

# Penerapan Digital Signature Menggunakan Metode RSA Untuk Menvalidasi Keaslian Ijazah SMA Swasta Bina Artha

Erwin Vasi Waruwu \*, Nurcahyo Budi Nugroho \*\*, Fifin Sonata \*\*

\* Sistem Infromasi, STMIK Triguna Dharma

\*\*Sistem Informatika, STMIK Triguna Dharma

---

## Article Info

### Article history:

Received Apr 19<sup>th</sup>, 2020

Revised Aug 20<sup>th</sup>, 2021

Accepted Sept 5<sup>th</sup>, 2021

---

### Keyword:

Digital Signature

Metode RSA

Validasi Ijazah

SMA Swasta Bina Artha

---

## ABSTRAK

Dalam perkembangan teknologi yang begitu cepat, pemanfaatan jaringan internet meningkat pesat juga. Sehingga kejahatan dalam pemalsuan maupun penyadapan data tidak dapat dipungkiri. Salah satu dokumen penting yang sering dilakukan modifikasi atau pemalsuan adalah ijazah. Ditambah dengan permasalahan yang dimana dalam setiap pengecekan ijazah membutuhkan waktu yang lama. Oleh sebab itu, SMA Swasta Bina Artha membutuhkan aplikasi yang dapat menjamin keamanan keaslian ijazah sehingga menghindari terjadinya duplikat maupun modifikasi ijazah. Dan supaya setiap instansi yang akan melakukan pengecekan keaslian ijazah tidak perlu menunggu waktu yang lama untuk mendapatkan infromasi yang di mau. Sistem pengamanan yang diterapkan ialah penerapan *digital signature* menggunakan metode RSA. Sehingga dalam melakukan validasi ijazah waktu yang diperlukan akan lebih efektif dan efisien.

Hasil program yang dibuat menunjukkan bahwa sistem yang dibangun dengan berbasis web dapat meminimalisir modifikasi atau pemalsuan ijazah SMA Swasta Bina Artha. Selain itu juga memudahkan setiap instansi dalam menadapatkan infromasi ijazah dengan melakukan validasi ijazah SMA Swasta Bina Artha dalam penerapan *digital signature* menggunakan metode RSA.

Copyright © 2021 STMIK Triguna Dharma.

All rights reserved.

---

## Corresponding Author:

Nama : Erwin Vasi Waruwu

Sistem Infromasi

STMIK Triguna Dharma

Email: erwinvasi2017@gmail.com

---

## 1. PENDAHULUAN

Ijazah merupakan dokumen penting yang merupakan salah satu syarat yang digunakan saat melamar pekerjaan pada suatu instansi maupun saat melanjutkan pendidikan di perguruan tinggi. Sehingga ada segelintir orang yang tidak bertanggung jawab memodifikasi maupun memalsukan ijazah dengan pemanfaatan teknologi yang semakin canggih. Berdasarkan kutipan dari *website* linputan6.com [1], salah satu anggota DPRD yang baru saja dilantik pada Agustus 2019 menggunakan ijazah SMA Palsu setelah di periksa di Dinas Pendidikan.

Oleh sebab itu, SMA Swasta Bina Artha membutuhkan sistem yang dapat meminimalis modifikasi atau pemalsuan ijazah dengan teknik validasi. Salah teknik validasi yang dapat dipakai untuk mengidentifikasi keabsahan sebuah dokumen adalah dengan penerapan *digital signature*. Penerapan *digital signature* dapat menggunakan kriptografi asimetris yaitu metode RSA [2]. Metode RSA merupakan jenis kriptografi asimetris yang sangat populer dan aman dengan penggunaan angka kunci yang semakin besar [3]. Metode RSA dapat digunakan untuk pembentukan *digital signature* sehingga dapat melakukan validasi ijazah dengan efektif dan efisien.

## 2. METODE PENELITIAN

### 2.1 Validasi

Berdasarkan jurnal [4], Validasi adalah suatu tindakan pembuktian yang dilakukan sesuai dengan prosedur bahwa suatu dokumen/data benar-benar sesuai dengan dokumen/data asli yang sah. Sedangkan Badan POM RI memberikan definisi mengenai validasi sebagai tindakan pembuktian dengan cara yang sesuai bahwa tiap proses, bahan, prosedur, sistem, kegiatan, perlengkapan atau mekanisme yang digunakan dalam produksi maupun pengawasan mutu akan senantiasa mencapai hasil yang di inginkan.

### 2.2 Digital Signature

*Digital Signature* pertama kali diperkenalkan oleh Diffie dan Hellman pada tahun 1976 [2]. Tanda tangan digital (*digital signature*) merupakan suatu nilai kriptografis yang bergantung pada pesan dan pengirim [5]. Tanda tangan digital di gunakan untuk membuktikan keaslian identitas pengirim pesan dan juga memastikan keaslian pesan yang dikirim.

Cara kerja *digital signature* hampir sama dengan cara kerja “tanda tangan” dokumen biasa. Terdapat 2 algoritma pada sistem *digital signature*, yaitu algoritma *sign* untuk menandatangani sebuah dokumen  $M$  dan menghasilkan sebuah tanda tangan (*sign*)  $\rho$ , dan algoritma *verify* yang mengembalikan nilai *true* bila tanda tangan  $\rho$  memang milik penandatanganan dan untuk dokumen  $M$  [6].

### 2.3 Kriptografi

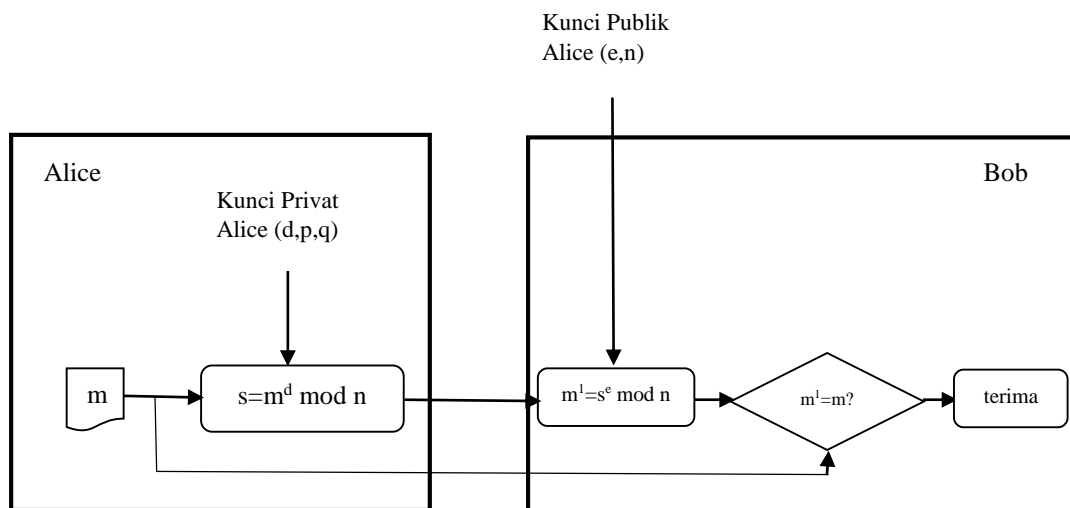
Kriptografi berasal dari bahasa Yunani yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan) [7]. Sebelum adanya komputer, alat yang digunakan dalam melakukan kriptografi adalah pensil dan kertas.

Kriptografi adalah suatu proses yang mengkonversi sebuah pesan plainteks menjadi sebuah cipherteks yang dibalik ke bentuk asli seperti semua, yang juga disebut sebagai proses decoding atau dekripsi [8].

### 2.4 Algoritma RSA

Algoritma RSA merupakan salah satu kriptografi asimetris (kunci publik) yang dimana terdiri dari kunci publik dan kunci rahasia. RSA ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman [9]. Nama RSA diambil dari ketiga penemu algoritma tersebut. Konsep RSA didasarkan pada faktorisasi angka besar yang berarti semakin besar urutan angka yang Anda miliki, semakin Anda terlindungi .

Di dalam sebuah referensi buku oleh Sadikin [6], terdapat sekma *digital signature* menggunakan metode RSA. Sistem kriptografi RSA dapat dimodifikasi sehingga memenuhi sistem *digital signature*.



Gambar 1. Skema digital signature dengan RSA

Skema digital signature dengan menggunakan sistem kriptografi RSA terdiri dari beberapa langkah, yaitu [6]:

#### 1. Pembangkit Kunci

Algoritma Pembangkit kunci sama dengan sistem kriptografi RSA, yaitu menghasilkan kunci publik  $K_{\text{publik}} = (e,n)$  dan kunci privat  $K_{\text{privat}} = d$ . Fungsi pembangkit kunci menggunakan objek RSA, yaitu objek yang merepresentasikan sistem kriptografi asimetrik RSA dengan mengembalikan hasil fungsi pembangkit kunci.

Algoritma Pembangkit Kunci RSA:

$$n = p \times q$$

$$\phi(n) = (p-1) \times (q-1)$$

$$e \in \mathbb{Z}_{\phi(n)} \text{ dengan } \text{gcd}(e, \phi(n)) = 1$$

$$d = e^{-1} \text{ pada } \mathbb{Z}_{\phi(n)}$$

$$K_{\text{publik}} = (e, n), K_{\text{privat}} = d$$

Keterangan:

- $p, q$  : Adalah bilangan prima
- $n$  : Adalah modulus yang digunakan
- $e$  : Adalah eksponen publik atau eksponen enkripsi
- $d$  : Adalah eksponen pribadi atau eksponen dekripsi

Direkomendasikan besar  $p$  dan  $q$  adalah 512 bit sehingga  $n$  berukuran 1024 bit. Karena  $p$  dan  $q$  adalah bilangan prima, maka  $\phi(n) = (p-1) \times (q-1)$ . Kemudian pilih sebuah integer  $e$  dipilih secara acak dari  $\mathbb{Z}_{\phi(n)}$  yang memenuhi  $\text{gcd}(e, \phi(n))$  sehingga  $e$  merupakan generator pada  $\mathbb{Z}_{\phi(n)}$ . Selanjutnya algoritma pembangkit kunci RSA menghitung  $d$  invers perkalian  $e$  pada  $\mathbb{Z}_{\phi(n)}$ . Pada akhirnya algoritma pembangkit kunci RSA menetapkan  $(e, n)$  sebagai kunci publik dan  $d$  sebagai kunci privat atau tetap dirahasiakan.

### 2. Algoritma sign

Algoritma *sign* menerima masukan sebuah pesan  $M$ , kunci privat dan kunci publik RSA. Algoritma *sign* menggunakan perhitungan eksponensial modular untuk mendapatkan *signature*  $\rho$ .

Algoritma *sign* skema *digital signature* RSA:

Input:  $M, K_{\text{privat}} = d, K_{\text{publik}} = (e, n)$   
 Output:  $\rho \{ \text{signature} \}$   
 $\rho = M^d \text{ mod } n$

### 3. Algoritma Verify

Bob mendapatkan  $(M, \rho)$  dari Alice. Bob memverifikasi  $(M, \rho)$  dengan menjalankan algoritma *Verify* yang diberikan oleh Algoritma dibawah ini:

Algoritma *Verify* skema *digital signature* RSA

Input :  $(M, \rho), K_{\text{publik}} = (e, n)$   
 Output : diterima  
 $M' = \rho^e \text{ mod } n$   
 If  $M = M'$  then  
     diterima = true  
 else  
     diterima = false  
 end if

## 3. ANALISA DAN HASIL

### 3.1 Analisa Sistem

Algoritma sistem merupakan penjelasan langkah-langkah penyelesaian masalah dalam perancangan sistem penerapan *digital signature* menggunakan metode RSA untuk memvalidasi kelasian ijazah. Berikut ini merupakan algoritma sistem skema *Digital Signature* Menggunakan Algoritma RSA sebagai berikut:

Langkah pertama dalam Algoritma RSA adalah melakukan inisialisasi terhadap nilai bilang prima  $p = 37$  dan  $q = 53$  yang diambil secara *random*.

Berikut ini adalah beberapa data dari ijazah yang akan di ubah menjadi digital signature. Dimana tahap yang pertama dilakukan adalah setiap karakternya/ plainteks diubah ke format *ASCII* (desimal).

Tabel 1. Data yang diubah ke kode ASCII

No	CHAR	DEC (ASCII)
1	0	48
2	0	48
3	4	52
4	2	50
5	7	55

6	4	52
7	5	53
8	E	69
9	R	82
10	W	87
11	I	73
12	N	78
13	0	48
14	1	49
15	4	52

Berikut skema digital signature dengan metode RSA:

1. Pembangkit Kunci *digital signature* RSA

- Pilihlah bilangan prima yang sudah di dapat diatas adalah  $(p) = 37$  dan nilai  $(q) = 53$ .
- Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian  $n = p * q$ ,  $n = 37 * 53 = 1961$
- Hitung  $(phi) n = (p-1) (q-1)$   
 $n = 36 * 52 = 1872$
- Pilih nilai  $e$  dengan syarat  $e > 1$  dan *greatest common divisor*  $(e, 1872) = 1$   
Nilai  $e$  yang di ambil adalah 61.

Bukti:

$(61, 1872)$

$$1872 \text{ mod } 61 = 42$$

$$61 \text{ mod } 42 = 19$$

$$42 \text{ mod } 19 = 4$$

$$19 \text{ mod } 4 = 3$$

$$4 \text{ mod } 3 = 1$$

$$3 \text{ mod } 1 = 0$$

- Sehingga  $d * e = 1 \text{ (mod } 1872)$  dan  $d < 1872$

$$d * 61 = 1 \text{ mod } 1872$$

$$d * 61 \text{ mod } 1872 = 1$$

$$d = 1381$$

Bukti:

$$1381 * 61 \text{ mod } 1972 = 1$$

Sehingga pasangan kunci yang di dapat adalah :

*Public key*( $e, n$ ) = (61, 1961) dan

*Private key*( $d, n$ ) = (1381, 1961)

2. Algoritma *Sign*

Setelah kunci publik dan kunci privat telah didapat, proses selanjutnya merubah setiap karakter atau  $M$  menjadi *sign* dengan rumus  $\rho = M^d \text{ mod } n$ .

$$\rho_1 = 48^{1381} \text{ mod } 1961 = 973$$

$$\rho_2 = 48^{1381} \text{ mod } 1961 = 973$$

$$\rho_3 = 52^{1381} \text{ mod } 1961 = 1907$$

$$\rho_4 = 50^{1381} \text{ mod } 1961 = 981$$

$$\rho_5 = 55^{1381} \text{ mod } 1961 = 1105$$

$$\rho_6 = 52^{1381} \text{ mod } 1961 = 1907$$

$$\rho_7 = 53^{1381} \text{ mod } 1961 = 1378$$

$$\rho_8 = 69^{1381} \text{ mod } 1961 = 1393$$

$$\rho_9 = 82^{1381} \text{ mod } 1961 = 1599$$

$$\rho_{10} = 87^{1381} \text{ mod } 1961 = 870$$

$$\rho_{11} = 73^{1381} \text{ mod } 1961 = 480$$

$$\rho_{12} = 78^{1381} \text{ mod } 1961 = 891$$

$$\rho_{13} = 48^{1381} \text{ mod } 1961 = 973$$

$$\rho_{14} = 49^{1381} \text{ mod } 1961 = 201$$

$$\rho_{15} = 52^{1381} \text{ mod } 1961 = 1907$$

Tabel 2. Hasil karakter M menjadi digital Signature

Karakter $M$	Desimal	Heksa ( <i>sign</i> )
48	973	3CD
48	973	3CD
52	1907	773

50	981	3D5
55	1105	451
52	1907	773
53	1378	562
69	1393	571
82	1599	63F
87	870	366
73	480	1E0
78	891	37B
48	973	3CD
49	201	C9
52	1907	773

3. Algoritma Verif

Langkah selanjutnya adalah melakukan validasi *digital signature* dari hasil *sign* pada tabel 3.3 dengan menggunakan kunci publik pada rumus  $M' = \rho^e \text{ mod } n$ .

$M'1 = 973^{61} \text{ mod } 1961 = 48$	$M'9 = 1599^{61} \text{ mod } 1961 = 82$
$M'2 = 973^{61} \text{ mod } 1961 = 48$	$M'10 = 870^{61} \text{ mod } 1961 = 87$
$M'3 = 1907^{61} \text{ mod } 1961 = 52$	$M'11 = 480^{61} \text{ mod } 1961 = 73$
$M'4 = 981^{61} \text{ mod } 1961 = 50$	$M'12 = 891^{61} \text{ mod } 1961 = 78$
$M'5 = 1105^{61} \text{ mod } 1961 = 55$	$M'13 = 973^{61} \text{ mod } 1961 = 48$
$M'6 = 1907^{61} \text{ mod } 1961 = 52$	$M'14 = 201^{61} \text{ mod } 1961 = 49$
$M'7 = 1378^{61} \text{ mod } 1961 = 53$	$M'15 = 1907^{61} \text{ mod } 1961 = 52$
$M'8 = 1393^{61} \text{ mod } 1961 = 69$	

Tabel 3. Hasil Verif dari *sign*

<i>Sign</i>	Kode ASCII	Plainteks
973	48	0
973	48	0
1907	52	4
981	50	2
1105	55	7
1907	52	4
1378	53	5
1393	69	E
1599	82	R
870	87	W
480	73	I
891	78	N
973	48	0
201	49	1
1907	52	4

Implementasi merupakan tahap yang dalam mengoperasikan sistem yang akan dibangun. Dalam bab ini akan dijelaskan bagaimana menjalankan sistem yang telah dibangun tersebut. Dibawah ini merupakan tampilan dari implementasi penerapan *digital signature* menggunakan metode RSA untuk memvalidasi keaslian ijazah.

3.2 Hasil

Sebelum sistem benar-benar bisa digunakan dengan baik, sistem harus melalui tahap pengujian terlebih dahulu untuk menjamin tidak ada kendala yang muncul pada saat sistem digunakan. Implementasi yang dilakukan terdapat beberapa tahap dan prosedur untuk menyelesaikan analisa yaitu apalikasi yang disetujui, melakukan penginstalan, pengujian data dan memulai menggunakan sistem baru.

### 1. Tampilan Form Login

*Form Login* adalah form yang dibuat untuk membatasi hak akses user lain dengan tata usaha. Untuk dapat masuk ke dalam menu pengolahan data ijazah, maka tata usaha harus melakukan login terlebih dahulu dengan menginputkan username dan password yang sudah tersimpan di dalam database dengan benar.

Berikut ini adalah tampilan form login adalah sebagai berikut:



The image shows a web browser window with the title "Silahkan Login !!!". Inside the window, there is a login form with the following elements:

- A label "Username" above a text input field containing the text "Username".
- A label "Password" above a text input field containing the text "Passowrd".
- A "Login" button located below the password field.

Gambar 2. Tampilan Form Login

### 2. Tampilan Menu Utama Pengolahan Data Ijazah

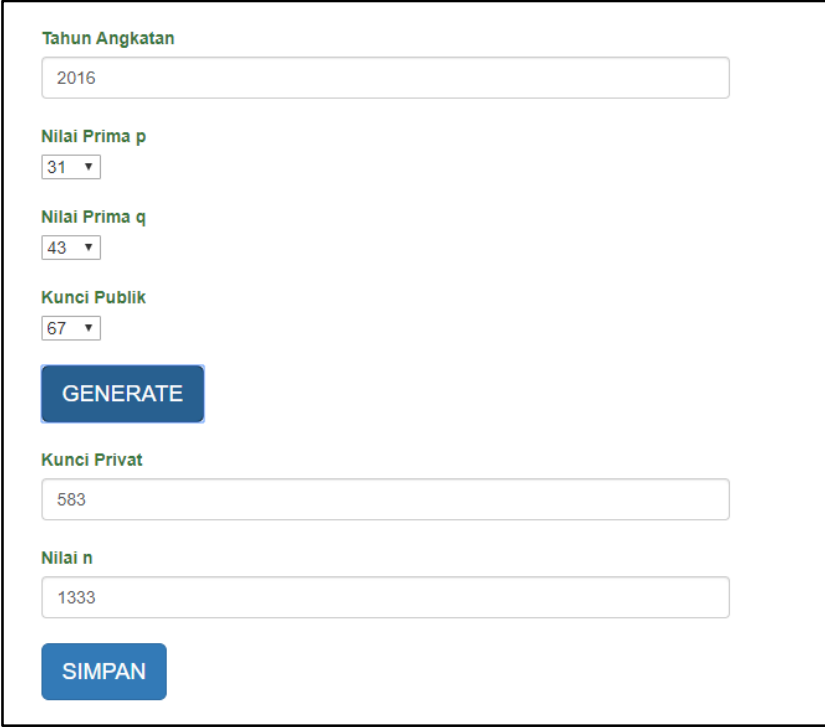
Halaman Menu Utama Pengolahan Data Ijazah merupakan halaman yang tampil ketika tata usaha berhasil login. Dalam halaman ini terdapat menu – menu aktifitas yang dapat dilakukan tata usaha dalam mengolah data ijazah. Berikut ini adalah tampilan halam menu utama pengolahan data ijazah yaitu sebagai berikut:



Gambar 3. Tampilan Halaman Menu Utama Pengolahan Data Ijazah

### 3. Tampilan Form Pembangkit Kunci

Halaman ini memiliki fungsi untuk melakukan pembangkit kunci. Berikut ini adalah tampilan form pembangkit kunci adalah sebagai berikut:



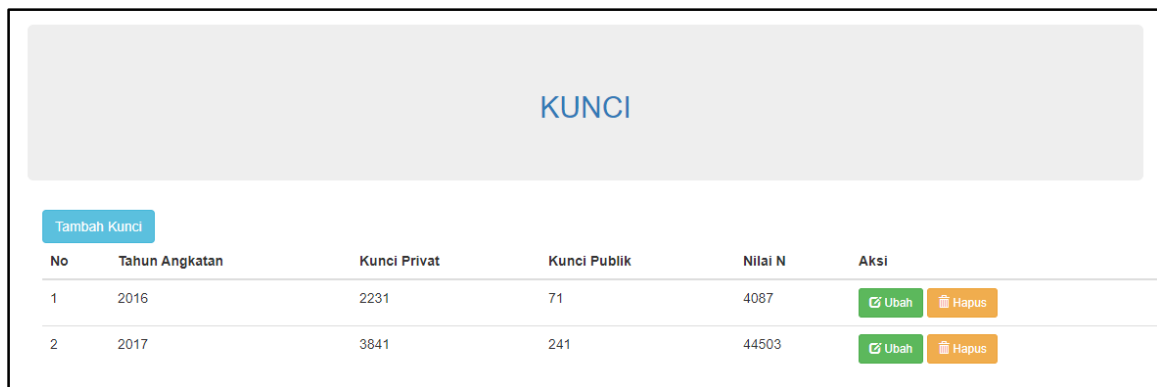
The image shows a web form for generating keys. It contains the following fields and buttons:

- "Tahun Angkatan": A text input field containing "2016".
- "Nilai Prima p": A dropdown menu showing "31".
- "Nilai Prima q": A dropdown menu showing "43".
- "Kunci Publik": A dropdown menu showing "67".
- A blue "GENERATE" button.
- "Kunci Privat": A text input field containing "583".
- "Nilai n": A text input field containing "1333".
- A blue "SIMPAN" button.

Gambar 4. Tampilan Form Pembangkit Kunci

#### 4. Tampilan Halaman Kunci

Halaman ini memiliki fungsi sebagai tempat menampilkan isi dari database pembangkit kunci yang telah dibuat. Berikut ini adalah tampilan halaman kunci yaitu sebagai berikut:

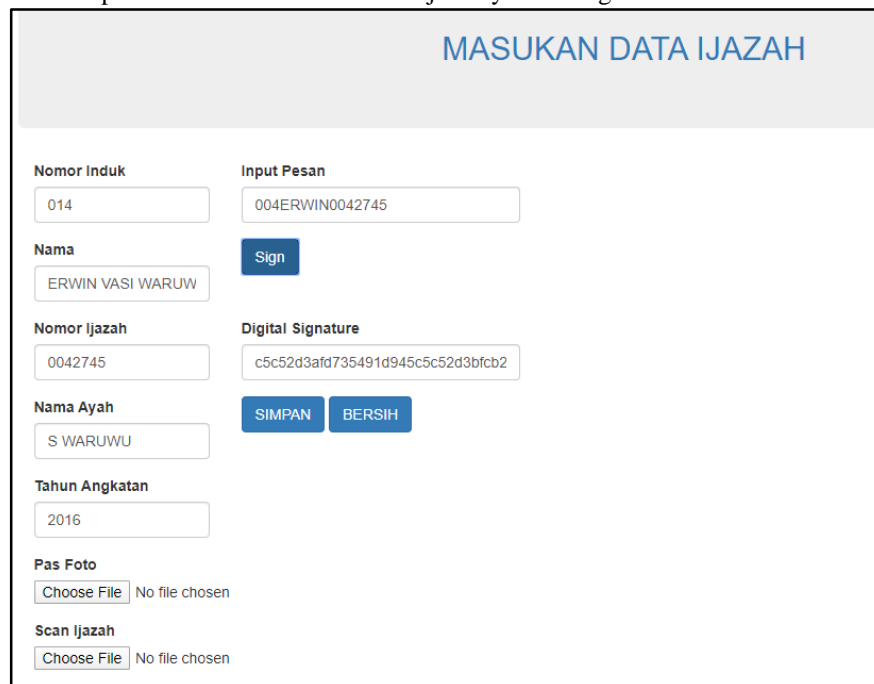


No	Tahun Angkatan	Kunci Privat	Kunci Publik	Nilai N	Aksi
1	2016	2231	71	4087	<a href="#">Ubah</a> <a href="#">Hapus</a>
2	2017	3841	241	44503	<a href="#">Ubah</a> <a href="#">Hapus</a>

Gambar 5. Tampilan Halaman Kunci

#### 5. Tampilan Form Masukan Data Ijazah

Tampilan form ini digunakan untuk menginput data ijazah dan juga pembentukan *digital signature*. Berikut ini adalah tampilan dari form masukan data ijazah yaitu sebagai berikut:



**MASUKAN DATA IJAZAH**

Nomor Induk:

Input Pesan:

Nama:  [Sign](#)

Nomor Ijazah:

Digital Signature:

Nama Ayah:  [SIMPAN](#) [BERSIH](#)

Tahun Angkatan:

Pas Foto:  No file chosen

Scan Ijazah:  No file chosen

Gambar 6. Tampilan Form Masukan Data Ijazah


Halaman data ijazah berfungsi untuk menampilkan data ijazah yang telah di input dari form masukan data ijazah. Berikut adalah tampilan dari halaman data ijazah yaitu sebagai berikut:

DATA IJAZAH							
No	No Induk	Nama	No Ijazah	Nama Ayah	Tahun Angkatan	Digital Signature	Aksi
1	014	ERWIN VASI WARUWU	0042745	S WARUWU	2016	c5e7a2d3afd735491d945c5c52d3bf	<a href="#">Ubah</a> <a href="#">Hapus</a> <a href="#">Cetak</a>
2	066	SARIHON SITUMEANG	0042770	HD SITUMEANG	2017	3f890e6467425a7a4ae5da43df53f8	<a href="#">Ubah</a> <a href="#">Hapus</a> <a href="#">Cetak</a>

Gambar 7. Tampilan Halaman Data Ijazah

#### 6. Tampilan Form Validasi

Form Validasi digunakan untuk menginput digital signature dalam memvalidasi keaslian ijazah. Berikut adalah tampilan form menu validasi yaitu sebagai berikut:

VALIDASI IJAZAH	
<p>Nomor Ijazah</p> <input type="text" value="0042745"/>	<p>Data Ijazah Valid</p> <p>ERWIN VASI WARUWU</p>
<p>Tahun Angkatan</p> <input type="text" value="2016"/>	
<p>Input Digital Signature</p> <input type="text" value="c5e7a2d3afd735491d945c5c52d3bf"/>	
<input type="button" value="Validasi"/>	

Gambar 8. Tampilan Form Validasi

#### 7. Tampilan Lampiran Digital Signature

Lampiran digital signature digunakan untuk melampirkan hasil dari digital signature yang telah di buat. Berikut adalah tampilan dari form lampiran *digital signature* sebagai berikut:

Lampiran Digital Signature	
Nama	: ERWIN VASI WARUWU
No. Ijazah	: 0041222
Tahun Angkatan	: 2016
Digital Signature	: 46554b611db6606462a464666049e632
Kunjungi alamat <a href="http://www.SMASBA.com">www.SMASBA.com</a> untuk validasi	

Gambar 9. Tampilan Lampiran Digital Signature

#### 4. KESIMPULAN

Dari hasil pembahasan mengenai aplikasi penerapan *digital signature* menggunakan metode RSA untuk memvalidasi keaslian ijazah SMA Swasta Bina Artha dapat diambil kesimpulan adalah sebagai berikut:



1. Dengan penerapan *digital signature* terhadap penyelesaian masalah pada SMA Swasta Bina Artha dalam memvalidasi keaslian ijazah sangat baik, hal ini ditandai dengan kemudahan dalam mendapatkan informasi ijazah yang diinginkan.
2. Metode RSA dapat diterapkan dalam penerapan *digital signature* untuk memvalidasi keaslian ijazah SMA Swasta Bina Artha.
3. Upaya pemodelan penerapan *digital signature* yang dirancang dapat dilakukan, yang diawali dengan analisis masalah kebutuhan kemudian dilakukan pemodelan.
4. Dalam merancang penerapan *digital signature* yang mengadopsi metode RSA dapat digunakan dalam penyelesaian masalah di SMA Swasta Bina Artha.

### UCAPAN TERIMA KASIH

Saya Mengucapkan terimakasih kepada Ketua Yayasan STMIK Triguna Dharma, kepada Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom selaku Dosen Pembimbing I saya, kepada Ibu Fifin Sonata, S.Kom., M.Kom selaku Dosen Pembimbing II saya, kepada kedua orang tua saya yang selalu memberi dukungan dan teman seperjuangan.

### REFERENSI

- [1] M. G. Yunas, "Diduga Palsukan Ijazah SMA, Anggota DPRD Probolinggo Ditahan," 2019. [Online]. Available: <https://www.liputan6.com/news/read/4080115/diduga-palsukan-ijazah-sma-anggota-dprd-probolinggo-ditahan>.
- [2] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, pp. 184–191, 2016.
- [3] D. Pratama, "Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks," *J. Pseudocode*, vol. 3, no. 1, pp. 44–49, 2016.
- [4] N. A. M. S. M. Mohamad Ali Murtadho, "Implementasi Quick Response (Qr) Code Pada Aplikasi Validasi Dokumen Menggunakan Perancangan Unified Modelling Language (Uml)," *Antivirus J. Ilm. Tek. Inform.*, vol. 10, no. 1, pp. 42–50, 2016.
- [5] N. Wiyono and M. Hardjianto, "Pengamanan Email Menggunakan Algoritma RSA dan Digital Signature SHA-1 Berbasis Mobile," vol. 4, no. 2, pp. 1–11, 2016.
- [6] R. Sadikin, *Kriptografi untuk keamanan jaringan*. 2012.
- [7] A. Pradipta, "Implementasi Metode Caesar Cipher Alfabets Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *Indones. J. Netw. Secur.*, vol. 5, no. 3, pp. 3–6, 2016.
- [8] M. Nasrun *et al.*, "ANALISIS PERBANDINGAN ANTARA ALGORITMA KRIPTOGRAFI SERPENT DAN AES PADA IMPLEMENTASI ENKRIPSI SMS DI PERANGKAT ANDROID ANALYSIS OF COMPARATION BETWEEN CRYPTOGRAPHIC ALGORITHM SERPENT AND AES IN SMS ENCRYPTION ON ANDROID DEVICE IMPLEMENTATION," vol. 2, no. 2, pp. 3511–3517, 2015.
- [9] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015.

**BIBLIOGRAFI PENULIS**

	Nama	:	Erwin Vasi Waruwu
	T.T.L	:	Aek Babura, 08 Juli 1998
	Jenis Kelamin	:	Laki-Laki
	Program Studi	:	Sistem Informasi STMIK Triguna Dharma
	Deskripsi	:	Sedang Menempuh jenjang Strata Satu (S1) dengan program studi sistem informasi di STMIK Triguna Dharma.
	Nama	:	Nurcahyo Budi Nugroho, S.Kom., M.Kom
	NIDN	:	0130038201
	Jenis Kelamin	:	Laki-laki
	Deskripsi	:	Dosen tetap STMIK Triguna Dharma pada program studi teknik informatika dengan fokus bidang keilmuan Pemrograman dan Keamanan Komputer
	Nama	:	Fifin Sonata, S.Kom., M.Kom
	NIDN	:	0124128202
	Jenis Kelamin	:	Perempuan
	Deskripsi	:	Dosen tetap STMIK Triguna Dharma pada program studi manajemen informatika dan fokus pada bidang keilmuan Analisis Algoritma, Optimasi dan Decision Support System serta aktif dalam organisasi Asosiasi Peneliti Sumatera Utara (APSU) dan Ikatan Ahli Informatika Indonesia (IAII) . Telah mempublikasikan sebanyak 17 naskah jurnal dan prosiding dibidang Ilmu komputer. Menjabat sebagai Koordinator Bidang Kerjasama di Asosiasi Peneliti Sumatera Utara (APSU) Prestasi : Memenangkan Hibah Penelitian Kemenristek Dikti Tahun 2018