DAFTAR PUSTAKA

Alam. K. M. R., & Tamura. S. (2018). Electronic Voting – Scopes and Limitations, International Conference on Informatics, Electronics & Vision, Bangladesh.

Ariandoko. W. (2011). Penggunaan Timing Attack Sebagai Salah Satu Jenis Serangan pada Kriptografi, Makalah Penelitian, Institut Teknologi Bandung, Bandung.

Bajaj. S., Chitkara. V., Bindlish. A., Nangia. H., & Jain. R. (2018).E-Voting using Homomorphic Encryption, Proceedings of 4th International Conference on Computer and Management ICCM, Bharati Vidyapeeth College of Engineering, Delhi, India.

Bustami. A., & Bahri. S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review, Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), Vol. 7, p-ISSN : 0126 – 4036.

CQR. (2023). Timing Attacks, https://cqr.company/web-vulnerabilities/timingattacks/. 28 Februari 2023, diakses pada 31 Januari 2024.

Faturahman. I., Kusyanti. A., & Siregar. R. A. (2020). Implementasi Algoritme Enkripsi Homomorphic Schmidt-Takagi Versi 2 pada Sistem E-Voting, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 4, No. 11, Hal. 3956-3962.

Hardjaloka. L., & Simarmata. V. M. (2011). E-Voting: Kebutuhan vs. Kesiapan (Menyongsong) E-Demokrasi, Jurnal Konstitusi, Vol. 8, No. 4.

Hartopo. M., & Munir. R. (2017). Pengembangan Aplikasi E-Voting Menggunakan Enkripsi Homomorfik, Tugas Akhir(TA), Institut Teknologi Bandung, Bandung.

Hermawati. F. D., Tahir. M., Syaifurrohman. M., Hikmah. M., Amroin. J. A., Bahruddin. M., & Irsyad. I. (2023). Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard), Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI), Vol. 2 No. 2, Hal. 45-56.

Indrawan. D., & Mashur. D. (2023). Inovasi Pemilihan Kepala Desa Berbasis EVoting Di Desa Batu Gajah Kecamatan Pasir Penyu Kabupaten Indragiri Hulu, Jurnal Administrasi Negara, Vol. 1 No. 1, Hal. 1-14.

Kho. Y., Heng. S., & Chin. J. (2022). Review of Cryptographic Electronic Voting, Review, MDPI, Switzerland.

Makkaoui. K. E., Ezzati. A., Beni-Hssane. A., & Ouhmad. S. (2018). A swift Cloud Paillier scheme to protect sensitive data confidentiality in cloud computing, The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018), Morocco.

Medileh. S., Laouid. A., Hammoudeh. M., Kara. M., Bejaoui. T., Eleyan. A., & Al-Khalidi. M. (2023). A Multi-Key with Partially Homomorphic Encryption Scheme for Low-End Devices Ensuring Data Integrity, MDPI, Switzerland.

Mulya. M. F., Rismawati. N., & Trisanto. D. (2019). Analisis Dan Perancangan Simulasi Algoritma Paillier Cryptosystem Pada Pesan Text Dengan Presentation Format Binary, Octal, Hexadecimal dan Base64, Faktor Exacta, Vol. 13, No. 4, pp. 208–215.

Munir. R. (2023). Enkripsi Homomorfik, Teaching Materials, Institut Teknologi Bandung, Bandung.

Munjal. K., & Bhatia. R. (2023). Analysing RSA and PAILLIER homomorphic Property for security in Cloud, 4th International Conference on Innovative Data Communication Technology and Application.

Nakai. T., Suzuki. D., & Fujino. T. (2021). Timing Black-Box Attacks: Crafting Adversarial Examples through Timing Leaks against DNNs on Embedded 31 Devices, IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2021, No. 3, pp. 149–175.

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Lecture Notes in Computer Science, 1592, 223-238. https://www.lamsade.dauphine.fr/~litwin/cours98/Doc-cours-clouds/Pai99pai.pdf, diakses pada 28 Februari 2024.

Panggabean. A. R. (2020). Implementasi Algoritma Paillier Cryptosystem Untuk Keamanan Data Video Mpeg Pada Aplikasi Chat, Jurnal Informasi dan Teknologi Ilmiah (INTI), Vol. 8, No. 1, Hal. 1-6.

Press, R. (2021). Side-channel attacks explained: everything you need to know, https://www.rambus.com/blogs/side-channel-attacks/. 14 Oktober 2021, diakses pada 31 Januari 2024.

Purba. J. A. N., Sinaga. D., & Purba. S. R. (2019). Implementasi Algoritma Paillier Cryptosystem Pengamanan Audio, Seminar Nasional Teknologi Komputer & Sains (SAINTEKS), Hal. 898 – 902.

Purba. J. A. N., Zebua. T., & Hondro. R. K. (2019). Implementasi Algoritma Paillier Cryptosystem Pengamanan Citra Digital Pada Aplikasi Chat, KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), Vol. 3, No. 1, pp. 299–306.

Rajak. A. M., & Agustia. R. D. (2021). Purwarupa Sistem E-Voting Menggunakan Enkripsi Homomorphic Di Komisi Pemilihan Umum Kota Bandung, JUPITER : Jurnal Penelitian Mahasiswa Teknik Dan Ilmu Komputer, Vol. 1, No. 1.

Rocha. V. F., & Lopez. J. (2018). An Overview on Homomorphic Encryption Algorithms, Final Graduation Project, State University Of Campinas Institute Of Computing, São Paulo.

Standaert. F. (2016). Introduction to Side-Channel Attacks, Université Catholique de Louvain, Belgium.

Suharsono. T. N., & Yulianto. F. A. (2021). Skema Keamanan Sistem E-Voting, e-book, LeutikaPrio, Yogyakarta.

Supriyadi., Ronal., & Yuliana. (2023). Studi Perbandingan Skema Enkripsi Homomorfik Dalam Voting System E-Suara, Jurnal Jaringan Sistem Informasi Robotik (JSR), Vol. 7, No. 1.

Thabit. F., Can. O., Alhomdy. S., Al-Gaphari. G. H., & Jagtap. S. (2022). Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing, International Journal of Intelligent Networks, Turkey.

Zhao. M., & Geng. Y. (2019). Homomorphic Encryption Technology for Cloud Computing, 8th International Congress of Information and Communication Technology, ICICT 2019.