

**CRYPTOGRAPHIC ALGORITHMS USING FINITE STATE
MACHINE, BERNOULLI AND LUCAS NUMBERS**

Rachna Navalakhe and Harsha Atre*

Department of Applied Mathematics and Computational Science,
Shri Govindram Seksaria Institute of Technology and Science,
Vallabh Nagar, Indore - 452003, Madhya Pradesh, INDIA

E-mail : sgsits.rachna@gmail.com

*Department of Applied Science,
SAGE University, Indore - 452020, Madhya Pradesh, INDIA

E-mail : atre.harsha.p22@gmail.com

(Received: Jan. 29, 2021 Accepted: Sep. 25, 2021 Published: Dec. 30, 2021)

Abstract: The aim of this paper is to propose a new cryptographic encryption and decryption algorithms using finite state machine and explicit forms of recurrence relations that is Bernoulli numbers and Lucas numbers. The efficiency of the proposed algorithm has been analyzed and the analysis shows an improved cryptographic protection in digital communications. The authenticity of algorithms is assured because in these algorithms we have used multiple set of keys to encipher the original message and its inverse to decipher the original message again. The algorithms has different levels of security which enhance the chances to keep our data or information confidential and secure for long time. There are many states in finite state machine to calculate the appropriate output. In every state it takes a new recurrence relation which depends upon the input. To compute the output we apply mathematical operation which is our cipher text. At each level we have number of cipher text which increases the data security. With the use of this algorithms, we can send information securely through the communication channel because we have used different recurrence relations at each level of input.

Keywords and Phrases: Cryptography, Lucas Numbers, Moore machine, Mealy