

Quiz-5

[illegible]

At first, I defined a function as “encrypt” with using MD5. Then, I transformed the input from “string” into “byte”, and printed the 4 MSB.

To find the string that 4 MSB was equal to the printed 4 MSB, I used

a “for” loop to find the value. If the 4 MSB of the cipher text was as same as the 4 MSB before, we find the plaintext which was we wanted.

c606196ea460a3a53ac3e81c614b990b
9cc7 1000000000000000000000000000000078229

Using the example, the 4 MSB of the example plaintext is “9cc7”. And with using the program, we could find “1000000000000000000000000078229” is also the plaintext that could be encrypted as “9cc7xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx”.

Using the example, the 4 MSB of the example plaintext is “9cc7”. And with