INTISARI

ANALISIS IMPLEMENTASI MULTIPLE PRIME NUMBER PADA RSA TERHADAP PERFORMA DAN KEAMANAN

Oleh

Perdo Kurniawan
22/495564/PPA/06311

Salah satu modifikasi dalam algoritma RSA adalah dengan menggunakan *Multiple Prime Number*. Modifikasi ini dilakukan dengan tujuan untuk meningkatkan keamanan ataupun performa pada algoritma RSA. Berbagai penelitian yang ada sudah banyak melakukan penerapan *Multiple Prime Number* dalam modifikasi tersebut. Namun, evaluasi terhadap keamanan hanya terbatas pada durasi waktu pemfaktoran bilangan prima.

Pada penelitian ini, dilakukan analisis terhadap berbagai variasi *multiple prime number*. Variasi ini terdiri dari 2, 3, 4 dan 8 bilangan prima yang digunakan pada *private key*. Evaluasi tidak hanya melibatkan faktorisasi bilangan prima, tetapi juga aspek lainnya yaitu *public key exponent*, *private key exponent* dan juga penggunaan *plaintext*. Dari evaluasi tersebut dapat diketahui keberhasilan serangan yang digunakan, waktu untuk melakukan serangan dan total durasi waktu eksekusi penggunaan variasi dari *Multiple Prime Number*. Serangan yang digunakan pada penelitian ini yaitu *coppersmith*, *wiener* dan *bruteforce*.

Penelitian menggunakan skema *small public key exponent*, *small private key* dan *small prime number* untuk melakukan pengujian implementasi *Multiple Prime Number*. Dari hasil eksperimen yang telah dilakukan pada skema tersebut, didapatkan hasil bahwa penggunaan *Multiple Prime Number* tidak menunjukkan peningkatan keamanan yang jauh lebih baik dan justru malah menambah durasi waktu eksekusi algoritma.

Kata Kunci: RSA, Multiple Prime, Analisis, Kriptografi, Serangan

ABSTRACT

ANALYSIS OF MULTIPLE PRIME NUMBER IMPLEMENTATION IN RSA ON ALGORITHM PERFORMANCE AND SECURITY

By

Perdo Kurniawan
22/495564/PPA/06311

One of the modifications in the RSA algorithm is to use Multiple Prime Numbers. This modification was made to improve the security or performance of the RSA algorithm. Various existing studies have carried out the application of Multiple Prime Numbers in this modification. However, the evaluation of security is limited to the factor complexity of prime numbers.

In this study, an analysis was carried out on various variations of multiple prime numbers. This variation consists of 2, 3, 4 and 8 prime numbers used in the private key. Evaluation does not only involve the complexity of prime number factors, but also other aspects, namely the public key exponent, private key exponent and also the use of plaintext. From this evaluation it can be seen the success of the attack used, the time to carry out the attack and the total running time using the variation of the Multiple Prime Number. The attacks used in this research are coppersmith, wiener and bruteforce.

This study uses a small public key exponent, small private key and small prime number scheme to test the implementation of Multiple Prime Numbers. From the results of experiments that have been carried out on the scheme, it was found that the use of Multiple Prime Numbers does not show a much better increase in security and instead adds to the complexity of the algorithm.

Keywords: RSA, Multiple Prime, Analysis, Cryptography, Attack