Enhancement of RSA Key Generation Using Identity

Norhidayah Muhammad[a], Jasni Mohamad Zain[a], M. Y. M. Saman[b], Mohd Fadhil Ramle[c]
[a]University of Malaysia Pahang, Gambang 26300, Kuantan, Pahang Darul Makmur, Malaysia
[b]University Malaysia Terengganu, 21300, Terengganu, Malaysia
[c]Kolej Komuniti Kuala Terengganu, Terengganu, Malaysia

ABSTRACT
The purpose of this paper is to enhance previous algorithm called Tripathi algorithm. The Tripathi algorithm proposes an RSA based algorithm to generate cryptographic keys using user identity such as email address of a person. This algorithm used user's identity to replace the numbers that are used as a public key in the RSA algorithm. However, the Tripathi algorithm cannot use all of the users' email addresses as a public key. This is because, there are two reasons why it is unable to use all email addresses: (i) this algorithm use the same modulo value for every email, if the email is not related prime to modulo value, the new email should be entered. (ii) Entered email is composed of odd and even number. If the email is even number, then it cannot be the public key. Therefore the Tripathi algorithm needs to be improved. Proposed algorithm called CLB-RSA has been implemented. This algorithm can used all user emails as a public key, and this achievement is after two experiments are done on this study.

DOI: 10.1007/978-3-319-07674-4_64