REFERENCES

[1] Z. Z. Mammeri, *Cryptography: Algorithms, Protocols, and Standards for Computer Security*, 1st ed. John Wiley & Sons, Incorporated, 2024.

[2] N. I. of Standards and Technology, "Advanced encryption standard (aes)," U.S. Department of Commerce, NIST FIPS 197-upd1, May 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *CACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] K. Somsuk, "The special algorithm based on rsa cryptography for signing and verifying digital signature," *Heliyon*, vol. 11, no. 4, p. e42481, 2025.

[6] E. G. AbdAllah, Y. R. Kuang, and C. Huang, "Advanced encryption standard new instructions (aes-ni) analysis: Security, performance, and power consumption," in *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering*, ser. ICCAE 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 167–172.

[7] Z. Lu, "Analysis on aes encryption standard and safety," in *Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022)*, vol. 12462. SPIE, 2023, pp. 292–297.

[8] A. Dasso, A. Funes, D. Riesco, and G. Montejano, "Computing power, key length and cryptanalysis. an unending battle?" Preprint, arXiv:2011.00985, nov 2020. [Online]. Available: https://doi.org/10.48550/arXiv.2011.00985

[9] L. K. Grover, "From schrödinger's equation to the quantum search algorithm," *Am. J. Phys.*, vol. 69, no. 7, pp. 769–777, 2001.

[10] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A review of the present cryptographic arsenal to deal with post-quantum threats," *Procedia Computer Science*, vol. 215, pp. 834–845, 2022, 4th International Conference on Innovative Data Communication Technology and Application.

[11] C. Gidney, "How to factor 2048 bit rsa integers with less than a million noisy qubits (2025)," Preprint, arXiv:2505.15917, may 2025.