DAFTAR PUSTAKA

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022a). *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*. https://doi.org/10.6028/NIST.IR.8413

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022b). *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*. https://doi.org/10.6028/NIST.IR.8413

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2024). *Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/NIST.IR.8528

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2025). *Status report on the fourth round of the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/NIST.IR.8545

An, S., Kim, S., Jin, S., Kim, H. B., & Kim, H. S. (2018). Single trace side channel analysis on NTRU implementation. *Applied Sciences (Switzerland)*, *8*(11). https://doi.org/10.3390/app8112014

Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations. *International Conference on Information Networking*,

2023-January, 146–151. https://doi.org/10.1109/ICOIN56518.2023.10048976

Bima Setiawan, A. (2025). Penggunaan Cryptography dalam Keamanan Pesan Digital. *Journal of Computer Science and Information Technology*, *1*(2), 60–66. https://doi.org/10.70716/jocsit.v1i2.261

De Boer, K., & Van Woerden, W. (2025). *Lattice-based Cryptography A survey on the security of the lattice-based NIST finalists*.

Delibasic, M., Habibovic, A., Hanjalic, N., & Husagic, E. (2020). *Some Improvements of the Parallel Karatsuba Algorithm*. IEEE.

Dzahabi, Z. Y., Hayaty, N., & Bettiza, M. (2025). CRYPTOGRAPHY OF CHACHA20 and RSA ALGORITHMS for TEXT SECURITY. *Journal of Computer Networks, Architecture and High Performance Computing*, *7*(1), 290–301. https://doi.org/10.47709/cnahpc.v7i1.5345

Eid, A. H., & Ismail, A. S. (2025). An Analytical Review on Lattice-Based Cryptography. *Journal of Physics: Conference Series*, *3075*(1). https://doi.org/10.1088/1742-6596/3075/1/012013

Käppler, S. A., & Schneider, B. (2022). *Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms*.

Kundu, R., De Piccoli, A., & Visconti, A. (2022). *Public Key Compression and Fast Polynomial Multiplication for NTRU using the Corrected Hybridized NTT-Karatsuba Method*. https://orcid.org/0000-0001-5689-8575

Liu, Y., Zhang, Y., Lu, X., Cheng, Y., & Yin, Y. (2025). *DAWN: Smaller and Faster NTRU Encryption via Double Encoding*.

Longa, P., & Naehrig, M. (2016). *Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography*.

Maqsood, F., Ahmed, M., Mumtaz Ali, M., & Ali Shah, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 8, Issue 6). www.ijacsa.thesai.org

Meyer, A. (2025). *Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems*. http://arxiv.org/abs/2505.08791

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020a). *Status report on the second round of the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/NIST.IR.8309

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020b). *Status report on the second round of the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/NIST.IR.8309

Navid Bin Anwar, M., Hasan, M., Hasan, M., Loren, J. Z., & Tanjim Hossain, S. M. (2019). Comparative Study of Cryptography Algorithms and Its' Applications. In *International Journal of Computer Networks and Communications Security* (Vol. 7, Issue 5). www.ijcncs.org

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. In *ACM Computing Surveys* (Vol. 51, Issue 6). Association for Computing Machinery. https://doi.org/10.1145/3292548

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms. *IEEE Access*, *13*, 89003–89024. https://doi.org/10.1109/ACCESS.2025.3571307

Pazrian Nurul Latip. (2025). IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DALAM PENGAMANAN FILE TEKS. *Jurnal Riset Sistem Informasi*, *2*(3), 01–04. https://doi.org/10.69714/k6pr0s45

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, *10*(4), 283–424. https://doi.org/10.1561/0400000074

Purba, R., Pardosi, A., Darmawan, H., Sitorus, A. A., & Adiputra Pardosi, I. (2019). Pengamanan Data Teks Dengan NTRU Dan Modulus Function Pada Koefisien IHWT Citra Warna. *Julyxxxx*, *20*, 1–5.

Satriawan, A., Mareta, R., & Lee, H. (2024). *A Complete Beginner Guide to the Number Theoretic Transform (NTT)*.

Satriawan, A., Syafalni, I., Mareta, R., Anshori, I., Shalannanda, W., & Barra, A. (2023). Conceptual Review on Number Theoretic Transform and Comprehensive Review on Its Implementations. In *IEEE Access* (Vol. 11, pp. 70288–70316). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2023.3294446

Scrivano, A. (2025). *A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing*. http://arxiv.org/abs/2508.00832

Shah, & Gor. (2025). *Comprehensive Survey of Symmetric and Public-Key Cryptographic Algorithms: Foundations, Attacks, and Applications*.

Shen, Y., Sun, Z., & Zhou, T. (2021). Survey on Asymmetric Cryptography Algorithms. *2021 International Conference on Electronic Information Engineering and Computer Science, EIECS 2021*, 464–469. https://doi.org/10.1109/EIECS53707.2021.9588106

Tambe-Jagtap, S. N. (2023). A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions. *SHIFRA*, *2023*, 43–52. https://doi.org/10.70470/shifra/2023/006

Vaishnavi, A., & Pillai, S. (2021). Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. *Journal of Physics: Conference Series*, *1964*(4). https://doi.org/10.1088/1742-6596/1964/4/042002

Venkata Rajesh Krishna Adapa. (2025). Architecting quantum-resistant cybersecurity: A framework for transitioning to post-quantum cryptographic systems. *International Journal of Science and Research Archive*, *14*(1), 737–746. https://doi.org/10.30574/ijsra.2025.14.1.0110

Xing, Y., & Li, S. (2021). A compact hardware implementation of cca-secure key exchange mechanism crystals-kyber on fpga. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2021*(2), 328–356. https://doi.org/10.46586/tches.v2021.i2.328-356

Yu, Z. (2023). Historical research on classification of Classical Cryptography. *Theoretical and Natural Science*, *11*(1), 166–172. https://doi.org/10.54254/2753-8818/11/20230403

Zhang, Q. (2021). An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. *Proceedings - 2021 2nd International Conference on Computing and Data Science, CDS 2021*, 616–622. https://doi.org/10.1109/CDS52072.2021.00111

Zhou, S., Xue, H., Zhang, D., Wang, K., Lu, X., Li, B., & He, J. (2018). *Preprocess-then-NTT Technique and Its Applications to KYBER and NEWHOPE*.

Zhu, Y., Liu, Z., & Pan, Y. (2019). *When NTT Meets Karatsuba: Preprocess-then-NTT Technique Revisited*.