JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

Implementasi Asimetris Kuantum dalam Kriptografi Modern untuk Enkripsi Data Satu Arah

Raihan Muzafi[1], Arif Abdillah[2], Ainul Marziah[3], Shaffanisa Aulia Rizky[4], Abdi Prizayanto[5*], Aisyah Nurhiqmah[6]
[1,2,3,4,5,6]Program Studi Sistem Informasi Universitas Malikussaleh,Indonesia
Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu, Kota Lhokseumawe, Aceh 24355 email:
[5]abdiprizayanto@gmail.com, [6]aisyah.220180034@mhs.unimal.ac.id [2]arif.220180138@mhs.unimal.ac.id

ABSTRACT

In a company, data security is very important. Data security and integrity issues must be considered to prevent information from falling into the hands of unauthorized persons. Therefore, a good mechanism is needed to secure data, which can be done through various cryptographic methods, which are generally divided into two categories: symmetric and asymmetric. Currently, the development of quantum computing shows extraordinary potential, especially in the field of cryptography. The phenomenon of quantum supremacy, where quantum computers can solve problems that cannot be solved by classical computers, is increasingly being felt. This raises uncertainty in the existing data security system, because various cryptographic algorithms and protocols are predicted to be quickly solved by sufficiently powerful quantum computers. To overcome this potential insecurity, the field of cryptography must adapt, one of which is through the concept of quantum key distribution which offers a new standard in secure communication. In symmetric key cryptography, a secure communication channel is required for key delivery, and the concept of quantum key distribution is a promising alternative to overcome this problem. This study aims to explore the implementation of quantum asymmetric cryptography in one-way data encryption, as well as assess its effectiveness in improving information security.

Kata Kunci: *Data security, cryptography, quantum computing, quantum key distribution, asymmetric cryptography*

PENDAHULUAN

Di era disrupsi teknologi yang berkembang pesat, setiap sektor harus beradaptasi untuk mempertahankan nilai dan relevansinya. Salah satu ancaman disrupsi terbesar yang diprediksi akan muncul setelah era kecerdasan buatan adalah komputasi kuantum. Komputasi kuantum, yang menggabungkan fisika kuantum, ilmu komputer, dan teori informasi, menawarkan potensi luar biasa dalam menyelesaikan masalah yang tidak dapat dipecahkan oleh komputer klasik. Dengan memanfaatkan fenomena kuantum seperti superposisi dan keterikatan, komputer kuantum diharapkan dapat menjadi superkomputer yang mendominasi di masa depan.

Perkembangan ini membawa dampak signifikan pada berbagai bidang, termasuk keamanan komunikasi. Saat ini, sistem keamanan komunikasi sangat bergantung pada kriptografi, yang sebagian besar dibangun berdasarkan prinsip matematis. Keamanan ini diciptakan melalui perhitungan yang sulit dipecahkan oleh komputer klasik dalam waktu yang efisien. Namun, kehadiran komputer kuantum berdaya tinggi mengancam integritas sistem kriptografi yang ada, terutama skema kriptografi asimetris seperti RSA. Algoritma Shor, yang dikembangkan oleh *Peter Shor*, dapat memecahkan masalah faktorisasi bilangan besar dengan cepat, sehingga mengancam keamanan sistem kriptografi kunci publik.

Dalam konteks ini, implementasi kriptografi asimetris kuantum muncul sebagai solusi yang menjanjikan untuk meningkatkan keamanan komunikasi. Dengan memanfaatkan prinsip-prinsip mekanika kuantum, metode ini dapat menciptakan sistem enkripsi data satu arah yang lebih aman dan efisien. Salah satu pendekatan utama dalam kriptografi asimetris kuantum adalah distribusi kunci kuantum (*quantum key distribution*), yang memungkinkan dua pihak untuk berbagi kunci rahasia dengan cara yang aman dan dapat mendeteksi adanya penyadapan.

Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis efektivitas implementasi kriptografi asimetris kuantum dalam konteks enkripsi data satu arah. Dengan memahami keunggulan dan tantangan yang dihadapi, diharapkan penelitian ini dapat memberikan rekomendasi untuk penerapan lebih luas dalam sistem komunikasi modern, serta berkontribusi pada pengembangan solusi kriptografi yang lebih aman di era komputasi kuantum.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

KAJIAN LITERATUR

Keamanan Data

Keamanan data merupakan upaya untuk melindungi data dari akses tidak sah, perubahan, atau perusakan. Dalam konteks perusahaan, keamanan data sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad). Teknologi informasi modern menghadapi berbagai ancaman, termasuk peretasan, pencurian data, dan penyadapan, sehingga penerapan sistem keamanan yang kuat menjadi hal krusial.

Kriptografi

Kriptografi adalah ilmu dan seni mengamankan informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca tanpa pengetahuan tertentu. Kriptografi dibagi menjadi dua kategori utama:

- **Kriptografi Simetris:** Menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Contoh algoritma: AES (*Advanced Encryption Standard*), DES (*Data Encryption Standard*).
- **Kriptografi Asimetris:** Menggunakan sepasang kunci, yaitu kunci publik dan kunci privat. Informasi yang dienkripsi dengan kunci publik hanya bisa didekripsi dengan kunci privat yang sesuai. Contoh algoritma: RSA, ElGamal.

Komputasi Kuantum

Komputasi kuantum adalah pendekatan komputasi yang menggunakan prinsip mekanika kuantum, seperti superposisi dan keterikatan kuantum *(entanglement*), untuk memproses informasi. Komputer kuantum memiliki kemampuan eksponensial dalam menyelesaikan masalah tertentu yang sulit atau mustahil diselesaikan oleh komputer klasik.

Salah satu algoritma kuantum yang paling terkenal adalah:

- **Algoritma Shor**: Digunakan untuk faktorisasi bilangan besar dalam waktu polinomial, yang secara signifikan mengancam sistem kriptografi kunci publik seperti RSA.
- **Algoritma Grover**: Menyediakan percepatan kuadrat dalam pencarian database tak terstruktur, yang juga berdampak pada keamanan kriptografi simetris.

Ancaman Komputasi Kuantum terhadap Kriptografi Sebagian besar sistem kriptografi yang digunakan saat ini bergantung pada kompleksitas matematis tertentu. Komputasi kuantum memiliki potensi untuk merusak sistem ini dengan menyelesaikan persoalan-persoalan kompleks tersebut secara lebih cepat. RSA dan ECC (*Elliptic Curve Cryptography*), yang saat ini banyak digunakan dalam komunikasi digital, dapat dipecahkan oleh komputer kuantum menggunakan algoritma Shor.

Kriptografi Kuantum

Kriptografi kuantum adalah bentuk kriptografi yang memanfaatkan hukum mekanika kuantum untuk menciptakan sistem komunikasi yang aman. Berbeda dari kriptografi klasik, kriptografi kuantum memungkinkan deteksi adanya gangguan atau penyadapan dalam proses pertukaran kunci.
Salah satu konsep utama dalam kriptografi kuantum adalah:

Quantum Key Distribution (QKD): Metode untuk mendistribusikan kunci rahasia antara dua pihak dengan aman menggunakan partikel kuantum (biasanya foton). Salah satu protokol QKD yang paling terkenal adalah BB84, yang dikembangkan oleh *Charles Bennett* dan *Gilles Brassard* pada tahun 1984. QKD menjamin keamanan karena setiap percobaan penyadapan akan menyebabkan perubahan pada keadaan kuantum, yang dapat dideteksi oleh penerima.

Enkripsi Data Satu Arah (*One-Way Encryption*)

Enkripsi satu arah adalah proses pengubahan data ke dalam bentuk terenkripsi tanpa kemungkinan untuk dikembalikan ke bentuk semula tanpa informasi khusus. Fungsi ini sering digunakan dalam sistem keamanan untuk menyimpan kata sandi atau dalam sistem autentikasi. Dalam konteks kuantum, penggunaan kunci yang dibentuk melalui QKD memungkinkan penerapan enkripsi satu arah yang lebih aman karena penyadapan pada proses pembentukan kunci dapat diketahui secara real-time.

METODE PENELITIAN

Penelitian ini mengimplementasikan sistem enkripsi dan dekripsi berbasis simulasi *Quantum Key Distribution* (QKD) dengan pendekatan protokol BB84 serta algoritma XOR untuk enkripsi data satu arah. Aplikasi ini dikembangkan menggunakan bahasa pemrograman Python dengan framework *Flask* sebagai *backend server* dan antarmuka web.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

Arsitektur Sistem

Sistem terdiri dari dua bagian utama:

- **Frontend**: Halaman web yang memungkinkan pengguna melakukan input teks untuk dienkripsi dan melakukan dekripsi ciphertext.
- **Backend**: Proses logika kriptografi dilakukan di server menggunakan simulasi algoritma kuantum dan enkripsi XOR.

Proses Simulasi *Quantum Key Distribution* (QKD)

QKD dilakukan dengan mengikuti simulasi protokol BB84 melalui langkah-langkah berikut:

- **Generate Random Bit & Basis (Alice dan Bob):**
  Sistem menghasilkan n bit acak untuk Alice, dan basis acak '+' dan 'x' untuk Alice dan Bob.
- **Proses Pengukuran Qubit:**
  Bob melakukan pengukuran terhadap bit dari Alice berdasarkan basis-nya sendiri. Jika basis Alice dan Bob sama, maka hasil pengukuran sama; jika tidak, maka hasilnya acak.
- **Penyaringan Kunci (*Key Sifting*):**
  Hanya bit dengan basis yang cocok antara Alice dan Bob yang digunakan sebagai kunci kuantum.

Proses Enkripsi

- Teks asli dari pengguna diubah menjadi representasi bit 8-bit per karakter.
- Bit pesan kemudian dienkripsi menggunakan algoritma XOR dengan kunci hasil QKD.
- Hasil enkripsi dalam bentuk bit kemudian dikodekan menjadi karakter *readable* (alfanumerik dan simbol) agar mudah dikirim dan ditampilkan.
- Informasi hasil enkripsi ditampilkan ke pengguna, termasuk bit pesan asli, bit kunci kuantum, dan *ciphertext*.

Proses Deskripsi

- Ciphertext yang dikirim pengguna di-decode kembali ke bentuk bit
- Kunci kuantum yang dimasukkan pengguna diubah ke bentuk bit
- Proses XOR dilakukan ulang antara *cipher bits* dan *key bits* untuk mendapatkan plaintext bit
- Bit hasil dekripsi dikonversi kembali ke teks

Pengujian dan Evaluasi

Sistem diuji melalui antarmuka web dengan input pesan *plaintext* dan proses enkripsi. Validasi dilakukan dengan memastikan pesan dapat dikembalikan secara tepat melalui proses dekripsi menggunakan kunci kuantum yang sama.

HASIL DAN PEMBAHASAN

Tampilan Antarmuka dan Alur Sistem

Aplikasi yang dikembangkan menggunakan framework *Flask* berhasil menampilkan antarmuka web sederhana yang terdiri atas dua halaman utama, yaitu halaman enkripsi dan halaman dekripsi. Pada halaman enkripsi, pengguna dapat memasukkan teks ke dalam kolom input. Sistem kemudian akan menghasilkan *ciphertext*, bit pesan asli, bit kunci kuantum, serta hasil *encoding* akhir yang ditampilkan secara real-time.

Sementara itu, pada halaman dekripsi, pengguna dapat memasukkan *ciphertext* beserta kunci kuantum (yang diperoleh saat proses enkripsi) untuk memperoleh kembali pesan asli setelah proses dekripsi selesai. Keberhasilan proses ini mengindikasikan bahwa integrasi antara sisi *frontend* dan *backend* telah berjalan secara optimal.

Hasil Simulasi Quantum Key Distribution

Sistem berhasil melakukan simulasi protokol BB84 melalui beberapa tahapan, yaitu:

- Pembentukan bit acak oleh Alice serta pemilihan basis acak oleh Alice dan Bob
- Proses pengukuran qubit oleh Bob
- Penyaringan kunci berdasarkan kesesuaian basis antara Alice dan Bob

Contoh hasil output dari proses simulasi:

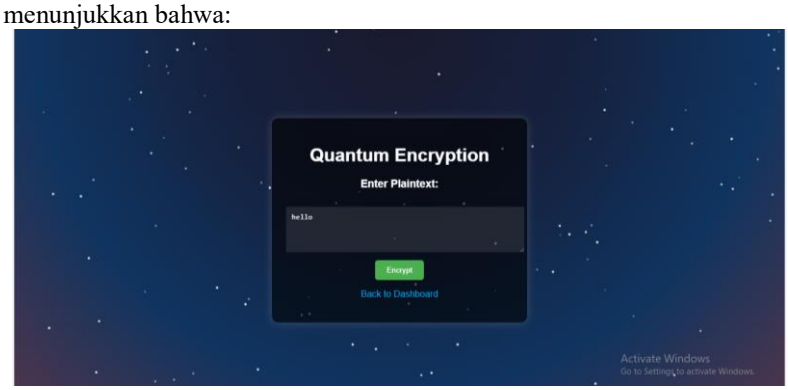
- Bit Alice: 10100101
- Basis Alice: +x++xx+x
- Basis Bob: +x+x++x+
- Kunci kuantum (basis cocok): 1011

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

Bit yang digunakan dalam proses enkripsi diambil dari bit Alice yang basisnya sesuai dengan basis Bob, sehingga membentuk kunci kuantum bersama secara aman.

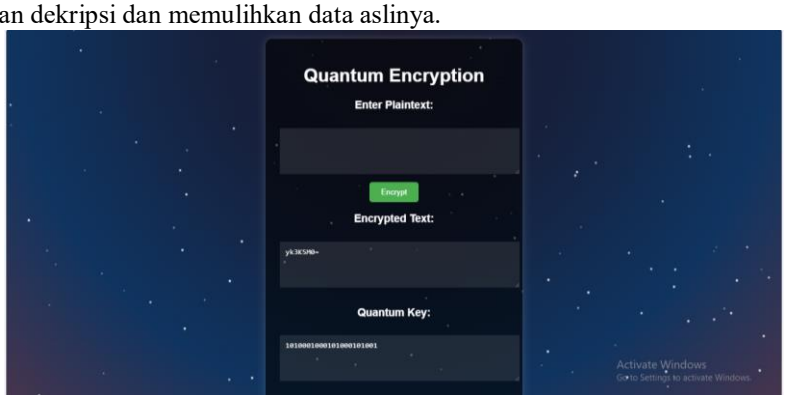
Proses Enkripsi dan Dekripsi

Proses enkripsi menunjukkan bahwa:



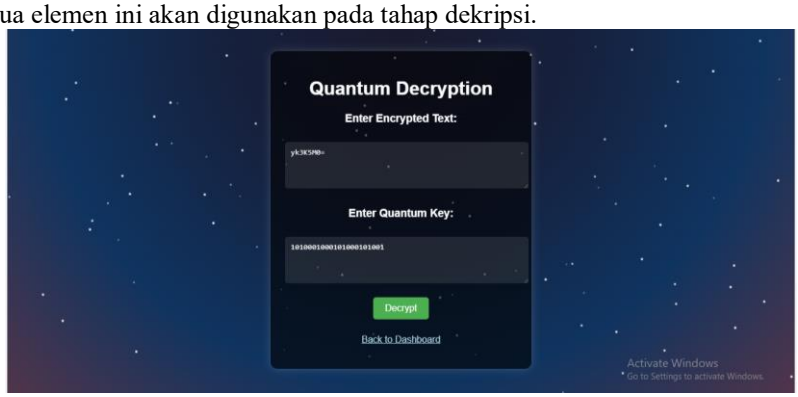
Gambar 1. Proses input plaintext pada halaman Quantum Encryption

Pada halaman ini, pengguna diarahkan ke fitur *Quantum Encryption* untuk memasukkan *plaintext* yang ingin dienkripsi. Setelah mengetik plaintext ke dalam kotak input, pengguna dapat menekan tombol *Encrypt* untuk memproses enkripsi menggunakan konsep kriptografi kuantum berbasis jurnal yang diimplementasikan. Setelah proses enkripsi selesai, pengguna akan diarahkan ke halaman dekripsi, di mana *plaintext* yang telah dienkripsi dapat diinput kembali untuk dilakukan dekripsi dan memulihkan data aslinya.



Gambar 2. Hasil *output Quantum Encryption*

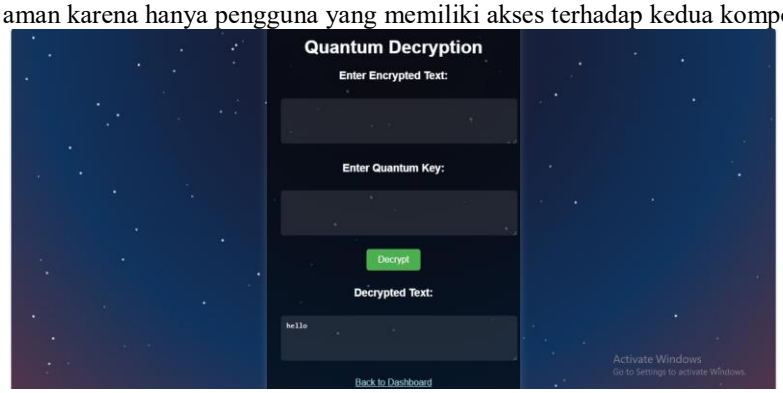
Pada tahap enkripsi, pengguna diminta untuk memasukkan *plaintext* pada halaman enkripsi. Setelah pengguna menekan tombol *Encrypt*, sistem akan menghasilkan dua *output*, yaitu *Cipher Text* (teks terenkripsi) dan *Quantum Key* (kunci kuantum dalam bentuk bilangan biner). *Cipher Text* dan *Quantum Key* yang dihasilkan harus disimpan oleh pengguna, karena kedua elemen ini akan digunakan pada tahap dekripsi.



Gambar 3. Proses *input* Enkripsi Teks dan Kunci Kuantum pada halaman *Quantum Decryption*

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

Di halaman dekripsi, pengguna akan diminta untuk memasukkan *Cipher Text* dan *Quantum Key* tersebut agar sistem dapat mengembalikan teks terenkripsi menjadi *plaintext* asli. Dengan mekanisme ini, proses enkripsi dan dekripsi menjadi lebih aman karena hanya pengguna yang memiliki akses terhadap kedua komponen penting tersebut.



Gambar 4. Hasil *output Quantum Deccryption*

Setelah memproses *Cipher Text* dan *Quantum Key* yang diberikan, sistem berhasil mendekripsi pesan terenkripsi dan mengembalikannya menjadi *plaintext* asli.
Implementasi:

- *Plaintext*: **Hello**
- Kunci QKD: **10100010001010001010 01**
- *Ciphertext*: **yk3K5M0=** (contoh hasil *encoding*)

Pada proses dekripsi, penggunaan *ciphertext* dan kunci kuantum yang sesuai berhasil mengembalikan pesan asli secara utuh, dalam hal ini "Hello".

Evaluasi Keberhasilan Sistem

Pengujian dilakukan secara manual dengan mencocokkan hasil enkripsi dan dekripsi menggunakan kunci kuantum yang sama. Hasil evaluasi menunjukkan bahwa:

- Jika kunci kuantum yang digunakan sesuai dengan yang dipakai saat proses enkripsi, maka dekripsi berhasil mengembalikan pesan dengan akurat.
- Jika terjadi perubahan pada kunci kuantum, maka hasil dekripsi tidak terbaca atau menghasilkan pesan yang salah.

Hasil ini menegaskan bahwa integritas kunci kuantum sangat menentukan keberhasilan proses enkripsi-dekripsi, serta mampu mensimulasikan prinsip utama QKD, yakni deteksi terhadap penyadapan melalui ketidaksesuaian hasil.

Pembahasan

Sistem yang dikembangkan menunjukkan bahwa pendekatan simulatif terhadap *Quantum Key Distribution* (QKD) dapat diimplementasikan dalam skala aplikasi web sederhana. Protokol BB84 yang disimulasikan terbukti memiliki keunggulan dalam hal:

- Keamanan pada proses pertukaran kunci
- Kemampuan mendeteksi intervensi atau penyadapan
- Penerapan algoritma XOR sebagai metode enkripsi satu arah yang ringan namun efektif

Namun demikian, perlu dicatat bahwa sistem ini masih berupa simulasi berbasis perangkat lunak konvensional, sehingga belum melibatkan aspek fisik dari komputasi kuantum.

Keamanan sejati dari QKD hanya dapat tercapai melalui implementasi dengan perangkat keras kuantum, seperti penggunaan foton dan polarizer dalam pengiriman kunci.

KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi simulatif kriptografi asimetris kuantum, khususnya dengan pendekatan protokol *Quantum Key Distribution* (QKD) BB84 dan algoritma XOR, mampu memberikan solusi enkripsi data satu arah yang aman dan efisien. Sistem yang dikembangkan berbasis web ini berhasil membuktikan bahwa proses enkripsi dan dekripsi dapat berjalan optimal ketika kunci kuantum yang digunakan konsisten. Hasil evaluasi

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.35

menegaskan bahwa integritas dan kesesuaian kunci kuantum sangat penting dalam menjamin keamanan dan keberhasilan dekripsi data.

Meskipun masih berupa simulasi perangkat lunak dan belum melibatkan perangkat keras kuantum sesungguhnya, pendekatan ini memberikan gambaran awal yang menjanjikan untuk pengembangan sistem keamanan data modern yang tahan terhadap ancaman dari komputasi kuantum. Dengan begitu, penelitian ini dapat menjadi langkah awal dalam memahami serta mengembangkan sistem kriptografi yang lebih aman di masa depan.

REFERENSI

[1] A. Fadhlurohman, *Simulasi Pemanfaatan Quantum Key Distribution dalam Pengiriman Kunci Kriptografi Simetris*, Makalah IF4020 Kriptografi, Semester I Tahun 2021/2022, Institut Teknologi Bandung, 2021.

[2] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi," *J. Teknol. dan Sist. Informasi (JTSI)*, vol. 4, no. 2, pp. 394–405, Sep. 2023.

[3] Basri, "Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi," *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 16–21, Sep. 2016.

[4] F. Fakhrizal, A. B. Pasaribu, S. Wulandari, dan R. A. Putri, "Implementasi Security System Menggunakan Kriptografi Algoritma Simetris Untuk Pengamanan Video," *Bigint Computing Journal*, vol. 1, no. 1, pp. 9–18, Mar. 2023.

[5] S. Hulu, "Implementasi Algoritma Kriptografi Simetris Dalam Pengamanan Data Absensi Guru Dan Pegawai Pada Website Sekolah SMK Dharma Caraka Teluk Dalam Menggunakan RC4 Chiper," *Jurnal Informatika*, vol. 1, no. 4, pp. 1–7, Mar. 2024.

[6] V. Miansyah dan R. Laipaka, "Perancangan Aplikasi Kriptografi Simetris Menggunakan Algoritma Hill Cipher dan Advanced Encryption Standard," *Jurnal TISI*, vol. 1, 2017.

[7] T. H. Saputro, N. H. Hidayati, dan E. I. H. Ujianto, "Survei Tentang Algoritma Kriptografi Asimetris," *Jurnal Informatika Polinema*, vol. 6, no. 2, pp. 67–72, Feb. 2020.

[8] A. S. Aswandi, M. N. Sutoyo, dan A. Pradipta, "Analisis Performa dan Keamanan Implementasi Kriptografi AES untuk Penyandian Dokumen Berbasis Web," J. MNEMONIC, vol. 8, no. 1, pp. 24–32, Feb. 2025.

[9] Z. Arif dan A. Nurokhman, "Studi Komparatif Algoritma RSA dan AES pada Enkripsi dan Dekripsi Citra Digital," J. Rekayasa dan Manajemen Sistem Informasi, vol. 4, no. 2, pp. 394–405, Sep. 2023.

[10] N. F. S. M. L. Dewi dan M. F. Ilmy, "Penerapan Enkripsi Hibrida AES-RSA untuk Meningkatkan Keamanan Layanan Slip Gaji Digital," J. Jaringan dan Elektronika, vol. 3, no. 1, pp. 45–52, Jan. 2025.