Homework Number:	06
Name:	Samitha Ranasinghe
ECN Login:	sranasi
Due Date:	02/28/2023

Problem 1

For generating the 2 prime numbers, I used the given prime number generator to keep generating 2 prime numbers of 128 bits long until 2 are produced where they are not equal and totient is coprime to e.

For encryption, RSA is implemented where the same methodology of AES followed to grab blocks of 128 bits and pad from right if less. And then extend to 256 bits from left to bring tp to 256. Then it is encrypted by calling pow function and raising to e and modulus with n which is p multiplied by q.

For decryption, the same process as encryption is done except 256-bit blocks are grabbed and the exponentiation value is the multiplicative inverse of e where the modulus is the totient of n. CRT is then implemented to get the plaintext where the p and q are treated as factors of n. The CRT gives the plaintext block which is written to file after padding is removed.

Problem 2

For encryption, the encryption process in Problem 1 is repeated 3 times after 3 n is produced from 6 prime numbers. The produced cyphers are written to 3 separate files.

For cracking, the separate n values are used to produce the 3 values for each cypher and n value which is the product of the other two n values, the multiplicative inverse of the previous values with n as the modulus for each n respectively. The sum is then taken and then modded with the product of all n to produce the cube value of the plain text. The cube root is then taken using the given function