CSCI262 - Systems Security

Student Name: Chong Hui Wen

Student ID: 7311436

**Must run in Linux

**Have to download the openssl library first before compiling

Compile:

$ gcc -std=c99 avltree.h avltree.c helper.h helper.c Rainbow.c -o Rainbow -lssl -lcrypto -lm

$ ./Rainbow <filename>

Additional Notes:

A 'wordlist.txt' and 'rainbow.txt' file has been provided as part of the folder.

Reduction Function Implementation:

To go about doing the reduction function, it takes in ant int i and a unsigned char pointer md5_digest.

With the use of bitwise operators, and bit shifting in order to get the 32-bit width of the message digest,

which is 128-bit/32 byte hex value to decode it to a MD5_LONG type, which is a macro for unsigned int (called digest_sum).

After getting the bit sum for the unsigned int (digest_sum), I take the value and apply the modulo of 26 to the power of the int

that i passed in. The i has been defined as a global array with 4 possible values of 12, 8, 6, and 4 based on how many

words the password contains. After doing the calculations to get an integer, I endcode the value back to an unsigned

char pointer and return that to be hashed again.