Project Report
CS406 - Cryptography

Ameya Vikrama Singh (210070007)
Krishna Agaram (210051003)

April 28, 2023

1 Implementing DES

1.1 Feistel Network

A Feistel network is an invertible Pseudo-Random function construction. It is used in implementing block ciphers from the heuristic of Substitution-Permutation Ciphers. A Feistel network consists of multiple "rounds". In each round, we do the following:

$$F_n(a_n, b_n) = (b_n, a_n \oplus f(b_n))$$

where f is a (supposedly) pseudorandom function henceforth called the Feistel function. The Feistel construction is provably pseudorandom under the assumption that f is pseudorandom.

1.2 DES - The Data Encryption Standard

The Data Encryption Standard uses a Feistel network of 16 rounds.