World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

A Hill Cipher Based on the Kish-Sethuraman Protocol

Authors : Kondwani Magamba

Abstract : In the idealized Kish-Sethuraman (KS) protocol,messages are sent between Alice and Bob each using a secret personal key. This protocol is said to be perfectly secure because both Bob and Alice keep their keys undisclosed so that at all times the message is encrypted by at least one key, thus no information is leaked or shared. In this paper, we propose a realization of the KS protocol through the use of the Hill Cipher.

Keywords : Kish-Sethuraman Protocol, Hill Cipher, MDS Matrices, encryption
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020