Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

An Attack on $N = p^2q$ with Partially Known Bits on the Multiple of the Prime Factors

Ruzai, W. N. A.[1], Adenan, N. N. H.[1], Ariffin, M. R. K. *[1], Ghaffar, A. H. A.[2], and Johari, M. A. M.[2]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2]*Department of Mathematics & Statistics, Faculty of Sciences, Universiti Putra Malaysia, Malaysia*

*E-mail: *rezal@upm.edu.my*
**Corresponding author*

Received: 17 June 2021
Accepted: 7 October 2021

Abstract

This paper presents a cryptanalytic study upon the modulus $N = p^2q$ consisting of two large primes that are in the same-bit size. In this work, we show that the modulus N is factorable if e satisfies the Diophantine equation of the form $ed - k(N - (ap)^2 - apbq + ap) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Our attack is feasible when some amount of Least Significant Bits (LSBs) of ap and bq is known. By utilising the Jochemsz-May strategy as our main method, we manage to prove that the modulus N can be factored in polynomial time under certain specified conditions.

Keywords: partial-key exposure attack; integer factorization problem; Jochemsz-May strategy; least significant bits.