A comparative analysis of cryptographic algorithms

Dheeraj N. Kashyap

Department of Artificial Intelligence and Machine Learning, Jyothy Institute of Technology,
Karnataka, India
Corresponding Author: Dheeraj N. Kashyap
Email: dheeraj.nk20@gmail.com

Abstract:

With billions of internet users worldwide and the continuous growth of digital communication, data security has become a critical issue. Confidential data shared over the internet is vulnerable to cyber-attacks, and thus, there is an urgent need to secure the information transmitted over the network. Cryptographic algorithms play a crucial role in protecting sensitive information from unauthorized access. In this research paper, we perform a comparative analysis of different cryptographic algorithms and evaluate their time complexity. We investigate the efficiency and security of each algorithm to determine which one is comparatively better for data protection. Security. We conducted experiments to calculate the time complexity of these algorithms based on the length of the message or string that is encrypted. Our study evaluated the efficiency and security of each algorithm to determine which one is better suited for data protection. Our findings show that the evaluated algorithms have different levels of time complexity, with some algorithms being faster than others for messages of different lengths. The results of our study provide insights into the strengths and weaknesses of different cryptographic algorithms and can be useful for researchers, cybersecurity professionals, and organizations concerned with data security.