J-SISKO TECH
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
P:ISSN : 2621-8976 E-ISSN : 2615-5133 ■ 45
Vol.3, No.2, Juli 2020, pp.45-55

PENERAPAN DIGITAL SIGNATURE MENGGUNAKAN METODE RSA UNTUK MENVALIDASI KEASLIAN IJAZAH SMA SWASTA BINA ARTHA

Erwin Vasi Waruwu, Azanuddin, Fifin Sonata, Iskandar Zulkarnain
Program Studi Sistem Informasi, STMIK Triguna Dharma
Jl. A.H Nasution No.73 Medan, Sumatera Utara, 20142
*E-mail: m_dahria@trigunadharma.ac.id

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 permasalah yang dimana dalam setiap pengecekan ijazah membutuhkan waktu yang lama. Oleh sebab itu, SMA Swasta Bina Arha membutuhkan aplikasi yang dapat menjamin keamanan keaslian ijazah sehingga menghindari terjadinya duplikat maupun modifikasi ijazah. Dan supaya setiap instansi yang akan melakukan pengecekkan keaslian ijazah tidak perlu menunggu waktu yang lama untuk mendapatkan infromasi yang di mau. Sistem pengamanan yang diterapkan ialah penerapan *digital siganture* menggunakan metode RSA. Sehingga dalam melakukan validasi ijazah waktu yang diperlukan akan lebih efektif dan efesien.
Hasil program yang dibuat menunjukkan bahwa sistem yang dibangun dengan berbasis web dapat menimalisir 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* menunggunakan metode RSA.

Kata kunci : *Digital Signature* Metode RSA Validasi Ijazah SMA Swasta Bina Artha

Abstract

In the rapid development of technology, the use of internet networks is also increasing rapidly. So that crimes in data forgery and interception cannot be denied. One of the important documents that is often modified or falsified is a certificate. Coupled with the problem that every certificate checking takes a long time. Therefore, Bina Arha Private High School needs an application that can guarantee the security of the authenticity of the diploma so as to avoid duplicate or modification of the certificate. And so that every agency that will check the authenticity of the diploma does not have to wait a long time to get the desired information. The security system applied is the application of digital siganture using the RSA method. So that in validating the certificate the time needed will be more effective and efficient.

The program results show that a web-based system can minimize modification or falsification of Bina Artha Private High School certificates. In addition, it also makes it easier for each agency to obtain certificate information by validating the Bina Artha Private High School diploma in implementing digital signatures using the RSA method.

Keywords: *Digital* Signature RSA Method Validation of Bina Artha Private High School Diploma

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 efesien.

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 sebuh dokumen *M* dan menghasilkan sebuah tanda tangan (*sign*) *ρ,* dan algoritma *verify* yang mengembalikan nilai *true* bila tanda tangan *ρ* memang milik penandatangan dan untuk dokumen *M* [6].

2.3 Kriptografi

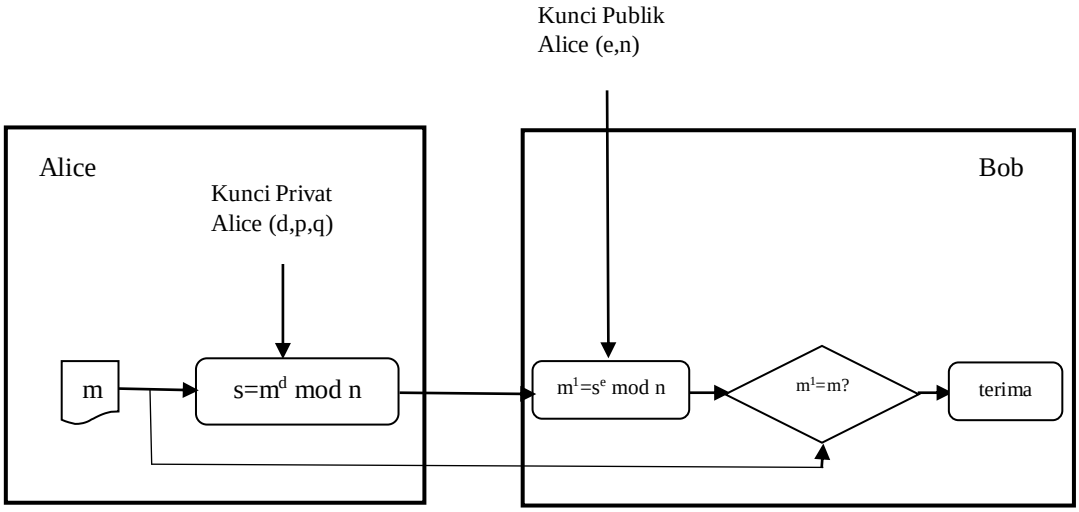
Kriptografi berasal dari bahasa Yunani yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan) [7]. Sebelum adanya komputer, alat yang digunakan dalam melakukan kriptografi adalaha pensil dan kertas.

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 [10].

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*publik = (e,n) dan kunci privat *K*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 x q
ϕ(n) = (p-1) x (q-1)
$e \xleftarrow{R} Z_{\phi(n)}$ dengan gcd *(e,ϕ(n))* = 1
$d = e^{-1}$ pada $Z_{\phi(n)}$
K_{Publik} = *(e,n)*, K_{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 *ϕ(n) = (p-1) x (q-1).* Kemudian pilih sebuah integer *e* dipilih secara acak dari $Z_{\phi(n)}$ yang memenuhi gcd*(e,ϕ(n))* sehingga *e* merupakan generator pada $Z_{\phi(n)}$. Selanjutnya algoritma pembangkit kunci RSA menghitung *d* invers perkalian *e* pada $Z_{\phi(n)}$. 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 ρ*.

Algoritma *sign* skema *digital signature* RSA:
Input: *M* , Kprivat = d, K publik =(e,n)
Output: *ρ* {*signature*}

$\rho = M^{d} \bmod n$

3. Algoritma *Verify*

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

Algoritma *Verify* skema *digital signature* RSA

```
Input    : (M, ρ), Kpublik = (e,n)
Output   : diterima
M' = ρ^e mod n
If M  = M' then
        diterima = true
else
        diterima = false
end if
```

1. ANALISA DAN HASIL

3.1 Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah-langkah penyelesaian masalah dalam perancangan sistem penerapan *digital signature* menggunakan metode RSA untuk menvalidasi kelasian ijazah. Berikut ini merupakan algoritma sistem sknema *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	Plainteks	Kode *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

a. Pilihlah bilangan prima yang sudah di dapat diatas adalah (*p*) = 37 dan nilai (*q*) = 53.

b. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian *n*= *p* * *q*
n= 37 * 53 = 1961

c. Hitung (*phi*) *n*= (*p-1*) (q-1)

*n= 36 * 52* = 1872

d. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e,1872)* = 1

Nilai *e* yang di ambil adalah 61.

Bukti:

(61, 1872)

1872 mod 61 = 42
61 mod 42 = 19
42 mod 19 = 4
19 mod 4 = 3
4 mod 3 = 1
3 mod 1 = 0

e. Sehingga *d * e = 1* (mod 1872) dan *d* < 1872

*d * 61 = 1 mod 1872*
*d * 61 mod 1872 =1*
d = 1381

Bukti:

1381 * 61 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 $\rho = M^d \ mod \ n.$

$\rho 1 = 48^{1381} \ mod \ 1961 = 973$
$\rho 2 = 48^{1381} \ mod \ 1961 = 973$
$\rho 3 = 52^{1381} \ mod \ 1961 = 1907$
$\rho 4 = 50^{1381} \ mod \ 1961 = 981$
$\rho 5 = 55^{1381} \ mod \ 1961 = 1105$
$\rho 6 = 52^{1381} \ mod \ 1961 = 1907$
$\rho 7 = 53^{1381} \ mod \ 1961 = 1378$
$\rho 8 = 69^{1381} \ mod \ 1961 = 1393$
$\rho 9 = 82^{1381} \ mod \ 1961 = 1599$
$\rho 10 = 87^{1381} \ mod \ 1961 = 870$
$\rho 11 = 73^{1381} \ mod \ 1961 = 480$
$\rho 12 = 78^{1381} \ mod \ 1961 = 891$
$\rho 13 = 48^{1381} \ mod \ 1961 = 973$
$\rho 14 = 49^{1381} \ mod \ 1961 = 201$
$\rho 15 = 52^{1381} \ mod \ 1961 = 1907$

Tabel 2 Hasil karakter *M* menjadi *digital Signature*

Karakter *M*	**Desimal**	**Heksa (*sign)***
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 $M' = \rho^e$ mod n.

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

Tabel 3 Hasil Verif dari *sign*

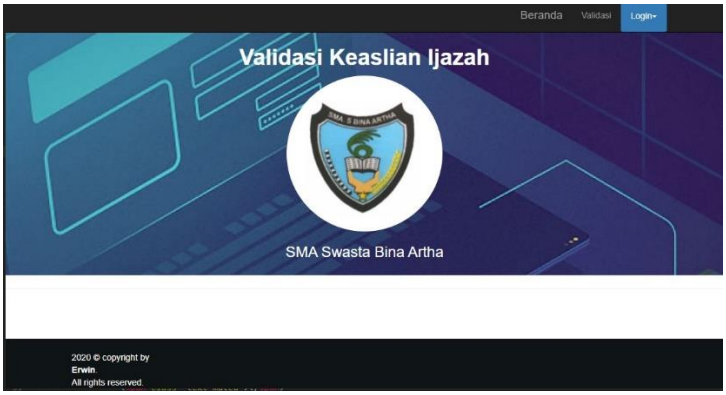
Sign	**Kode ASCII**	**Plainteks**
973	48	0
973	48	0
1907	52	4
981	50	2
1105	55	7
1907	52	4
1378	53	5
1393	69	E
1599	82	R
870	87	W
480	73	I
891	78	N
973	48	0
201	49	1
1907	52	4

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 menvalidasi keaslian ijazah.

3.2 Tampilan Halaman Menu Utama

Saat pertama kali menjalankan sistem, maka halaman menu utama yang akan pertama kali tampil. Dimana dalam halaman utama ini, dapat diakses oleh semua user. Adapun aktifitas

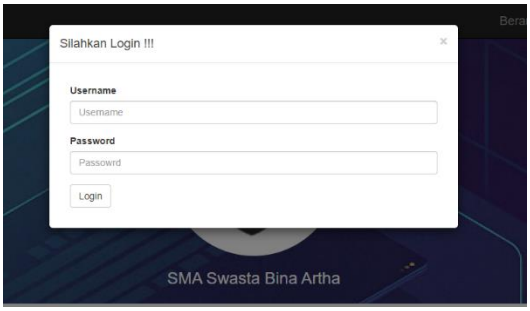
yang dapat dilakukan didalam halaman ini adalah membuka form validasi dan juga login. Di bawah ini merupakan tampilan halaman menu utama adalah sebagai berikut:



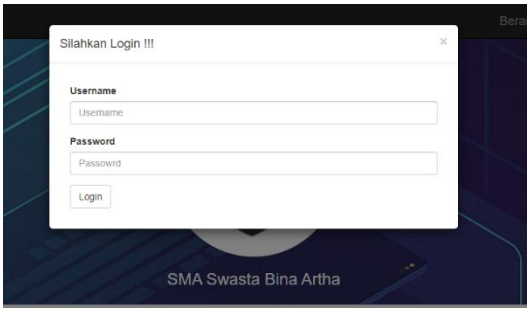
Gambar 3 Tampilan Halaman Menu Utama

3.3 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:



Gambar 4 Tampilan Form Login



Gambar 4 Tampilan Form Login

3.4 Tampilan Halaman Menu Utama Pengolahan Data Ijazah

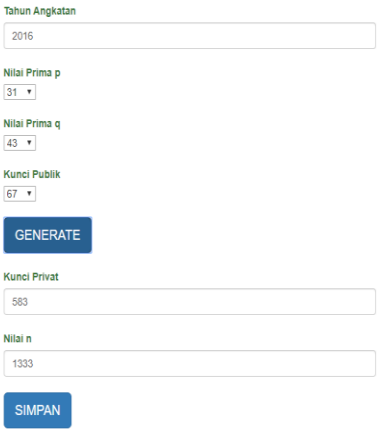
Halaman Menu Utama Pengolahan Data Ijazah merupakan halaman yang tampil ketika tata usaha berhasil login. Dalam halaman ini terdapat menu – menu aktifitas yang dapat

dilakukan tata usaha dalam mengolah data ijazah. Berikut ini adalah tampilan halam menu utama pengolahan data ijazah yaitu sebagai berikut:

Gambar 5 Tampilan Halaman Menu Utama Pengolahan Data Ijazah

3.4Tampilan Form Pembangkit Kunci

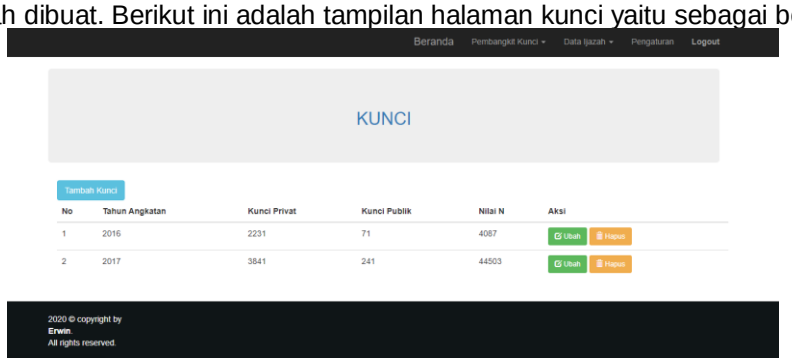
Halaman ini memiliki fungsi untuk melakukan pembangkit kunci. Berikut ini adalah tampilan form pembangkit kunci adalah sebagai berikut:



Gambar 6 Tampilan Form Pembangkit Kunci

3.5 Tampilan Halaman Kunci

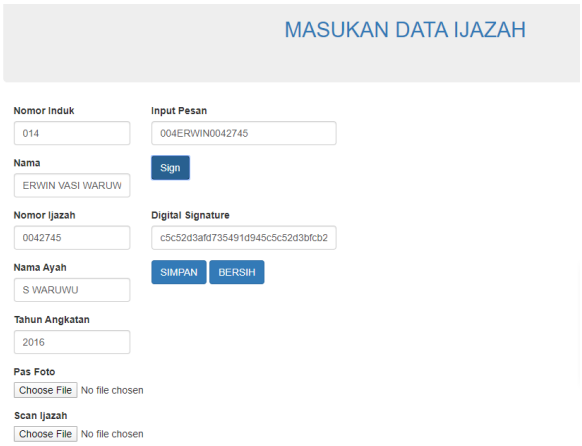
Halaman ini memiliki fungsi sebagai tempat menampilkan isi dari database pembangkit kunci yang telah dibuat. Berikut ini adalah tampilan halaman kunci yaitu sebagai berikut:



Gambar 7 Tampilan Halaman Kunci

3.6 Tampilan Form Masukan Data Ijazah

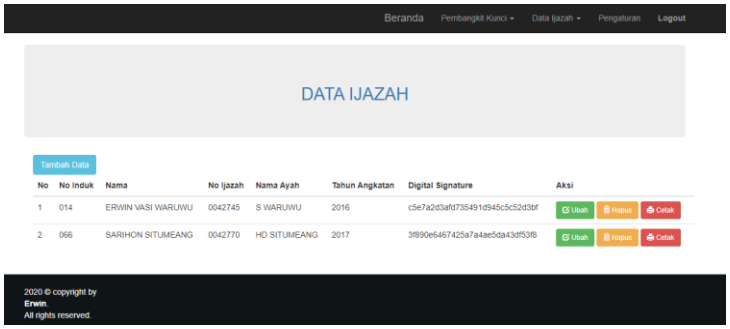
Tampilan form ini digunakan untuk menginput data ijazah dan juga pembentukan *digital signature*. Berikut ini adalah tampilan dari form masukan data ijazah yaitu sebagai berikut:



Gambar 8 Tampilan Form Masukan Data Ijazah

3.7 Tampilan Halaman Data Ijazah

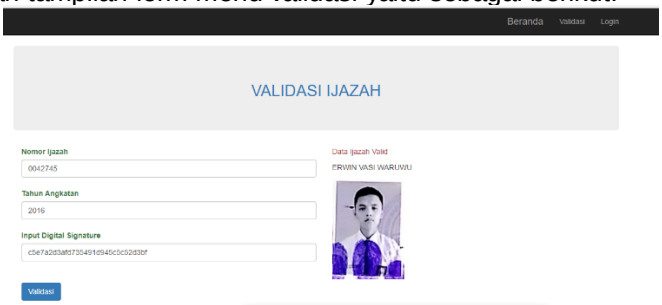
Halaman data ijazah berfungsi untuk menampilkan data ijazah yang telah di input dari form masukan data ijazah. Berikut adalah tampilan dari halaman data ijazah yaitu sebagai berikut:



Gambar 9 Tampilan Halaman Data Ijazah

3.4 Tampilan Form Validasi

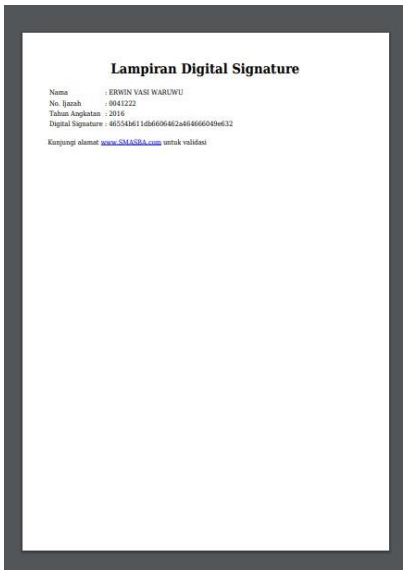
Form Validasi digunakan untuk menginput digital signature dalam menvalidasi keaslian ijazah. Berikut adalah tampilan form menu validasi yaitu sebagai berikut:



Gambar 10 Tampilan Form Validasi

3.4 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:



Gambar 11 Tampilan Lampiran *Digtal Signature*

4. KESIMPULAN

Dari hasil pembahasan mengenai aplikasi penerapan *digital signature* menggunakan metode RSA untuk menvalidasi 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 menvalidasi keaslian ijazah sangat baik, hal ini ditandai dengan kemudahan dalam mendapatkan informasi ijazah yang diinginkan.
2. Metode RSA dapat diterapkan dalam penerpan *digital signature* untuk menvalidasi keaslian ijazah SMA Swasta Bina Artha.
3. Upaya pemodelkan penerapan *digital signature* yang dirancang dapat dilakukan, yang diawali dengan analisis masalah kebutuhan kemudian dilakukan pemodelan.
4. Dalam merancang penerapan *digital singature* yang mengadopsi metode RSA dapat digunakan dalam penyelesaian masalah di SMA Swasta Bina Artha.

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 Chiper Alphabet 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 ANALISYS 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.

[10] A. H. Mansour, "Analysis of RSA Digital Signature Key Generation using Strong Prime," *Int. J. Comput.*, vol. 24, no. 1, pp. 28–36, 2017.

[11] F. Wongso, "Perancangan Sistem Informasi Penjualan Berbasis Java Studi Kasus Pada Toko Karya Gemilang Pekanbaru," *J. Ilm. Ekon. dan Bisnis*, vol. 12, no. 1, pp. 46–60, 2015.