DAFTAR PUSTAKA

[1] R. Munir, *Kriptogafi*. Bandung: Institut Teknologi Bandung, 2021.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology — CRYPTO '85 Proceedings*, H. C. Williams, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426.

[3] N. Koblitz,, "Use of elliptic curves in cryptography," in *Elliptic curve cryptosystems*, vol. 48, no. 177, 1987, pp. 417–426.

[4] L. Yang, Q. Zhang, and J. Li, "Cryptanalysis of two tripartite authenticated key agreement protocols," August 2015, pp. 159–162.

[5] H. Xiong, Z. Qin, and F. Li, "Simulatability and security of certificateless threshold signatures without random oracles," in *2008 International Conference on Computational Intelligence and Security*, vol. 2, 2008, pp. 308–313.

[6] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2004, pp. 119–132.

[7] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*. IEEE, 2008, pp. 245–256.

[8] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis, and Y. C. Stamatiou, "Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, 2011, pp. 715–720.

[9] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd ed. Pearson Education, 2002.

[11] J. Marcel, *Studi dan Implementasi Algoritma Elliptic Curvepada Mobile Devices*. Bandung: Institut Teknologi Bandung, 2007.

[12] D. Brown, *SEC 2: Recommended Elliptic Curve DomainParameters*. Certicom Corp, 2010.

[13] I. Kholissodin, *Penggunaan Kriptosistem Kurva Elliptik untukEnkripsi dan Dekripsi Data*. Surabaya: Universitas Airlangga, 2007.

[14] H. A. Aronsson, "Zero knowledge protocols and small systems," 1995.

[15] B. Forouzan, *Cryptography & Network Security*, ser. McGraw-Hill Forouzan Networking. McGraw-Hill Publishing, 2007.

[16] G. I. Simari, "A primer on zero knowledge protocols," 2002.

[17] B. Schneier and P. Sutherland, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. USA: John Wiley and Sons, Inc., 1995.

[18] J. Kizza, "Feige-fiat-shamir zkp scheme revisited," *International Journal of Computing and ICT Research*, vol. 4, 07 2010.

[19] N. Shabbir and S. R. Hassan, "Routing protocols for wireless sensor networks (wsns)," in *Wireless Sensor Networks*, P. Sallis, Ed. Rijeka: Intech Open, 2017, ch. 2.