DAFTAR PUSTAKA

[1] A. Premana, G. Fitralisma, A. Yulianto, M. B. Zaman, and M. A. Wiryo, "Pemanfaatan teknologi informasi pada pertumbuhan ekonomi dalam era disrupsi 4.0," *J. Econ. Manag. (JECMA)*, vol. 2, no. 2, pp. 1–6, 2020.

[2] D. Wiryany, S. Natasha, and R. Kurniawan, "Perkembangan teknologi informasi dan komunikasi terhadap perubahan sistem komunikasi Indonesia," *J. Nomosleca*, vol. 8, no. 2, pp. 242–252, 2022.

[3] V. Sharma, A. Chauhan, H. Saxena, S. Mishra, and S. Bansal, "Secure file storage on cloud using hybrid cryptography," in *Proc. 5th Int. Conf. Inf. Syst. Comput. Netw. (ISCON)*, Oct. 2021, pp. 1–6.

[4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[5] F. R. S. Taka, "Secure communication by combined Diffe-Hellman key exchange based AES encryption and Arabic text steganography," *J. Inf. Hiding Multim. Signal Process.*, vol. 12, no. 4, pp. 186–198, 2021.

[6] S. Dusane, M. Iliyaz, and A. Suresh, "Implementation of E2EE using Python," in *Emerg. Technol. Data Mining Inf. Secur.: Proc. IEMIS 2022, vol. 3*, pp. 635–642, 2022.

[7] K. K. Nalla, "Securing chat applications: Strategies for end-to-end encryption and cloud data protection," *World Journal of Advanced Engineering Technology and Sciences*, vol. 13, no. 2, pp. 528–540, 2024.

[8] T. Isobe and R. Ito, "Security analysis of end-to-end encryption for Zoom meetings," *IEEE Access*, vol. 9, pp. 90677–90689, 2021.

[9] A. Adithya, K. Kulkarni, and S. Saha, "Applications of RSA and AES256 in end-to-end encryption using Diffie-Hellman key exchange," *International Research Journal of Engineering and Technology (IRJET)*, vol. 9, no. 9, Sep. 2022.

[10] C. Gupta and N. S. Reddy, "Enhancement of security of Diffie-Hellman key exchange protocol using RSA cryptography," in *J. Phys.: Conf. Ser.*, vol. 2161, no. 1, p. 012014, 2022.

[11] A. Ghani, S. U. Jan, S. A. Chaudhry, R. Ahmad, and D. H. Kim, "MCDHSLKAP: Modified computational Diffie-Hellman based secure and lightweight key agreement protocol for decentralized edge computing networks," *IEEE Access*, 2024.

[12] R. Patgiri, "privateDH: An enhanced Diffie-Hellman key exchange protocol using RSA and AES algorithms," *Cryptology ePrint Archive*, 2021.

[13] E. Dritsas, M. Trigka, and P. Mylonas, "Performance and security analysis of the Diffie-Hellman key exchange protocol," in *Proc. 19th Int. Workshop Semantic Soc. Media Adapt. Pers. (SMAP)*, Nov. 2024, pp. 166–171.

[14] A. A. Ahmed and O. M. Barukab, "Unforgeable digital signature integrated into lightweight encryption based on effective ECDH for cybersecurity mechanism in Internet of Things," *Processes*, vol. 10, no. 12, p. 2631, 2022.

[15] O. İşler, "Implementation and performance evaluation of elliptic curve cryptography over SECP256R1 on STM32 microprocessor," *Cryptology ePrint Archive*, 2024.

[16] Y. Yan, "The overview of elliptic curve cryptography (ECC)," in *J. Phys.: Conf. Ser.*, vol. 2386, no. 1, p. 012019, 2022.

[17] B. Arunkumar and G. Kousalya, "Secure and lightweight elliptic curve cipher suites in SSL/TLS," *Comput. Syst. Sci. Eng.*, vol. 40, no. 1, 2022.

[18] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, “Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model,” *Comput. Netw.*, vol. 199, p. 108465, 2021.
[19] S. Cohney, A. Kwong, S. Paz, D. Genkin, N. Heninger, E. Ronen, and Y. Yarom, “Pseudorandom black swans: Cache attacks on CTR_DRBG,” in *Proc. IEEE Symp. Security Privacy (SP)*, May 2020, pp. 1241–1258.
[20] M. Rodríguez, J. Lázaro, U. Bidarte, J. Jiménez, and A. Astarloa, “A fixed-latency architecture to secure GOOSE and sampled value messages in substation systems,” *IEEE Access*, vol. 9, pp. 51646–51658, 2021.
[21] S. H. Murad and K. H. Rahouma, “Implementation and performance analysis of hybrid cryptographic schemes applied in cloud computing environment,” *Procedia Comput. Sci.*, vol. 194, pp. 165–172, 2021.
[23] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[24] D. J. Bernstein, “Curve25519: New Diffie-Hellman speed records,” in *Lect. Notes Comput. Sci.*, vol. 3958, pp. 207–228, Springer, 2006.
[25] A. Langley, M. Hamburg, and S. Turner, “RFC 7748: Elliptic Curves for Security,” IETF, Jan. 2016.
[26] Y. Zhong, “An overview of RSA and OAEP padding,” *Highlights Sci. Eng. Technol.*, vol. 1, pp. 82–86, 2022.
[27] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, “Systematic and critical review of RSA based public key cryptographic schemes: Past and present status,” *IEEE Access*, vol. 9, pp. 155949–155976, 2021.
[28] J. Jonsson and B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2,” RFC 8017, Nov. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc8017
[29] National Institute of Standards and Technology, “FIPS PUB 197: Advanced Encryption Standard (AES),” Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[30] C. Paar and J. Pelzl, *Understanding Cryptography*. Springer, 2010.
[31] J. Hua, X. Dong, S. Sun, Z. Zhang, L. Hu, and X. Wang, “Improved MITM cryptanalysis on Streebog,” *Cryptology ePrint Archive*, 2022.