https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Volume 1, Nomor 2, 2025, Hal. 215-222
ISSN : 3090-3289

IMPLEMENTASI RSA (RIVEST SHAMIR ADLEMAN) BERBASIS CHINESE REMAINDER THEOREM (CRT) DAN STEGANOGRAFI END OF FILE (EOF) UNTUK PENYISIPAN DAN KEAMANAN PESAN PADA CITRA DIGITAL

Resti Tri Andari[1], I Gusti Prahmana[2], Darjat Saripurna[3]
Sistem Informasi, STMIK Kaputama Binjai[1,2]
Sistem Informasi, STMIK Triguna Dharma, Medan[3]
E-mail: andariresti7@gmail.com[1], darjatsaripurna@gmail.com[2], igustiprahmana4@gmail.com[3]

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat menuntut adanya metode keamanan data yang lebih efektif, khususnya dalam menjaga kerahasiaan pesan digital. Penelitian ini mengimplementasikan algoritma RSA (*Rivest Shamir Adleman*) berbasis *Chinese Remainder Theorem* (CRT) yang dipadukan dengan metode steganografi *End of File* (EOF) untuk penyisipan dan keamanan pesan pada citra digital. Algoritma RSA digunakan untuk mengenkripsi pesan sehingga hanya dapat dibaca oleh pihak yang memiliki kunci privat, sementara CRT digunakan untuk mempercepat proses enkripsi dan dekripsi. Selanjutnya, pesan yang telah terenkripsi disisipkan ke dalam citra digital menggunakan metode EOF yang relatif sederhana, efisien, dan tidak mengubah kualitas citra asli secara signifikan. Hasil implementasi menunjukkan bahwa kombinasi RSA CRT dan steganografi EOF mampu meningkatkan keamanan pesan, di mana pesan yang disisipkan tidak dapat dideteksi secara kasat mata serta tetap dapat diekstraksi kembali dengan akurasi tinggi. Dengan demikian, metode ini dapat menjadi alternatif solusi dalam pengamanan pesan rahasia pada media digital.

Kata kunci **Analisis Sentimen, Ekowisata, Support Vector Machine, TF-IDF, Kuesioner**

ABSTRACT

The rapid development of information technology requires more effective methods to ensure data security, particularly in maintaining the confidentiality of digital messages. This research implements the RSA (Rivest Shamir Adleman) algorithm based on the Chinese Remainder Theorem (CRT) combined with the End of File (EOF) steganography method for message embedding and security in digital images. The RSA algorithm is used to encrypt messages so that only authorized parties with the private key can read them, while CRT enhances the efficiency of the encryption and decryption processes. Furthermore, the encrypted message is embedded into the digital image using the EOF method, which is simple, efficient, and does not significantly alter the quality of the original image. The results show that the combination of RSA-CRT and EOF steganography successfully improves message security, as the embedded message cannot be visually detected and can be extracted with high accuracy. Thus, this method can serve as an alternative solution for securing confidential messages in digital media.

Keywords ***RSA, Chinese Remainder Theorem (CRT), Steganography, End of File (EOF), Digital Image, Message Security***

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk dalam hal keamanan data (Utomo et al., 2023). Ancaman terhadap integritas dan kerahasiaan informasi semakin meningkat seiring dengan berkembangnya metode serangan siber. Oleh karena itu, diperlukan suatu teknik yang mampu memberikan perlindungan data secara optimal. Dalam konteks pengamanan data digital, kriptografi dan steganografi merupakan dua disiplin ilmu yang sering digunakan untuk melindungi informasi. Kriptografi berfokus pada penyandian pesan, sedangkan steganografi berfokus pada penyembunyian keberadaan pesan itu sendiri (Kusumadewi et al., 2021).

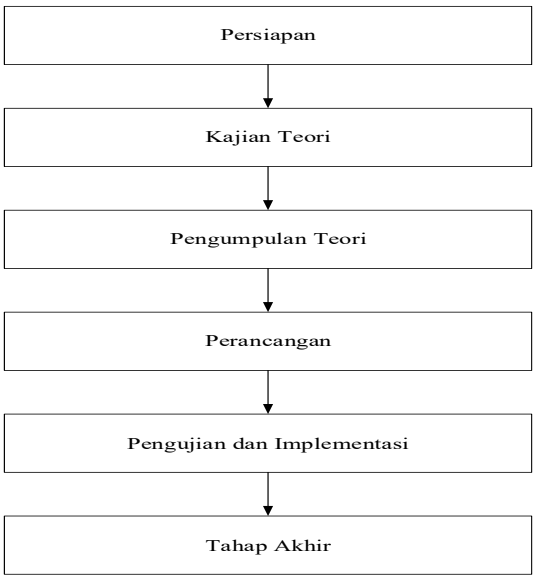
RSA (Rivest Shamir Adleman) merupakan algoritma kriptografi kunci publik yang banyak digunakan untuk mengamankan data dalam komunikasi digital (Mohamad et al., 2021). RSA bekerja secara asimetris dengan menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Keunggulan utama RSA terletak pada kekuatan matematisnya, yakni kesulitan faktorisasi bilangan prima besar sehingga sangat sulit dipecahkan tanpa kunci privat (Munir, 2019). Namun, algoritma RSA memiliki kelemahan dalam proses dekripsi yang relatif lambat, terutama pada perangkat dengan keterbatasan sumber daya komputasi. Untuk mengatasi hal tersebut, diterapkan pendekatan Chinese Remainder Theorem (CRT) yang dikenal sebagai RSA CRT untuk mempercepat proses dekripsi dengan membagi operasi modular menjadi dua bagian lebih kecil, yaitu berdasarkan bilangan prima p dan q. Pendekatan ini tidak menurunkan tingkat keamanan tetapi dapat meningkatkan efisiensi dekripsi hingga sekitar empat kali lipat dibanding RSA standar (Suryawanshi, 2023).

Selain teknik kriptografi, steganografi juga menjadi salah satu metode yang efektif untuk meningkatkan keamanan data. Steganografi merupakan teknik penyembunyian pesan rahasia di dalam media digital tanpa menimbulkan perubahan visual atau struktural pada file asal. Salah satu metode yang digunakan adalah End of File (EOF), di mana pesan ditempelkan pada bagian akhir file baik berupa citra, audio, maupun video (Sanbenfri Saragih et al., 2023). Pendekatan ini tidak mempengaruhi tampilan visual atau audio, namun hanya menambah ukuran file sesuai panjang pesan yang disisipkan (Cahyono & Yasin, 2023).

Dengan mengombinasikan Algoritma RSA CRT dan Steganografi EOF, diharapkan dapat meningkatkan keamanan penyimpanan dan pengiriman pesan dalam citra digital. Kriptografi akan menjamin kerahasiaan isi pesan, sementara steganografi akan menyamarkan keberadaan pesan tersebut. Kombinasi ini menciptakan sistem keamanan berlapis (Sari & Gunawan, 2024). Berdasarkan latar belakang di atas, maka penelitian ini berfokus pada perancangan dan implementasi sistem yang mengintegrasikan kedua teknik tersebut untuk menciptakan sistem penyisipan pesan yang aman dan efisien.

2. METODE PENELITIAN

Metodologi penelitian yang digunakan adalah pendekatan kualitatif dengan studi pustaka dan eksperimen. Metode ini bertujuan untuk menganalisis dan merancang sebuah sistem aplikasi yang mengimplementasikan kombinasi algoritma kriptografi dan steganografi.



Gambar 1. Alur Kerja Penelitian

2. 1 Kerangka Kerja

Penelitian ini mengikuti alur kerja yang terstruktur, dimulai dari tahap persiapan, kajian teori, pengumpulan data, perancangan, hingga implementasi dan pengujian.

1. **Persiapan**: Tahap awal meliputi identifikasi masalah, perumusan tujuan, dan batasan penelitian.
2. **Kajian Teori**: Mengumpulkan landasan teori dari berbagai literatur, seperti buku, jurnal, dan artikel ilmiah, yang berkaitan dengan kriptografi, steganografi, algoritma RSA, Chinese Remainder Theorem (CRT), dan metode EOF.
3. **Pengumpulan Data**: Dilakukan melalui studi pustaka (*library research*) untuk mendapatkan referensi yang kuat.
4. **Perancangan**: Melakukan perancangan sistem menggunakan Unified Modeling Language (UML) seperti *use case diagram* dan *activity diagram* (Putra & Andriani, 2019), serta membuat *flowchart* (Rosaly & Prasetyo, 2020) untuk menggambarkan alur kerja sistem secara logis. Perancangan antarmuka juga dilakukan untuk memberikan gambaran awal aplikasi.
5. **Implementasi dan Pengujian**: Mengimplementasikan rancangan sistem ke dalam bahasa pemrograman Visual Basic .NET 2010 (Rahmahdani & Yahfizham, 2024). Pengujian fungsional dan performa dilakukan untuk memvalidasi sistem dan mengevaluasi efisiensi algoritma.

2. 2 Perancangan Sistem

Sistem dirancang untuk memiliki dua proses utama: enkripsi-encoding dan decoding-dekripsi.

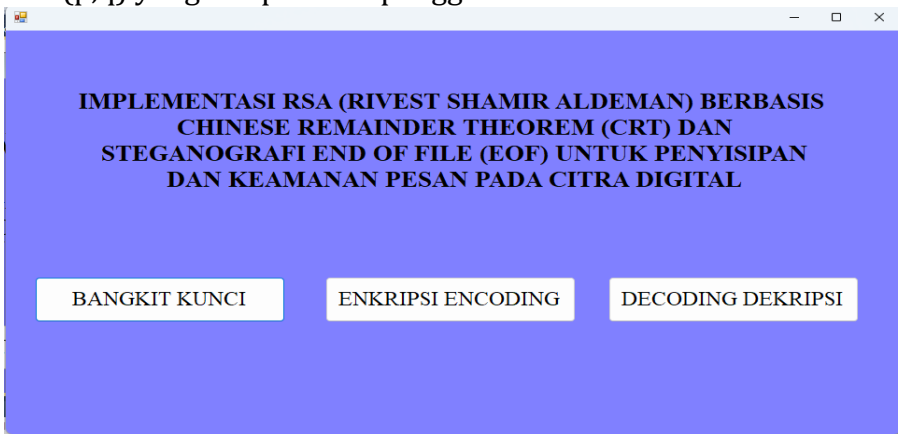
1. Pesan dienkripsi menggunakan algoritma RSA CRT dengan kunci publik. Hasil enkripsi (ciphertext) kemudian disisipkan ke dalam citra digital menggunakan metode steganografi EOF. Citra yang telah disisipi pesan disebut citra stego.
2. **Proses Decoding dan Dekripsi**: Pengguna memilih citra stego. Sistem mengekstrak pesan terenkripsi dari bagian akhir file menggunakan metode EOF. Data hasil ekstraksi kemudian didekripsi menggunakan kunci privat RSA CRT untuk mengembalikan pesan ke bentuk aslinya (*plaintext*).

3. HASIL DAN PEMBAHASAN

Implementasi sistem ini menghasilkan sebuah aplikasi desktop yang dapat melakukan proses enkripsi dan steganografi pesan pada citra.

3.1 Implementasi Algoritma RSA CRT

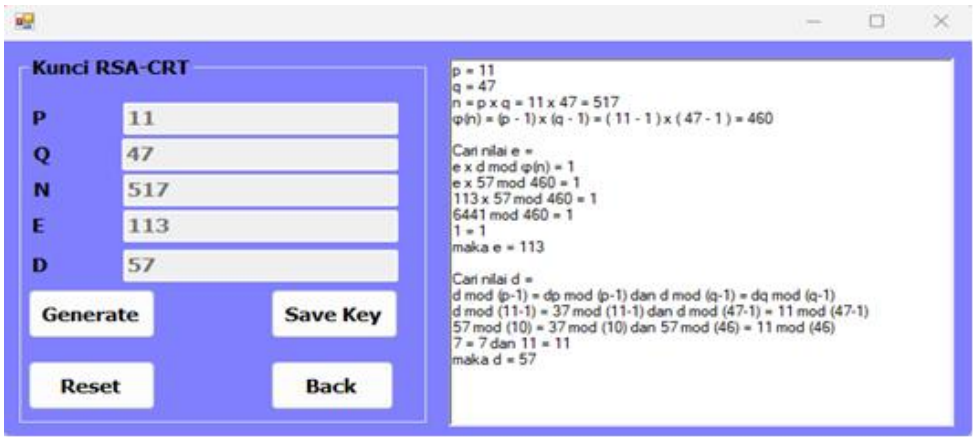
Proses enkripsi dan dekripsi pesan berhasil diimplementasikan. Perhitungan manual menunjukkan bahwa pesan asli "Hidup tetap berjalan" berhasil dienkripsi menjadi ciphertext dan kemudian dikembalikan ke pesan aslinya melalui proses dekripsi. Penggunaan CRT dalam proses dekripsi terbukti meningkatkan kecepatan komputasi. Proses pembangkitan kunci RSA CRT juga berjalan dengan baik, di mana kunci publik (e,n) dan kunci privat (d,n) serta parameter CRT (dp,dq,qinv) berhasil dihitung dari dua bilangan prima (p,q) yang diinput oleh pengguna.



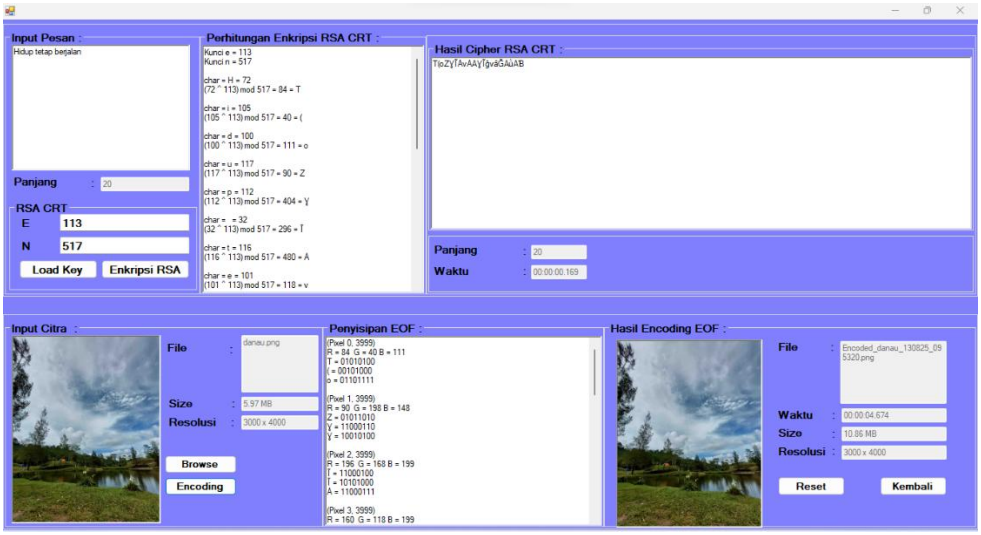
Gambar 2. Tampilan Halaman Utama

3.2 Implementasi Steganografi EOF

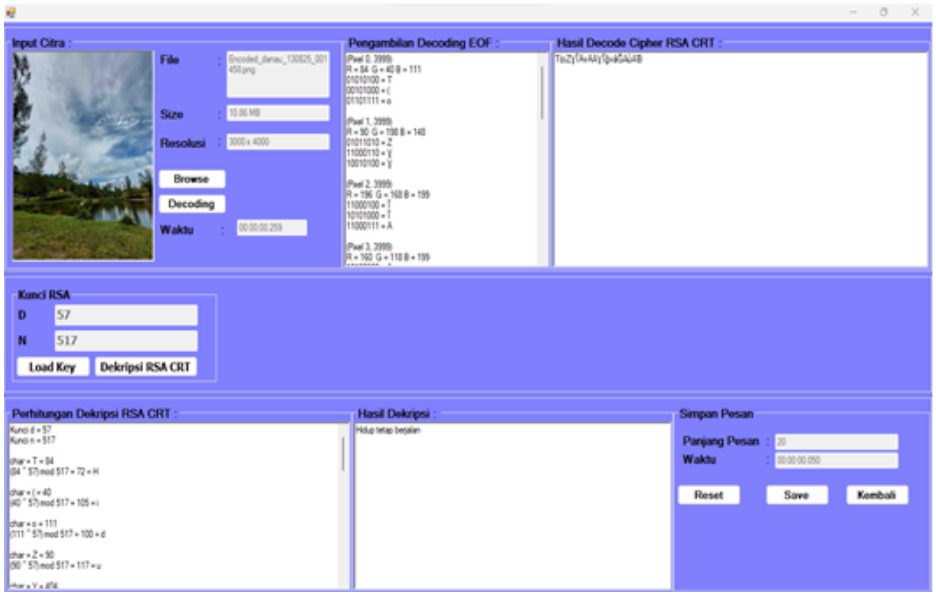
Metode steganografi EOF diimplementasikan dengan menambahkan data ciphertext hasil enkripsi RSA CRT ke bagian akhir file citra. Pengujian terhadap citra dengan berbagai format (JPEG, PNG, BMP) menunjukkan bahwa penambahan data tidak mengubah tampilan visual dari citra tersebut. Hal ini sejalan dengan karakteristik metode EOF yang menyembunyikan pesan di luar struktur data visual, sehingga tidak terdeteksi oleh mata manusia. Uji coba menunjukkan adanya peningkatan ukuran file citra stego dibandingkan citra asli, yang sebanding dengan panjang pesan yang disisipkan.



Gambar 3. Tampilan Bangkit Kunci



Gambar 4. Tampilan Halaman Enkripsi Encoding



Gambar 5. Tampilan Halaman Decoding Dekripsi

3.3 Pengujian Sistem

Pengujian dilakukan untuk memvalidasi fungsionalitas dan performa sistem.

1. **Uji Fungsionalitas**: Setiap fitur, mulai dari pembangkitan kunci, enkripsi, penyisipan, ekstraksi, hingga dekripsi, berfungsi dengan baik dan menghasilkan keluaran yang sesuai dengan rancangan. Pesan yang dienkripsi dan disisipkan berhasil diekstrak dan didekripsi kembali menjadi pesan asli tanpa kerusakan data.
2. **Uji Performa**: Performa sistem diukur berdasarkan waktu eksekusi proses enkripsi dan dekripsi. Meskipun tidak ada perbandingan langsung dengan RSA standar dalam penelitian ini, konsep teoritis yang didukung oleh literatur (Lestari et al., 2021) menunjukkan bahwa penggunaan CRT secara signifikan mengurangi waktu dekripsi, menjadikannya lebih efisien terutama untuk pesan dengan panjang yang besar.
3. **Uji Keamanan**: Sistem ini menyediakan dua lapisan keamanan. Lapisan pertama adalah enkripsi RSA yang melindungi isi pesan, dan lapisan kedua adalah steganografi EOF yang menyembunyikan keberadaan pesan. Pendekatan ini memberikan perlindungan ganda terhadap serangan.

4. KESIMPULAN & SARAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat ditarik beberapa kesimpulan:

a. Algoritma RSA berbasis CRT berhasil diimplementasikan untuk meningkatkan efisiensi proses enkripsi dan dekripsi pesan tanpa mengurangi tingkat keamanan.
b. Metode steganografi End of File (EOF) terbukti efektif untuk menyisipkan pesan terenkripsi ke dalam citra digital tanpa mengubah kualitas citra secara signifikan, karena metode ini hanya menambahkan data pada bagian akhir file.
c. Kombinasi RSA CRT dan steganografi EOF mampu menjaga kerahasiaan pesan, di mana pesan yang disisipkan tidak dapat dideteksi secara visual maupun melalui analisis sederhana.
d. Proses ekstraksi pesan dapat dilakukan dengan tingkat akurasi yang tinggi, sehingga pesan asli dapat dipulihkan kembali tanpa mengalami kerusakan data.

Untuk pengembangan penelitian selanjutnya, terdapat beberapa saran yang dapat dipertimbangkan:

a. Melakukan pengujian perbandingan kinerja antara RSA CRT dengan algoritma kriptografi lain seperti ECC (*Elliptic Curve Cryptography*) untuk mengetahui tingkat efisiensi dan keamanan yang lebih baik.
b. Mengembangkan metode EOF agar mampu menyisipkan pesan dengan ukuran lebih besar atau pada format file lain seperti video atau audio.
c. Melakukan uji coba sistem menggunakan metode deteksi steganografi (*steganalysis*) untuk mengetahui sejauh mana keamanan metode EOF mampu bertahan dari serangan pihak ketiga.

6. DAFTAR PUSTAKA

Ayu Binangkit, C.A., Voutama, A. & Heryana, N. (2023) ‘Pemanfaatan UML (Unified

Modeling Language) dalam Perencanaan Sistem Pengelolaan Sewa Alat Musik Berbasis Website', *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(2), pp. 1429–1436.

Cahyono, A.D. & Yasin, M. (2023) 'Implementasi steganografi menggunakan metode end of file (EOF) dalam pengamanan data (Studi kasus pada file AVI, MP3, dan JPEG)', *Jurnal MIPA dan Pembelajarannya*, 2(9), p. 7.

Imam, C. (2019) 'Mobile-Based National University Online Library Application Design', *Jurnal Mantik*, 3(2), pp. 10–19.

Kusumadewi, N., Permana, S.D. & Purba, A. (2021) 'Kombinasi Algoritma Vigenere Cipher dan Steganografi LSB pada Aplikasi Pengamanan Pesan Teks', *Jurnal Ilmu Komputer dan Sistem Informasi*, 9(1), pp. 1–8.

Lestari, R., Buaton, R. & Gultom, I. (2021) 'Penerapan Algoritma OTP dan Algoritma RSA CRT dalam Pengamanan Citra', *J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)*, 4(2), p. 180.

Malvi, A. & Painem, P. (2020) 'Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)', *Informatik: Jurnal Ilmu Komputer*, 16(2), p. 67.

Mohamad, M.S.A., Din, R. & Ahmad, J.I. (2021) 'Research trends review on RSA scheme of asymmetric cryptography techniques', *Bulletin of Electrical Engineering and Informatics*, 10(1), pp. 487–492.

Munir, R. (2019) *Kriptografi: Teori dan Implementasi (Edisi Kedua)*. Bandung: Informatika.

Prasetyo, A. & Wulandari, S. (2022) 'Perbandingan Kinerja Algoritma Kriptografi RSA dan ECC pada Tanda Tangan Digital', *Jurnal Sistem Informasi Bisnis*, 12(1), pp. 1–8.

Putra, D.W.T. & Andriani, R. (2019) 'Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD', *Jurnal TeknoIf*, 7(1), p. 32.

Rahmahdani, S. & Yahfizham. (2024) 'Perancangan Sederhana Menggunakan Bahasa Pemrograman Visual Basic .Net 2010 dengan Database MySQL', *Journal of Informatics and Business*, 1(4), pp. 213–222.

Ramdany, S. (2024) 'Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web', *Journal of Industrial and Engineering System*, 5(1).

Rosaly, R. & Prasetyo, A. (2020) 'Flowchart beserta fungsi dan simbol-simbol', *Journal of Chemical Information and Modeling*, 2(3), pp. 5–7.

Saragih, S., Simanjuntak, E., Rajagukguk, Y.S., Silalahi, D.F. & Lumbanbatu, S. (2023) 'Steganography of Text Insertion into Image with End of File (EOF) Method', *Jurnal Teknik Indonesia*, 2(1), pp. 8–12.

Sari, E.P. & Gunawan, D. (2024) 'Analisis Perbandingan Kombinasi Algoritma Kriptografi dan Steganografi untuk Pengamanan Data Digital', *Jurnal Teknologi Informasi dan Ilmu Komputer*, 11(1), pp. 1–10.

Stallings, W. (2020) *Cryptography and Network Security: Principles and Practice*. Pearson.

Utomo, I., Mulyono, W., Kusumawati, Y. & Ningrum, N.K. (2023) 'Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit dalam Cipher', *Jurnal Teknologi Informasi*, 14(1), pp. 16–28.

Yuliani, R.N., Widiastuti, D. & Haryanto, A. (2024) 'Perancangan Algoritma Post-Quantum Cryptography untuk Keamanan Data Jangka Panjang', *Jurnal Komputer dan Aplikasi*, 15(1), pp. 1–9.

Suryawanshi, Y. et al. (2023) 'Chinese Remainder Theorem based Performance Analysis of RSA Cryptosystem', *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(8), pp. 523–526.