ECE 4300 Topic Selection

RC5 Features

- Fast. Only uses computer primitives like 2’s complement addition, XOR, left-shift, and their inverses
- RC5 has 2 words. Each word is denoted with w/r/b. w = word size in bits, r = number of rounds, b = key size in bytes. w can be 16, 32, 64. r and b range from 0 - 255.
- Uses: Not many. Largely outdated and insecure compared to other available cryptography algorithms/functions. Note that RC5 is a more primitive version of RC6.