RESCON 2025 CMS 21

A VARIANT OF RIVEST-SHAMIR-ADLEMAN (RSA) CRYPTOSYSTEM USING GENERALISED CONTINUED FRACTIONS AND CHINESE REMAINDER THEOREM

K.H.K. Madhuwanthi* and P.G.R.S. Ranasinghe

Department of Mathematics, University of Peradeniya, Peradeniya, Sri Lanka.
*s19434@sci.pdn.ac.lk

Cryptography is essential for securing digital communication by ensuring confidentiality, integrity, and authenticity. Among public-key cryptosystems, Rivest-Shamir-Adleman (RSA) is one of the most widely used. In this study, we present an improved version of RSA by introducing Generalised Continued Fractions (GCF) for constructing encryption exponents and applying the Chinese Remainder Theorem (CRT) with Garner's algorithm for efficient decryption. The main novelty of this work lies in the use of GCF to generate the public exponent. This approach enables the selection of large and irregular exponents that reduce the risk of common weaknesses, such as low-exponent or structured-exponent attacks. While predictable patterns could raise concerns in key generation, their impact is negligible when the exponents produced are sufficiently large and flexible, because security in RSA depends primarily on the hardness of factoring the modulus. To complement this, CRT and Garner's algorithm, which are already established as standard techniques for improving RSA performance, are incorporated to minimise the computational cost of modular exponentiation during decryption. Their role here is to enhance efficiency, while the real contribution is the introduction of GCF for exponent construction. By combining secure exponent design with proven optimisation techniques, the proposed scheme improves decryption performance without reducing cryptographic strength. This research therefore contributes a practical approach that balances efficiency and security. It is especially suitable for lightweight cryptographic applications and secure digital communications, where both computational speed and robust security are essential.

Keywords: Chinese Reminder Theorem, Cryptography, Garner's algorithm, Generalised continued fractions