DAFTAR PUSTAKA

Bhattacharya, S., Garcia-Morchon, O., Player, R., & Tolhuizen, L, 2019, *Achieving secure and efficient lattice-based public-key encryption: The impact of the secret-key distribution*.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehle, D., 2018, *Crystals - Kyber: A CCA-secure module-lattice-based KEM*, 2018 IEEE European Symposium on Security and Privacy (EuroS&P).

Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H., 2008, *An introduction to mathematical cryptography* (Vol. 1), New York: Springer.

Langlois, A., & Stehlé, D., 2014, *Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography*, Springer.

Malik, D. S., Mordeson, J. M., & Sen, M. K., 1997, *Fundamentals of abstract algebra*, McGraw-Hill.

Micciancio, D., 2017, *Minkowski's theorem*, diakses dari University of California San Diego, Lattices Algorithms and Applications, https://cseweb.ucsd.edu/classes/fa21/cse206A-a/

Peikert, C., 2016, *A Decade of Lattice Cryptography*, Now Publisher.

Roman, S., 2005, *Advanced linear algebra*, Springer.

Romine, C. H., 2015, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, USA.

Stinson, D. R., & Paterson, M., 2018, *Cryptography: Theory and Practice, 4th ed.*, CRCPress.

St Pierre, J. A., 2023, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, USA.

Wahyuni, S., Wijayanti, I. E., Yuwaningsih, D. A., & Hartanto, A. D., 2016, *Teori Ring dan Modul*, Gadjah Mada University Press.