UNIVERSITAS
GADJAH MADA
Sistem Kriptografi ElGamal atas Bilangan Bulat Gauss dan Aplikasinya pada Tanda Tangan Digital
Raka Bukhari, Uha Isnaini, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

Adleman, L. M. 1979. A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography. *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, 55–60.

Awad, Y., Jomaa, D., Alkhezi, Y., dan Hindi, R. 2025. A New Approach Combining RSA and ElGamal Algorithms: Advancements in Encryption and Digital Signatures Using Gaussian Integers. *Jordanian Journal of Computers and Information Technology*, 11(1), 54–72. DOI: 10.5455/jjcit.71-1720618955.

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

Conrad, K. 2013. *The Gaussian Integers*. University of Connecticut.

Cross, J. T. 1983. The Euler ϕ-Function in the Gaussian Integers. *The American Mathematical Monthly*, 90(8), 518–528. DOI: 10.2307/2322785.

Diffie, W. dan Hellman, M. E. 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. DOI: 10.1109/TIT.1976.1055638.

Donaldson, N. 2021. *Gaussian Integers and Rings of Algebraic Integers*. University of California, Irvine.

Dummit, D. S. dan Foote, R. M. 2004. *Abstract Algebra*. Third Edition. John Wiley & Sons, Inc.

ElGamal, T. 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4), hal. 469-472.

El-Kassar, A. N., Rizk, M., Mirza, N. M., dan Awad, Y. A. 2001. ElGamal Public Key Cryptosystem in the Domain of Gaussian Integers. *International Journal of Applied Mathematics*, 7(4), 405–412.

Fraleigh, J. B. 2004. *A First Course in Abstract Algebra*. Seventh Edition. Pearson Education.

UNIVERSITAS
GADJAH MADA
Sistem Kriptografi ElGamal atas Bilangan Bulat Gauss dan Aplikasinya pada Tanda Tangan Digital
Raka Bukhari, Uha Isnaini, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Haraty, R. A., El-Kassar, A. N., dan Shebaro, B. M. 2006. A Comparative Study of ElGamal Based Digital Signature Algorithms. *Journal of Computational Methods in Sciences and Engineering*, 6(S1), S147–S156. DOI: 10.3233/JCM-2006-6S112.

Hoffstein, J., Pipher, J., dan Silverman, J. H. 2014. *An Introduction to Mathematical Cryptography*. Second Edition. Springer.

Ireland, K. dan Rosen, M. 1990. *A Classical Introduction to Modern Number Theory*. Second Edition. Springer-Verlag.

Khalaf, H. A. dan Khalaf, R. Z. 2024. Hybrid Cryptosystem Using Polybius and ElGamal Algorithm Over the Gaussian Integers. *Academic Science Journal*, 2(1), 135–147. DOI: 10.24237/ASJ.02.01.707B.

Lee, G. T. 2018. *Abstract Algebra: An Introductory Course*. Springer Undergraduate Mathematics Series. Springer, Cham. DOI: 10.1007/978-3-319-77649-1.

Malik, D. S., Mordeson, J. M., dan Sen, M. K. 1997. *Fundamentals of Abstract Algebra*. The McGraw-Hill Companies, Inc.

Menezes, A. J., van Oorschot, P. C., dan Vanstone, S. A. 1996. *Handbook of Applied Cryptography*. CRC Press.

Pohlig, S. C. dan Hellman, M. E. 1978. An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance. *IEEE Transactions on Information Theory*, 24(1), 106–110. DOI: 10.1109/TIT.1978.1055817.

Sajjad, M., Shah, T., Haq, T. U., Almutairi, B., dan Xin, Q. 2024. SPN Based RGB Image Encryption over Gaussian Integers. *Heliyon*, 10(9), e30353. DOI: 10.1016/j.heliyon.2024.e30353.

Stinson, D. R. dan Paterson, M. B. 2018. *Cryptography: Theory and Practice*. Fourth Edition. Chapman and Hall/CRC.