**CYBR 505 Computer Science Foundations for Cybersecurity**

**Assignment: Exploring RSA Cryptographic Algorithm**

**Ron Rivest, Adi Shamir, Leonard Adleman (RSA) cryptographic algorithm**  
  
In RSA everyone has their own encryption and decryptions keys where encryption keys are public, but decryption keys are private. The security of RSA algorithm also verifies the digital signatures eliminating the forgery of signature. This is an example of asymmetric encryption.  
 **RSA Key Generation**  
1. Generate two different **prime** numbers p and q  
p = 11 q = 13

2. Calculate the product **n** = p x q  
n = 11 x 13 = 143

3. Calculate the **totient** ϕ(n) = (p-1) (q-1)

= (p-1) (q-1)

= (11-1) (13-1)

= 10 x 12 = 120

**Encryption**Each user has their own encryption procedure denoted by E. Let the encryption key be (e, n).

1. Select for **public key**, such that 1 < E < ϕ(n) and gcd(ϕ(n), e) =1  
*- must be a prime number  
- less than a totient*

*- must not be a factor of totient*

So, we will use public key value of 7 which satisfies the above condition.  
**Public Key = [e, n] = [7,143]  
-------------------------------------------------------------  
Encrypting the plain text where message (m)=8:**

= me / mod n   
= 87 / mod 143   
= 2097152 / mod 143 = 57

**Therefore, the cipher text (c)= 57**

**-------------------------------------------------------------**

**Decryption**Each user has their own decryption procedure denoted by D. Let the decryption key be (d, n).

1. Select a **private key**, such that  
- product of D and E, divided by T must result in a remainder of 1

(D\*E) mod T = 1, (**103**\*7)/ mod 120

So, we will use **private key** value of 103 which satisfies the condition.

**Private Key = [d, n] = [103,143]**

**-------------------------------------------------------------**

**Decrypting the cipher text:**=cd / mod n

= 57103 / mod 143 = **8** 🡨 original plain text

**-------------------------------------------------------------**

**CONCLUSION:**  
So, with the help of RSA cryptographic algorithm I was able to **encrypt** the secret **message ‘8’** with public key [7,143] and **decrypt** the message with private key [103,143].