Kabeer Ahmed SE-19028

LAB 9

Exercise:

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

- **Choose two distinct prime numbers, such as P=61 q=53**
- **Compute n = pq giving n=?**
- **Compute the totient of the product as ϕ(n) = (p − 1)(q − 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.**
- **Compute d, the modular multiplicative inverse of e (mod ϕ(n)) yielding d=?**

n = 61*53 = 3233

ϕ(n) =60*52 =3120

e = 65537

d = 2753