

DAFTAR PUSTAKA

- [1] Adkins, W.A., Weintraub, S.H., 1992, *Algebra: An Approach via Module Theory*, Springer-Verlag, New York.
- [2] Ajtai, M., 1996, "Generating hard instances of lattice problems", *Quaderni di Matematica*, 13:1–32.
- [3] Buchanan, William J ., 2023, "Security and So Many Things", Asecuritysite.com. <https://asecuritysite.com/>, diakses pada tanggal 31 Oktober 2023 pukul 21.00 WIB.
- [4] Cohen, H., 1996, *A Course in Computational Algebraic Number Theory* , Springer, Berlin, Heidelberg.
- [5] Davidowitz, N.S., 2018, "Ring-SIS and Ideal Lattices", www.noahsd.com, Diakses pada tanggal 3 Mei 2023.
- [6] Hoffstein, J., Pipher, J., Silverman, J. H., (2008), *An introduction to mathematical cryptography (Vol. 1)*, New York, Springer.
- [7] Ling, S., Xing, C., 2004, *Coding theory: a first course*. Cambridge University Press.
- [9] National Institute of Standards and Technology Interagency, 2022, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", NIST IR 8413-upd1.
- [9] National Institute of Standards and Technology Interagency, 2023, "Module-Lattice-based Key-Encapsulation Mechanism Standard", FIPS 203.
- [10] Macciancio, D., Goldwasser, S., 2002, *Complexity Of Lattice Problems A Cryptographic Perspective*, Springer Science Business Media, New York.



- [11] Malik, D. S., Mordeson, J. M., dan Sen, M. K., 1997, *Fundamentals of abstract algebra*. McGraw-Hill.
- [12] 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- C-0096, and by the Alfred P. Sloan Foundation.
- [13] Regev, O., 2005, "On lattices, learning with errors, random linear codes, and cryptography", J. ACM, 56(6):1–40.
- [14] Stinson, R.D., 2006, *Cryptography Theory And Practice*, Third Edition, CRC Press.
- [15] Wahyuni, S., Wijayanti, I.E, Yuwaningsih, D.A, Ari Hartanto, A.D, 2016, *Teori Ring dan Modul*, Gadjah Mada University Press.