**PARALLEL AND DISTRIBUTED COMPUTING PACKAGE– ABSTRACT**

DES ALGORITHM

**TEAM MEMBERS**

KANISHKA K(21PD18)

RAJANEHA R(21PD27)

**AIM**

The objective of the project is to parallelize the DES algorithm using both OpenMP and MPI. By parallelizing DES, the project aims to demonstrate how the encryption and decryption process can be accelerated by distributing the workload across multiple processing units or nodes.

**DES**

The Data Encryption Standard (DES) is a symmetric-key algorithm used for encryption and decryption of digital data. DES operates on 64-bit blocks of plaintext using a 56-bit key, undergoing a series of permutations, substitutions, and transpositions to produce ciphertext.

**INFERENCE**

**OpenMP Parallelization:** In the OpenMP implementation, the DES algorithm is parallelized using shared memory parallelism. The encryption process and the reversal of round keys are parallelized using different sections within a parallel region. This approach leverages multicore processors to speed up the computation of DES.

**MPI Parallelization**: In the MPI implementation, the DES algorithm is parallelized using distributed memory parallelism. Each MPI process operates independently on a portion of the data, and communication between processes is managed using MPI communication primitives. The encryption process is distributed across multiple MPI processes, allowing for parallel execution on a cluster or network of computers.

Overall, the project showcases the effectiveness of parallel programming techniques in accelerating cryptographic algorithms like DES, thereby improving their efficiency and scalability in modern computing environments.