**Lab 9**

**Exercise**

1. Perform RSA encryption and decryption. The parameters used here are small. Verify your results

with cryptool?

1. Choose two distinct prime numbers, such as P=61 q=53



1. Compute n = pq giving n=?



1. Compute the totient of the product as φ(n) = (p − 1)(q − 1)



1. Choose any number 1 < e < 3120 that is co-prime to 3120. Choosing a prime number for e

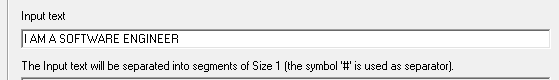
leaves us only to check that e is not a divisor of 3120.

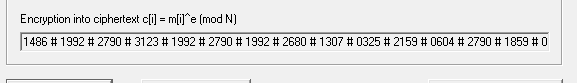


1. Compute d, the modular multiplicative inverse of e (mod φ(n)) yielding d=?

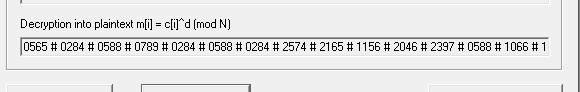


**ENCRYPTION:**





**DECRYPTION:**

****