I did not add integrity or authenticity check creating “t” by using the “ka” other half of the key, therefore I never check if t’ = t.

I used “part2_file.txt” as the file string and “part2_enc.txt” is the output of the encryption function. Then I input the “part2_enc.txt” and decrypted it to the file name “part2_dec.txt”. We can see part2_file.txt and part2_dec.txt are identical.

In this case the two files are identical and have the same output when viewed through NotePad++.

Most of the hex handle functions are from StackOverFlow and as long as they worked, I did not feel the need to re-write those functions myself. I aimed at the bigger picture in trying to put all the pieces together to get the encryption and decryption working.

Also disclaimer: I had issue decrypting because I already converted the encrypted message to hex, therefore I had to divide cipher_text.length by 2 because hex is multiplied by two. This was one of the issues I ran into while decrypting, which caused an out of range argument.