ECE: Information and Network Security
Computer Project 2, Due Date: March 8, 2006
Spring 2005

Project Description

In this project, your team will implement the Baby DES algorithm described in the textbook. You should implement your code in MATLAB.

Your implementation should allow for an arbitrary amount of rounds and also be able to perform decryption. Upon implementation of Baby DES, you should do the following:

1. Choose a sample input bitstring, and a corresponding random key. Calculate the corresponding ciphertext when you conduct 1 round, 2 rounds, 3 rounds, and 4 rounds of the Feistel structure in Baby DES. Additionally, verify that the decryption procedure works for each case.

2. Check to see whether there are any weak keys for baby DES (with 3 rounds). A weak key is one such that when we encrypt a plaintext twice we get back the plaintext, i.e. a weak key K satisfies $E_K(E_K(M)) = M$ for any possible M (Note: Finding a key K such that $E_K(E_K(M)) = M$ holds for one M is not enough, you must show it for all M. Additionally, there may or may not be any... its up for you to tell me.).

3. Implement a CBC version of Baby DES and encrypt a plaintext message of 48 bits. Show what happens if you have two plaintexts that differ in the 14th bit.

What to Turn In

Having completed implementing your implementation, you must test the validity of your implementation. Explain any particular strategies you used to implement Baby DES, as well as any *implementation* lessons you learned during the implementation. Your team will turn in a short report (roughly 6 pages) that describes the design approach you used in implementing your function library. Additionally, answer the questions described in the items above. In addition to your report, you must attach a print-out of your library's 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.

Important Note:

The source code from different teams **will** be compared in order to see if there is any plagiarism. Duplication of source code or homework solutions or any other other course work will not be tolerated. Any perceived plagiarism will be directed to appropriate departmental and college-level (Engineering or FAS) officials for evaluation.