## DAFTAR PUSTAKA


Dworkin, Morris. 2001. "*Recommendation for Block Cipher Modes of Operation*: Methods and Techniques". NIST Special Publication 800-38A 2001 Edition, National Institute of Standards and Technology.

Ferguson, Niels. 1999. "*Impossible differentials in Twofish*". Twofish Technical Report #5. Counterpane System.

Kromodimoeljo, Sentot. 2010. *Teori & Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.

Mao, Wenbo. 2003. *Modern Cryptography: Theory and Practice*. Prentice Hall PTR.

Menezes, Alfred J., dkk. 1996. *Handbook of Applied Cryptography*. Waterloo. CRC Press.

Microsoft Developer Network (MSDN). 2012. "RNGCryptoServiceProvider Class". Dalam http://msdn.microsoft.com/en-us/library/system.security .cryptography.rngcryptoserviceprovider.aspx. Diakses 2 Juni 2013.

Moriai, Shiho dan Yiqun Lisa Yin. 2000. "Cryptanalisis of Twofish (II)". NTT Multimedia Communications Laboratories.

Nechvatal, James, dkk. 2000. "*Report on the Development of the Advanced Encryption Standard (AES)"*. National Institute of Standards and Technology.

Rizvi, S.A.M., Syed Zeeshan Hussain, dan Neeta Wadhwa. 2011. "*Performance Analysis of AES and TwoFish Encryption Schemes*". International Conference on Communication Systems and Network Technologies, IEEE Computer Society 2011, pp. 76-79, vol-3.

RSA Laboratories. 2012. "Password-Based Cryptography Standard". Public-Key Cryptography Standards #5 v2.1. EMC Corporation.

Singh, Aarti. 2000. "*Study of MDS matrix used in Twofish AES (Advanced Encryption Standard) Algorithm and its VHDL Implementation*". Technical report. Central Electronics Engineering Research Institute.

Schneier, Bruce dkk. 1998. "*Twofish: A 128-Bit Block Cipher*". AES Submission. Counterpane System.

Schneier, Bruce dkk. 2000. "*The Twofish Team's Final Comments on AES Selection*". Counterpane System.

Schneier, Bruce dan Doug Whiting. 2000. "*A Performance Comparison of the Five AES Finalists*". *AES Candidate Conference 2000*, pp. 123-135.

Stallings, William. 2010. *Cryptography and Network Security Principles and Practices Fifth Edition*. Prentice Hall.

Stallings, William. 2010. *Network Security Essentials: Applications and Standards Fourth Edition*. Pearson Education Inc.

Turan, Meltem S. dkk. 2010. "Recommendation for Password-Based Key Derivation Part 1: Storage Applications". NIST Special Publication 800-132. National Institute of Standards and Technology.

Random.org. Tanpa Tahun. "Introduction to Randomness and Random Numbers". Dalam http://www.random.org/randomness/. Diakses 2 Juni 2013.