DAFTAR PUSTAKA

Abdullah, A. (2022). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. *IJERT*, *11*(6).

Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions. *Information*, *13*(10), 442. https://doi.org/10.3390/info13100442.

Agrawal, A., Pattiwar, A., Jammoria, A. S., Modi, R., & Raja, S. P. (2025). Secure system to secure crime data using hybrid RSA-AES and hybrid Blowfish-Triple DES. *International Journal of Electronic Security and Digital Forensics*, 1(1). https://doi.org/10.1504/IJESDF.2025.10059534.

Almazari, M. M., Taqieddin, E., Shatnawi, A. S., & Al-Shara, Z. (2023). An evaluation of the RSA private keys and the presence of weak keys. *Journal of Discrete Mathematical Sciences & Cryptography*, 26(8), 2273–2284. https://doi.org/10.47974/JDMSC-1670

Al-Kadei, F. H. M. S., Mardan, H. A., & Minas, N. A. (2020). Speed Up Image Encryption by Using RSA Algorithm. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1302–1307. https://doi.org/10.1109/ICACCS48705.2020.9074430.

Aminuddin, A. (2020). Android Assets Protection Using RSA and AES Cryptography to Prevent App Piracy. *2020 3rd International Conference on Information and Communications Technology (ICOIACT)*, 461–465. https://doi.org/10.1109/ICOIACT50329.2020.9331988.

Bae, S. (2019). Big-O Notation. In *JavaScript Data Structures and Algorithms* (pp. 1–11). Apress. https://doi.org/10.1007/978-1-4842-3988-9_1.

Chivers, I., & Sleightholme, J. (2015). An Introduction to Algorithms and the Big O Notation. In *Introduction to Programming with Fortran* (pp. 359–364). Springer International Publishing. https://doi.org/10.1007/978-3-319-17701-4_23.

Choi, H., & Seo, S. C. (2021). Optimization of PBKDF2 Using HMAC-SHA2 and HMAC-LSH Families in CPU Environment. *IEEE Access*, 9, 40165–40177. https://doi.org/10.1109/ACCESS.2021.3065082.

SEKOLAH PASCASARJANA

CNN Indonesia. (2021, February 17). Pakar sayangkan nama dan jabatan pegawai Kejaksaan RI bocor. *CNN Indonesia*. Retrieved June 14, 2024, from https://www.cnnindonesia.com/teknologi/20210217192212-185-607578/pakar-sayangkan-nama-dan-jabatan-pegawai-kejaksaan-ri-bocor.

Dhami, J., Dave, N., Bagwe, O., Joshi, A., & Tawde, P. (2021). Deep Learning Approach To Predict Software Development Life Cycle Model. *2021 International Conference on Advances in Computing, Communication, and Control (ICAC3)*, 1–7. https://doi.org/10.1109/ICAC353642.2021.9697271.

Dossou-Yovo, V., Nitaj, A., & Togbé, A. (2024). Improved cryptanalysis of RSA. *Journal of Discrete Mathematical Sciences and Cryptography*, 27(3), 945–961. https://doi.org/10.47974/JDMSC-1570

Dr Asha Ambhaikar, Mr. A. G. (2021). AES and RSA-Based Hybrid Algorithms for Message Encrytion & Decrytion. *INFORMATION TECHNOLOGY IN INDUSTRY*, *9*(1), 273–279. https://doi.org/10.17762/itii.v9i1.129.

Durge, R. S., & Deshmukh, V. M. (2025). Securing cloud data: A hybrid encryption approach with RSA and AES for enhanced security and performance. *Journal of Integrated Science and Technology*, 13(3). https://doi.org/10.62110/sciencein.jist.2025.v13.1060

Easttom, W. (2022). *Modern Cryptography* (2nd ed.). Springer International Publishing. https://doi.org/10.1007/978-3-031-12304-7.

Fadlil, A., Riadi, I., & Nugrahantoro, A. (2020). Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *11*(3), 155. https://doi.org/10.24843/LKJITI.2020.v11.i03.p04.

Gaur, S. S., Kalsi, H. S., & Gautam, S. (2019). A comparative study and analysis of cryptographic algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH. *International Journal Of Research In Electronics And Computer Engineering (IJRECE)*, *7*(1), 996–999.

Iuorio, A. F., & Visconti, A. (2019). Understanding Optimizations and Measuring Performances of PBKDF2. In I. Woungang & S. K. Dhurandher (Eds.), *2nd International Conference on Wireless Intelligent and Distributed Environment for*

SEKOLAH PASCASARJANA

Communication (pp. 101–114). Springer International Publishing. https://doi.org/10.1007/978-3-030-11437-4_8

Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 791–796. https://doi.org/10.1109/ESCI50559.2021.9397005.

Jain, J. K., Chauhan, D., & Singh, A. (2025). A survey on cryptographic algorithms and information security practices. In *Advances in Information Security and Privacy* (pp. 261–298). IGI Global. https://doi.org/10.4018/979-8-3693-8014-7.ch012.

Jintcharadze, E., & Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 1–5. https://doi.org/10.1109/EWDTS50664.2020.9224901.

Joseph, S., Fred, W., & Olaoye, G. (2023). *Network security in the Old Age: Protecting Information and Structures*.

Khan, M. A., & Sadiq, Mohd. (2011). Analysis of black box software testing techniques: A case study. *The 2011 International Conference and Workshop on Current Trends in Information Technology (CTIT 11)*, 1–5. https://doi.org/10.1109/CTIT.2011.6107931.

Kumari, A., Pranav, P., Dutta, S., & Chakraborty, S. (2023). Empirical and statistical comparison of RSA and El-Gamal in terms of time complexity (pp. 111–120). https://doi.org/10.1007/978-3-031-18497-0_9.

Kusnadi, I. T., dkk. (2019). *Pemodelan sistem berbasis objek with UML (Edisi ke-1)*. Graha Ilmu. ISBN: 978-623-228-311-4.

Kuznetsov, O., Rusnak, A., Yezhov, A., Kuznetsova, K., Kanonik, D., & Domin, O. (2024). Merkle trees in blockchain: A Study of collision probability and security implications. *Internet of Things*, *26*, 101193. https://doi.org/10.1016/j.iot.2024.101193.

Lee, D., & Park, N. (2021). Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. *Multimedia Tools and Applications*, *80*(26–27), 34517–34534. https://doi.org/10.1007/s11042-020-08776-y.

SEKOLAH PASCASARJANA

Liu, Y., Gong, W., & Fan, W. (2018). Application of AES and RSA Hybrid Algorithm in E-mail. *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 701–703. https://doi.org/10.1109/ICIS.2018.8466380.

Ma, L., Sun, X., & Jin, W. (2020). Symmetric–asymmetric hybrid encryption and decryption system based on chaotic iris phase mask and computer-generated holography. *Optical Engineering*, 59(8). https://doi.org/10.1117/1.OE.59.8.083106.

Meftah, A., Yusef Sa'ad, H. H., Al-Ashmoery, Y., Saad, A.-M. H. Y., Sa'd, A. H. Y., & Alwesabi, K. (2024). A comparative analysis of cryptography algorithms in information security. *2024 10th International Conference on Computing, Engineering and Design (ICCED)*, 1–6. https://doi.org/10.1109/ICCED64257.2024.10983680

Mei, Y. (2017). Using the HashChain to Improve the Security of the Hadoop. *Proceedings of the 3rd Annual International Conference on Electronics, Electrical Engineering and Information Science (EEEIS 2017)*. https://doi.org/10.2991/eeeis-17.2017.82.

Merahe, R. K., Nogwina, M., Ntlatywa, P., Makhoere, L., Modiba, N., & Chibaya, C. (2024). White-box processing of large prime numbers used in the RSA algorithm. In *2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 133–137). IEEE. https://doi.org/10.1109/IMITEC60221.2024.10851164.

Munir, R. (2019). *Kriptografi* (edisi kedua). Bandung: Informatika Bandung. ISBN 978-623-7131-05-2.

Murtaza, A., Pirzada, S. J. H., Hasan, M. N., Xu, T., & Jianwei, L. (2019). Parallelized Key Expansion Algorithm for Advanced Encryption Standard. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, 609–612. https://doi.org/10.1109/ICSESS47205.2019.9040825

Nagaraj, S., & Mohanraj, E. (2020). Enhanced Selective Encryption method for Bigdata Sensing Stream using one way Hash Chain Algorithm. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 297–302. https://doi.org/10.1109/ICACCCN51052.2020.9362915.

SEKOLAH PASCASARJANA

Pardeshi, M., Sheu, R.-K., & Yuan, S.-M. (2022). Hash-chain fog/edge: A mode-based hash-chain for secured mutual authentication protocol using zero-knowledge proofs in fog/edge. *Sensors*, 22(2), 607. https://doi.org/10.3390/s22020607.

Phalke, S., Vaidya, Y., & Metkar, S. (2022). Big-O Time Complexity Analysis Of Algorithm. *2022 International Conference on Signal and Information Processing (IConSIP)*, 1–5. https://doi.org/10.1109/ICoNSIP49665.2022.10007469.

Ping, H. (2022). Network information security data protection based on data encryption technology. *Wireless Personal Communications*, 126(3), 2719–2729. https://doi.org/10.1007/s11277-022-09838-0

Priyanka, M. P., Prasad, E. L., & Reddy, A. R. (2016). FPGA implementation of image encryption and decryption using AES 128-bit core. *2016 International Conference on Communication and Electronics Systems (ICCES)*, 1–5. https://doi.org/10.1109/CESYS.2016.7889929.

Qiuyuan Huang, Renzhi Cao, Bobin Deng, & Xingfu Wang. (2011). Hash-chain based Public Key Management Algorithm of Mobile Ad hoc network. *2011 IEEE International Conference on Computer Science and Automation Engineering*, 247–251. https://doi.org/10.1109/CSAE.2011.5953214.

Rathee, T., & Singh, P. (2021). Secure data sharing using Merkle hash digest based blockchain identity management. *Peer-to-Peer Networking and Applications*, *14*(6), 3851–3864. https://doi.org/10.1007/s12083-021-01212-4.

Rinderle-Ma, S., Mangler, J., & Ritter, D. (2024). Fundamentals of Information Systems Interoperability (1st ed.). *Springer International Publishing*. https://doi.org/10.1007/978-3-031-48322-6.

Scripcariu, L., Diaconu, F., Matasaru, P. D., & Gafencu, L. (2018). AES vulnerabilities study. *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–4. https://doi.org/10.1109/ECAI.2018.8678930.

Shokunbi, O., Uche, O., Akinwunmi, D., Akinwumi, H., Awodele, O., & Ayankoya, F. (2024). Emerging Security Threat in the SDLC and Mitigations. *2024 IEEE SmartBlock4Africa*, 1–11. https://doi.org/10.1109/SmartBlock4Africa61928.2024.10779490.

SEKOLAH PASCASARJANA

Sholikhatin, S. A., Kuncoro, A. P., Munawaroh, A. L., & Setiawan, G. A. (2023). Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security. *Edu Komputika Journal*, *9*(1), 60–67. https://doi.org/10.15294/edukomputika.v9i1.57389.

Siva, F., Assegaf, S. M. U., Pahlevi, S. A., & Yaqin, M. A. (2023). Survei Metode-Metode Software Development Life Cycle dengan Metode Systematic Literature Review. *ILKOMNIKA: Journal of Computer Science and Applied Informatics*, 5(2), 36–52. https://doi.org/10.28926/ilkomnika.v5i2.447.

Smith, J., Doe, A., White, B., Black, C., & Grey, D. (2022). Enhancing data security and integrity using hashchain in information systems. *In 2022 IEEE Future Networks World Forum (FNWF)* (pp. 123-129). IEEE. https://doi.org/10.1109/FNWF55208.2022.00021

Su, S.-L., Wuu, L.-C., & Jhang, J.-W. (2007). A new 256-bits block cipher – Twofish256. *2007 International Conference on Computer Engineering & Systems*, 166–171. https://doi.org/10.1109/ICCES.2007.4447043.

Tajuddin, M., Bachtiar, A., Sriwinarti, N. K., Juliansyah, A., Rizal, A. A., & Ismarmiaty. (2020). *Sistem informasi*. Yogyakarta: Deepublish. ISBN 978-623-02-1397-7.

Tiwari, D., Singh, A., & Prabhakar, A. (2020). *Performance Analysis of AES, RSA and Hashing Algorithm Using Web Technology* (pp. 413–418). Springer. https://doi.org/10.1007/978-981-15-2369-4_35.

Venugopal, K., & Kolluru, V. S. (2024). *Evaluating user vulnerabilities* (pp. 161–192). IGI Global. https://doi.org/10.4018/979-8-3693-9491-5.ch008

Veronica, L., Bayu, S., & Aris, S. (2010). Perancangan perangkat lunak untuk keamanan informasi pada email dengan menggunakan algoritma AES dan RSA (Tesis, Program Studi Magister Sistem Informasi). Universitas Diponegoro.

Visconti, A., Bossi, S., Ragab, H., & Calò, A. (2015). On the Weaknesses of PBKDF2. In M. Reiter & D. Naccache (Eds.), *Cryptology and Network Security* (pp. 119–126). Springer International Publishing. https://doi.org/10.1007/978-3-319-26823-1_9.

Wang, J., Wang, W., Yang, J., Yu, Z., Han, J., & Zeng, X. (2015). Parallel implementation of AES on 2.5D multicore platform with hardware and software co-

SEKOLAH PASCASARJANA

design. *2015 IEEE 11th International Conference on ASIC (ASICON)*, 1–4. https://doi.org/10.1109/ASICON.2015.7517001.

Waybhase, S. K., & Adakane, P. (2022). Data Security using Advanced Encryption Standard(AES). *IJERT*, *11*(6). https://doi.org/10.17577/IJERTV11IS060338.

Zhang, Z., Liu, X., Li, M., Yin, H., Zhu, L., Khoussainov, B., & Gai, K. (2024). HCA: Hashchain-Based Consensus Acceleration Via Re-Voting. *IEEE Transactions on Dependable and Secure Computing*, 21(2), 775–788. https://doi.org/10.1109/TDSC.2023.3262283

Zhao, C., Shi, M., Huang, M., & Du, X. (2019). Authentication Scheme Based on Hashchain for Space-Air-Ground Integrated Network. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC.2019.8761821.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/IJWGS.2018.095647.

Zou, L., Ni, M., Huang, Y., Shi, W., & Li, X. (2020). Hybrid Encryption Algorithm Based on AES and RSA in File Encryption (pp. 541–551). Springer. https://doi.org/10.1007/978-981-15-3250-4_68.

SEKOLAH PASCASARJANA