Cryptography Blockchain

Lab 1 - DES

Lab Report

CARVAJAL Mateo
CHAHINE Maroun
DOS ANJOS GUIMARAES Bernardo

5IF | OT4
November 2025

Analysis of our DES function

All our results can be found in the CSV file and in the txt file. The source code of the DES for each exercise are also available in the py files and named respectively.

The performance of the DES implementation was evaluated across message sizes ranging from 2^10 to 2^26 bytes, and the results show a clear linear relationship between input size and encryption time. Because DES operates on fixed 64-bit (8-byte) blocks, larger messages simply require proportionally more block-level operations, resulting in predictable and consistent scaling. As the message size doubled, the encryption time also roughly doubled, confirming the expected $O(n)$ time complexity. No significant performance anomalies or nonlinear behavior were observed, indicating that overhead from key scheduling and initialization becomes negligible compared to the cost of processing large volumes of data. Overall, the implementation demonstrates stable and scalable performance, with encryption time increasing smoothly with message size as anticipated for a block-cipher–based design.