DAFTAR PUSTAKA

Abdeldaym, R.S., Elkader, Hate, M.A. dan Hussein, R., 2019, Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem, *International Journal of Electronic and Engineering*, [Online] 10 (1), 51–64, tersedia di DOI:10.6636/IJEIE.201903.

Al-kaabi, S.S. dan Belhaouari, S.B., 2019, A Survey on Enhanced RSA Algorithms, *Journal of Computer and Information Technology (CS & IT)*, [Online] 123–142, tersedia di DOI:10.5121/csit.2019.90411.

Al-naji, F.H. dan Zagrouba, R., 2020, A survey on continuous authentication methods in Internet of Things environment, *Computer Communications*, [Online] 163 (Sept), 109–133, tersedia di DOI:10.1016/j.comcom.2020.09.006.

Albalawi, A., 2019, A Survey on Authentication Techniques for the Internet of Things, *2019 International Conference on Computer and Information Sciences (ICCIS)*, [Online], 2019 IEEE, Sakaka, Saudi Arabia., hal. 1–5, tersedia di DOI:10.1109/ICCISci.2019.8716401.

Alkady, Y., Habib, M.I. dan Rizk, R.Y., 2013, A New Security Protocol Using Hybrid Cryptography Algorithms, *2013 9th International Computer Engineering Conference (ICENCO)*, [Online], 2013 Giza, Egypt., hal. 109–115, tersedia di DOI:10.1109/ICENCO.2013.6736485.

Allied Telesis, 2017, *OpenVPN: Feature Overview and Configuration Guide*, C613-22017 edisi, Allied Telesis, Singapore.

Asghar, M.R., Dán, G., Miorandi, D. dan Chlamtac, I., 2017, Smart Meter Data Privacy : A Survey, *IEEE Communication Surveys and Tutorials*, [Online] 19 (4), 2820–2835, tersedia di DOI:10.1109/COMST.2017.2720195.

Asghar, M.R., Hu, Q. dan Zeadally, S., 2019, Cybersecurity in industrial control systems: Issues, technologies, and challenges, *Computer Networks*, [Online] 165106946, tersedia di DOI:10.1016/j.comnet.2019.106946.

Azees, M., 2019, Reply to Comments on Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, 20 (9), 2925097,

Bahig, H.M., Mahdi, M.A., Alutaibi, K.A., AlGhadhban, A. dan Bahig, H.M., 2020, Performance Analysis of Fermat Factorization Algorithms, *International Journal of Advanced Computer Science and Applications*, [Online] 11 (12), 340–352, tersedia di DOI:10.14569/IJACSA.2020.0111242.

Balasubramanian, B., Manivasagam, G. dan Kumar, A., 2017, Metrics for Performance Evaluation of Encryption Algorithms, *International Journal of Advance Research in Science and Engineering*, 6 (3), 62–72,

Banerjee, S., Odelu, V., Das, A.K., Srinivas, J., Kumar, N., Chattopadhyay, S. dan Choo, K.R., 2019, A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment, *IEEE Internet of Things Journal*, 6 (5), 8739–8752,

Bansal, M., Gupta, S. dan Mathur, S., 2021, Comparison of ECC and RSA Algorithm with DNA Encoding for IoT Security, *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, [Online] 1340–1343, tersedia di DOI:10.1109/ICICT50816.2021.9358591.

Barker, E., 2020, Recommendation for Key Management – Part 1: General. *NIST SP 800-57 Part 1 Rev 5*. (May) hal.1–142.

Bellare, M. dan Rogaway, P., 1993, Random oracles are practical: a paradigm for designing efficient protocols, *1st ACM Conference on Computer and Communications Security*, (November 1993), 62–73,

Bittinger, M.L., Ellenbogen, D.J. dan Surgent, S.A., 2012, *Calculus and Its Applications*, Tenth Edit, Deirdre Lynch, Jennifer Crum, dan Rachel S. Reeve (ed.), Addison-Wesley, Singapore., [Online]. tersedia di DOI:10.2307/3612210.

Blömer, J. dan May, A., 2004, A generalized Wiener attack on RSA, *Lecture Notes in Computer Science (LNCS Springer)*, [Online] 2947 (May), 1–13, tersedia di DOI:10.1007/978-3-540-24632-9_1.

Bunder, M., Nitaj, A., Susilo, W. dan Tonien, J., 2017, A generalized attack on RSA type cryptosystems, *Theoretical Computer Science*, [Online] 70474–81, tersedia di DOI:10.1016/j.tcs.2017.09.009.

Canberra, 2015, Canberra: Part of Mirion Technology. *Instituto de Engenharia Nuclear: Progress Report*.

Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Bal, S., Roy, S., Sarkar, M.K., Kumar, S. dan Das, R., 2017, ACAFP : Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication . A Review on RSA Algorithm, *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference*, [Online], 2017 Bangkok, Thailand., hal. 332–337, tersedia di DOI:10.1109/IEMECON.2017.8079618.

Colak, I., Sagiroglu, S., Fulli, G. dan Yesilbudak, M., 2016, A survey on the critical issues in smart grid technologies, *Renewable and Sustainable Energy Reviews*, [Online] 54 (Nov.), 396–405, tersedia di DOI:10.1016/j.rser.2015.10.036.

Daileda, R.C., 2015, The Fermat factorization method, *Number Theory*, 7 edisi, Trinity University, San Antonio., hal.

Deng, L. dan Gao, R., 2021, Certificateless two-party authenticated key agreement scheme for smart grid, *Information Sciences*, [Online] 543 (Jan), 143–156,

tersedia di DOI:10.1016/j.ins.2020.07.025.

Ebenezer, J. dan Murty, S.A.V.S., 2015, Deployment of Wireless Sensor Network for Radiation Monitoring, *Proc. of 2015 International Conf. od Computing and Networks Communications (CoCoNet'15)*, [Online], 2015 Trivandum, India., hal. 27–32, tersedia di DOI:10.1109/CoCoNet.2015.7411163.

Elezi, M. dan Raufi, B., 2015, Conception of Virtual Private Networks using IPsec suite of protocols , comparative analysis of distributed database queries using different IPsec modes of encryption, *Procedia - Social and Behavioral Sciences*, [Online] 1951938–1948, tersedia di DOI:10.1016/j.sbspro.2015.06.206.

Elhoseny, M. dan Shankar, K., 2020, Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique, *IEEE Transaction on Reliability*, [Online] 69 (3), 1077–1086, tersedia di DOI:10.1109/TR.2019.2915800.

Envinet, 2017, *Envinet: Environmental Radiation Detection at a Glance*. (September).

Fabro, M., 2007, *Control Systems Cyber Security : Defense-in- Depth Strategies Control Systems Cyber Security :* (May).

Fakroon, M., Alshahrani, M., Gebali, F. dan Traore, I., 2020, Secure remote anonymous user authentication scheme for smart home environment, *Internet of Things*, [Online] 9 (100158), 1–20, tersedia di DOI:10.1016/j.iot.2020.100158.

Fan, Q., Chen, J., Jegatha, L. dan Luo, M., 2021, A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, *Journal of Systems Architecture*, [Online] 117 (102112), 1–12, tersedia di DOI:10.1016/j.sysarc.2021.102112.

Fan, S., Ye, F., Guo, J., Liang, Y., Xu, G., Zhang, X., Qian, Y. dan Engineering, E., 2015, A Security Protocol for Wireless Sensor Networks Designed for Monitoring Smart Grid Transmission Lines, *23rd International Conf. on Computer Communication and Networks (ICCCN)*, [Online], 2015 Shanghai, China., hal. 1–7, tersedia di DOI:10.1109/ICCCN.2014.6911789.

Fang, D., Qian, Y. dan Hu, R.Q., 2020, A Flexible and Efficient Authentication and Secure Data Transmission Scheme for IoT Applications, *IEEE Internet of Things Journal*, [Online] 7 (4), 3474–3484, tersedia di DOI:10.1109/JIOT.2020.2970974.

Farhadi, M.F., Nikooghadam, M., Hossein, A.M. dan Movali, B., 2020, A lightweight key management protocol for secure communication in smart grids, *Electric Power Systems Research*, [Online] 178 (September 2019), 1–8, tersedia di DOI:10.1016/j.epsr.2019.106024.

Ford, V., Siraj, A. dan Rahman, M.A., 2017, Secure and efficient protection of

consumer privacy in Advanced Metering Infrastructure supporting fine-grained data analysis, *Journal of Computer and System Sciences*, [Online] 83 (July), 84–100, tersedia di DOI:10.1016/j.jcss.2016.06.005.

Gagneja, K. dan Singh, K.J., 2015, A Survey and Analysis of Security Issues on RSA Algorithm, *International Journal of Applied Sciences, Engineering, and Technology*, [Online] 11 (8), 847–853, tersedia di DOI:10.19026/rjaset.11.2094.

Gaudry, P., Guillevic, A., Heninger, N. dan Thomé, E., 2020, *Integer factorization*.

Gope, P., 2020, PMAKE : Privacy-aware multi-factor authenticated key establishment scheme for Advance Metering Infrastructure in smart grid, *Computer Communications*, [Online] 152 (December 2019), 338–344, tersedia di DOI:10.1016/j.comcom.2019.12.042.

Grover, J. dan Sharma, S., 2016, Security Issues in Wireless Sensor Network - A Review, *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, [Online], 2016 Noida, India., hal. 397–404, tersedia di DOI:10.1109/ICRITO.2016.7784988.

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. dan Soyata, T., 2019, A survey on cybersecurity , data privacy , and policy issues in cyber-physical system deployments in smart cities ☆, *Sustainable Cities and Society*, [Online] 50 (August 2018), 101660, tersedia di DOI:10.1016/j.scs.2019.101660.

Hamamreh, R.A. dan Jamoos, M.A., 2013, Hash Algorithm for Data Integrity based on Matrix Combination, *Proceedings of International Arab Conference on Information Technology*, 2013 Al-Quds University, Al-Quds., hal. 1–5,

Hamdi, S.M., Zuhori, S.T., Mahmud, F. dan Pal, B., 2014, *A Compare between Shor ' s Quantum Factoring Algorithm and General Number Field Sieve*, [Online] (April), tersedia di DOI:10.1109/ICEEICT.2014.6919115.

Hermawan, N.T.E., Winarko, E. dan Ashari, A., 2020, An Application of Defense in Depth Concept for Securing Data Transmission in Radiation Monitoring System for Nuclear Installation, *Proceeding of International Conference on Nuclear Science Technology and Application*, 2020 Indonesian Nuclear Energy Agency, Jakarta., hal. 1–10,

Hermawan, N.T.E., Winarko, E. dan Ashari, A., 2018, Securing Data Transmission for Radiation Monitoring System in Nuclear Installation, *International Journal of Computer Application*, 179 (22), 32–40,

Hermawan, N.T.E., Winarko, E., Ashari, A. dan Akhmad, Y.R., 2021, High Secure Initial Authentication Protocol based on EPNR Cryptosystem for Supporting Radiation Monitoring System, *International Journal of Intelligent Engineering and Systems*, [Online] 4 (August), 1–14, tersedia di

DOI:10.22266/ijies2019.xxxx.xx.

Hiromoto, R.E., Sachenko, A., Kochan, V., Koval, V., Turchenko, V., Roshchupkin, O., Yatskiv, V. dan Kovalok, K., 2014, Mobile Ad Hoc Wireless Network for Pre- and Post-Emergency Situations in Nuclear Power Plant, *Proc. of the 2nd IEEE International Symposium on Wireless Systems*, 2014 Offenburg, Germany., hal. 92–96,

Hong, H., Hu, B. dan Sun, Z., 2019, Toward secure and accountable data transmission in Narrow Band Internet of Things based on blockchain, *International Journal of Distributed Sensor Network*, [Online] 15 (4), 1–10, tersedia di DOI:10.1177/1550147719842725.

Hussain, M., Mehmood, A., Khan, S., Khan, M.A. dan Iqbal, Z., 2019, Authentication Techniques and Methodologies used in Wireless Body Area Networks, *Journal of Systems Architecture*, [Online] 101 (September), 101655, tersedia di DOI:10.1016/j.sysarc.2019.101655.

Hwang, R.J., Su, F.F., Yeh, Y.S. dan Chen, C.Y., 2005, An efficient decryption method for RSA cryptosystem, *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, [Online] 1585–590, tersedia di DOI:10.1109/AINA.2005.97.

IAEA, 2005, *Environmental and Source Monitoring for Purposes of Radiation Protection*. hal.1–107.

IAEA, 2011, IAEA Nuclear Security Series No. 17 Computer Security at Nuclear Facilities. *IAEA Nuclear Security Series*. (17).

International Telecommunication Union, 2003, *Transmission Systems and Media, Digital Systems and Networks*.

Intila, C., Gerardo, B. dan Medina, R., 2016, A study of public key "e" in RSA algorithm, *IOP Conference Series: Materials Science and Engineering*, [Online] 482 (1), 1–9, tersedia di DOI:10.1088/1757-899X/482/1/012016.

Intila, C.A., Gerardo, B. dan Medina, R.P., 2018, Modified rsa algorithm based on key generation 1, *Proceeding of The IIER International Conference*, 2018 Manila, Philippines., hal. 1–6,

Islam, M.A., Islam, M.A., Islam, N. dan Shabnam, B., 2018, A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers, *Journal of Computer and Communications*, [Online] 06 (03), 78–90, tersedia di DOI:10.4236/jcc.2018.63006.

ISO/IEC, 2013, *Information technology — Security techniques — Entity authentication assurance framework*. 2013 (1).

ITUT, 1991, Security Architecture for Open Systems Interconection. *The International Telegraph and Telephone Consultative Comittee, Recommendation X.800*.

Jaju, S.A. dan Chowhan, S.S., 2015, A Modified RSA Algorithm to Enhance Security for Digital Signature, *2015 International Conference and Workshop on Computing and Communication, IEMCON 2015*, [Online], 2015 IEEE., hal. 1–5, tersedia di DOI:10.1109/IEMCON.2015.7344493.

Kamardan, M.G., Aminudin, N., Che-Him, N., Sufahani, S., Khalid, K. dan Roslan, R., 2018, Modified Multi Prime RSA Cryptosystem, *Journal of Physics: Conference Series*, [Online] 995 (1), 1–6, tersedia di DOI:10.1088/1742-6596/995/1/012030.

Karati, A., Fan, C. dan Hsu, R., 2019, Provably Secure and Generalized Signcryption With Public Verifiability for Secure Data Transmission, *IEEE Internet of Things Journal*, [Online] 6 (6), 10431–10440, tersedia di DOI:10.1109/JIOT.2019.2939204.

Kaur, A. dan Singh, S., 2016, A Hybrid Technique of Cryptography and Watermarking for Data Encryption and Decryption, *2016 Fourth International Conference on Parallel, Distributed and Grod Computing (PDGC)*, 2016 Waknaghat, India., hal. 351–356,

Kim, D., 2014, Cyber security issues imposed on nuclear power plants, *Annals of Nuclear Energy*, [Online] 65141–143, tersedia di DOI:10.1016/j.anucene.2013.10.039.

Knoll, G.F., 2010, *Radiation Detection and Measurement*, Fourth Edi, Jennifer Welter dan Debra Matteson (ed.), John Wiley & Sons, Inc, Danvers, US., [Online]. tersedia di DOI:10.1007/s13398-014-0173-7.2.

Koblitz, N. dan Menezes, A.J., 2004, A Survey of Public-Key Cryptosystems, *SIAM Review*, 4 (64), 599–634,

Kodama, Y., Odajima, T., Arima, E. dan Sato, M., 2020, Evaluation of Power Management Control on the Supercomputer Fugaku, *2020 IEEE International Conference on Cluster Computng (CLUSTER)*, [Online], 2020 IEEE, Kobe, Japan., hal. 484–493, tersedia di DOI:10.1109/CLUSTER49012.2020.00069.

Krishnamoorthy, M. dan Perumal, V., 2017, Secure and efficient hand-over authentication in WLAN using elliptic curve RSA, *Computers and Electrical Engineering*, [Online] 64552–566, tersedia di DOI:10.1016/j.compeleceng.2017.06.002.

Kromodimoeljo, S., 2009, *Teori & Aplikasi Kriptografi*, Pertama, SPK IT Consulting, Bandung.

Kumar, M.G.V., 2016, *A Survey on Current Key Issues and Status in Cryptography*, 2016 hal. 0–5,

Kurera, C. dan Navoda, D., 2018, Node-to-Node Secure Data Transmission Protocol for Low-power IoT Devices, *2018 International Conference on Advances in ICT Emerging Regions (ICTer)*, 2018 IEEE., hal. 332–338,

Landsberger, S. dan Tsoulfanidis, N., 2015, *Measurement & Detection Of Radiation*, Fourth, CRC Press, New York.

Li, X., Wu, F., Kumari, S., Xu, L., Kumar Sangaiah, A. dan Choo, K.-K.R., 2019, A provably secure and anonymous message authentication scheme for smart grids, *Journal of Parallel and Distributed Computing*, [Online] 132 (Oct), 242–249, tersedia di DOI:10.1016/j.jpdc.2017.11.008.

Liu, C. dan Chung, Y., 2017, Secure user authentication scheme for wireless healthcare, *Computers and Electrical Engineering*, [Online] 59250–261, tersedia di DOI:10.1016/j.compeleceng.2016.01.002.

Liu, X., Zhang, R. dan Zhao, M., 2019, A robust authentication scheme with dynamic password for wireless body area networks, *Journal of Computer Networks*, [Online] 161220–234, tersedia di DOI:10.1016/j.comnet.2019.07.003.

Lone, A.H. dan Khalique, A., 2016, Generalized RSA using 2 k Prime Numbers with Secure Key Generation, *International Journal of Security and Communication Networks*, [Online] 9 (September), 4443–4450, tersedia di DOI:10.1002/sec.

Luo, X.I., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C. dan Tian, Z., 2020, A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment, *IEEE Access*, [Online] 867192–67204, tersedia di DOI:10.1109/ACCESS.2020.2978525.

Lüy, E., Karatas, Z.Y. dan Ergin, H., 2016, Comment on " An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)" Encryption :, *Journal of Information Security and Applications*, [Online] 301–2, tersedia di DOI:10.1016/j.jisa.2016.03.006.

M. Abd Zaid, M. dan Hassan, S., 2018, Lightweight RSA Algorithm Using Three Prime Numbers, *Journal of Engineering and Applied Sciences*, [Online] 14 (5), 9032–9035, tersedia di DOI:10.36478/jeasci.2019.9032.9035.

Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X. dan Sangaiah, A.K., 2018, An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, *Future Generation Computer Systems*, [Online] 81 (Apr), 557–565, tersedia di DOI:10.1016/j.future.2017.05.002.

Makkaoui, K. El, Beni-Hssane, A., Ezzati, A. dan El-Ansari, A., 2017, Fast Cloud-RSA Cloud-RSA Scheme for Promoting Promoting Data Data Confidentiality in the the Cloud Computing, *Procedia Computer Science*, [Online], 2017 Elsevier B.V., hal. 33–40, tersedia di DOI:10.1016/j.procs.2017.08.282.

Mamun, A., Rahman, S.S., Shaon, T.A. dan Hossain, M.A., 2017, Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte, *International Journal of Computer and Communications (IJCNC)*, [Online] 9 (2), 69–88, tersedia di DOI:10.5121/ijcnc.2017.9206.

Manu dan Goel, A., 2017, Encryption algorithm using dual modulus, *3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT 2017)*, [Online], 2017 IEEE., hal. 1–4, tersedia di DOI:10.1109/CIACT.2017.7977331.

Maqsood, F., Ahmed, M., Mumtaz, M. dan Ali, M., 2017, Cryptography: A Comparative Analysis for Modern Techniques, *International Journal of Advanced Computer Science and Applications*, [Online] 8 (6), 442–448, tersedia di DOI:10.14569/ijacsa.2017.080659.

Mishra, A., Abdulganiyu, A., Gana, U.M. dan Awwal, A., 2019, Survey and Analysis of Data Encryption Methods and Development of A Security Model to Encrypt / Decrypt Messages, *International Journal of Engineering and Technical Research (IJETR)*, 0869 (March), 190–195,

Mishra, D., Dharminder, D., Yadav, P., Rao, Y.S., Vijayakumar, P. dan Kumar, N., 2020, A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party, *Journal of Information Security and Applications*, [Online] 55 (102648), 1–9, tersedia di DOI:10.1016/j.jisa.2020.102648.

Mollin, R.A., 2007, *An Introduction To Cryptography*, Second Edi, Chapman & Hall/CRC, New York., [Online]. tersedia di DOI:10.4324/9780203414040.

Mumtaz, M. dan Ping, L., 2019, Forty years of attacks on the RSA cryptosystem: A brief survey, *Journal of Discrete Mathematical Sciences and Cryptography*, [Online] 22 (1), 9–29, tersedia di DOI:10.1080/09720529.2018.1564201.

Nawej, C.M. dan Owolawi, P.A., 2018, *Evaluation and Modelling of Secured Protocols ' Spent Transmission Time*, 3–7,

Nikooghadam, M., Amintoosi, H., Islam, S.K.H. dan Moghadam, M.F., 2020, A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance, *Journal of Systems Architecture*, [Online] (101955), 1–16, tersedia di DOI:10.1016/j.sysarc.2020.101955.

NISA, U., 2017, *Technical Introduction to Cyber Security at Nuclear and Radiological Facilities*.

NIST, 2015a, *FIPS PUB 180-4 Secure Hash Standard (SHS)*. (August).

NIST, U., 2001, *Advanced Encryption Standard*. [Online]. hal.1–51. tersedia di DOI:10.1201/9781439833032.ch89.

NIST, U., 2015b, *FIPS PUB 180-4 Secure Hash Standard (SHS)*. (August).

Nivetha, A., S, P.M. dan J, S.K., 2015, Modified RSA Encryption Algorithm using Four Keys, *International Journal of Engineering Research and Technology (IJERT)*, 3 (07), 3–7,

Orueta, G.D., Ruiz, E.S.C., Alonso, N.O. dan Gil, M.C., 2017, *Quality of Service - Regulation Manual*, [Online]. tersedia di DOI:10.1201/b16521-13.

Padmaja, C.J.L., Bhagavan, V.S. dan Srinivas, B., 2016, RSA Encryption using Three Mersenne Primes, *International Journal of Chemical Sciences*, 14 (4), 2273–2278,

Panda, P.K. dan Chattopadhyay, S., 2017, A hybrid security algorithm for RSA cryptosystem, *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*, [Online] tersedia di DOI:10.1109/ICACCS.2017.8014644.

Pandey, G. dan Pal, S.K., 2016, Polynomial selection in number field sieve for integer factorization, *Perspectives in Science*, [Online] 8101–103, tersedia di DOI:10.1016/j.pisc.2016.04.007.

Patil, A.A. dan Mali, S., 2016, Hybrid Cryptography Mechanism for Securing Self-Organizsed Wireless Network, *2016 Proceedings of 3rd International Conference on Advanced Comuting and Communication Systems (ICACCS)*, [Online], 2016 Coimbatore, India., hal. 1–4, tersedia di DOI:10.1109/ICACCS.2016.7586356.

Patil, P., Narayankar, P., Narayan, D.G. dan Meena, S.M., 2016, A Comprehensive Evaluation of Cryptographic Algorithms : DES , 3DES, AES, RSA and Blowfish, *Procedia Computer Science*, [Online], 2016 Elsevier Masson SAS, Nagpur, India., hal. 617–624, tersedia di DOI:10.1016/j.procs.2016.02.108.

Peng, L., Hu, L., Lu, Y., Xu, J. dan Huang, Z., 2017, Cryptanalysis of Dual RSA, *Designs, Codes and Cryptography*, [Online] 83 (1), 1–21, tersedia di DOI:10.1007/s10623-016-0196-5.

Pir, R.M., 2016, Security improvement and Speed Monitoring of RSA Algorithm, *International Journal of Engineering Development and Research*, 4 (1), 195–200,

Rathore, M.M., Paul, A., Ahmad, A., Chilamkurti, N., Hong, W. dan Seo, H., 2018, Real-time secure communication for Smart City in high-speed Big Data environment, *Future Generation Computer Systems*, [Online] 83 (Jun), 638–652, tersedia di DOI:10.1016/j.future.2017.08.006.

Reinhardt, S., 2013, *SARA Spectroscopic Gamma Detector User Manual*, 1.8.0, Envinet GmbH, Munich, Germany.

Rivest, R., Shamir, A. dan Adleman, L., 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, 21120–126,

Roy, K.S. dan Kalita, H.K., 2017, A Survey on Authentication Schemes in IoT, *2017 International Conference on Information Technology*, [Online], 2017 IEEE, Bhubaneswar, India., hal. 1–6, tersedia di DOI:10.1109/ICIT.2017.56.

Sadikin, R., 2012, Isi buku inin banyak merepresentasikan Buku Crytograhy and Network Security (Stalling, 2006), *Kriptografi untuk Keamanan Jaringan*, Pertama, Arie Prabawati (ed.), Andy Offset, Yogyakarta.

Sahu, J., Singh, V., Sahu, V. dan Chopra, A., 2017, An Enhanced Version of RSA to Increase the Security, *Journal of Network Communications and Emerging Technologies (JNCET)*, 7 (4), 2395–5317,

Sann, Z., Soe, T. thi, Knin, K.W.M. dan Win, Z.M., 2019, Performance Comparison of Asymmetric Cryptography (Case study- Mail message), *APTIKOM Journal on Computer Science and Information Technologies*, [Online] 4 (3), 105–111, tersedia di DOI:10.11591/aptikom.j.csit.147.

Sattler, P., 2014, *Environmental Radiation Monitoring Systems (ERMS)*. [Online]. tersedia di DOI:10.1016/B978-0-323-11237-6.00023-6.

Schneier, B., 2015, *Applied Crypthography protocol, Algorithm, and Source Code in C*, Second Edi, John Wiley & Sons, Inc.

Shankar, S.K., Tomar, A.S. dan Tak, G.K., 2015, Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs, *Procedia Computer Science*, [Online] 70 (1), 455–461, tersedia di DOI:10.1016/j.procs.2015.10.078.

Shen, J., Chang, S., Shen, J., Liu, Q. dan Sun, X., 2018, A lightweight multi-layer authentication protocol for wireless body area networks, *Future Generation Computer Systems*, [Online] 78956–963, tersedia di DOI:10.1016/j.future.2016.11.033.

Shen, J., Gui, Z., Chen, X., Member, S., Zhang, J. dan Xiang, Y., 2020, Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks, *IEEE Transactions on Dependable and Secure Computing*, [Online] XX (XX), tersedia di DOI:10.1109/TDSC.2020.3025288.

Shuai, M., Liu, B., Yu, N., Xiong, L. dan Wang, C., 2020, Efficient and privacy-preserving authentication scheme for wireless body area networks, *Journal of Information Security and Applications*, [Online] 52 (102499), 1–10, tersedia di DOI:10.1016/j.jisa.2020.102499.

Shuai, M., Yu, N., Wang, H. dan Xiong, L., 2019, Anonymous authentication scheme for smart home environment with provable security, *Computers & Security*, [Online] 86132–146, tersedia di DOI:10.1016/j.cose.2019.06.002.

Skibba, R., 2021, Japan ' s Fugaku Supercomputer Crushes Competition , But Likely Not for, *Engineering*, [Online] 7 (1), 6–7, tersedia di DOI:10.1016/j.eng.2020.12.003.

Somsuk, K., 2018, The improvement of initial value closer to the target for Fermat's factorization algorithm, *Journal of Discrete Mathematical Sciences and Cryptography*, [Online] 21 (7–8), 1573–1580, tersedia di DOI:10.1080/09720529.2018.1502737.

Somsuk, K., 2020, The new integer factorization algorithm based on Fermat's Factorization Algorithm and Euler's theorem, *International Journal of*

Electrical and Computer Engineering, [Online] 10 (2), 1469–1476, tersedia di DOI:10.11591/ijece.v10i2.pp1469-1476.

Stallings, W., 2017, *Cryptography and Network Security*, Seventh Ed, Marcia J. Horton, Tracy Johnson, Kristy Alaura, dan Abhijit Baroi (ed.), Pearson Prentice Hall, Singapore.

Stinson, D.R., 1995, *Cryptography: Theory and practice*, Third Edit, Kenneth H. Rosen (ed.), Chapman & Hall/CRC, New York, US., [Online]. tersedia di DOI:10.1016/0898-1221(95)90225-2.

Stinson, D.R. dan Paterson, M.B., 2019, *Cryptography: Theory and Practice*, 4 edisi, CRC Press, New York, US.

Suarez-Albela, M., Fernandez-Carames, T.M., Fraga-Lamas, P. dan Castedo, L., 2018, A practical performance comparison of ECC and RSA for resource-constrained IoT devices, *2018 Global Internet of Things Summit, GIoTS 2018*, [Online] tersedia di DOI:10.1109/GIOTS.2018.8534575.

Susilo, W., Tonien, J. dan Yang, G., 2020, A generalised bound for the Wiener attack on RSA, *Journal of Information Security and Applications*, [Online] 53102531, tersedia di DOI:10.1016/j.jisa.2020.102531.

Susilo, W., Tonien, J. dan Yang, G., 2021, Computer Standards & Interfaces Divide and capture : An improved cryptanalysis of the encryption standard algorithm RSA, *Computer Standards & Interfaces*, [Online] 74 (July 2020), 103470, tersedia di DOI:10.1016/j.csi.2020.103470.

Swami, B., Singh, R. dan Choudhary, S., 2016a, Dual Modulus RSA based on Jordan-Totient function, *Procedia Technology*, [Online] 241581–1586, tersedia di DOI:10.1016/j.protcy.2016.05.143.

Swami, B., Singh, R. dan Choudhary, S., 2016b, Dual Modulus RSA based on Jordan-Totient function, *Procedia Technology*, [Online] 241581–1586, tersedia di DOI:10.1016/j.protcy.2016.05.143.

Tan, H., Choi, D., Kim, P., Pan, S. dan Chung, I., 2018, Comments on Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks, *IEEE Transaction on Intelligent Transportation Systems*, 19 (7), 2149–2151,

Teixeira, A., Matos, A., Souto, A. dan Antunes, L., 2011, Entropy measures vs. Kolmogorov complexity, *Entropy*, [Online] 13 (3), 595–611, tersedia di DOI:10.3390/e13030595.

Thangavel, M., Varalakshmi, P., Murrali, M. dan Nithya, K., 2015, ScienceDirect An Enhanced and Secured RSA Key Generation Scheme (ESRKGS), *Journal of Information Security and Applications*, [Online] 203–10, tersedia di DOI:10.1016/j.jisa.2014.10.004.

Thirumalai, C., Mohan, S. dan Srivastava, G., 2020, An efficient public key secure

scheme for cloud and IoT security, *Computer Communications*, [Online] 150 (November 2019), 634–643, tersedia di DOI:10.1016/j.comcom.2019.12.015.

Timothy, D.P. dan Santra, A.K., 2017, A Hybrid Cryptography Algorithm for Cloud Computing Security, *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, [Online], 2017 IEEE, Vellore, India., hal. 1–5, tersedia di DOI:10.1109/ICMDCS.2017.8211728.

Tocchi, A., Roca, V., Angrisani, L., Bonavolonta, F. dan Moriello, R.S. Lo, 2017, First step towards an IoT implementation of a wireless sensors network for environmental radiation monitoring, *Proc. of IEEE International Conf. on Instrumentation and Measurment Tecnology*, [Online], 2017 Turin, Italy., hal. 1–6, tersedia di DOI:10.1109/I2MTC.2017.7969754.

Ukwuoma, H.C. dan Hammawa, M.B., 2015, Optimised Key Generation for RSA Encryption, *Journal of Innovative Systems Design and Engineering*, 6 (March), 35–45,

Vahdati, Z., Yasin, S.M.D., Ghasempour, A. dan Salehi, M., 2019, Comparison of ECC and RSA algorithms in IoT devices, *Journal of Theoretical and Applied Information Technology*, 97 (16), 4293–4308,

Vijayakumar, P., Azees, M., Kannan, A. dan Deborah, L.J., 2016, Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks, *IEEE Transaction on Intelligent Transportation Systems*, 17 (4), 1015–1028,

Vogel, D., Onayemi, Y. dan Murad, V., 2016, Integer Factorization Algorithms, *Teaching Course - Math Project*, 1–20,

Wu, M.E., Tso, R. dan Sun, H.M., 2014, On the improvement of Fermat factorization using a continued fraction technique, *Future Generation Computer Systems*, [Online] 30 (1), 162–168, tersedia di DOI:10.1016/j.future.2013.06.008.

Yaacoub, J., Noura, H., Salman, O. dan Chehab, A., 2020, Internet of Things Security analysis of drones systems : Attacks , limitations , and recommendations, *Internet of Things*, [Online] 11100218, tersedia di DOI:10.1016/j.iot.2020.100218.

Yang, L.T., Huang, G., Feng, J. dan Xu, L., 2017, Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing, *Information Sciences*, [Online] 387254–265, tersedia di DOI:10.1016/j.ins.2016.10.017.

Yassein, M.B., Hmeidi, I., Shatnawi, F., Mardini, W. dan Khamayseh, Y., 2019, Smart Home Is Not Smart Enough to Protect You - Protocols , Smart Home Is Not Smart Enough to Protect You - Protocols , Challenges and Open Issues Challenges and Open Issues, *Procedia Computer Science*, [Online] 160134–141, tersedia di DOI:10.1016/j.procs.2019.09.453.

Zadiraka, V., Nykolaychuk, Y. dan Ivasiev, S., 2015, The theory of factorization multidigit numbers, *Proceedings of 13th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2015*, [Online] 221–225, tersedia di DOI:10.1109/CADSM.2015.7230841.

Zaid, M.M.A. dan Hassan, S., 2018, Lightweight RSA Algorithm Using Three Prime Numbers, *International Journal of Engineering and Technology*, 7293–295,

Zhang, A., Wang, L., Ye, X. dan Lin, X., 2017, Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems, *IEEE Transactions on Information Forensics and Security*, [Online] 12 (3), 662–675, tersedia di DOI:10.1109/TIFS.2016.2631950.

Zhang, L., Zhao, L., Yin, S., Chi, C., Liu, R. dan Zhang, Y., 2019, A lightweight authentication scheme with privacy protection for smart grid communications, *Future Generation Computer Systems*, [Online] 100 (Nov), 770–778, tersedia di DOI:10.1016/j.future.2019.05.069.

Zhang, X., Ye, F., Fan, S., Guo, J., Xu, G. dan Qian, Y., 2016, An adaptive security protocol for a wireless sensor-based monitoring network in smart grid transmission lines, *Security and Communication Networks*, [Online] 9 (Oct.), 60–71, tersedia di DOI:10.1002/sec.1382.

Zhang, Z., 2010, On the effectiveness of a generalization of Miller's primality theorem, *Journal of Complexity*, [Online] 26 (2), 200–208, tersedia di DOI:10.1016/j.jco.2010.01.002.

Zhou, C., 2018, Comments on Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems, *IEEE Transaction on Information Forensics and Security*, 13 (7), 1869–1870.