126
Unit Separator	1F	31	?	3F	63	_	5F	95	Delete	7F	127

Tabel 3.2 *Plaintext* Yang Sudah Diubah ke Kode ASCII Desimal

Plaintext	**Kode ASCII**
0	48
9	57
4	52
/	47
1	49
0	48
0	48
4	52
7	55
0	48
8	56
-	45
1	49
1	49
-	45
2	50
0	48
1	49
9	57

Setelah *plaintext* diubah ke kode ASCII desimal selanjutnya proses enkripsi dengan rumus $C = P^e \ mod \ n$ yaitu sebagai berikut:

$C_1 = P^e \ mod \ n$
$= 48^3 \ mod \ 187$
$= 75$

$C_2 = P^e \ mod \ n$
$= 57^3 \ mod \ 187$
$= 63$

$C_3 = P^e \ mod \ n$
$= 52^3 \ mod \ 187$

= 171

C_4 = P^e *mod* n
= 47^3 *mod* 187
= 38

C_5 = P^e *mod* n
= 49^3 *mod* 187
= 26

C_6 = P^e *mod* n
= 48^3 *mod* 187
= 75

C_7 = P^e *mod* n
= 48^3 *mod* 187
= 75

C_8 = P^e *mod* n
= 52^3 *mod* 187
= 171

C_9 = P^e *mod* n
= 55^3 *mod* 187
= 132

C_{10} = P^e *mod* n
= 48^3 *mod* 187
= 75

C_{11} = P^e *mod* n
= 56^3 *mod* 187
= 23

C_{12} = P^e *mod* n
= 45^3 *mod* 187
= 36

C_{13} = P^e *mod* n
= 49^3 *mod* 187
= 26

C_{14} = P^e *mod* n
= 49^3 *mod* 187
= 26

C_{15} = P^e *mod* n
= 45^3 *mod* 187
= 56

C_{16} = P^e *mod* n
= 50^3 *mod* 187
= 84

C_{17} = P^e *mod* n
= 48^3 *mod* 187
= 75

C_{18} = P^e *mod* n
= 49^3 *mod* 187
= 26

C_{19} = P^e *mod* n
= 57^3 *mod* 187
= 63

Setelah *ciphertext* diperoleh langkah selanjutnya merubah *ciphertext* ke bilangan *hexadecimal* yaitu sebagai berikut:

Tabel 3.3 Hasil Enkripsi

Plaintext	***Ciphertext***	***Kode Hexadecimal***
48	75	4b
57	63	3f
52	171	ab
47	38	26
49	26	1a
48	75	4b
48	75	4b
52	171	ab
55	132	84
48	75	4b
56	23	17
45	56	38
49	26	1a
49	26	1a

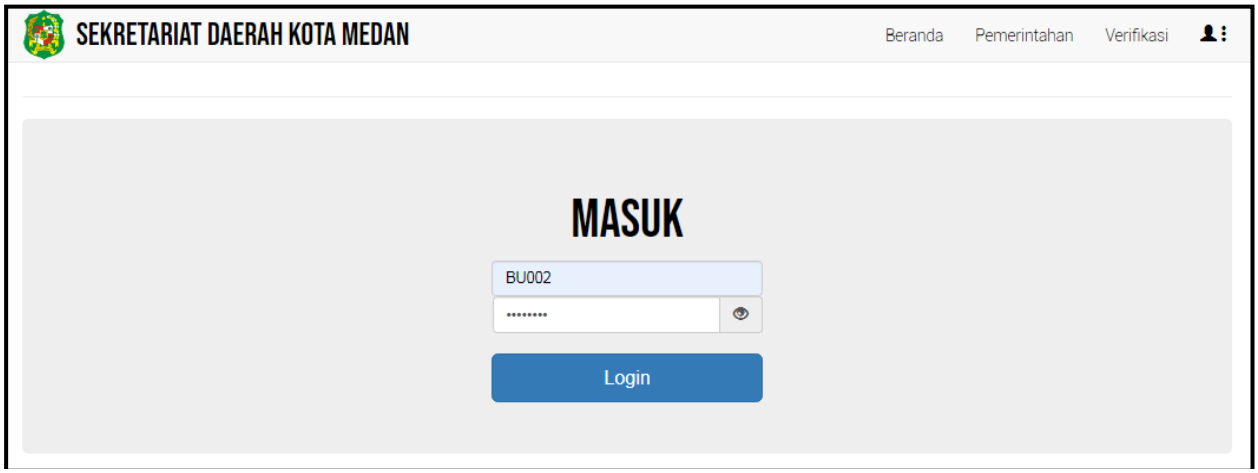
Tabel 3.3 Lanjutan Dari Hasil Enkripsi

Plaintext	***Ciphertext***	***Kode Hexadecimal***
45	56	38
50	84	54
48	75	4b
49	26	1a
57	63	3f

4 PENGUJIAN DAN IMPLEMENTASI

4.1 Tampilan Halaman *Form Login*

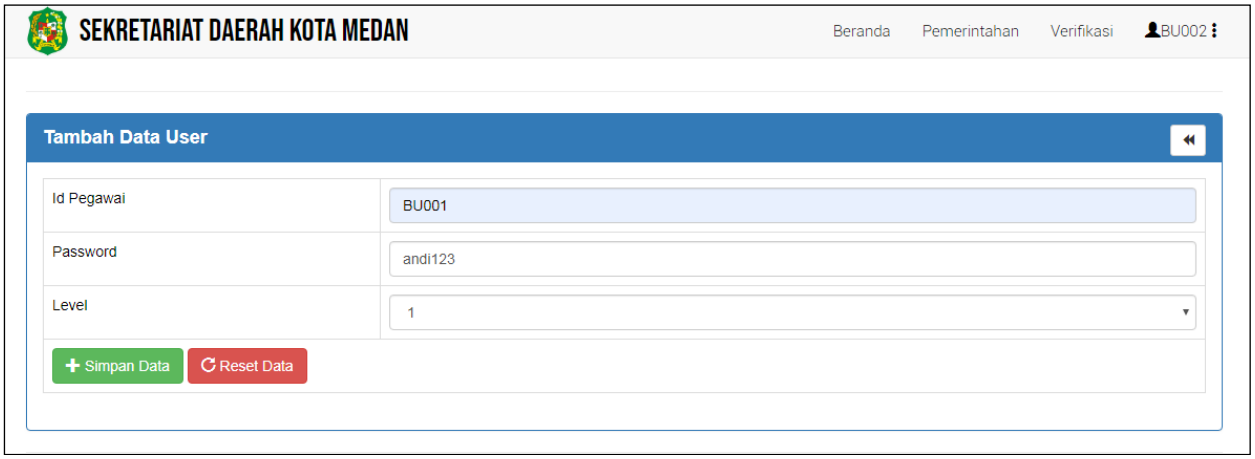
Halaman ini berfungsi sebagai proses masuk bagi setiap pengguna untuk dapat mengakses halaman admin. Berikut ini adalah tampilah halaman *form login* yaitu sebagai berikut:



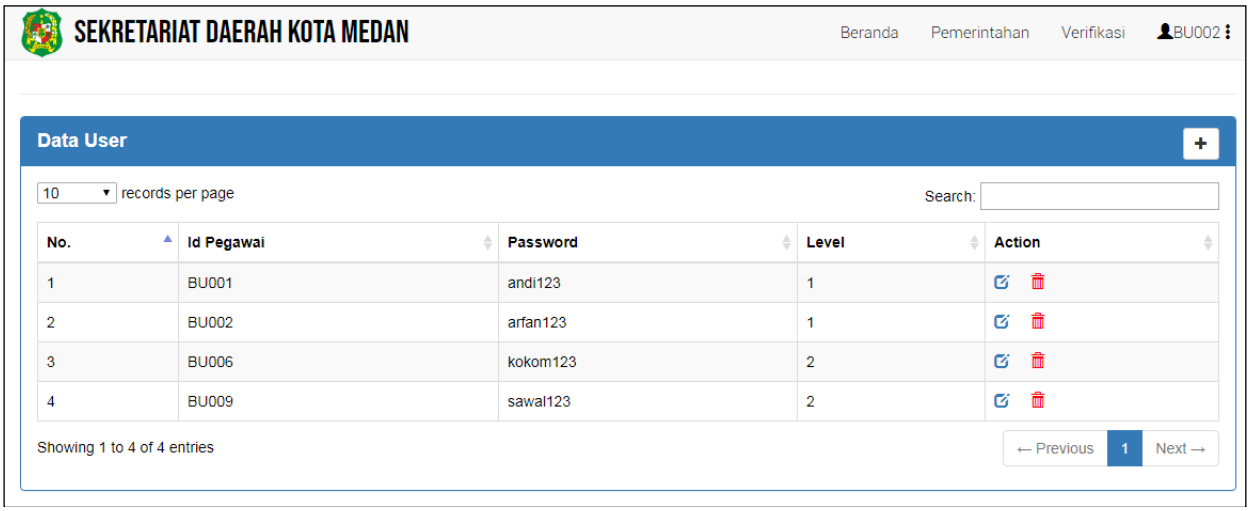
Gambar 4.1 Tampilan Halaman *Form Login*

4.2 Tampilan Halaman *Form User*

Halaman ini berfungsi untuk menambah, mengubah, dan menghapus data pengguna. Berikut ini adalah tampilan dari halaman *form user* yaitu sebagai berikut:



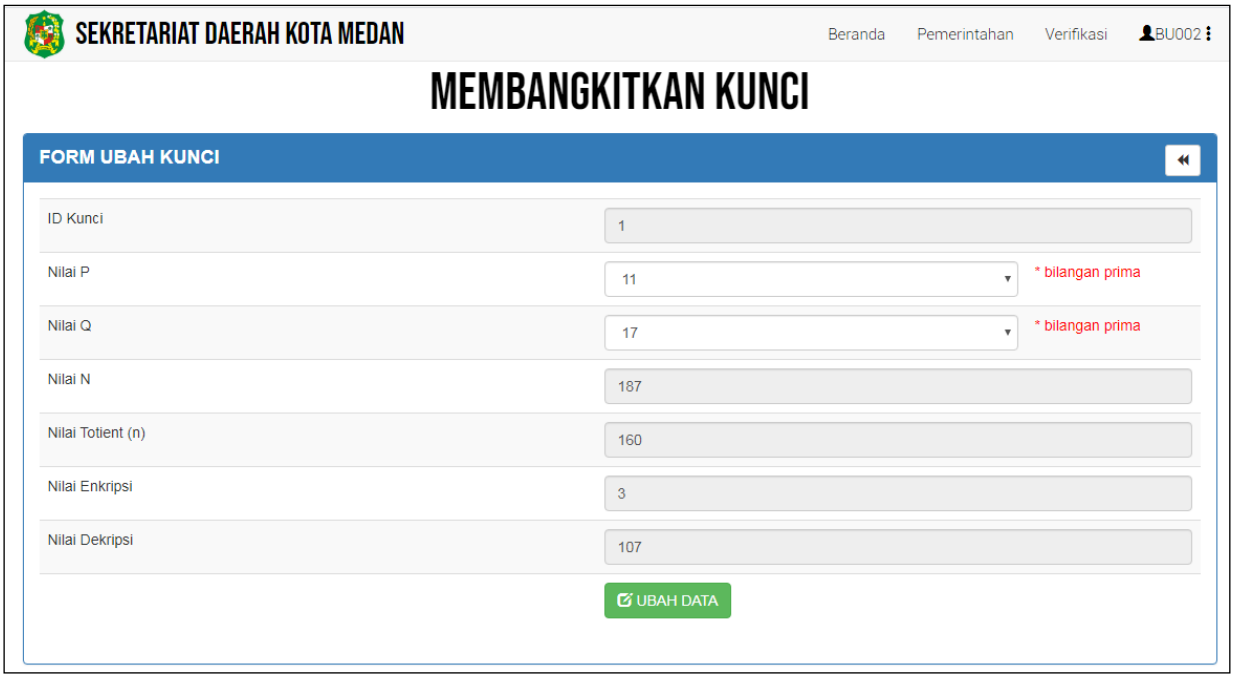
Gambar 4.2 Tampilan Halaman *Form Input* Data *User*



Gambar 4.3 Tampilan Halaman *Form* Daftar Data *User*

4.3 Tampilan Halaman *Form* Pembangkit Kunci

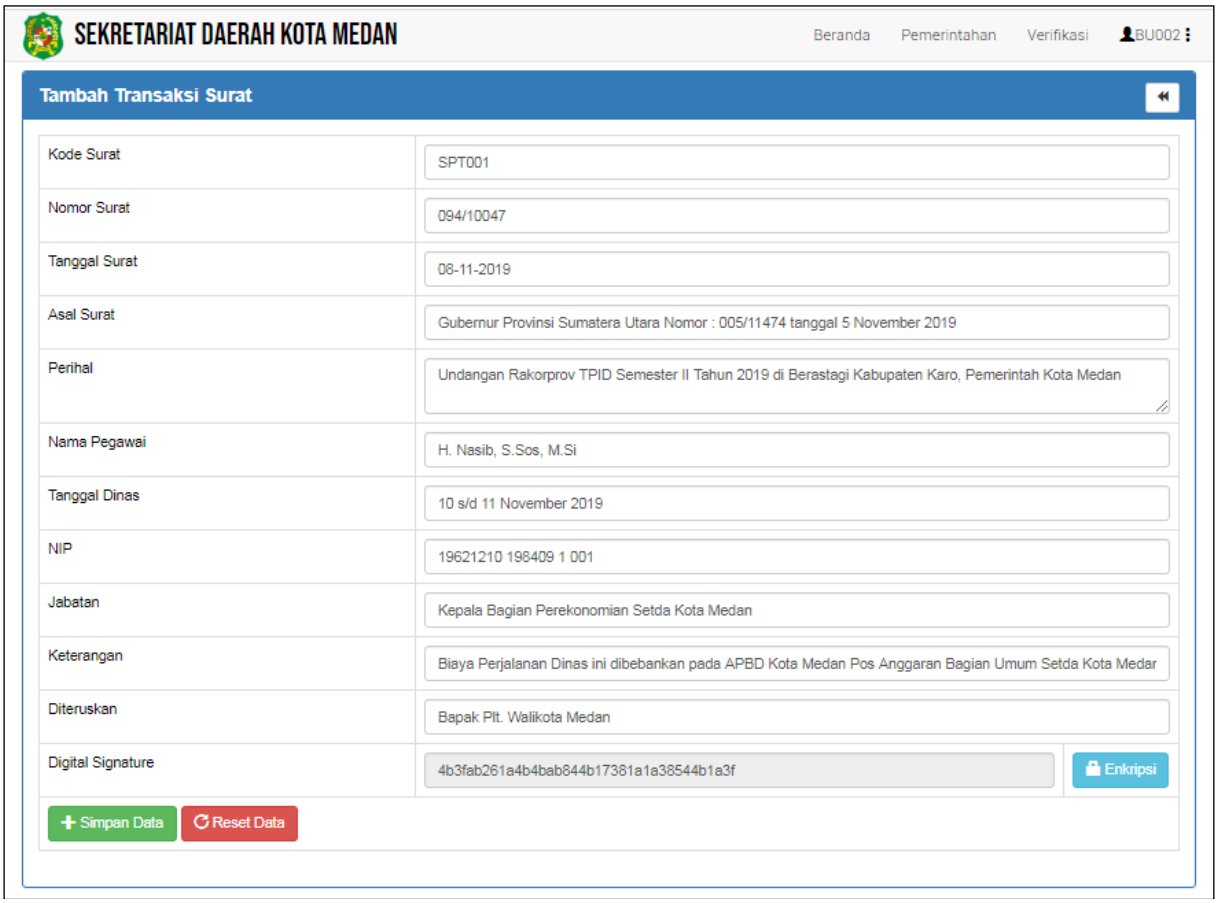
Pada halaman ini terdapat proses untuk membangkitkan kunci. Berikut ini adalah tampilan halaman *form* pembangkit kunci yaitu sebagai berikut:



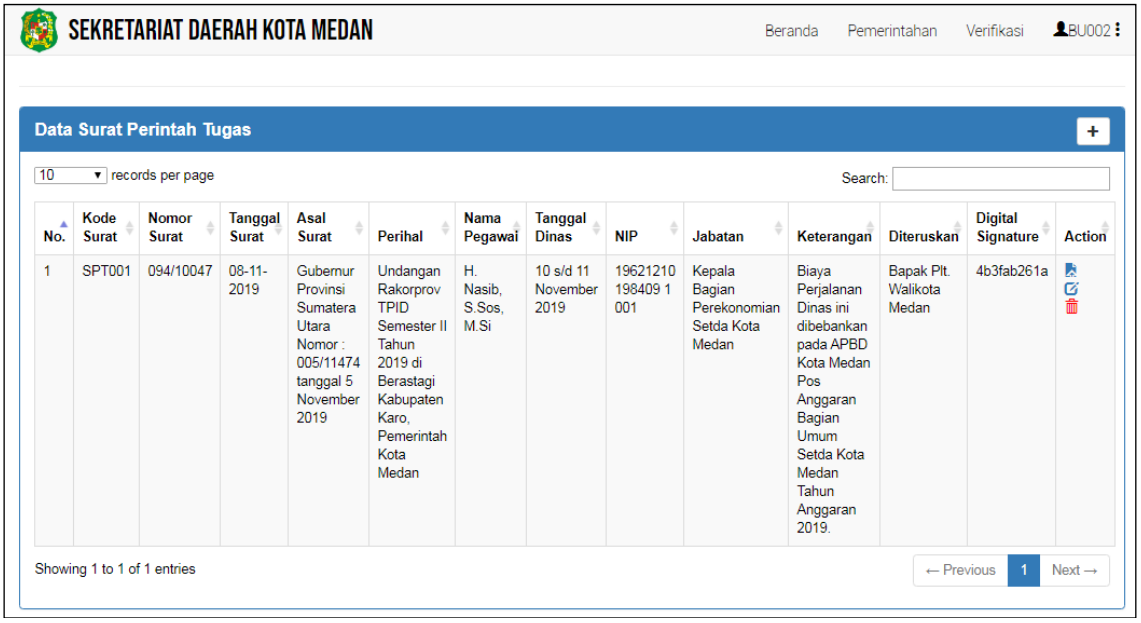
Gambar 4.4 Tampilan Halaman *Form* Pembangkit Kunci

4.4 Tampilan Halaman *Form* SPT dan Enkripsi

Berikut ini adalah tampilan dari halaman *form* SPT dan enkripsi yaitu sebagai berikut:



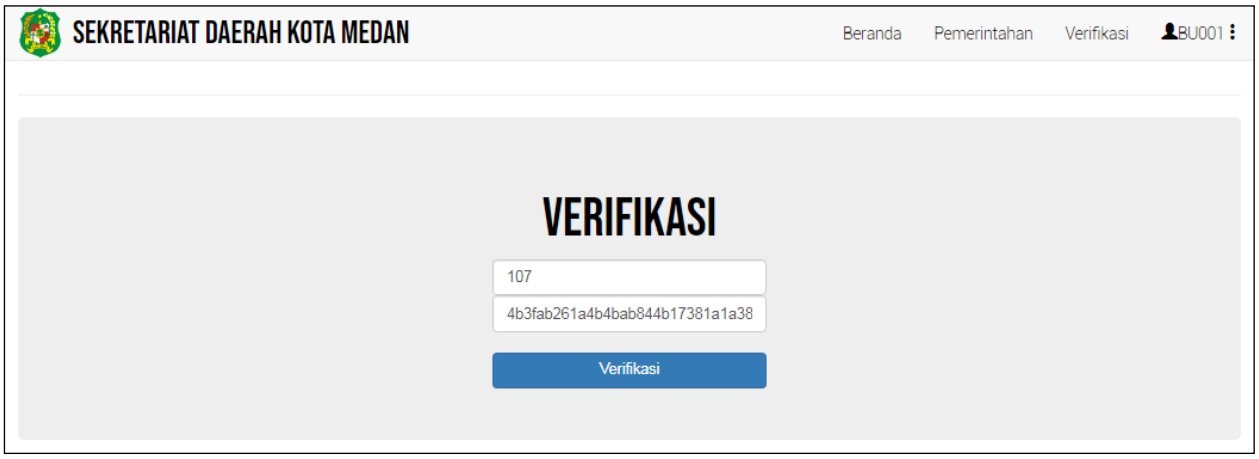
Gambar 4.5 Tampilan Halaman *Form Input* Data SPT



Gambar 4.6 Tampilan Halaman *Form* Daftar Data SPT

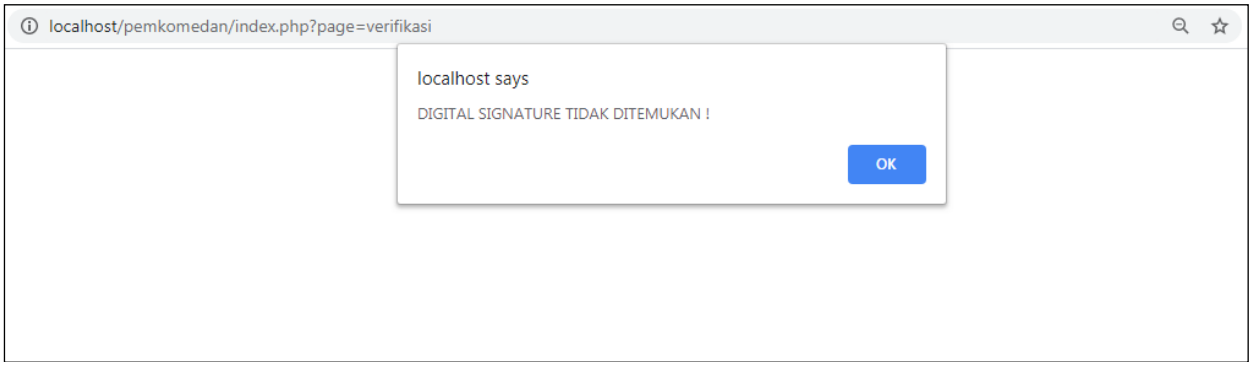
4.5 Tampilan Halaman *Form* Verifikasi

Berikut ini adalah tampilan halaman *form* verifikasi yaitu sebagai berikut:



Gambar 4.7 Tampilan Halaman *Form* Verifikasi

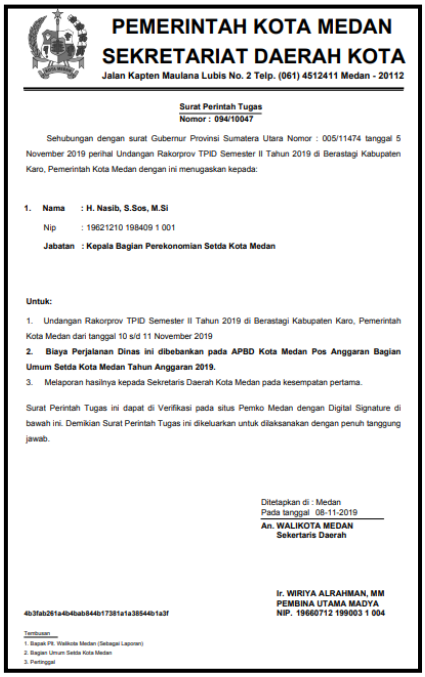
Gambar 4.8 Tampilan Ketika *Digital Signature* Benar



Gambar 4.9 Tampilan Ketika *Digital Signature* Salah

4.6 Tampilan Dokumen SPT

Pada halaman ini terdapat dokumen SPT beserta *digital signature*. Berikut ini adalah tampilan dokumen SPT yaitu sebagai berikut:



PEMERINTAH KOTA MEDAN
SEKRETARIAT DAERAH KOTA
Jalan Kapten Maulana Lubis No. 2 Telp. (061) 4512411 Medan - 20112

Surat Perintah Tugas
Nomor : 094/10047

Sehubungan dengan surat Gubernur Provinsi Sumatera Utara Nomor : 005/11474 tanggal 5 November 2019 perihal Undangan Rakorprov TPID Semester II Tahun 2019 di Berastagi Kabupaten Karo, Pemerintah Kota Medan dengan ini menugaskan kepada:

1. **Nama : H. Nasib, S.Sos, M.Si**
   Nip : 19621210 198409 1 001
   Jabatan : Kepala Bagian Perekonomian Setda Kota Medan

Untuk:

1. Undangan Rakorprov TPID Semester II Tahun 2019 di Berastagi Kabupaten Karo, Pemerintah Kota Medan dari tanggal 10 s/d 11 November 2019
2. **Biaya Perjalanan Dinas ini dibebankan pada APBD Kota Medan Pos Anggaran Bagian Umum Setda Kota Medan Tahun Anggaran 2019.**
3. Melaporan hasilnya kepada Sekretaris Daerah Kota Medan pada kesempatan pertama.

Surat Perintah Tugas ini dapat di Verifikasi pada situs Pemko Medan dengan Digital Signature di bawah ini. Demikian Surat Perintah Tugas ini dikeluarkan untuk dilaksanakan dengan penuh tanggung jawab.

Ditetapkan di : Medan
Pada tanggal 08-11-2019
An. WALIKOTA MEDAN
Sekertaris Daerah

Ir. WIRIYA ALRAHMAN, MM
PEMBINA UTAMA MADYA
NIP. 19660712 199003 1 004

4b3fab261a4b4bab844b17381a1a38544b1a3f

Tembusan
1. Bapak Pit. Walikota Medan (Sebagai Laporan)
2. Bagian Umum Setda Kota Medan
3. Peringgal

Gambar 4.10 Tampilan Dokumen SPT

5. KESIMPULAN

Berdasarakan perumusan dan pembahasan bab-bab sebelumnya dapat diambil beberapa kesimpulan dan beberapa saran.

1. Dalam mengatasi masalah yang terjadi pada kantor Sekretariat Daerah Kota Medan untuk memverifikasi keaslian pada SPT menggunakan algortima RSA yaitu dengan melihat begitu pentingnya SPT sehingga dokumen tersebut harus terjaga keasliannya dengan menggunakan kriptografi dan menerapkan algoritma RSA.
2. Berdasarkan hasil analisa, algoritma RSA dapat diterapkan dalam pemecahan masalah di kantor Sekretariat Daerah Kota Medan dalam hal memverifikasi keaslian SPT.
3. Dalam merancang aplikasi menggunakan algoritma RSA yang dapat digunakan dalam memverifikasi keaslian SPT pada kantor Sekretariat Daerah Kota Medan yaitu dengan membuat pemodelan sistem seperti *use case* diagram, *activity* diagram, dan *class* diagram, kemudian membuat *flowchart* algoritma sistem, selanjutnya membangun *database* untuk menampung dan menyimpan data, terakhir pembuatan program menggunakan pemrograman berbasis *web*.
4. Sistem yang dirancang selanjutnya diuji dan diimplementasikan dengan memasukkan data-data sesuai dengan yang ada pada bab-bab sebelumnya, kemudian jika hasil *output*nya sesuai dengan data manual maka dalam pengujian sistem ini berjalan dengan baik, menambahkan data ke *database*, perintah *update* untuk merubah data di *database*, perintah *delete* untuk menghapus data di *database*, proses enkripsi berjalan dengan baik, proses pembuatan digital signature berjalan dengan baik, dan proses verifikasi berjalan dengan baik juga.
5. Untuk penelitian selanjutnya, sebaiknya menggunakan kunci yang lebih besar sehingga tingkat keamanannya lebih terjamin.
6. Sistem dapat dikembangkan dengan mengkombinasikan dua algoritma seperti algoritma RSA dan algoritma SHA (*Secure Hasing Algorithm*).

UCAPAN TERIMA KASIH

Terimakasih kepada Bapak Faisal Taufik S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan saran, arahan dan dukungannya serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Bapak Rico Imanta Ginting, S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan saran, arahan dan dukungannya serta motivasi, sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu.

REFERENSI

[1] R. Nasution, Niti, "Kombinasi Rsa-Crt Dengan Random Lsb Untuk Keamanan Data Di Kanwil Kementerian Agama Prov. Sumatera Utara," Vol. 5341, No. April, Pp. 32–42, 2017.
[2] G. E. Setyawan, A. Pinandito, And F. Pradana, "Performasi Kalkulasi Hash Sha-1 Pada Sistem Embbeded Arduino Performance Calculation Of Hash Sha-1 In Embedded System Using Arduino," Pp. 39–45, 2015.
[3] F. Nuraeni, Y. H. Agustin, And I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan Rsa Dan Sha-512 Pada Proses Legalisasi Ijazah," Pp. 8–9, 2018.
[4] D. P. Precilia And A. Izzuddin, "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (Md5)," Vol. 5, No. 1, Pp. 14–19, 2015.
[5] Y. Anshori, A. Y. E. Dodu, And D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Pada Tanda Tangan Digital," Vol. 18, No. 2, Pp. 110–121, 2019.
[6] R. Sadikin, *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi, 2018.
[7] N. Safarina, "Penerapan Algoritma Rsa Dan Des Pada Pengamanan File Teks," Pp. 55–60, 2017.

BIOGRAFI PENULIS

	**Dinda Utari**, Perempuan kelahiran Medan, 19 Agustus 1998, anak pertama dari dua bersaudara ini merupakan seorang mahasiswi STMIK Triguna Dharma yang sedang dalam proses menyelesaikan skripsi.
	**Faisal Taufik, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.
	**Rico Imanta Ginting, S.Kom., M.Kom**, Beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.