# SaDS HW 6

Inti Mendoza

## Problem 6.1

See `criptographer.cpp`

## Problem 6.2

See `criptographer.cpp`. File encrypted is `tux.txt`. The encrypted file is `tux_ encr.txt`. The decrypted file is `tux_ decr.txt`. Simple versions are `tux_ encr_ simple.txt`, and `tux_ decr_ simple.txt`. Simpler versions has some shades still of what the normal image should be like (at least better than normal encryption version which is still pretty hard to see).

## Problem 6.3

1. For the block cipher step, an adversary has a finite number of possibilities. Although expensive, it is computationally possible, although it is solved with $\frac{1}{p_x}$ thus it is negligible. As one ventures down, one multiples against a negligible function which ends in a negligible function. So it is secure as probability of adversary to guess right key, is negligible after all. Therefore E is comp-ing secure.
2. Adversary can have a plaintext encrypted (by him) with all possible ways of encrypting that plaintext. After encrypting his plaintext with out encryption, a mere plaintext check is enough to find out our encryption key. Therefore, E is not CPA-ing secure.