4th International Artificial Intelligence and Data Science Congress

March 14-15, 2024 : İzmir, Turkey

Fast Decryption Methods for The Somsuk-RSA Cryptosystem

Muhammad Asyraf Asbullah[1*], Nur Adira Mohamad Azlan[2]

[1]*Centre for Foundation Studies in Science of Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Malaysia*

[*]*(ma_asyraf@upm.edu.my) Email of the corresponding author*

Abstract – In today's digital landscape, safeguarding data transmission and storage is paramount, with the RSA cryptosystem standing as a crucial guardian through its asymmetric encryption mechanism. Despite its effectiveness, the Somsuk-RSA variant has emerged to enhance security measures, albeit with computational challenges, particularly during decryption. This research addresses these challenges by proposing innovative approaches to expedite decryption time. The key proposition involves replacing the Euler function with the Carmichael function, a strategic move to enhance efficiency compared to the original RSA and Somsuk-RSA. A comprehensive analysis of the decryption process reveals a notable slowdown in the Somsuk-RSA method, prompting refinement. The study, conducted across prime sizes of 512, 1024, and 2048 bits, underscores the efficacy of the New Somsuk-RSA Cryptosystem, demonstrating a noteworthy improvement in data decryption speed compared to the conventional Somsuk-RSA method. Thus, this research contributes valuable insights into optimizing the Somsuk-RSA variant, paving the way for enhanced data security and more efficient cryptographic processes in the evolving digital era.

Keywords – Asymmetric, Encryption, RSA, Carmichael Function, Cryptography