RSA Encryption Algorithm

The security depends on the difficulty of factoring large numbers:



Refer to getLargePrime.py for details about generating large primes.

The length of p and q should be 1024 bits.

Euler’s Theorem:

(m must be a prime OR gcd(a,m) = 1,  is called the Euler’s Totient)

(gcd(m, n) = 1)

Key Generation:



(Refer to EulerTotient.py for the method to get e)



After key generation, have to be securely destroyed.

also need to be destroyed because ,which is easy to reconstruct p and q.

Encrypt:



(Length of message m is smaller than length of n)

Decrypt:



Correctness:



If m and n are relative primes:



If m and n are NOT relative primes:



Therefore, no matter whether m and n are relative primes or not, the encrypted message can always be correctly decrypted.

