DAFTAR PUSTAKA

Chaves, R., Kuzmanov, G., Sousa, L. and Vassiliadis, S., 2006, *Improving SHA-2 hardware implementations, Cryptographic Hardware and Embedded Systems-CHES 2006,* 298-310, Springer Berlin Heidelberg.

Delfs, Hans dan Knebl, Helmut, 2007, *"Symmetric-key encryption", Introduction to cryptography: principles and applications*, Springer, ISBN 9783540492436.

Diffie, W., dan Hellman, M. E., 1976, *"New directions in cryptography", Information Theory*, IEEE Transactions on, 22(6), 644-654.

Drake, J.J., Lanier, Z., Mulliner, C., Fora, P.O., Ridley, S.A., Wicherski, G., 2014. *Android Hacker's Handbook.* John Wiley & Sons.

ElGamal, T., 1985, *A public key cryptosystem and a signature scheme based on discrete logarithms, Advances in Cryptology*, 10-18, Springer Berlin Heidelberg.

Haraty, R. A., El-Kassar, A. N., & Shebaro, B. M., 2006, *A comparative study of ElGamal based digital signature algorithms, Journal of Computational Methods in Science and Engineering,* 6, 147-156.

Jarusombat, S., dan Kittitornkun, S., 2006, *"Digital signature on mobile devices based on location", Communications and Information Technologies*, IEEE, 866-870.

Kaur, R., dan Kaur, A., 2012, *"Digital signature", Computing Sciences (ICCS),* 2012 International Conference on, IEEE, 295-301.

Kuo, Wen-Chung, 2007, *"On ElGamal Signature Scheme", Future Generation Communication and Networking*, IEEE, 2, 151-153.

Liu, J. M., Cheng, X. G., & Wang, X. M., 2006, *"Methods to Forge ElGamal Signatures and Determine Secret Key", Advanced Information Networking and Applications*, IEEE, 1, 859-862.

McDonnell, T., Ray, B., Kim, M., 2013. *An Empirical Study of API Stability and Adoption in the Android Ecosystem, 29th IEEE International Conference on*

Software Maintenance (ICSM). Presented at the 2013 29th IEEE International Conference on Software Maintenance (ICSM), pp. 70–79.

Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A., 1996, *Handbook of applied cryptography*, CRC press.

Mu, Y., & Varadharajan, V., 1998, *"Anonymous secure e-voting over a network", Computer Security Applications Conference*, IEEE, 14, 293-299.

Mullen, Gary dan Mummert, Carl, 2007, *Finite fields and applications*, American Mathematical Society, 112, ISBN 9780821844182.

Northcutt, S., 2008, Hash Function, *http://www.sans.edu/research/security-laboratory/article/hash-functions*, diakses tanggal 1 juni 2016.

Nyberg, K., dan Rueppel, R. A., 1996, *"Message recovery for signature schemes based on the discrete logarithm problem", Designs, Codes and Cryptography*, 7(1-2), 61-81.

Paar, C., & Pelzl, J., 2009, *Understanding cryptography: a textbook for students and practitioners,* Springer Science & Business Media.

Rivest, Ronald L., 1990, *"Cryptology", J. Van Leeuwen, Handbook of Theoretical Computer Science,* 1, Elsevier.

Silva, J.E., 2003. *An overview of cryptographic hash functions and their uses*. GIAC.

Yoon, H.J., 2012, *A Study on the Performance of Android Platform, International Journal on Computer Science and Engineering*, 4, 532-537.

Zhang, Y., Xu, Q., Liu, Z., 2011, *"A new non-interactive deniable authentication protocol based on generalized ElGamal signature scheme", Information Technology and Artificial Intelligence Conference*, IEEE, 1, 193-197.