

DAFTAR PUSTAKA

Akbar, R. and Nasution, M. I. P. (2024). Analisis keamanan data pada aplikasi mobile banking. *Journal of Sharia Economics Scholar (JoSES)*, 2(2):80–82.

Akshay, S. (2025). Hybrid aes-rsa encryption and decryption for secure data transmission. *International Journal of Research Publication and Reviews*, 6(10):1615–1621.

Amalya (2023). Peran mekanisme kriptografi dalam menjamin integritas data digital. *Jurnal Teknologi Informasi*, 12(3):120–135.

Amin, M. M. (2016). Implementasi kriptografi klasik pada komunikasi berbasis teks. *Jurnal Pseudocode*, 3(2):129–130.

Ananda, S. P., Lukman, S., and Irfan (2022). Analisa metode kriptografi modern advance encryption standard (aes) 128 bit dalam mengenkripsi dan mendekripsi file dokumen digital. *Jurnal Ilmiah KOMPUTASI*, 21(3):333–344.

Auliyaha, A. I. and Purnawansyah (2020). Implementasi kombinasi algoritma enkripsi rivest shamir adleman (rsa) dan algoritma kompresi huffman pada file document. *Indonesian Journal of Data and Science*, 1(1):23–28.

Bader, A. S., Sagheer, A. M., and Yaseen, L. (2020). *Design and implementation of a secure mobile banking system based on Elliptic Curve Integrated Encryption Schema*. Springer.

Barker, E. and Kelsey, J. (2015). Recommendation for random number generation using deterministic random bit generators. Technical Report NIST SP 800-90A Rev. 1, National Institute of Standards and Technology (NIST).

Bufalo, M., Bufalo, D., and Orlando, G. (2021). A note on the computation of the modular inverse for cryptography. *Axioms*, 10(2):116.

Curlin, P. S. (2025). A survey of hardware-based aes sboxes: Area, performance, and security. *ACM Computing Surveys*, 57(9):229.

Damjanovic, B. (2017). Algorithm aes - structure, transformations and performance. *Aktuelnosti*, 10:1–25.

detikFinance (2025). Ojk catat jumlah kerugian korban scam tembus rp 700 m. Berita Online.

Dewi, S. K. (2024). Perbandingan cryptography klasik vigenere cipher dengan cryptography modern rc4 dalam tingkat keamanan jaringan komputer. *Jurnal Multi Media dan IT*, 8(2):130–137.

Dong, Z. (2015). Detecting and locating man-in-the-middle attacks in fixed wireless networks. *Journal of Computing and Information Technology*, 23(4):283–293.

Fauzi, G. A. (2025). Kombinasi aes dan hmac untuk pengamanan parameter url dari serangan sql injection. *International Journal of Cryptography and Network Security*, 12(2):101–112.

Fortune Indonesia (2024). Bssn: Ada 102 juta anomali trafik serangan siber hingga juli 2024. Berita Online.

Gauthama Raman, M. and Mohideen, S. K. (2024). Modified modular exponentiation for a faster implementation of rsa algorithm on fpga. *International Journal of Engineering Research & Technology (IJERT)*, 12(5):91–93.

Kontan (2024). Transaksi mobile banking diprediksi tembus rp 24,4 kuadriliun tahun ini, melesat 47%.

Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., and Hutson, J. (2024). Symmetric and asymmetric encryption algorithms for cryptography – a comparative analysis in ai era. *International Journal of Advanced Computer Science and Applications*, 15(12):1–6.

Latif, B. J. (2023). Analisis penggunaan kriptografi pada proses autentikasi bca mobile. *Makalah II4031 Kriptografi dan Koding, Semester II Tahun 2022/2023*.

- Lidl, R. and Niederreiter, H. (1997). *Finite fields*. Cambridge University Press.
- Lopez-Rojas, E. (2017). Synthetic financial datasets for fraud detection. Kaggle Dataset.
- Lydia, M. S., Budiman, M. A., and Rachmawati, D. (2018). *On using Pollard's $p-1$ algorithm to factor RPrime RSA modulus*. SCITEPRESS.
- Mahto, D. and Yadav, D. K. (2018). Performance analysis of rsa and elliptic curve cryptography. *International Journal of Network Security*, 20(4):625–635.
- Malhotra, T. and Kadyan, S. (2024). Mobile banking security risks: An analysis. *Journal of Information Systems Engineering and Management*, 10(52s):1066–1070.
- Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (2001). *Handbook of applied cryptography*. CRC Press, 8th edition.
- Mukhtisar, I., Tarigan, R. R., and Evriyenni (2024). Pengaruh efisiensi, keamanan dan kemudahan terhadap minat nasabah bertransaksi menggunakan mobile banking. *JIHBI: Global Journal of Islamic Banking and Finance*, 3(1):60–64.
- National Institute of Standards and Technology (2016). Secure hash standard (shs). Technical Report 180-4, U.S. Department of Commerce.
- National Institute of Standards and Technology (2023). Advanced encryption standard (aes).
- Ramadhoni and Santoso (2023). Solusi hmac untuk mengatasi serangan man-in-the-middle pada mobile banking. *Jurnal Keamanan Informasi dan Aplikasi Mobile*, 16(1):30–45.
- Ridwan, M., Arifin, Z., and Yulianto (2016). Rancang bangun e-voting dengan menggunakan keamanan algoritma rivest shamir adleman (rsa) berbasis web. *Jurnal Informatika Mulawarman*, 11(2):22–28.
- Sai Kiran, R. and Harini, M. (2023). Evaluating efficiency of hmac and digital signatures to enhance security in iot. *International Journal of Computer Science and Technology*, 15(4):123–135.

Saputro, T. H., Hidayati, N., and Ujianto, E. I. H. (2020). Survei tentang algoritma kriptografi asimetris. *Jurnal Informatika Polinema*, 8(1):67–71.

Shoup, V. (2009). *A computational introduction to number theory and algebra*. Cambridge University Press, 2nd edition.

Sitompul, R. S. U. and Nasution, M. I. P. (2024). Pentingnya kepatuhan keamanan informasi dalam mengurangi risiko data breach. *MAESWARA: Jurnal Riset Ilmu Manajemen dan Kewirausahaan*, 2(1):6–7.

Somsuk (2024). Keamanan protokol dan mekanisme kriptografi untuk mobile banking. *Jurnal Kriptografi dan Keamanan Informasi*, 15(2):45–60.

Stallings, W. (2023). *Cryptography and network security: Principles and practice*. Pearson, 8th edition.

Syahputra, C., Nafiisah, S. S., Gultom, S. R., Affandi, R., and Perdanas, A. (2026). Analisis performa algoritma quick sort dan merge sort pada pengurutan data besar (big data) menggunakan notasi big-o. *Jurnal Teknik Informatika dan Multimedia*, 6(1):367–379.

Intelligentia - Dignitas