DAFTAR PUSTAKA

Anton, H., & Rorres, C. (2013). Elementary linear algebra: applications version. John Wiley & Sons.

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

Hoffstein, J., & Silverman, J. H. (1998). Invertibility in truncated polynomial rings (Vol. 9). Technical report, NTRU Cryptosystems, 1998. Report.

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.

Ling, S., & Xing, C. (2004). Coding theory: a first course. Cambridge University Press.

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

Micciancio, D., & Goldwasser, S. (2012). *Complexity of lattice problems: a cryptographic perspective* (Vol. 671). Springer Science & Business Media.

Nguyen, P. Q., & Vallée, B. (2010). The LLL algorithm. Springer Berlin Heidelberg.

Roman, S., Axler, S., & Gehring, F. W. (2005). Advanced linear algebra (Vol. 3). New York: Springer.

Silverman, J. H. (1999). Estimated breaking times for NTRU lattices. NTRU Technical Note #012, 1999. Available from http://www.ntru.org.

Stinson, D. R., & Paterson, M. (2018). Cryptography: theory and practice. CRC press.