CS211 ALGORITHMS & DATA STRUCTURES II

LAB 5

Dr. Phil Maguire

CRYPTOGRAPHY

Pen and Paper Exercise

1. Calculate 7^{29} mod 11 by hand (see crypto notes).
2. Your public key is (29, 2, 3) and your private key is 5. Bob uses your public key to send you a message. He sends you the cipher (23, 27). Use your private key to obtain the secret message code number. Read over the lecture notes to get the required formulas.

Programming Exercise

Write a program that takes *encoded.txt* as input and outputs the European language that it is in. It is one of these languages: http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/

Put the text through your Huffman frequency code to get a frequency profile, and then compare it against these European languages to see which one is the best match. Come up with some metric for quantifying how good the fit is.

encrypt.java shows how the ciphertext was generated.

Advanced Programming Exercise

Write a program that decrypts *encoded.txt* as much as possible, so it becomes apparent what famous piece of text this is. 2% bonus CA will be awarded to the first to crack it.