Lab 1

Deliverable: when you have completed the lab, e-mail me to tell me what type of file the secret file is and what the secret is. Also, the secret will help you on Test #1.

There is no deadline, but remember you have to make progress every week so you'll either have to complete this before lab #2 is assigned (in about 2-3 weeks) or give up, or put off starting on lab 2, but you need to be working on labs every week.

Do not share the secret (it's a hint about a question on test #1) with any of your classmates after you decrypt the file.

On the course website, I will post the following files:

lab1.pdf – this file

lab1.pdf.ciphertext – the ciphertext for this file using my secret key.

secret.ciphertext – an encrypted file, if you decrypt it with the secret key (after using linear cryptanalysis to figure out what the key is) and use the Linux *file* command you should be able to see what type of file it is and proceed accordingly.

sdes16.cc – The C++ code I use for encryption and decryption. This is a modified version of SDES that is 16-bits, uses a 48-bit key in 3 16-bit parts for the round keys, and has no initial or final permutation.

I recommend encrypting your own test file with your own key and testing your linear cryptanalysis techniques on that. Then when you've honed your cryptanalytic capabilities, apply your code to do a known plaintext attack on lab1.pdf. I don't recommend brute force attacks on a 48-bit key, but if you can figure out the last round key or the last couple of rounds and brute force the other 16 or 32 bits that's okay. You can adapt my old code for the 8-bit cipher that's at http://nsfsecurity.pr.erau.edu if you like, I don't recommend using Bubble Sort to sort the subkeys for 16-bit, though.

If you finish early, work on differential cryptanalysis and then if you send me a file to encrypt with my secret key via e-mail I'll be happy to encrypt that file and send it back