**Software Design**

The software is written in Python 3. I chose this language because I am very familiar with it, and enjoy using it. The software design consists of three classes, corresponding to MT19937, the stream cipher, and the hacking tool, along with a main entry-point. I chose Object Oriented Programming (OOP) design over procedural, because all three major components of my project consist of closely related functionality and state.

MersenneTwister19937

*\_\_init\_\_(self, seed)*

*\_initialize\_state(self, seed)*

*\_twist(self)*

*\_temper(self)*

*next\_word(self)*

StreamCipher

*\_\_init\_\_(self)*

*\_untemper(self, word)*

MThacker

*hack\_stream(self, stream\_cipher)*

*decrypt(self, ciphertext)*

**Software Operation**

**Example Output**

**Accomplishment Summary**

MT19937 Algorithm class constants

n = 624

\_\_init\_\_(seed)

\_initialize\_state(seed)

index = n + 1

**MersenneTwister19937**

\_initialize\_state(seed)

\_initialize\_state(seed)

\_initialize\_state(seed)

\_initialize\_state(seed)

**MersenneTwister19937**

**MersenneTwister19937**