International J.of Multidispl.Research & Advcs. in Engg.(IJMRAE),
ISSN 0975-7074, Vol. 4, No. I (January 2012), pp. 99-108

NEW STREAM CIPHER BASED ON DYNAMIC S-BOX USED IN AES ALGORITHM

CHANDRASEKHARAPPA T. G. S., PREMA K. V. AND KUMARA SHAMA

Department of Electronics and Communication Engineering,
Manipal Institute of Technology
Manipal 576104, India.

Abstract

At present RC-4 is very commonly used stream cipher, RC-4 is used in the SSL/TLC (Secure Sockets Layer / Transport Layer Security) standards that have been defined for communication between web browser and servers. It is a variable key-size stream cipher with byte-oriented operation. The algorithm is based on the use of a random permutation operation. As suggested by Shannon, for good security system both diffusion and confusion properties are necessary. Since RC-4 consists of only permutation operation it satisfies diffusion effect. In our new stream cipher system we have tried to impose the diffusion effect by random permutation and the confusion effect by an affine transformation and dynamic S-box. In turn our new stream cipher is more secured against any algebraic attacks like linear, differential and XSL attacks.

Keywords: AES algorithm, affine transformation, confusion, diffusion, stream cipher