DAFTAR PUSTAKA

Bart, B., 2021. Updating to Zoom version 5.0 – Zoom Help Center. [online] Support.zoom.us. <https://support.zoom.us/hc/en-us/articles/ 360043555772> [Diakses 19 Agustus 2021].

Docs.microsoft.com. 2021. SymmetricAlgorithmNames.AesEcb Property (Windows.Security.Cryptography.Core) - Windows UWP applications. [online]: <https://docs.microsoft.com/en-us/uwp/api/windows.security.cryptography.core.symmetricalgorithmnames.aesecb?view=winrt-20348> [Diakses 19 Agustus 2021].

Fuhr, T., Jaulmes, E., Lomne, V. dan Thillard, A., 2013, 'Fault attacks on AES with faulty ciphertexts only', Proceedings - 10th Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2013, pp. 108–118. doi: 10.1109/FDTC.2013.18.

Jayasinghe, D., Ragel, R., Ambrose, J.A., Ignjatovic, A. dan Parameswaran, S., 2014, 'Advanced modes in AES: Are they safe from power analysis based side channel attacks?', 2014 32nd IEEE International Conference on Computer Design, ICCD 2014, pp. 173–180. doi: 10.1109/ICCD.2014.6974678.

Kaushik, P. dan Majumdar, R., 2018, 'Timing attack analysis on AES on modern processors', 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, 2018-Janua, pp. 462–465. doi: 10.1109/ICRITO.2017.8342471.

Möller, B., Duong, T. dan Kotowicz, K., 2014, 'This POODLE Bites: Exploiting The SSL 3.0 Fallback', Security Advisory, pp. 1–6. Available at: https://www.openssl.org/~bodo/ssl-poodle.pdf.

Stallings, W., 2017, Cryptography and Network Secuirty. 7th edn.

Wang, Q., Wang, A., Wu, L. dan Zhang, J., 2016, 'A new zero value attack combined fault sensitivity analysis on masked AES', Microprocessors and Microsystems, 45, pp. 355–362. doi: 10.1016/j.micpro.2016.06.014.

Wei, Y., Lu, J. dan Hu, Y., 2011, 'Meet-in-the-middle attack on 8 rounds of the AES block Cipher under 192 key bits', Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6672 LNCS(60833008), pp. 222–232. doi: 10.1007/978-3642-21031-0_17.

Yau, A.K.L., Paterson, K.G. dan Mitchell, C.J., 2005, 'Padding oracle attacks on CBC-mode encryption with secret and random IVs', Lecture Notes in Computer Science, 3557, pp. 299–319. doi: 10.1007/11502760_20.

Yuan, Y., Wu, L., Zhang, X. dan Yang, Y., 2018, 'Side-channel collision attack based on multiple-bits', Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID, 2017-Octob, pp. 1–5. doi: 10.1109/ICASID.2017.8285732.