

## DAFTAR PUSTAKA

- Buchmann, J. A., 2000, *Introduction to Cryptography*, Springer-Verlag New York, Inc., USA.
- Cohen, H., 1996, *A Course in Computational Algebraic Number Theory*, Springer, New York.
- Fraleigh, John B., 2000, *A First Course in Abstract Algebra*, Sixth Edition, AddisonWesley Publishing Company, Inc., USA.
- Friedl, S., 2014, *An Elementary Proof of the Group Law for Elliptic Curves*, <https://www.math.rice.edu/~friedl/papers/AAELLIPTIC.PDF>, 20 Januari 2004, diakses 12 November 2017.
- Hankerson, D., Menezes A.J., dan Vanstone S., 2004, *Guide to Elliptic Curve Cryptography*, Springer.
- Johnson, D., Menezes, A. dan Vanstone, S., 2001, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, *International Journal of Information Security*, 1, 1, 36-63.
- Malik, D.S., Mordeson, J.N., dan Sen, M.K., 1997, *Fundamentals of Abstract Algebra*, McGraw-Hill, New York.
- Menezes, A., OorschotP., dan Vanstone, S., 1996, *Handbook of Applied Cryptography*, CRC Press.
- Paar, C., dan Pelzl, J., 1998, *Understanding Cryptography*, Springer, New York.
- Rahardjo, Budi dkk, 2014. *Pengantar Kurva Eliptik dan Lapangan Hingga serta Aplikasinya untuk Kriptografi*, Penerbit ITB, Bandung.
- Rosen, K., 1986, *Elementary number theory and its applications*, Addison-Wesley Publishing Company.



Schoof, R., 1995, *Counting Points on Elliptic Curves over Finite Fields*, *Journal de Theorie des Nombres de Bordeaux*, 7, 219-254.

Silverman, J.H., 2009, *The Arithmetic of Elliptic Curves*, Springer, New York.

Stinson, D.R., 2006, *Cryptography, Theory and Practice*, Chapman Hall/CRC.

Washington L.C., 2008, *Elliptic Curves: Number theory and Cryptography*, Chapman Hall/CRC, Boca Raton.