DAFTAR PUSTAKA

A, B., & Chauhan, G. (2023). Development and Implementation of an Efficient *Chatting* Application for Mobile Devices. *International Journal of Research Publication and Reviews*, *4*(5), 6374–6381. https://doi.org/10.55248/gengpi.4.523.43343

Abikoye, O. C., Haruna, A. D., Abubakar, A., Akande, N. O., & Asani, E. O. (2019). Modified Advanced Encryption Standard Algorithm for Information Security. *Symmetry*, *11*(12), 1484. https://doi.org/10.3390/sym11121484

Alatawi, M., & Saxena, N. (2023). SoK: An Analysis of *End-to-End Encryption* and Authentication Ceremonies in Secure Messaging Systems. *WiSec 2023 - Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 187–201. https://doi.org/10.1145/3558482.3581773

Alkhyeli, M., Alkhyeli, S., Aldhaheri, K., & Lamaazi, H. (2023). Secure Chat Room Application Using AES-GCM Encryption and SHA-256. *2023 15th International Conference on Innovations in Information Technology (IIT)*, 180–185. https://doi.org/10.1109/IIT59782.2023.10366418

Ananya Mishra, Madhav Aggarwal, & Akshat Tiwari. (2024). Concealing And Encrypting: Dual Approaches to Data Security in The Digital Age. *International Research Journal on Advanced Engineering and Management (IRJAEM)*, *2*(08), 2543–2552. https://doi.org/10.47392/IRJAEM.2024.0368

Ansh Goel, Harshit Baliyan, Shivam Tyagi, & Neeti Bansal. (2024). End to end encryption of chat using advanced encryption standard-256. *International Journal of Science and Research Archive*, *12*(1), 2018–2025. https://doi.org/10.30574/ijsra.2024.12.1.0923

Asgap Putra Zulian, A., Kartarina, K., & Dharma, I. M. Y. (2026). Analisis Pengamanan File Menggunakan Enkripsi dan Dekripsi dengan Algoritma AES-GCM-SIV. *Edu Elektrika Journal*, *13*(1), 15–23. https://doi.org/10.15294/eduel.v13i1.26826

Asghar, A., Shifa, A., & Asghar, M. N. (2024). Survey on Video Security: Examining Threats, Challenges, and Future Trends. *Computers, Materials & Continua*, *80*(3), 3591–3635. https://doi.org/10.32604/cmc.2024.054654

Awachat, S., Chahande, A., Gadge, S., Shastrakar, S., & Gajbhiye, K. (2021). A Secure Cloud Based *Chatting* Application with Hybrid Cryptography. *International Journal of Computational and Electronic Aspects in Engineering*, *2*(2). https://doi.org/10.26706/ijceae.2.2.20210413

Barbosa, M., & Farshim, P. (2018). *Indifferentiable Authenticated Encryption* (pp. 187–220). https://doi.org/10.1007/978-3-319-96884-1_7

Chung, W., Hwang, S., Kim, S., Lee, B., & Lee, J. (2025). *Making GCM Great Again: Toward Full Security and Longer Nonces* (pp. 33–61). https://doi.org/10.1007/978-3-031-91107-1_2

Dar, M. A., Askar, A., Alyahya, D., & Bhat, S. A. (2021). Lightweight and Secure Elliptical Curve Cryptography (ECC) Key Exchange for Mobile Phones.

International Journal of Interactive Mobile Technologies (IJIM), *15*(23), 89–103. https://doi.org/10.3991/ijim.v15i23.26337

Darmansyah, D., & Hasugian, A. H. (2025). ENKRIPSI PESAN CHAT MENGGUNAKAN ALGORITMA CHACHA20 PADA APLIKASI KOMUNIKASI *REAL-TIME*. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *10*(2), 544–554. https://doi.org/10.36341/rabit.v10i2.6220

Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Dungog, J. M. (2025). *A Python-Based Simulation and Security Analysis of ChaCha20 and AES for Secure Data Transmission in Resource-Constrained Environments*. www.ijfmr.com

El-Dalahmeh, A., El-Dalahmeh, M., Razzaque, M. A., & Li, J. (2024). Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. *SECURITY AND PRIVACY*, *7*(6). https://doi.org/10.1002/spy2.446

Feng, Y. (2024). Design of an Encryption Chat Application Based on ChaCha20-Poly1305. In *Highlights in Science, Engineering and Technology CSIC* (Vol. 2023).

Gandhi, A., Das, A., & Cherukuri, A. K. (2026). *On Implementing Hybrid Post-Quantum End-to-End Encryption*. https://arxiv.org/pdf/2601.14926

Go, K., & Lee, S. (2025). Lightweight Encryption for Raw-Format Live Video *Streaming* Over Automotive Ethernet. *Electronics Letters*, *61*(1). https://doi.org/10.1049/ell2.70483

Gueron, S., Langley, A., & Lindell, Y. (2019). *AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption*. https://doi.org/10.17487/RFC8452

Gueron, S., & Lindell, Y. (2015). GCM-SIV: Full nonce misuse-resistant authenticated encryption at under one cycle per byte. *Proceedings of the ACM Conference on Computer and Communications Security*, *2015-October*, 109–119. https://doi.org/10.1145/2810103.2813613

Hadi, H. H., & Neamah, A. A. (2024). An image encryption method based on modified elliptic curve Diffie-Hellman key exchange protocol and Hill Cipher. *Open Engineering*, *14*(1). https://doi.org/10.1515/eng-2022-0552

Hafeez, M. A., Shakib, K. H., & Munir, A. (2025). A Secure and Scalable Authentication and Communication Protocol for Smart Grids. *Journal of Cybersecurity and Privacy*, *5*(2), 11. https://doi.org/10.3390/jcp5020011

Hernandi, H. R., & Christian Chandra, J. (2024). Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *4*(1), 12–22. https://doi.org/10.36080/kresna.v4i1.131

Heru, A. T., Faisal, & Manalu, S. R. (2024). File Encryption and Decryption Application using Elliptic CurveDiffie-Hellman Algorithm and Chaotic Map

Function. *Procedia Computer Science*, *245*, 39–48. https://doi.org/10.1016/j.procs.2024.10.227

Iwata, T., & Minematsu, K. (2016). Stronger Security Variants of GCM-SIV. *IACR Transactions on Symmetric Cryptology*, 134–157. https://doi.org/10.46586/tosc.v2016.i1.134-157

Jirjees, S. W., Alkhalid, F. F., & Hasan, A. M. (2023). Text Encryption by Indexing ASCII of Characters Based on the Locations of Pixels of the Image. *Traitement Du Signal*, *40*(2), 791–796. https://doi.org/10.18280/ts.400240

Kim, K., Choi, S., Kwon, H., Kim, H., Liu, Z., & Seo, H. (2020). PAGE—Practical AES-GCM Encryption for Low-End Microcontrollers. *Applied Sciences*, *10*(9), 3131. https://doi.org/10.3390/app10093131

Knodel, M., Celi, S., Kolkman, O., & Grover, G. (2024). Definition of *End-to-end Encryption*. *Cryptology EPrint Archive*. https://eprint.iacr.org/2024/2085

Krawczyk, H., & Eronen, P. (2010). *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. https://doi.org/10.17487/rfc5869

Mattsson, J. P. (2024). *Collision-Based Attacks on Block Cipher Modes - Exploiting Collisions and Their Absence*. https://eprint.iacr.org/2024/1111

Mehmood, A., Khan, A. N., Natgunanathan, I., Shafique, A., Khan, I. A., & Khan, A. ur R. (2025). Enhanced lightweight and compromised-resilient image encryption for resource constrained environments. *PLOS ONE*, *20*(3), e0320046. https://doi.org/10.1371/journal.pone.0320046

Perkasa, M. J. P., Ramdan, H. M., Maliki, A. J., & Somantri. (2025). Implementation of Secure End-to-End Encrypted Chat Application Using Diffie–Hellman Key Exchange and AES-256 in a Microservice Architecture †. *Engineering Proceedings*, *107*(1). https://doi.org/10.3390/engproc2025107098

Poettering, B., & Rösler, P. (2020). Combiners for AEAD. *IACR Transactions on Symmetric Cryptology*, 121–143. https://doi.org/10.46586/tosc.v2020.i1.121-143

Rose, S. J., Ozkaya, U., Yasmin, S., Jabin, S., Hasan, R., & Kabir, E. (2023). *An Efficient Unicode encoded in UTF-16 text cryptography based on the AES algorithm*.

Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024). A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography. *International Journal of Computer Science and Mobile Computing*, *13*(4), 68–87. https://doi.org/10.47760/ijcsmc.2024.v13i04.008

Senthilkumar, M., Suthendran, K., & Ravi, V. (2024). Enhancing Medical Image Security through a Novel Framework: Crypto-aware Elliptic Curve Diffie-hellman with Key Derivation Function. *The Open Bioinformatics Journal*, *17*(1). https://doi.org/10.2174/0118750362303634240624112446

Serrano, R., Duran, C., Sarmiento, M., Pham, C. K., & Hoang, T. T. (2022). ChaCha20–Poly1305 Authenticated Encryption with Additional Data for

Transport Layer Security 1.3. *Cryptography*, *6*(2). https://doi.org/10.3390/cryptography6020030

Shchur, N., Pokotylo, O., & Bailiuk, Y. (2023). ELLIPTIC CURVE CRYPTOGRAPHY AND ITS PRACTICAL APPLICATION. *Cybersecurity: Education, Science, Technique*, *1*(21), 48–64. https://doi.org/10.28925/2663-4023.2023.21.4864

Tuo, Z. (2023). A comparative Analysis of AES and RSA algorithms and their integrated application. *Theoretical and Natural Science*, *25*(1), 28–35. https://doi.org/10.54254/2753-8818/25/20240893

Utama Siahaan, A. P. (2024). *SECURE IMAGE ENCRYPTION AND TRANSMISSION USING AES AND BASE64 ENCODING: PERFORMANCE AND SIZE ANALYSIS*.

Yang, J., & Johansson, T. (2020). An overview of cryptographic primitives for possible use in 5G and beyond. *Science China Information Sciences*, *63*(12), 220301. https://doi.org/10.1007/s11432-019-2907-4

Zai, S. A. P., Niska, D. Y., Indra, Z., Saputra, K., & Perdana, A. (2025). Implementation of a Hybrid Cryptosystem Using ChaCha20 and ECC for Image Encryption in an Android Application. *Sinkron*, *9*(4), 1988–1997. https://doi.org/10.33395/sinkron.v9i4.15274

Zhiqiang, H., Rauf, A., Nazir, A., Tchier, F., Aslam, A., & Tola, K. A. (2025). Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication

support. *Scientific Reports*, *15*(1), 39951. https://doi.org/10.1038/s41598-025-23592-w