

## DAFTAR PUSTAKA

- Alfie Amanilla Aziz. (2009). Implementasi Tanda Tangan Digital Menggunakan Metode Ong-Schnorr-Shamir dan Euclidean pada Teks. *Skripsi*. Fakultas Sains dan Teknologi UIN Syarif Hidayatullah.
- Baldoni, M. W. , Ciliberto, C. and Cattaneo, G. M. Piacentini. 2009. *Elementary Number Theory, Cryptography and Codes*. Berlin Heidelberg : Springer-Verlag.
- Biggs, Norman L. 2008. *Codes: An Introduction to Information Communication and Crypyography*. London: Springer-Verlag.
- Elizabeth, Dorothy and Denning, Robling. 1982. *Cryptography and Data Security*. Canada: Addison-Wesley Publishing Company.
- Everest, Graham and Ward, Thomas. 2005. *An Introduction to Number Theory*. London: Springer-Verlag.
- Fraleigh, John. B. 2001. *A First Course In Abstract Algebra*. Canada: Addison-Wesley Publishing Company.
- Gallian, Joseph. A. 2013. *Contemporary Abstract Algebra*. Boston: Brooks/Cole.
- Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. (2012). Hash Function Requirements for Schnorr Signature. *Laporan Penelitian*. IBM Research .
- Hoffstein, Jeffrey , Pipher, Jill, and Silverman, Joseph H. 2008. *An Introduction to Mathematical Cryptography*. New York : Springer-Verlag.
- Jain, Raj. (2011). *Digital Signature*. *Makalah*. Washington University.
- Katz, Jonathan. 2010. *Digital Signatures*. New York : Springer.
- Keng, Hua Loo. 1982. *Introduction to Number Theory*. Berlin Heidelberg: Springer-Verlag.
- Laura Savu. (2012). Combining Public Key Encryption with Schnorr Digital Signature. *Journal of Software Engineering and Applications* (Nomor 5). Hlm. 102-108.
- Mao, Wenbo. 2004. *Modern Cryptography: Theory & Practice*. New Jersey : Prentice-Hall Publisher.

- Menezes, Oorschot, and Vanstone. 1997. *Handbook of Applied Cryptography*. Florida : CRC Press.
- Mirawati. (2013). Implementasi *Digital Signature* dengan Algoritma RSA dan Lehmann *Prime* pada Pesan Teks. *Skripsi*. Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.
- Muharram Huda W. (2003). Perkembangan Enkripsi Fungsi Hash pada SHA (Secure Hash Algorithm). *Jurnal Ilmu Komputer dan Teknologi Informasi* (Vol. III, nomor 2).
- Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika Bandung.
- Piyush Gupta dan Sandeep Kumar. (2014). A Comparative Analysis of SHA and MD5 Algorithm. *International Journal of Computer Science and Information Technologies* (Vol. 5 nomor 3). Hlm. 4492-4495.
- Praveen Gauravaram, John Kelsey, Lars R. Knudsen and Soren S. Thomsen . (2010). On Hash Functions Using Checksums. *International Journal of Information and Security* (Vol. 9). Hlm. 137–151.
- Rininda Ulfa Arizka. (2010). Penerapan Sistem Kriptografi Elgamal atas  $\mathbb{Z}_p^*$  dalam Pembuatan Tanda Tangan Digital. *Skripsi*. FMIPA UNY.
- Stallings, William. 2005. *Cryptography and Network Security Principles and Practices*. New Jersey: Pearson Education.
- Stark, Harold M. 1998. *An Introduction to Number Theory*. Massachusetts: Markham Publishing Company.
- Stinson, D.R. 2006. *Cryptography Theory and Practice*. Boca Raton : CRC Press.
- Sukirman. 2006. *Pengantar Teori Bilangan*. Yogyakarta : Hanggar Kreator.
- Trappe, Wade and Washington, Lawrence C. 2002. *Introduction Cryptography with Coding Theory*. New Jersey : Prentice-Hall.
- Yao-Chang Yu and Ting-Wei Hou. (2014). An Efficient Forward-Secure Group Certificate Digital Signature Scheme to Enhance EMR Authentication Process. *International Federation Medical and Biological Engineering* (Vol. 52). Hlm. 449-457.
- Yus Gias Vembrina. (2013). Pengujian Bilangan Prima. *Makalah Penelitian*. Teknik Informatika ITB.