Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Aplikasi Verifikator Keaslian Ijazah Berbasis Quick Response (QR) Code Dengan Algoritma RSA

Muhammad Al-fatih Ritonga[1], Dicky Nofriansyah[2], Purwadi[3]

[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]alfatihmuhammad2003@gmail.com, [2]dickynofriansyah@ymail.com, [3]purwadi.triguna@gmail.com
Email Penulis Korespondensi: alfatihmuhammad2003@gmail.com

Article History:
Received Jun 12th, 2024
Revised Jul 12th, 2024
Accepted Jul 30th, 2024

Abstrak

Ijazah merupakan dokumen resmi yang diberikan oleh institusi pendidikan untuk mengakui pencapaian seorang individu dalam menyelesaikan program pendidikan tertentu. Dalam era teknologi saat ini, keaslian ijazah menjadi sangat penting untuk memastikan integritas pendidikan. Kasus pemalsuan ijazah telah menjadi masalah serius, merugikan individu dan merusak citra lembaga pendidikan. Oleh karena itu, diperlukan langkah-langkah efektif untuk menjaga keamanan dan keaslian ijazah, khususnya di SMP IT AL UMM Smart Centre. Penelitian ini mengembangkan solusi untuk mengatasi pemalsuan ijazah dengan mengadopsi teknologi kriptografi, khususnya algoritma *Rivest Shamir Adleman* (RSA), dan *Quick Response* (QR) *Code*. Dengan menyematkan *QR Code* yang dihasilkan melalui algoritma RSA pada dokumen ijazah, diharapkan dapat meningkatkan keamanan dan keaslian ijazah. Metode ini melibatkan proses enkripsi dan dekripsi yang memastikan bahwa hanya pihak yang berwenang yang dapat memverifikasi keabsahan ijazah. Hasil penelitian menunjukkan bahwa aplikasi verifikator keaslian ijazah yang dikembangkan mampu mengurangi risiko pemalsuan dan meningkatkan kepercayaan terhadap keabsahan ijazah. Implementasi teknologi *QR Code* dan algoritma RSA di SMP IT AL UMM Smart Centre terbukti efektif dalam mengamankan dokumen ijazah. Aplikasi ini memberikan solusi yang handal dan dapat diandalkan oleh semua pihak yang terlibat, baik dari segi pendidikan maupun penerimaan di jenjang selanjutnya.

Kata Kunci : Ijazah, Kriptografi, Rivest Shamir Adleman (RSA), QR Code

Abstract

Diplomas are official documents issued by educational institutions to acknowledge an individual's achievement in completing a specific educational program. In today's technological era, the authenticity of diplomas has become very important to ensure the integrity of education. Cases of diploma forgery have become a serious problem, harming individuals and tarnishing the image of educational institutions. Therefore, effective measures are needed to safeguard the security and authenticity of diplomas, particularly at SMP IT AL UMM Smart Centre. This research develops a solution to address diploma forgery by adopting cryptographic technology, specifically the Rivest Shamir Adleman (RSA) algorithm, and Quick Response (QR) Code. By embedding a QR Code generated through the RSA algorithm on diploma documents, it is expected to enhance the security and authenticity of diplomas. This method involves encryption and decryption processes that ensure only authorized parties can verify the diploma's validity. The research results show that the developed diploma authenticity verifier application can reduce the risk of forgery and increase confidence in diploma validity. The implementation of QR Code technology and the RSA algorithm at SMP IT AL UMM Smart Centre has proven effective in securing diploma documents. This application provides a reliable solution that can be trusted by all parties involved, both in education and subsequent levels of acceptance.

Keyword : *Diploma, Cryptography, Rivest Shamir Adleman (RSA), QR Code*

1. PENDAHULUAN

Ijazah adalah dokumen resmi yang diberikan oleh lembaga pendidikan untuk mengakui prestasi individu dalam menyelesaikan program pendidikan. Dalam era teknologi saat ini, keaslian ijazah sangat krusial untuk memastikan

integritas pendidikan. Keamanan dan keaslian ijazah memainkan peran penting dalam mencegah penipuan, pemalsuan, dan penyalahgunaan dokumen ini. Pada 2022, Mahkamah Agung memutuskan 140 kasus pemalsuan ijazah [1]. Ini merugikan individu dan merusak citra lembaga pendidikan serta kepercayaan masyarakat terhadap ijazah.

SMP IT AL UMM Smart Centre, lembaga pendidikan menengah yang menggabungkan pendidikan akademis, agama, dan teknologi, serius menghadapi masalah pemalsuan ijazah di era inovasi teknologi. Tantangan ini semakin kompleks seiring dengan inovasi teknologi yang juga dapat digunakan untuk pemalsuan ijazah yang lebih akurat. Untuk mengatasi tantangan ini, perlu menerapkan solusi kriptografi dengan digital signature dan QR Code berbasis algoritma RSA pada dokumen ijazah. Pendekatan ini diharapkan dapat secara efektif meningkatkan keamanan dan keaslian dokumen ijazah, serta mencegah potensi penipuan, pemalsuan, dan penyalahgunaan dokumen tersebut dalam lingkungan pendidikan yang aman dan terpercaya.

Kriptografi adalah ilmu yang mempelajari cara menjaga keamanan pesan selama pengiriman dengan teknik pengamanan tertentu. Tujuannya adalah mencegah pihak yang tidak berhak melihat atau menyalahgunakan informasi asli [2]. Dalam kriptografi, terdapat dua proses utama: enkripsi, untuk mengubah pesan menjadi tidak terbaca, dan dekripsi, untuk mengembalikan ke bentuk aslinya [3]. Berbagai algoritma kriptografi, seperti RSA, digunakan untuk mengamankan dokumen elektronik dan memberikan solusi dalam menghadapi tantangan keamanan informasi [4]. RSA merupakan salah satu algoritma kriptografi yang menggunakan dua kunci berbeda untuk melakukan enkripsi dan dekripsi [5]. RSA merupakan salah satu temuan penting dalam kriptografi kunci publik, algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk melakukan tanda tangan (*signing*) [6]. Seperti pada penelitian sebelumnya, algoritma RSA berhasil diadopsi dalam mengamankan dokumen elektronik [7].

2. METODOLOGI PENELITIAN

Metode penelitian adalah pendekatan sistematis dan terorganisir yang digunakan untuk merancang studi, mengumpulkan data, menganalisis informasi, dan menyusun hasil. Tujuannya adalah menjawab pertanyaan penelitian atau mencapai tujuan tertentu. Proses ini mencakup berbagai teknik dan strategi untuk memastikan validitas dan reliabilitas data serta kesimpulan yang diambil.

2.1 Tahapan Penelitian

Metode penelitian merupakan suatu pendekatan sistematis dan terorganisir yang digunakan untuk merancang, mengumpulkan data, menganalisis, dan menyusun informasi dalam rangka menjawab pertanyaan penelitian atau mencapai tujuan penelitian tertentu. Adapun tahapan penelitian ini sebagai berikut.

a. Pengumpulan Data
   Pengumpulan data adalah teknik untuk mengumpulkan informasi tentang subjek penelitian. Berikut merupakan teknik pengumpulan data yang dilakukan.
   1. Observasi
      Dalam penelitian ini dilakukan pengamatan langsung ke SMP IT AL UMM Smart Centre. Di SMP IT AL UMM Smart Centre di lakukan analisis masalah yang dihadapi terkait dalam mengamankan dokumen ijazah. Selain itu juga di lakukan sebuah analisis kebutuhan dari permasalahan yang ada sehingga dapat dilakukan pemodelan sistem.
   2. Wawancara
      Pengumpulan data dengan melakukan tanya jawab langsung dengan Kepala Sekolah yaitu Bapak Maramuda, S.Pd. Wawancara dilakukan guna mendapatkan alur kerja pada objek yang diteliti yang akan digunakan dalam mengembangkan fitur-fitur yang akan dibangun.

b. Studi Literatur
   Dalam penelitian ini, dilakukan pengumpulan referensi sebagai bahan pendukung untuk memenuhi kebutuhan dari masalah penelitian. Dengan mencari banyak jurnal yang membahas tentang verifikasi keaslian dokumen, algoritma RSA, kriptografi, dan elemen-elemen lain. Diharapkan dapat membantu dalam menyelesaikan permasalahan yang terjadi di SMP IT AL UMM Smart Centre.

2.2 Kriptografi

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan dengan aman kepada penerima. Istilah kriptografi berasal dari kata-kata Yunani cryptos dan graphia, yang berarti "penulisan rahasia" [8]. Dalam kriptografi, terdapat lima tujuan utama, yang juga merupakan elemen keamanan data. Yaitu, *Privacy* (privasi)/ *Confidentiality* (kerahasiaan), *Integrity* (integritas), *Authenticity* (keaslian), *Availability* (ketersediaan), dan *Access Control* (kontrol akses) [9]. Algoritma kriptografi dibagi menjadi dua jenis berdasarkan kuncinya, yaitu algoritma simetris dan algoritma asimetris [10].

a. Algoritma simetris
   Berikut adalah algoritma yang menggunakan kunci simetris diantaranya adalah:
   1. *Data Encryption Standart* (DES).
   2. RC2, RC4, RC5, RC6.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. *International Data Encryption Algorithm* (IDEA).
4. *Anvanced Encryption Standart* (AES).
5. *One Time Pad* (OTP).

b. Algoritma asimetris
1. *Digital Signature Algorithm* (DSA).
2. *Rivest Shamir Adleman* (RSA).
3. *Diffie-Hellman* (DH).

Elliptic Curve Cryptography (ECC).

2.3 Rivest Shamir Adleman

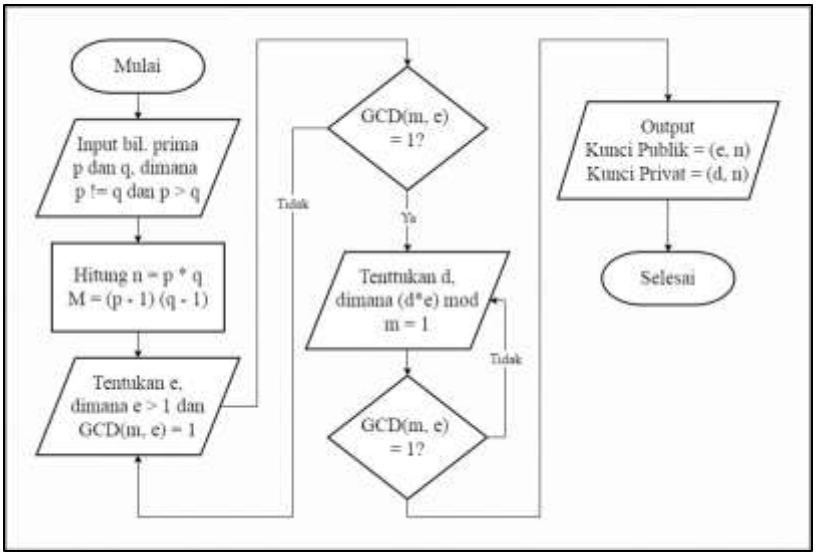
Menurut Ginting, Isnanto, dan Windasari dalam [11] RSA adalah algoritma kriptografi kunci publik yang ditemukan pada 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. RSA menggunakan dua kunci: kunci rahasia dan kunci publik. Enkripsi dan dekripsi RSA didasarkan pada bilangan prima dan aritmetika modulo. Kunci dekripsi bersifat rahasia, sedangkan kunci enkripsi disebut kunci publik. Algoritma RSA kuat karena proses eksponensialnya dan pemfaktoran bilangan nonprima. Penemunya mengusulkan dua faktor prima lebih dari 100 digit, sehingga hasil kalinya lebih dari 200 digit. Dengan algoritma pemfaktoran tercepat, Rivest dan kawan-kawan mengatakan butuh 4 milyar tahun untuk menemukan faktor bilangan 200 digit. Hingga kini, belum ada algoritma yang berhasil memfaktorkan bilangan besar, sehingga RSA tetap digunakan [12].

2.3.1 Tahapan Algoritma RSA

Algoritma RSA terdiri dari tiga tahap yaitu tahap pembangkitan kunci, tahap enkripsi dan dekripsi pesan. Berikut merupakan tahapan dari algoritma RSA.

a. Pembangkitan Kunci

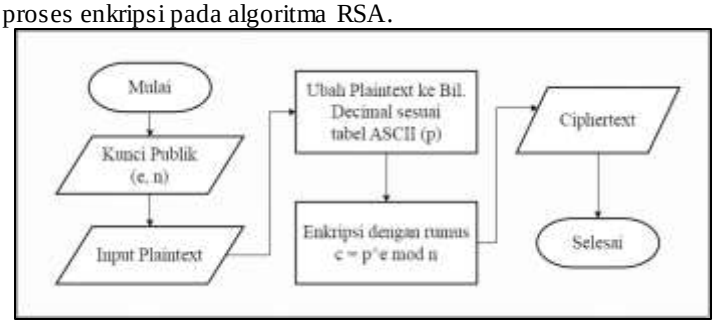
Proses pembangkitan kunci RSA adalah langkah-langkah yang dilakukan untuk menghasilkan sepasang kunci, yaitu kunci publik dan kunci privat, yang digunakan dalam algoritma enkripsi RSA. Berikut adalah *Flowchart* dari proses pembangkitan kunci RSA.



Gambar 1. *Flowchart* Pembangkitan Kunci

b. Enkripsi

Proses enkripsi merupakan proses untuk mengubah informasi atau data menjadi bentuk yang tidak dapat dibaca atau dimengerti tanpa kunci atau metode khusus. Proses enkripsi pada algoritma RSA menggunakan kunci publik. Berikut adalah *Flowchart* dari proses enkripsi pada algoritma RSA.

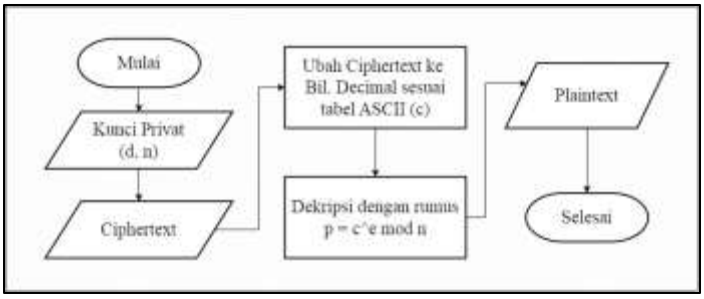


Gambar 2. *Flowchart* Enkripsi

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

c. Dekripsi

Proses Dekripsi adalah proses untuk mengembalikan *ciphertext* kedalam bentuk aslinya. Berikut adalah *Flowchart* dari proses dekripsi pada algoritma RSA.



Gambar 3. *Flowchart* Dekripsi

2.4 QR Code

QR Code adalah simbol dua dimensi yang pertama kali dikembangkan oleh Denso Wave, anak perusahaan Toyota. Tujuan dari QR Code ini adalah untuk menyampaikan informasi dan mendapatkan respons secara cepat. Untuk pertama kalinya, QR Code ini digunakan dalam proses pelacakan (sparepart) komponen kendaraan selama proses pembuatan kendaraan. Namun, seiring dengan peningkatan pengguna telepon seluler, QR Code telah digunakan di berbagai bidang bisnis. QR Code adalah versi baru dari barcode yang telah ada sebelumnya. Barcode memiliki kelemahan dimana barcode hanya dapat menyimpan informasi secara horizontal, sedangkan QR Code dapat menyimpan lebih banyak informasi baik secara horizontal maupun vertikal [13].

3. HASIL DAN PEMBAHASAN

3.1 Perhitungan Algoritma RSA

Perhitungan algoritma RSA ini merupakan penjelasan langkah-langkah penyelesaian masalah dalam dalam memverifikasi keaslian dokumen ijazah di SMP IT AL UMM Smart Centre. Berikut adalah langkah yang akan dilakukan dalam perhitunga RSA.

a. Pembangkita Kunci

Berikut adalah langkah-langkah dalam proses pembangkitan kunci RSA.

1. Pilih dua buah bilangan prima p dan q, $p \neq q$. Misal, p = 23, dan q = 17.
2. Hitung n = p * q
   n = 23 * 17
   n = 391
3. Hitung m = (p – 1) (q – 1)
   m = (23 – 1) (17 – 1)
   m = (22) (16)
   m = 352
4. Pilih nila e dengan syarat e > 1 dan GCD(m,e) = 1
   Nilai e yang diambil adalah 23.
   Bukti GCD(352, 23) = 1
   352 mod 23 = 7
   23 mod 7 = 2
   7 mod 2 = 1
   2 mod 1 = 0
5. Hitung d dengan persamaan (d * e) mod m = 1
   d * 23 mod 352 = 1
   d = 199
   Bukti : 199 * 23 mod 352 = 1
   Sehingga pasangan kunci yang didapatkan adalah
   Kunci enkripsi (public key) (e, n) = (23, 391) dan
   Kunci dekripsi (private key) (d, n) = (199, 391)

b. Enkripsi

Proses enkripsi adalah teknik untuk mengubah informasi atau data menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh orang yang tidak memiliki kunci atau kode yang benar. Pada proses enkripsi ini pesan yang akan dienkripsi adalah tanda tangan digital. Sebagai contoh yaitu, SMP/2022/000005/ANDREA/MARAMUDA.

Sebelum melakukan enkripsi, pesan tersebut diubah terlebih dahulu menjadi bilangan decimal berdasarkan table ASCII.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Tabel 1. Karakter untuk dienkripsi

P_i	Plaintext	Decimal	P_i	Plaintext	Decimal
1	S	83	17	A	65
2	M	77	18	N	78
3	P	80	19	D	68
4	/	47	20	R	82
5	2	50	21	E	69
6	0	48	22	A	65
7	2	50	23	/	47
8	2	50	24	M	77
9	/	47	25	A	65
10	0	48	26	R	82
11	0	48	27	A	65
12	0	48	28	M	77
13	0	48	29	U	85
14	0	48	30	D	68
15	5	53	31	A	65
16	/	47			

Selanjutnya karakter pada tabel 1 dienkripsi dengan rumus $C_i = P_i{}^e \ mod \ n$ dengan kunci enkripsi (e, n) = (23, 391). Berikut adalah hasil perhitungan *ciphertext*-nya.

$C_1 = 83^{23} \ mod \ 391 = 382$
$C_2 = 77^{23} \ mod \ 391 = 376$
$C_3 = 80^{23} \ mod \ 391 = 126$
$C_4 = 47^{23} \ mod \ 391 = 208$
$C_5 = 50^{23} \ mod \ 391 = 50$
$C_6 = 48^{23} \ mod \ 391 = 278$
$C_7 = 50^{23} \ mod \ 391 = 50$
$C_8 = 50^{23} \ mod \ 391 = 50$
$C_9 = 47^{23} \ mod \ 391 = 208$
$C_{10} = 48^{23} \ mod \ 391 = 278$
$C_{11} = 48^{23} \ mod \ 391 = 278$
$C_{12} = 48^{23} \ mod \ 391 = 278$
$C_{13} = 48^{23} \ mod \ 391 = 278$
$C_{14} = 48^{23} \ mod \ 391 = 278$
$C_{15} = 53^{23} \ mod \ 391 = 145$
$C_{16} = 47^{23} \ mod \ 391 = 208$
$C_{17} = 65^{23} \ mod \ 391 = 295$
$C_{18} = 78^{23} \ mod \ 391 = 124$
$C_{19} = 68^{23} \ mod \ 391 = 68$
$C_{20} = 82^{23} \ mod \ 391 = 312$
$C_{21} = 69^{23} \ mod \ 391 = 69$
$C_{22} = 65^{23} \ mod \ 391 = 295$
$C_{23} = 47^{23} \ mod \ 391 = 208$
$C_{24} = 77^{23} \ mod \ 391 = 376$
$C_{25} = 65^{23} \ mod \ 391 = 295$
$C_{26} = 82^{23} \ mod \ 391 = 312$
$C_{27} = 65^{23} \ mod \ 391 = 295$
$C_{28} = 77^{23} \ mod \ 391 = 376$
$C_{29} = 85^{23} \ mod \ 391 = 85$
$C_{30} = 68^{23} \ mod \ 391 = 68$
$C_{31} = 65^{23} \ mod \ 391 = 295$

Setelah dilakukan perhitungan, hasil enkripsi dengan algoritma RSA diubah kedalam bilangan hexadecimal untuk dijadikan tanda tangan digital. Berikut adalah tabel hasil enkripsinya.

Tabel 2. Hasil Enkripsi

Plaintext	Encrypt	Hexa	Plaintext	Encrypt	Hexa
83	382	17E	65	295	127
77	376	178	78	124	7C
80	126	7E	68	68	44
47	208	D0	82	312	138
50	50	32	69	69	45
48	278	116	65	295	127
50	50	32	47	208	D0
50	50	32	77	376	178
47	208	D0	65	295	127
48	278	116	82	312	138
48	278	116	65	295	127
48	278	116	77	376	178
48	278	116	85	85	55
48	278	116	68	68	44
53	145	91	65	295	127
47	208	D0			

c. Dekripsi

Proses dekripsi adalah langkah untuk mengubah data atau informasi yang telah dienkripsi kembali ke bentuk asalnya sehingga teks dapat dibaca dan dimengerti. Pada proses dekripsi ini *ciphertext* yang akan didekripsi adalah. 17E, 178, 7E, D0, 32, 116, 32, 32, D0, 116, 116, 116, 116, 116, 91, D0, 127, 7C, 44, 138, 45, 127, D0, 178, 127, 138, 127, 178, 55, 44, 127.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Sebelum melakukan dekripsi, *ciphertext* tersebut diubah terlebih dahulu menjadi bilangan *decimal* berdasarkan table ASCII.

Tabel 3. Karakter untuk didekripsi

C_i	Ciphertext	Decimal	C_i	Ciphertext	Decimal
1	17E	382	17	127	295
2	178	376	18	7C	124
3	7E	126	19	44	68
4	D0	208	20	138	312
5	32	50	21	45	69
6	116	278	22	127	295
7	32	50	23	D0	208
8	32	50	24	178	376
9	D0	208	25	127	295
10	116	278	26	138	312
11	116	278	27	127	295
12	116	278	28	178	376
13	116	278	29	55	85
14	116	278	30	44	68
15	91	145	31	127	295
16	D0	208			

Selanjutnya karakter pada tabel 3 didekripsi dengan rumus $P_i = {C_i}^d \ mod \ n$ dengan kunci enkripsi (d, n) = (199, 391). Berikut adalah hasil perhitungan *plaintext*-nya.

$P_1 = 382^{199} \ mod \ 391 = 83$
$P_2 = 376^{199} \ mod \ 391 = 77$
$P_3 = 126^{199} \ mod \ 391 = 80$
$P_4 = 208^{199} \ mod \ 391 = 47$
$P_5 = 50^{199} \ mod \ 391 = 50$
$P_6 = 278^{199} \ mod \ 391 = 48$
$P_7 = 50^{199} \ mod \ 391 = 50$
$P_8 = 50^{199} \ mod \ 391 = 50$
$P_9 = 208^{199} \ mod \ 391 = 47$
$P_{10} = 278^{199} \ mod \ 391 = 48$
$P_{11} = 278^{199} \ mod \ 391 = 48$
$P_{12} = 278^{199} \ mod \ 391 = 48$
$P_{13} = 278^{199} \ mod \ 391 = 48$
$P_{14} = 278^{199} \ mod \ 391 = 48$
$P_{15} = 145^{199} \ mod \ 391 = 53$
$P_{16} = 208^{199} \ mod \ 391 = 47$
$P_{17} = 295^{199} \ mod \ 391 = 65$
$P_{18} = 124^{199} \ mod \ 391 = 78$
$P_{19} = 68^{199} \ mod \ 391 = 68$
$P_{20} = 312^{199} \ mod \ 391 = 82$
$P_{21} = 69^{199} \ mod \ 391 = 69$
$P_{22} = 295^{199} \ mod \ 391 = 65$
$P_{23} = 208^{199} \ mod \ 391 = 47$
$P_{24} = 376^{199} \ mod \ 391 = 77$
$P_{25} = 295^{199} \ mod \ 391 = 65$
$P_{26} = 312^{199} \ mod \ 391 = 82$
$P_{27} = 295^{199} \ mod \ 391 = 65$
$P_{28} = 376^{199} \ mod \ 391 = 77$
$P_{29} = 85^{199} \ mod \ 391 = 85$
$P_{30} = 68^{199} \ mod \ 391 = 68$
$P_{31} = 295^{199} \ mod \ 391 = 65$

Setelah dilakukan dekripsi, hasil dekripsi diubah kedalam *character* berdasarkan tabel ASCII untuk mendapatkan pesan aslinya. Berikut adalah tabel hasil dekrispi.

Tabel 4. Hasil Dekripsi

Ciphertext	Decrypt	Char	Ciphertext	Decrypt	Char
382	83	S	295	65	A
376	77	M	124	78	N
126	80	P	68	68	D
208	47	/	312	82	R
50	50	2	69	69	E
278	48	0	295	65	A
50	50	2	208	47	/
50	50	2	376	77	M
208	47	/	295	65	A
278	48	0	312	82	R
278	48	0	295	65	A
278	48	0	376	77	M
278	48	0	85	85	U
278	48	0	68	68	D
145	53	5	295	65	A
208	47	/			

Berdasarkan hasil dekripsi pada tabel 4 didapat pesan aslinya adalah, SMP/2022/000005/ANDREA/MARAMUDA.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3.2 Penerapan QR Code

Pada proses ini, informasi yang akan disimpan kedalam *qr code* adalah tanda tangan digital yang dihasilkan dari algoritma RSA pada proses sebelumnya. Berikut adalah tanda tangan digital yang akan disimpan kedalam *qr code*. 17E1787ED0321163232D011611611611611691D01277C4413845127D017812713812717855441 27. Maka hasil penerapan *qr code* dari tanda tangan digital tersebut adalah.

Gambar 4. QR Code Hasil Enkripsi

3.3 Implementasi Sistem

a. Halaman Utama

Halaman Utama adalah tampilan pertama saat aplikasi dijalankan. Halaman ini memungkinkan pengguna mengunggah gambar QR Code untuk verifikasi keaslian ijazah. Berikut adalah tampilan antarmuka dari Halaman Utama.

Gambar 5. Tampilan Halaman Utama

b. Halaman Verifikasi

Halaman Verifikasi merupakan halaman untuk pengguna melakukan verifikasi ijazah dengan QR Code yang telah di-upload sebelumnya. Berikut tampilan antarmuka dari halaman verifikasi.

Gambar 6. Tampilan Halaman Verifikasi

c. Halaman Login

Halaman Login merupakan halaman untuk pengguna melakukan aktifitas login dimana login menjadi syarat untuk dapat mengakses halaman Dashboard. Berikut tampilan antarmuka dari halaman login.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Gambar 7. Tampilan Halaman Login

d. Halaman Dashboard
Halaman Dashboard merupakan halaman yang menampilkan informasi terkait data yang dimiliki sistem. Berikut tampilan antarmuka dari halaman dashboard.

Gambar 8. Tampilan Halaman Dashboard

e. Halaman Data Kunci
Halaman Data Kunci merupakan halaman yang berfungsi untuk menampilkan seluruh data kunci yang terdapat didalam *database*. Berikut tampilan antarmuka dari halaman data kunci.

Gambar 9. Halaman Data Kunci

f. Halaman Input Data Kunci
Halaman Input Data Kunci merupakan halaman untuk admin melakukan penambahan data kunci. Berikut tampilan antarmuka dari halaman input data kunci.

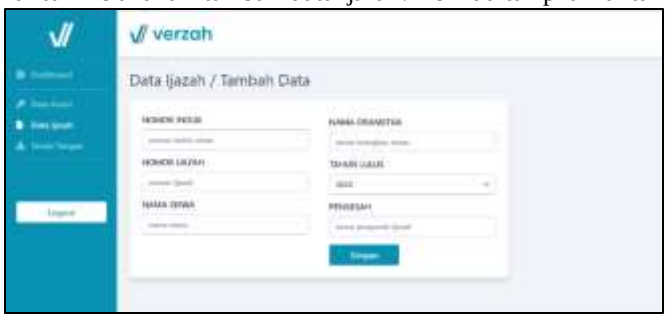
Gambar 10. Halaman Input Data Kunci

g. Halaman Data Ijazah
Halaman Data Ijazah merupakan halaman yang berfungsi menampilkan kesuluruhan data ijazah. Berikut tampilan antarmuka dari halaman data ijazah.

Gambar 11. Halaman Data Ijazah

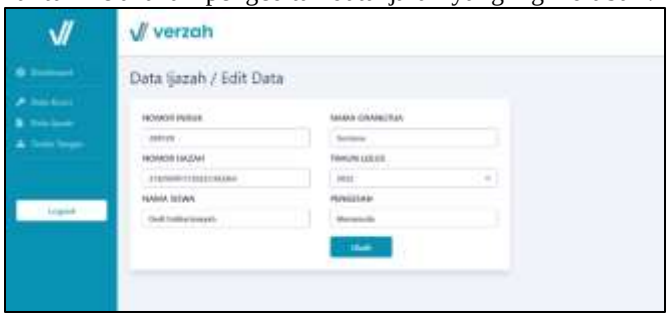
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 7 ; Nomor 2 ; Juli 2024 ; Page 246-256
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

h. Halaman Input Data Ijazah
Halaman ini berfungsi untuk melakukan tambah data ijazah. Berikut tampilan antarmuka halaman data ijazah.



Gambar 12. Halaman Input Data Ijazah

i. Halaman Edit Data Ijazah
Halaman ini berfungsi untuk melakukan pengeditan data ijazah yang ingin diubah.

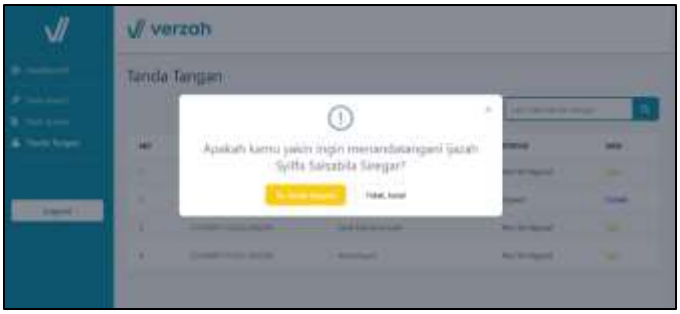


Gambar 13. Halaman Edit Data Ijazah

j. Halaman Tanda Tangan
Halaman Tanda Tangan merupakan halaman yang menampilkan kesuluruhan data ijazah yang telah ditanda tangani, didalam halaman ini juga dapat melakukan tanda tangan digital terhadap data ijazah yang belum ditanda tangani. Berikut tampilan halaman tanda tangan.

Gambar 14. Halaman Tanda Tangan

Tombol *Sign* berfungsi untuk menampilkan modal validasi bahwasannya data ijazah yang dipilih akan ditanda tangani.



Gambar 15. Tampilan Modal Validasi Tanda Tangan

k. Halaman Detail Tanda Tangan
Halaman ini akan menyajikan informasi dari data ijazah yang sudah dilakukan tanda tangan digital dan juga dapat melakukan unduh *QR Code*. Berikut tampilan halaman detail tanda tangan.

Gambar 16. Halaman Detail Tanda Tangan

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem verifikasi keaslian ijazah berbasis QR Code dan algoritma RSA. Sistem yang dihasilkan efektif dalam memastikan keamanan dan keaslian ijazah dengan cara mengenkripsi data ijazah dan menghasilkan QR Code yang hanya dapat diverifikasi oleh pihak yang berwenang. Pengujian sistem menunjukkan bahwa metode ini mampu mencegah pemalsuan ijazah dan memberikan tingkat keamanan yang tinggi. Dengan demikian, sistem ini dapat meningkatkan kepercayaan terhadap institusi pendidikan dan diharapkan dapat diterapkan secara luas untuk menjaga integritas dokumen pendidikan di berbagai tingkat. Penelitian ini juga membuka peluang untuk pengembangan lebih lanjut dalam meningkatkan keamanan dokumen dengan teknologi lainnya.

UCAPAN TERIMA KASIH

Terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah memberikan dukungan dan kontribusi dalam penyelesaian penelitian ini. Terima kasih kepada Allah SWT atas rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Ucapan terima kasih yang tulus juga disampaikan kepada keluarga tercinta atas doa, dukungan, dan motivasi yang tiada henti. Penulis berterima kasih kepada pembimbing skripsi yang telah memberikan bimbingan, arahan, dan saran berharga selama proses penelitian ini. Penghargaan yang setinggi-tingginya diberikan kepada SMP IT AL UMM Smart Centre. Penulis menyadari bahwa penelitian ini masih jauh dari sempurna, oleh karena itu saran dan kritik yang membangun sangat diharapkan untuk perbaikan di masa mendatang.

DAFTAR PUSTAKA

[1] M. Agung, "Direktori Putusan." https://putusan3.mahkamahagung.go.id/search.html?q=%22Pemalsuan+Ijazah%22

[2] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," vol. 4, no. 3, pp. 110–115, 2018.

[3] P. Purwadi, "Implementasi Kriptografi Merkle Hellman Dalam Mengamankan Data Nilai Siswa Smk Wira Kesuma Jaya Kec. Namo Rambe," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 4, no. 1, pp. 56–68, 2021, doi: 10.53513/jsk.v4i1.2612.

[4] V. No, J. Hal, K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," vol. 2, no. 1, pp. 6–11, 2023.

[5] I. Ramdhani, M. Khotib Arifai, J. Raya Puspitek Serpong No, and T. Selatan, "PERANCANGAN SISTEM PENGESAHAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITME RSA," *J. Ilmu Komput. JIK*, vol. 46, p. 2022, [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2013

[6] Yansiska and A. N. Utomo, "Pengamanan Data Digital Signature Dengan Menggunakan Metode Algoritma RSA dan Hash," *Incomtech*, vol. 12, no. 1, pp. 44–54, 2023.

[7] S. Alfarizi, A. R. Mulyawan, D. Gunawan, and R. Aryanti, "IMPLEMENTASI UNIFIED MODELLING LANGUAGE PADA SISTEM INFORMASI NASGOR DELIVERY BERBASIS WEB," *J. INTERKOM*, vol. 15, no. 2, pp. 42–52, 2020.

[8] E. V. Waruwu, N. B. Nugroho, and F. Sonata, "Penerapan Digital Signature Menggunakan Metode Rsa Untuk Menvalidasi Keaslian Ijazah Sma Swasta Bina Artha," *J. CyberTech*, vol. 1, no. 1, pp. 37–47, 2021.

[9] M. I. Afandi and N. Nurhayati, "Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android," *It (Informatic Tech. J.*, vol. 8, no. 1, pp. 30–41, 2020, doi: 10.22303/it.8.1.2020.30-41.

[10] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[11] A. Rifa'i and L. C. Sumartini, "Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-

Based," *J. E-Komtek*, vol. 3, no. 2, pp. 87–96, 2019, doi: 10.37339/e-komtek.v3i2.133.

[12] A. Cahya Putra, M. Simanjuntak, and Nurhayati, "PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH)," *J. Tek. Inform. Kaputama*, vol. 5, no. 1, pp. 76–84, 2021.

[13] N. Berliano Novanka Putra, F. Amalia Raihana, W. Michael Albert Mondong, and A. Rosadi Kardian, "Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 1, pp. 142–154, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik