DAFTAR PUSTAKA

Arboit, G. 2008. *Two Mathematical Security Aspects of the RSA Cryptosystem: Signature Padding Schemes and Key Generation with a Backdoor*.

Barrus, M., & Clark, W. E. 2022. *Elementary Number Theory*. LibreTexts.

Buchmann, J. A. 2004. *Introduction to Cryptography*. New York: Springer-Verlag.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. 2022. *Introduction to Algorithms, 4th ed*. The MIT Press. Cambridge, Massachusetts.

ETSI. 2007. *Electronic Signatures and Infrastructures (ESI): Algorithms and Parameters for Secure Electronic Signatures. Part 1: Hash Functions and Asymmetric Algorithms*. European Telecommunications Standards Institute, Valbonne.

Friedl, S. 2017. *An Elementary Proof of The Group Law For Elliptic Curves*.

Hoffstein, J., Pipher, J., & Silverman, J. H. 2008. *An Introduction to Mathematical Cryptography, 2nd ed*. New York: Springer-Verlag.

Ivanov, A., Stoianov, N. 2023. *Implications of the Arithmetic Ratio of Prime Numbers For RSA Security*. International Journal of Applied Mathematics and Computer Science. Vol 33 No. 1. 57–70.

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

Markelova, A.V. 2021. *Embedding Asymmetric Backdoors Into The RSA Key Generator*. Journal of Computer Virology and Hacking Techniques. Vol 17 No. 1. 37–46.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. 1996. *Handbook of Applied Cryptography*. CRC Press, Boca Raton.

NIST. 2019. *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. National Institute of Standards and Technology, Gaithersburg.

Pomerance, C. 2008. *Smooth Numbers and Quadratic Sieve*.

Rosen, K. H. 1986. *Elementary Number Theory and its Applications*. Addison-Wesley Publishing Company.

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

Wang, Z. 2017. *Elementary Proof of Dirichlet Theorem*.

Young, A. and Yung, M. 1996. *The Dark Side of "Black-Box" Cryptography, or: Should We Trust Capstone?*. Annual International Cryptology Conference.

Young, A. and Yung, M. 1997. *Kleptography: Using Cryptography Against Cryptography*. International Conference on the Theory and Application of Cryptographic Techniques.

Young, A. and Yung, M. 2004. *Malicious Cryptography : Exposing Cryptovirology*. Wiley Publishing, Inc.

Yung, M. (2005). *Kleptography: The Outsider Inside Your Crypto Devices, and its Trust Implications*. DIMACS Workshop on Theft in E-Commerce: Content, Identity, and Service.