Intro to Cryptography

Mark Anderson
Problem 6

May 16, 2019

1. For implementing the Rabin cryptosystem, I was able to successfully encrypt and decrypt the example given in the book. However I ran into a similar problem as in question 7 of my method for encryption/decryption relied on the calculation of very large primes, specifically $T^{p+1//4} mod p$ and even decrypting one letter with the large primes given in the prompt was taking too long. With the very small values of 127, and 131 it worked just fine, I was able to encrypt '4410' and retrieve the plaintexts: 4410, 5851, 15078, 16519. I believe I am missing a step somewhere that drastically reduces the size of that exponent, maybe a modular reduction or even a completely different number. The encryption is working fine, and even with the incredibly large primes is insanely fast, as its just quick multiplication and modulus.