JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Aplikasi Verifikator E-Sertifikat Seminar Oleh HIMSI TGD Berbasis QR Code Menggunakan Algoritma RSA

Luthfi Halim[1],Mhd. Gilang Suryanata[2], Usti Fatimah Sari Sitorus Pane[3]

[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]luthfihalim123@gmail.com, [2]suryanatagilang@gmail.com, [3]ustipaneee@gmail.com
Email Penulis Korespondensi: luthfihalim123@gmail.com

Abstrak
Seiring kemajuan teknologi digital, e-sertifikat semakin banyak digunakan sebagai bukti partisipasi dalam kegiatan akademik, namun juga rentan terhadap pemalsuan yang dapat merusak reputasi penyelenggara. Untuk mengatasi masalah ini, penelitian ini mengembangkan aplikasi web verifikasi e-sertifikat menggunakan QR Code dan algoritma kriptografi RSA sebagai tanda tangan digital, yang hasil enkripsinya dikonversi ke format heksadesimal dan disisipkan dalam QR Code. Sistem dikembangkan dengan model Waterfall melalui tahapan analisis, desain, implementasi, pengujian, dan penerapan. Hasil pengujian menunjukkan bahwa aplikasi mampu memverifikasi keaslian e-sertifikat secara efisien, akurat, dan aman, sehingga mendukung HIMSI STMIK Triguna Dharma dalam meningkatkan keamanan, mencegah pemalsuan, dan memperkuat kepercayaan terhadap validitas sertifikat yang diterbitkan.
Kata Kunci: E-Sertifikat, Kriptografi, RSA, QR Code, Tanda Tangan Digital, Verifikasi

Abstract
With the advancement of digital technology, e-certificates are increasingly used as proof of participation in academic activities, but they are also vulnerable to forgery, which can harm the reputation of organizers. To address this issue, this study developed a web-based application for verifying e-certificates using QR Code technology and the RSA cryptographic algorithm as a digital signature, where the encryption result is converted into hexadecimal format and embedded in the QR Code. The system was developed using the Waterfall model, encompassing the stages of requirement analysis, design, implementation, testing, and deployment. Test results show that the application can efficiently, accurately, and securely verify the authenticity of e-certificates, thereby helping HIMSI STMIK Triguna Dharma enhance certificate security, prevent forgery, and strengthen trust in the validity of issued certificates.
Keywords: *E-Certificate, Cryptography, RSA, QR Code, Digital Signature, Verification*

1. PENDAHULUAN

Sertifikat seminar merupakan dokumen resmi yang diberikan kepada peserta sebagai bukti keikutsertaan dalam suatu kegiatan, dan sering dijadikan dokumen pendukung dalam portofolio akademik maupun profesional. Seiring perkembangan teknologi, sertifikat kini banyak diterbitkan dalam format digital (e-sertifikat), yang memberikan kemudahan dalam proses distribusi dan verifikasi. Namun, penggunaan e-sertifikat juga menimbulkan risiko pemalsuan dokumen, yang dapat mengurangi kepercayaan terhadap penyelenggara acara, terutama di lingkungan perguruan tinggi.

Perguruan tinggi merupakan institusi yang aktif dalam menyelenggarakan seminar ilmiah, biasanya melibatkan dosen dan mahasiswa melalui organisasi kemahasiswaan [1]. Salah satu organisasi yang aktif di STMIK Triguna Dharma adalah Himpunan Mahasiswa Sistem Informasi (HIMSI). HIMSI memandang serius potensi penyalahgunaan e-sertifikat, karena dapat merusak reputasi lembaga dan nilai akademik dari kegiatan yang diselenggarakan. Untuk itu, dibutuhkan sistem keamanan yang mampu menjamin keaslian e-sertifikat secara digital.

Kriptografi adalah seni dan ilmu dalam menyandikan pesan sehingga tidak dapat dimengerti oleh pihak yang tidak berwenang. Metode ini berfungsi untuk melindungi kerahasiaan informasi. Isu keamanan data menjadi fokus utama dalam kriptografi[2] Setelah melalui tahap penyandian, teks terbuka akan berubah menjadi teks tersandi (ciphertext) yang tidak dapat dibaca secara langsung[3].

Sebagai solusi, penelitian ini mengusulkan sistem verifikasi e-sertifikat berbasis QR Code dan algoritma kriptografi RSA. QR Code digunakan sebagai media penyisipan digital signature hasil enkripsi, yang memastikan keabsahan e-sertifikat. RSA dipilih karena menggunakan dua kunci, yaitu public key dan private key[4]. Serta memiliki tingkat keamanan tinggi melalui konsep faktorisasi bilangan prima. Metode ini melindungi kerahasiaan data dan mencegah sertifikat dari pemalsuan [5].

2. METODOLOGI PENELITIAN

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

1. Observasi

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Pengamatan dilakukan di kampus Triguna Dharma (TGD) dengan menganalisis masalah yang dihadapi terkait dalam mengamankan dokumen e-sertifikat seminar terutama yang dikeluarkan oleh HIMSI TGD. Analisis kebutuhan sistem dilakukan terhadap permasalahan yang dihadapi sebagai dasar untuk membangun model sistem yang sesuai.

2. Wawancara
   Wawancara berfungsi sebagai metode untuk memverifikasi informasi yang telah dikumpulkan sebelumnya. Dalam penelitian ini, wawancara dilakukan secara langsung melalui tatap muka dan sesi tanya jawab dengan Saudara Aqil Sahri selaku BPH HIMSI TGD. Tahapan ini dilakukan guna memetakan alur kerja objek penelitian sebagai landasan perancangan fitur sistem.
3. Studi Pustaka
   Studi pustaka dilakukan melalui pengumpulan referensi-referensi ilmiah terkait autentikasi dokumen, algoritma RSA, dan sistem kriptografi. Sumber-sumber referensi yang diperoleh dari berbagai jurnal akademik diharapkan dapat memberikan solusi terhadap permasalahan autentikasi yang dihadapi oleh HIMSI TGD.

2.2 Kriptografi

Kriptografi berasal dari bahasa yunani *Cryptos* yang berarti rahasia dan *Graphein* yang berarti menulis, maka dari itu Kriptografi berarti "penulisan rahasia"[6]. Kriptografi terbagi dua berdasarkan kuncinya, yaitu kriptografi simetris dan asimetris[7]. Kriptografi simetris merupakan sebuah algoritma kriptografi yang dalam proses enkripsi dan dekripsi hanya menggunakan satu kunci[8]. Kriptografi asimetris merupakan sebuah algoritma kriptografi yang menggunakan dua kunci yang berbeda, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi[9].

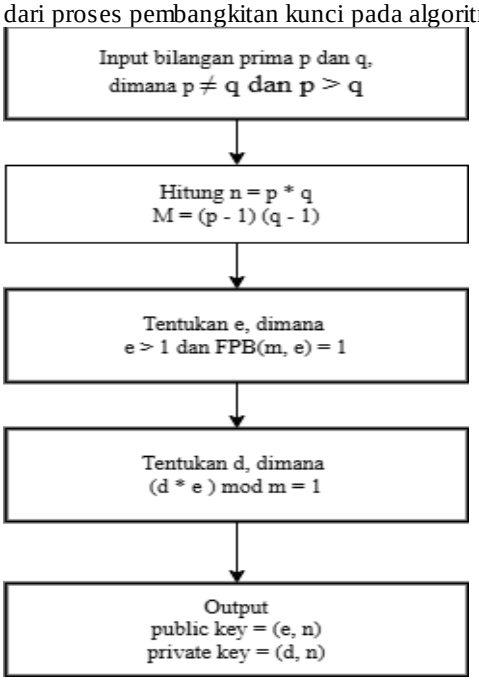
2.3 Rivest Shamir Adlemen

Menurut Ginting, Isnanto dan Windasari pada[10] RSA adalah algoritma kriptografi dengan kunci publik (asimetris) yang pertama kali ditemukan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Keamanan algoritma RSA berakar pada kesulitan dalam memecahkan masalah matematika tertentu, yakni memfaktorkan bilangan bulat besar menjadi faktor prima penyusunnya. Para penemu RSA menyarankan penggunaan bilangan prima yang sangat besar untuk menghasilkan kunci enkripsi yang sulit dipecahkan. Mereka memperkirakan bahwa membobol kunci RSA dengan panjang 200 digit akan membutuhkan waktu yang sangat lama, bahkan dengan komputer tercepat sekalipun. Hingga kini, belum ada metode yang cukup efisien untuk mengatasi tantangan ini. Oleh karena itu, RSA tetap menjadi pilihan yang populer dalam sistem keamanan pesan[11].

2.3.1 Tahapan Algoritma RSA

Pada penelitian ini terdapat dua tahapan pada algoritma RSA, yaitu sebagai berikut:

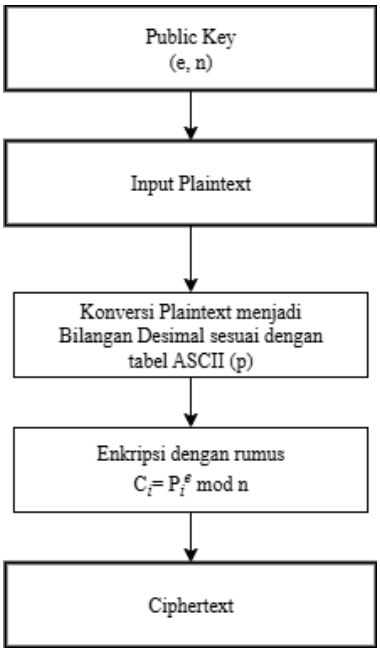
a. Pembangkitan Kunci
   Berikut adalah kerangka metode dari proses pembangkitan kunci pada algoritma RSA.



Gambar 1. Pembangkitan Kunci

b. Enkripsi
   Berikut adalah kerangka metode dari proses enkripsi kunci pada algoritma RSA.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi



Gambar 2. Enkripsi

2.4 Quick Response Code (QR Code)

QR *Code (Quick Response Code)* adalah jenis barcode dua dimensi yang pertama kali dikembangkan oleh perusahaan Jepang, Denso-Wave, pada tahun 1994. Awalnya, teknologi ini dirancang untuk mendukung sistem pendataan inventaris dalam industri otomotif, khususnya dalam melacak suku cadang kendaraan secara lebih efisien. Namun, seiring perkembangan teknologi, penggunaan QR *Code* semakin luas dan kini menjadi bagian penting dalam berbagai sektor, termasuk bisnis, jasa, pemasaran, serta promosi[12].

3. HASIL DAN PEMBAHASAN

3.1 Perhitungan Algoritma RSA

Perhitungan kriptografis berbasis algoritma RSA dirancang untuk melakukan verifikasi keaslian dokumen e-sertifikat seminar yang dikeluarkan oleh HIMSI TGD. Berikut langkah-langkah yang dilakukan dalam perhitungan.

1. Proses Pembangkitan Kunci

   Berikut merupakan langkah-langkah yang dilakukan dalam membangitkan kunci algoritma RSA

   a. Pilih dua bilangan prima p dan q, $p \neq q$.
      Misal,
      p = 11, dan q = 7.
   b. Hitung n = p * q
      n = 11 * 7
      n = 77
   c. Hitung m = (p – 1) (q – 1)
      m = (11 – 1) (7 – 1)
      m = (10) (6)
      m = 60
   d. Pilih nilai e dengan syarat e > 1 dan FPB(m, e) = 1
      Nilai e yang diambil adalah 7
      Pembuktian FPB(60, 7) =1
      60 mod 7 = 4
      7 mod 4 = 3
      4 mod 3 = 1
      3 mod 1 = 0
   e. Hitung d dengan persamaan (d * e) mod m =1
      d * 7 mod 60 = 1
      d = 43
      Pembuktian 43 * 7 mod 60 = 1

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

301 mod 60 = 1
Sehingga pasangan kunci yang didapatkan adalah
Kunci publik (e, n) = (7, 77) dan
Kunci privat (d, n) = (43, 77)

2. Enkripsi

Proses enkripsi merupakan sebuah metode dalam mentransformasikan pesan asli (plaintext) menjadi bentuk tersandi (ciphertext) yang tidak dapat dipahami tanpa kunci dekripsi yang valid. Dalam konteks ini, objek yang dienkripsi adalah tanda tangan digital. Sebagi contoh yaitu, HIMSI/026/2024-11-16/Angga/Kamil.

Sebelum melakukan enkripsi, pesan tersebut akan diubah terlebih dahulu menjadi bilangan desimal berdasarkan tabel ASCII.

Tabel 1. Karakter yang akan di enkripsi

Pi	*Plaintext*	*Decimal*	Pi	*Plaintext*	*Decimal*
1	H	72	17	1	49
2	I	73	18	-	45
3	M	77	19	1	49
4	S	83	20	6	54
5	I	73	21	/	47
6	/	47	22	A	65
7	0	48	23	n	110
8	2	50	24	g	103
9	6	54	25	g	103
10	/	47	26	a	97
11	2	50	27	/	47
12	0	48	28	K	75
13	2	50	29	a	97
14	4	52	30	m	109
15	-	45	31	i	105
16	1	49	32	l	108

Selanjutnya, karakter dari tabel 3.1 akan dienkripsi dengan menggunakan rumus $C_i = P_i^e \bmod n$. Dengan kunci publik (e, n) = (7, 77). Berikut adalah hasil perhitungan *ciphertext*-nya.

$C1 = 72^7 \bmod 77 = 30$
$C2 = 73^7 \bmod 77 = 17$
$C3 = 77^7 \bmod 77 = 0$
$C4 = 83^7 \bmod 77 = 41$
$C5 = 73^7 \bmod 77 = 17$
$C6 = 47^7 \bmod 77 = 75$
$C7 = 48^7 \bmod 77 = 27$
$C8 = 50^7 \bmod 77 = 8$
$C9 = 54^7 \bmod 77 = 54$
$C10 = 47^7 \bmod 77 = 75$
$C11 = 50^7 \bmod 77 = 8$
$C12 = 48^7 \bmod 77 = 27$
$C13 = 50^7 \bmod 77 = 8$
$C14 = 52^7 \bmod 77 = 24$
$C15 = 45^7 \bmod 77 = 45$
$C16 = 49^7 \bmod 77 = 14$
$C17 = 49^7 \bmod 77 = 14$
$C18 = 45^7 \bmod 77 = 45$
$C19 = 49^7 \bmod 77 = 14$
$C20 = 54^7 \bmod 77 = 54$
$C21 = 47^7 \bmod 77 = 75$
$C22 = 65^7 \bmod 77 = 41$
$C23 = 110^7 \bmod 77 = 33$
$C24 = 103^7 \bmod 77 = 5$
$C25 = 103^7 \bmod 77 = 5$
$C26 = 97^7 \bmod 77 = 48$
$C27 = 47^7 \bmod 77 = 75$
$C28 = 75^7 \bmod 77 = 26$
$C29 = 97^7 \bmod 77 = 48$
$C30 = 109^7 \bmod 77 = 32$
$C31 = 105^7 \bmod 77 = 63$
$C32 = 108^7 \bmod 77 = 59$

Setelah melakukan enkripsi dengan menggunakan algoritma RSA, ubah hasil enkripsi yang masih berbentuk bilangan desimal menjadi bentuk bilangan hexadesimal untuk dijadikan tanda tangan digital. Berikut adalah tabel hasil konversinya.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Plaintext (*decimal*)	*Ciphertext* (*decimal*)	*Hexadecimal*	Plaintext (*decimal*)	*Ciphertext* (*decimal*)	*Hexadecimal*
72	30	1E	49	14	0E
73	17	11	45	45	2D
77	0	00	49	14	0E
83	41	29	54	54	36
73	17	11	47	75	4B
47	75	4B	65	65	41
48	27	1B	110	33	21
50	8	08	103	5	05
54	54	36	103	5	05
47	75	4B	97	48	30
50	8	08	47	75	4B
48	27	1B	75	26	1A
50	8	08	97	48	30
52	24	18	109	32	20
45	45	2D	105	63	3F
49	14	0E	108	59	3B

3.2 Penerapan QR Code

Pada implementasi sistem ini, QR code berfungsi sebagai media penyimpanan untuk tanda tangan digital yang dihasilkan melalui komputasi kriptografis menggunakan algoritma RSA. Nilai tanda tangan digital yang dienkapsulasi dalam QR code adalah.1E110029114B1B08364B081B0B182D0E0E2D0E364B41210505304B1A30203F3B. Maka hasil pembangkitan qr code dari tanda tangan digital tersebut adalah

Gambar 3. QR *Code* Hasil Tanda Tangan

3.3 Implementasi Sistem

Berikut ini merupakan implementasi dari rancangan antarmuka *(interface)* sistem yang telah dibuat, menampilkan tampilan serta fungsi sesuai dengan desain yang dirancang sebelumnya:

1. Halaman Utama

   Pada halaman ini pengguna dapat mengunggah dokumen e-sertifikat seminar yang telah dilakukan tanda tangan digital. Berikut adalah tampilan antarmuka halaman utama yang telah telah dibangun.

Gambar 4. Tampilan Halaman Utama

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

2. Halaman Hasil Verifikasi
Halaman ini menampilkan hasil verifikasi dokumen e-sertifikat seminar yang telah dilakukan tanda tangan digital. Berikut adalah tampilan antarmuka halaman hasil verifikasi yang telah dibangun.

Gambar 5. Tampilan Halaman Hasil Verifikasi

3. Halaman Login
Pada halaman ini, yang dapat login hanyalah pihak HIMSI TGD. Login dilakukan dengan menginput kolom username dan password yang sesuai. Berikut adalah tampilan antarmuka halaman login yang telah dibangun

Gambar 6. Tampilan Halaman Login

4. Halaman Dashboard
Pada halaman ini akan menampilkan jumlah data yang ada pada setiap halaman. Berikut adalah tampilan antarmuka halaman dashboard yang telah dibangun.

Gambar 7. Tampilan Halaman Dashboard

5. Halaman Data Kunci
Pada halaman ini menampilkan kunci publik dan privat yang sesuai dengan judul seminar yang diadakan. Pengguna juga dapat menambahkan kunci baru untuk seminar yang baru diadakan. Berikut adalah tampilan antarmuka halaman data kunci.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Gambar 8. Tampilan Halaman Data Kunci

6. Halaman Data E-Sertifikat
   Pada halaman ini menampilkan data e-sertifikat seminar berupa nomor e-sertifikat, judul, nama peserta. Pengguna juga dapat menambahkan data baru serta melakukan edit dan hapus data. Berikut adalah tampilan antarmuka halaman data e-sertifikat.

Gambar 9. Tampilan Halaman Data E-Sertifikat

7. Halaman Tanda Tangan
   Pada halaman ini menampilkan data e-sertifikat seminar yang telah dan belum dilakukan tanda tangan digital. Pengguna dapat melakukan tanda tangan digital dan juga melihat detail. Berikut adalah tampilan antarmuka halaman data e-sertifikat.

Gambar 10. Tampilan Halaman Tanda Tangan

4. KESIMPULAN

Aplikasi verifikator e-sertifikat seminar HIMSI TGD berhasil dirancang dan dibangun menggunakan algoritma RSA dalam bentuk web berbasis PHP dan MySQL. Sistem ini mampu mengenkripsi data sertifikat menjadi QR code dan melakukan verifikasi dengan mencocokkan ciphertext ke database secara akurat tanpa dekripsi langsung. Berdasarkan hasil pengujian dan implementasi, seluruh fitur berjalan sesuai rancangan dan sistem terbukti efektif dalam meningkatkan keamanan serta efisiensi proses validasi e-sertifikat secara digital.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 385-392
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

UCAPAN TERIMAKASIH

Terimakasih saya ucapkan kepada Allah Swt yang memberikan rahmat dan karunia sehingga saya mampu menyelesaikan jurnal ini. Kemudian saya ucapkan terimakasih kepada Bapak Mhd. Gilang Suryanata dan Ibu Usti Fatimah Sari Sitorus Pane atas arahan dan bimbingannya selama proses pengerjaan skripsi ini hingga sampai ketahap penyusunan jurnal. Tak lupa saya ucapkan terimakasih juga kepada orangtua, saudara dan sahabat saya tercinta atas supo rt dan dukungannya kepada saya sehingga saya dapat menyelesaikan jurnal ini.

DAFTAR PUSTAKA

[1] F. Nurlaila and J. Riyanto, "Rancang Bangun Sistem Informasi Kegiatan Penunjang Akademik di Universitas Pamulang," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 6, no. 1, pp. 48–56, 2022.

[2] B. Olivia *et al.*, "Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard (Aes) Cryptographic Implementation in Data Security Using Advanced Encryption Standard (Aes) Algorithm," *J. Simantec*, vol. 11, no. 2, pp. 167–174, 2023.

[3] C. Repi, J. Titaley, and E. Ketaren, "Implementasi Kriptografi Dalam Pengamanan Data Gambar Menggunakan Algoritma Rsa," *J. TIMES*, vol. 13, no. 1, pp. 93–99, 2024.

[4] J. Tamba, "Implementasi Algoritma RSA (Rivest Shamir Adleman) dalamPengaman File Video," *Inf. dan Teknol. Ilm.*, vol. 11, no. 2, pp. 65–72, 2024

[5] W. Wahyudi, D. Hartama, I. O. Kirana, S. Sumarno, and I. Gunawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun," *J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 57–66, 2022.

[6] C. Irawan and E. H. Rachmawanto, "Implementasi Kriptografi dengan Menggunakan Algoritma Arnold's Cat Map dan Henon Map," *J. Masy.Inform.*, vol. 13, no. 1, pp. 15–32, 2022.

[7] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *J. Teknol. Sist. Inf.*, vol. 4, no. 2, pp. 394–405, 2023.

[8] A. A. I. Ramadhan, E. Z. Rivanti, and R. S. Zulva, "Implementasi Kriptografi AES Menggunakan Bahasa Java Programming: Meningkatkan Keamanan Data Melalui Enkripsi & Dekripsi Yang Kuat," *J. Pendidik. Teknol. Inf.*, pp. 20–26, 2023.

[9] Y. Lubis, I. Rusydi, and A. H. Elyas, "Implementasi Algoritma Kriptografi Tanda Tangan Digital Qrcode Pada Dokumen Dengan Menggunakan Metode Riverst Shamir Adleman (RSA)," vol. 18, pp. 1429–1439, 2024.

[10] A. C. Putra, M. Simanjuntak, and N. Nurhayati, "Penerapan Algoritma Rivest Shamir Adleman (Rsa) Untuk Mengamankan Database Program Keluarga Harapan (Pkh)," *J. Inform. Kaputama*, vol. 5, no. 1, pp. 99–107, 2021.

[11] N. Berliano Novanka Putra, F. Amalia Raihana, W. Michael Albert Mondong, A. Rosadi Kardian, P. Siber dan Sandi Negara, and J. Barat, "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.

[12] R. Gunawan, A. M. Yusuf, and L. Nopitasari, "Rancang Bangun Sistem Presensi Mahasiswa Dengan Menggunakan Qr Code Berbasis Android," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 47–58, 2021.