

## REFERENCES

- Abidi, A., Wang, Q., Bouallegue, B., Machhout, M., & Guyeux, C. (2016). Quantitative evaluation of chaotic CBC mode of operation. *2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, 88–92. <https://doi.org/10.1109/ATSIP.2016.7523053>
- Abraham, N. E. & Thomas, T. (2013). FPGA Implementation of Mix and Inverse Mix Column for AES Algorithm. *2013 International Journal for Scientific Research & Development (IJSRD)*, 1981–1984.
- Alimzhanova, Z., Nazarbayev, D., Tleubergen, A., & Alimzhanov, A. (2022). Analysis of Block Ciphers Characteristics for CBC and OFB Modes of Operation When Input Data are Shifted. *2022 International Conference on Smart Information Systems and Technologies (SIST)*, 1–4. <https://doi.org/10.1109/SIST54437.2022.9945788>
- Aziz, M. V. G., Wijaya, R., Prihatmanto, A. S., & Henriyan, D. (2013). HASH MD5 function implementation at 8-bit microcontroller. *2013 Joint International Conference on Rural Information & Communication Technology and Electric-Vehicle Technology (rICT & ICeV-T)*, 1–5. <https://doi.org/10.1109/rICT-ICeVT.2013.6741530>
- Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24–31. [https://doi.org/10.1016/S2212-5671\(15\)01077-1](https://doi.org/10.1016/S2212-5671(15)01077-1)
- Center for Strategic and International Studies. (2024). Significant cyber incidents since 2006. Center for Strategic and International Studies. <https://www.csis.org>
- Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014). A comparative survey of Symmetric and Asymmetric Key Cryptography. *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 83–93. <https://doi.org/10.1109/ICECCE.2014.7086640>
- Chen, D. (2023). *A Dive into Microcontrollers: A Dark Horse Technology*. University of Virginia.

- Fotovvat, A., Rahman, G. M. E., Vedaiei, S. S., & Wahid, K. A. (2021). Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes. *IEEE Internet of Things Journal*, 8(10), 8279–8290. <https://doi.org/10.1109/JIOT.2020.3044526>
- Gao, Y., Peng, Y., Xie, F., Zhao, W., Wang, D., Han, X., Lu, T., & Li, Z. (2013). Analysis of security threats and vulnerability for cyber-physical systems. *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*, 50–55.
- Güven, Y., Coşgun, E., Kocaoğlu, S., GeziCi, H., & Yilmazlar, E. (n.d.). *Understanding the Concept of Microcontroller Based Systems To Choose The Best Hardware For Applications*.
- Hamouda, B. E. H. H. (2020). Comparative Study of Different Cryptographic Algorithms. *Journal of Information Security*, 11(03), 138–148. <https://doi.org/10.4236/jis.2020.113009>
- Hashimoto, Y., Khandaker, Md. A.-A., Kodera, Y., Park, T., Kusaka, T., Kim, H., & Nogami, Y. (2017). An ECC Implementation with a Twisted Montgomery Curve over  $F_{q^{32}}$  on an 8-Bit Microcontroller. *2017 Fifth International Symposium on Computing and Networking (CANDAR)*, 445–450. <https://doi.org/10.1109/CANDAR.2017.90>
- Hasija, T., Ramkumar, K. R., Singh, B., Kaur, A., & Mittal, S. K. (2023). Symmetric Key Cryptography: Review, Algorithmic Insights, and Challenges in the Era of Quantum Computers. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–6. <https://doi.org/10.1109/ICCCNT56998.2023.10307081>
- Huang, Y.-L., Leu, F.-Y., Liu, J.-C., Yang, J.-H., Yu, C.-W., Chu, C.-C., & Yang, C.-T. (2013). Building a block cipher mode of operation with feedback keys. *2013 IEEE International Symposium on Industrial Electronics*, 1–4. <https://doi.org/10.1109/ISIE.2013.6563875>
- Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press.

- Kumar, N., Gupta, P., Sahu, M., & Rizvi, M. A. (2013). Boolean Algebra based effective and efficient asymmetric key cryptography algorithm: BAC algorithm. *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, 250–254. <https://doi.org/10.1109/iMac4s.2013.6526417>
- Lee, H., Lee, K., & Shin, Y. (2010). Implementation and performance analysis of AES-128 CBC algorithm in WSNs. In *2010 The 12th International Conference on Advanced Communication Technology (ICACT)* (pp. 243-248)
- Liu, D., Liu, Y., Liu, Z., Zhang, X., & Zhang, X. (2023). Analysis and Reflection on the Situation of Industrial Information Security Ransomware Attacks. *2023 8th International Conference on Data Science in Cyberspace (DSC)*, 354–358. <https://doi.org/10.1109/DSC59305.2023.00057>
- 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>
- Manjula G. & Mohan H.S. (2016). Constructing key dependent dynamic S-Box for AES block cipher system. *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 613–617. <https://doi.org/10.1109/ICATCCT.2016.7912073>
- Naser, S. M. (2021). CRYPTOGRAPHY: FROM THE ANCIENT HISTORY TO NOW, IT'S APPLICATIONS AND A NEW COMPLETE NUMERICAL MODEL. *International Journal of Mathematics and Statistics Studies*, 9(3), pp. 11-30.
- Nasser, Y. A., Bazzoun, M. A., & Abdul-Nabi, S. (2016). AES algorithm implementation for a simple low cost portable 8-bit microcontroller. *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, 203–207. <https://doi.org/10.1109/ICDIPC.2016.7470819>

- National Institute of Standards and Technology. (2020). *FIPS 197: Advanced encryption standard (AES) - Revision 1*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- Pawar, H. R., & Harkut, D. G. (2018). Classical and Quantum Cryptography for Image Encryption & Decryption. *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)*, 1–4. <https://doi.org/10.1109/RICE.2018.8509035>
- Prayitno, R. H., Sudiro, S. A., & Madenda, S. (2021). Avoiding lookup table in AES algorithm. *2021 Sixth International Conference on Informatics and Computing (ICIC)*, 1–6. <https://doi.org/10.1109/ICIC54025.2021.9632897>
- Srivastava, S., Tiwari, A., & Srivastava, P. K. (2022). Review on quantum safe algorithms based on Symmetric Key and Asymmetric Key Encryption methods. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 905–908. <https://doi.org/10.1109/ICACITE53722.2022.9823437>
- Stancu, F. A., Tranca, C. D., Chiroiu, M. D., & Rughinis, R. (2018). Evaluation of cryptographic primitives on modern microcontroller platforms. *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 1–6. <https://doi.org/10.1109/ROEDUNET.2018.8514127>
- Usman, M., Abidi, S. Z.-U.-A., Siddiqui, M. H. S., & Ibrahim, M. S. (2016). Implementation of Secure Force (64-bit) on low cost 8-bit microcontroller. *2016 International Conference on Open Source Systems & Technologies (ICOSST)*, 102–105. <https://doi.org/10.1109/ICOSST.2016.7838585>
- Utama, C. C., Syahputra, T., & Iswan, M. (2021). IMPLEMENTASI TEKNIK COUNTER PADA AIR MANCUR UNTUK MEMBUAT ANIMASI AIR BERBASIS MIKROKONTROLER ATMEGA 16. *JURNAL TEKNISI*, 1(1), 13. <https://doi.org/10.54314/teknisi.v1i1.484>
- Vaidehi, M., & Rabi, B. J. (2014). Design and analysis of AES-CBC mode for high security applications. *Second International Conference on Current Trends In*



UNIVERSITAS  
GADJAH MADA

**Implementation of AES-128 Algorithm on a Microcontroller for File Encryption and Decryption**  
Keitaro Wildan Ramadhan, Oskar Natan, S.ST., M.Tr.T.; Prof. Dr. Jazi Eko Istiyanto, M.Sc.  
Universitas Gadjah Mada, 2024 | Diunduh dari <http://etd.repository.ugm.ac.id/>

107

*Engineering and Technology - ICCTET 2014, 499–502.*  
<https://doi.org/10.1109/ICCTET.2014.6966347>