Dr. R. Beezer
Practicum #4
Simplified DES

Math 133
Fall 2003

The Data Encryption Standard (DES) is an example of a block cipher. It works on "chunks" of text 64 bits long in concert with a 56-bit key. Ed Schaefer's Simplified DES (SDES) is meant to have the same feel as DES, but with many fewer bits. It uses a 10-bit key to work on text 8 bits at a time.

Procedure

1. Read the instructions for SDES in Section 5.1 of Barr (starting p. 330), or in Schaefer's original paper (I'll be making everybody a copy).
2. Practice doing SDES by hand, as you will want to have this skill for the next exam.
3. Use my SDES calculator (link is on the WWW page) to help you with learning how to do these computations.
4. Participate in a distributed brute-force attack on SDS, as follows.
5. Here is some known plaintext, together with the corresponding ciphertext.

   Plaintext: S U _ O (ASCII Characters 83, 85, 95 and 79)
   Ciphertext: G / , ' (ASCII Characters 71, 47, 44 and 39)

   Use the ASCII code to convert the texts to binary. We will try (collectively) *all* possible keys to find the correct one. In class you will be assigned a "leading" 4 bits of a key, which you can complete $2^6 = 64$ different ways. Test these keys on the first byte of the plaintext/ciphertext pair above. When a key behaves correctly on the first byte, test it again on the next three bytes to see if it is the "real" key.
6. Send me an email listing the 64 keys and their effect in encrypting the first byte. If you had occassion to test any of the next three bytes, indicate when this happened. Also, if you discover the real key, let me know about it, and DO NOT divulge this information to anybody else in the class.

Grading

1. Full credit for a successful test of all 64 keys assigned to you.

Notes

1. This exercise "partitions" the "key-space." There are $2^{10} = 1024$ possible keys, enough to make it an annoying chore to test all of them. However with $2^4 = 16$ students, we can split up all the possible keys into $2^4 = 16$ groups of $2^{10}/2^4 = 2^{10-4} = 2^6 = 64$ keys, a more manageable size.

   This is entirely analagous to having a large number of computers (or specialized chips) all working simultaneously to test many different portions of the key-space.
2. Follow the link on the course page to read about how DES (a US government standard) was cracked by just such an effort.