Email encryption with Linear Congruential Generator

Phyo Wai Kyaw, Nang Saing Moon Kham

University of Computer Studies, Yangon

PhyowaiKyaw83@gmail.com

Abstract

E-mail is widely used all over the world in various fields such as economic, office, personal case and so on. It is easy to transport data from place to place in a short time. E-mail has become one of the most important means of communication. In this process, attackers interfere with E-mail by feeding and accessing data and also by taking these and transporting the false data to users. So, the mail security is necessary by using cryptography method to protect the danger of the attackers. In this paper, Linear Congruential Method(LCM) and River Shamir Adleman (RSA) are used for email encryption for lightweight for email. LCM in generating pseudo-random numbers is used to provide an alternative attitude for some cryptographic purpose.