Design of strong cryptographic schemes based on Latin Squares *

Saibal K. Pal †
Scientific Analysis Group
DRDO, Metcalfe House
Delhi 110 054, India

Shivam Kapoor ‡
Alka Arora §
Reshu Chaudhary ¶
Jatin Khurana ‖
Department of Computer Science
University of Delhi
Delhi 110 007, India

Abstract

A *Latin Square* (*LS*) of order n is an arrangement of n symbols in an $n \times n$ matrix form so that each symbol occurs in each row and each column exactly once. The total number of Latin Squares $LS(n)$ of order n increases rapidly with n. This helps to design cryptosystems using Latin Squares with a very large key-space. We define encryption and decryption using simple operations on Latin Squares. Different schemes are designed to make the system secure and easy to implement. Use of keyed permutations and construction of large quasigroups ensure that the system is resistant to different practical cryptographic attacks. Computer implementations show the simplicity and power of these schemes for future cryptographic applications in resource-constrained networks or in mobile devices.

Keywords and phrases : *Latin Square, quasigroup, keyed permutation, symmetric encryption.*

*This paper was presented at '*Pre-ICM International Convention on Mathematical Sciences*' held at Department of Mathematics, University of Delhi, 18-20 December, 2008.

†*E-mail*: skptech@yahoo.com

‡*E-mail*: shivam.dumca@gmail.com

§*E-mail*: arora.alka04@gmail.com

¶*E-mail*: reshu_dumca@yahoo.com

‖*E-mail*: jatinkhurana34@gmail.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 3, pp. 233–256
© Taru Publications