2023

【海報論文】

□一般組 ■研究生組

□大學組

11th台灣TAIWAN 工業與應用數學會年會 TWSIAM Annual Meeting

The study of different mathematical algorithms for the RSA Cryptosystem.

Jhong-Yu Guo(郭仲育), ***Department of Graduate Institute of Automation Technology, National Taipei University of Technology, Taipei 10608 Taiwan*** **(t110618033@ntut.org.tw)**
Advisor: Prof. Shih-Wen Chen(陳詩雯)

• Abstract

RSA is one of the popular public-key cryptosystems in cryptography. This study compares the computational speed of encryption and decryption processes for the RSA cryptosystem with three different mathematical algorithms, which are RSA-H modular Exponentiation, RSA-Fast Modular Exponentiation, and RSA-Chinese Remainder Theorem. The study used two 512-bit prime numbers as the same input parameters in these three algorithms for RSA operations.

• Methodology & Experimental results

In the public-key cryptosystems, if A wants to send a message to B, B needs to create a public key and a private key first. After B sends it's public key to A, A can use the public key to encrypt the message. When B receives the message, B can decrypt it by using his own private key, as shown in Fig. 1.

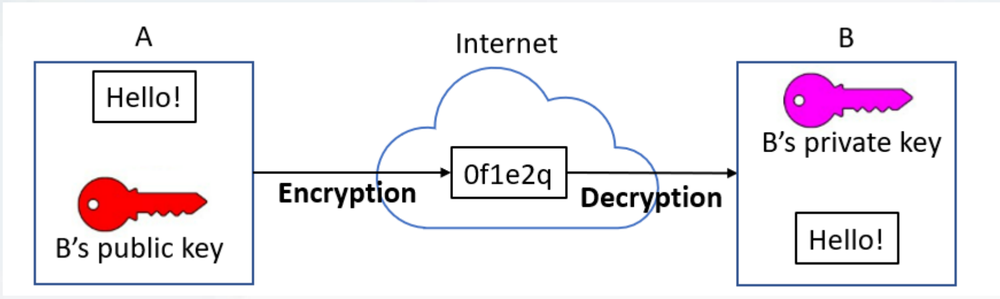
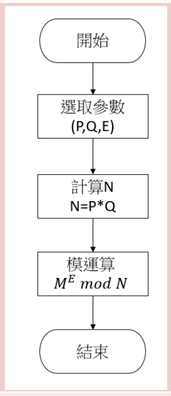
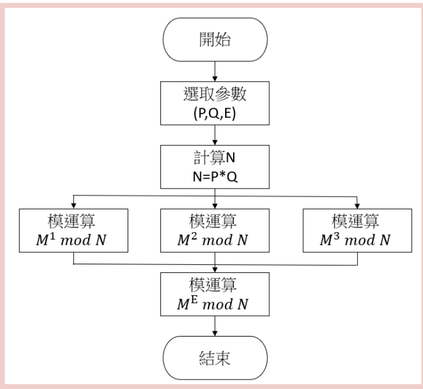
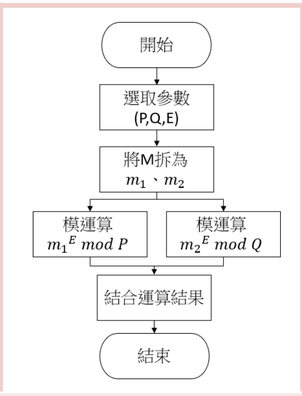


Fig. 1 The public-key cryptosystems in cryptography

The RSA cryptosystem is established by performing modular exponentiation using large prime numbers as input parameters. In general, the process of modular exponentiation is adopted intensively to find the public key and the private key. This is very time consuming, therefore, several mathematical algorithms with different ways of handling the bits for encryption and decryption were invented to achieve faster computation. Table 1 compares the computational times of encryption and decryption processes with three different mathematical algorithms.

Table 1. The performance of three different mathematical algorithms

	RSA – H modular Exponentiations	RSA - Exponentiations by squaring	RSA – Chinese Remainder Theorem
flowchart			
Time complexity	O(k^3) k means modulus bit length	O(log n) n means exponent size	O(k^3) k means modulus bit length
Encryption time(μs)	1999 μs	1000μs	1036μs
Decryption time(μs)	Over 10^4μs	26079μs	5231μs

In this study, various mathematical algorithms are implemented by using the GNU Multiple Precision Arithmetic Library (GMP library) in C language. The GMP library can handle big numbers beyond the range of data types that C/C++ can represent. At the same time, It ensures both calculation accuracy and speed of numbers with any length.

The mechanism of encryption and decryption in RSA uses a large number of modular exponentiations, which can be represented by the mathematical expression "$M\text{^}E \ \ mod \ N$". The calculation of RSA-H modular exponentiation and RSA-quick modular multiplication starts from the high-order bit to the low-order bit, but the former can only perform one bit operation at a time, while the latter can perform multiple-bits operation at once and store the results for subsequent operations. The Chinese Remainder Theorem in RSA decomposes a large modulus into two smaller modulus exponentiations, and then calculates the exponentiations separately. Finally, the Chinese Remainder Theorem is used to combine the results to accelerate the calculation.

• Conclusion

Table 1 shows that the RSA-Chinese Remainder Theorem algorithm has the highest computational efficiency because it splits the large multiplication operation into two smaller ones that are simultaneously computed and merged. In the future, we will add the Montgomery method and incorporate hardware acceleration to speed up the algorithm which can be applied to the system of smart cards, such as bank payment cards, ePassports, GSM SIM modules.

[1] 陳彥儒, "基於混合式基數字組式蒙馬哥利模數乘法演算法之RSA密碼演算法硬體架構," 國立中山大學, 碩士論文, July 2016.
[2] 吳啟典, "應用中國餘數定理之RSA與指數運算之錯誤攻擊分析," 國立中央大學, 碩士論文, 2010
[3] Jiankuo Dong, Guang Fan, and Tianyu Mao, "TEGRAS: An Efficient Tegra Embedded GPU-Based RSA Acceleration Server," IEEE Internet of Things Journal, vol.9, pp. 16850 - 16861, 2022.