**LAB 9**

**Question 1)**

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

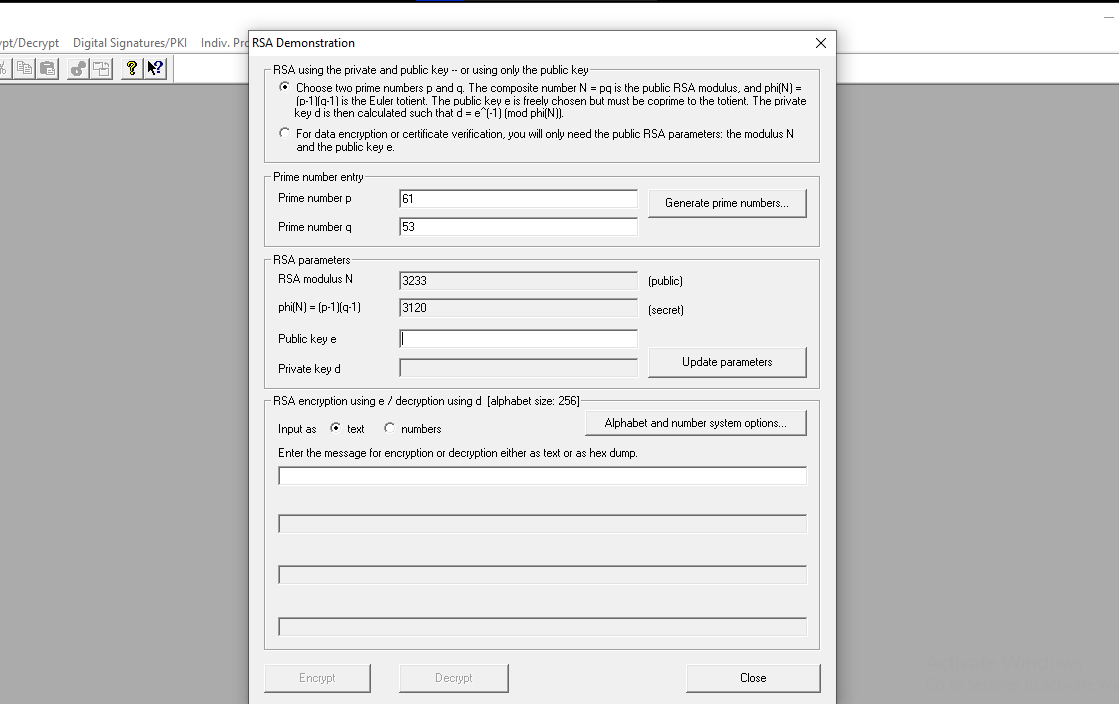
* **Choose two distinct prime numbers, such as P=61 q=53**
* **Compute n = pq giving n=?**
* **Compute the totient of the product as $(n) = (p − 1)(q − 1)**
* **Choose any number 1 <e < 3120 that is co-prime to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120.**
* **Compute d, the modular multiplicative inverse of e (mod (n)) yielding d**

**Answer )**

**Prime numbers =>** **p**=**61** and **q**=**53**

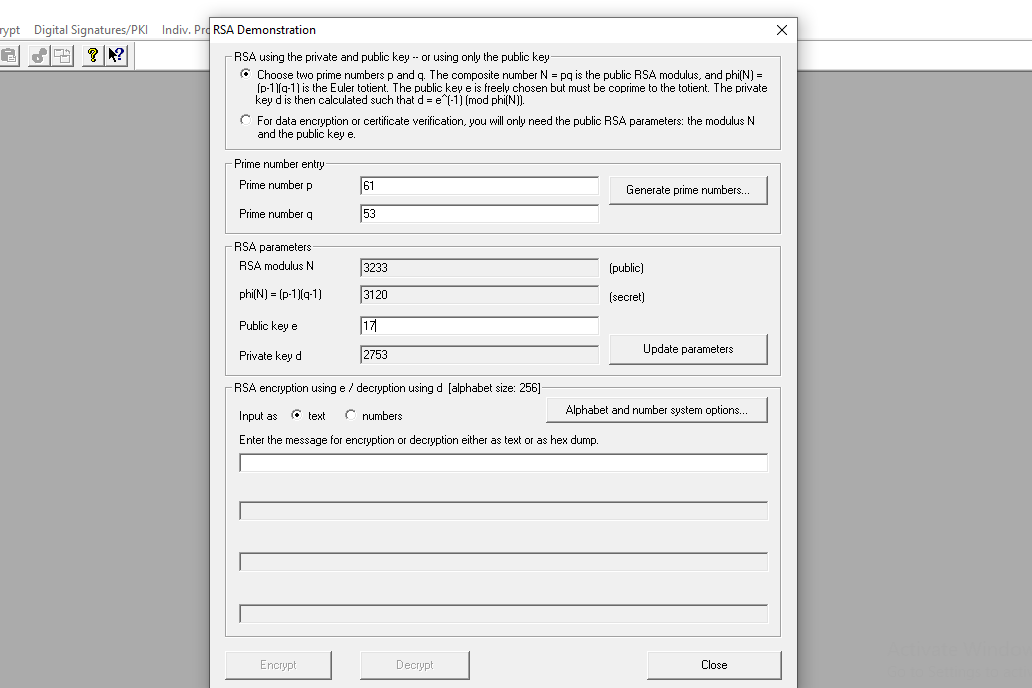
**n** **= p x q =>** **61x53** => **3233**

**Totient of the product** **=>** **ϕ(n)=(p−1)(q−1) = 60×52=3120**

****

As **e** should be **1**<**e**<**3120** and **e** is co-prime to **3120**

So, lets take **e=17** as it satisfies the conditions of being greater than **1**, less than **3120**, co-prime to **3120**, and not a divisor of **3120**



For the modular multiplicative inverse of ***e* (mod *ϕ*(*n*))**

We need to find ***d*** such that ***d*×*e* = 1 (mod*ϕ*(*n*)).**

Using the Extended Euclidean Algorithm or other methods, we find that

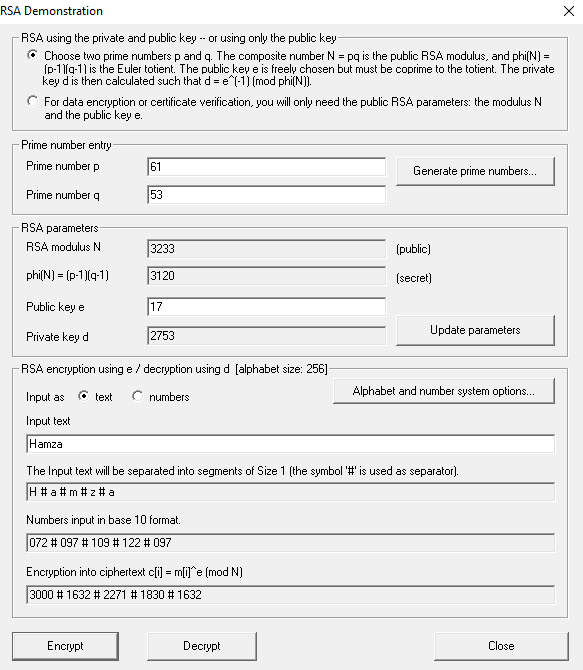
***d* = 2753** is the modular multiplicative inverse of ***e* = 17** modulo ***ϕ*(*n*)=3120**

Now, we have the public key **(*n*,*e*)** = **(3233,17)** and the private key ***d***=**2753**

Let's verify the encryption and decryption:

**ENCRYPTION:**

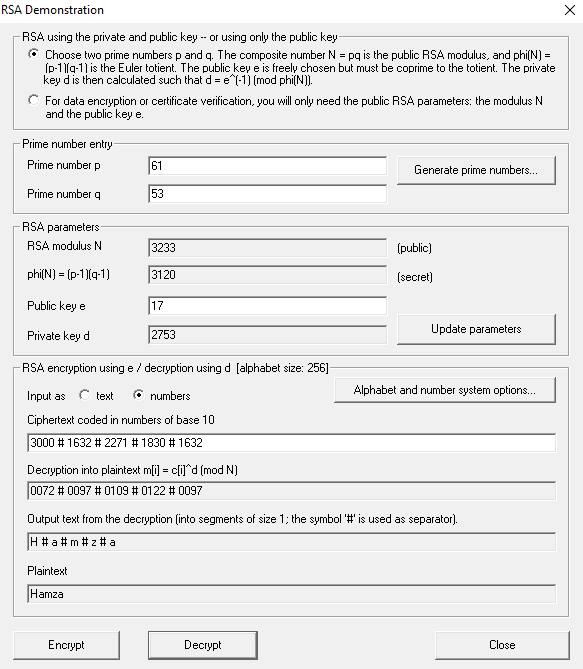
**Input text =** Hamza

****

**Encrypted text =** 3000 # 1632 # 2271 # 1830 # 1632

**DECRYPTION:**

**Input text =** 3000 # 1632 # 2271 # 1830 # 1632



**Decrypted text =** Hamza