Project Description

In this project, your team will implement the Baby DES algorithm described in the Trappe and Washington textbook in Matlab. (The reason for asking you to implement the Baby DES algorithm instead of the full DES is that I think it would be a cruel and monotonous exercise to ask you to type in the full S-boxes for full DES! Baby DES will give you the basic ideas.).

Your implementation should perform 4 Feistel Rounds, and be able to work with any randomly generated key and any randomly generated plaintext. Additionally, your code should be able to perform decryption.

What to Turn In

Having completed implemented Baby DES, your team will turn in a short report (less than 6 pages) that describes the design approach you used in implementing your function library. Explain any data structures you used, or any clever tricks you used to make your implementation more efficient. In addition to your report, you must attach a print-out of your source code.

Your grade will be based upon the clarity and thoroughness of your report. Be sure to include the name of all team members on the report.