DAFTAR PUSTAKA

Adkins, W., A., Weintraub, S.H., (1992). *Algebra: An Approach via Module Theory*. Springer-Verlag, New York.

Ali, S., (2021). *Serangan Reduksi Latis LLL (Lenstra - Lenstra - Lovasz) pada Sistem Kriptografi NTRU (Nth Degree Truncated Polynomial Ring)*. Skripsi.Jurusan Matematika FMIPA UGM, Yogyakarta.

Anton, H., & Rorres, C., (2014). *Elementary Linear Algebra : Applications Version*. 11th Edition. John Wiley and Sons.

Ajtai, M., (1996). *Generating Hard Instances of Lattice Problems*. Quaderni di Matematika. 13:1-32.

Davidowitz, N.S., (2018). *Ring-SIS and Ideal Lattices*. https://people.csail.mit.edu/vinodv/6876-Fall2018/RingSISclass.pdf.Diakses pada Februari 2024.

Diffie, W., & Hellman, M., E., (1976). *New Directions in Cryptography*. IEE Transactions on Information Theory. vol. IT-22, no. 6, pp-644-65.

Kinanty, F.P.,(2022). *MATRU : Sistem Kriptografi Berbasis NTRU*. Skripsi. Jurusan Matematika FMIPA UGM, Yogyakarta.

Fraleigh, J. B., (1993). *A First Course in Abstract Algebra*. Fifth Edition. Addison Wesley Publishing Company, inc., USA.

Georgescu, A., (2012). *An LWE-based Key Transfer Protocol with Anonymity*. Tatra Mountains MathematicalPublications. 53: 119-135.

Hoffstein, J.,Pipher, J., Silverman, J.H., (2008). *An Introduction to Matehematical Cryptography (Vol.1)*. New York, Spinger.

Ingemarsson, I., Tang, D., & Wong, C., (1982). *A conference key distribution system*. IEEE Transactions on Information Theory. 28(5), 714–720. https://doi.org/10.1109/tit.1982.1056542

Ling, S., Xing, C., (2004). *Coding Theory : a First Course*. Cambridge University Press.

Liu, J., & Peikert, C. (2017). *Learning With Errors and Learning With Rounding are Equivalent*. Retrieved from https://eprint.iacr.org/2017/634.pdf.

Lyubashevsky, V., Peikert, C., & Regev, O. (2010). *On Ideal Lattices and Learning with Errors over Rings*. In Lecture notes in computer science (pp. 1–23). https://doi.org/10.1007/978-3-642-13190-5_1.

Malik, D.S., Mordeson, J.M., Sen, M.K., (1997). *Fundamental of Abstract Algebra*. McGraw-Hill.

National Institute of Standards and Technology Interagency (NIST), (2022). *Status Report on the Third of the NIST Post-Quantum Cryptography Standaedization Process*. NIST IR 8413-upd1.

Peikert, C., (2016). *A Decade of Lattice Cryptography*. Lattice Survey, Supported by the National Science Foundation Under CAREER Award CCF-1054495, by DARPA under agreement number FA8750-11-0096, and by the Alfred P. Sloan Foundation.

Regev, O., (2005). *On Lattice, Learning With Error, Random Linear Codes, and Cryptography*. J. ACM, 56(6):1-40.

Roman, S., Axler, S., & Gehring, F.W., (2005). *Advanced Linear Algebra*. Third Edition. New York : Spinger.

Stinson, R.D., & Paterson, M., (2018). *Cryptography : Theory and Pactice*.Forth Edition. CRC Press.

Wahyuni, S., Wijayanti, I.E., D.A, Ari Hartanto, A.D. (2016). *Teori Ring dan Modul*. Universitas Gadjah Mada University Press.

Zhi-Min, Y., Zheng-Jun, J., Shi-Chun, L., (2015). *Diffie-Hellman Key Exchange Protocol based on Ring-LWE*. The Open Cybernetics & Systemics Journal, 9 : 1033-1037.