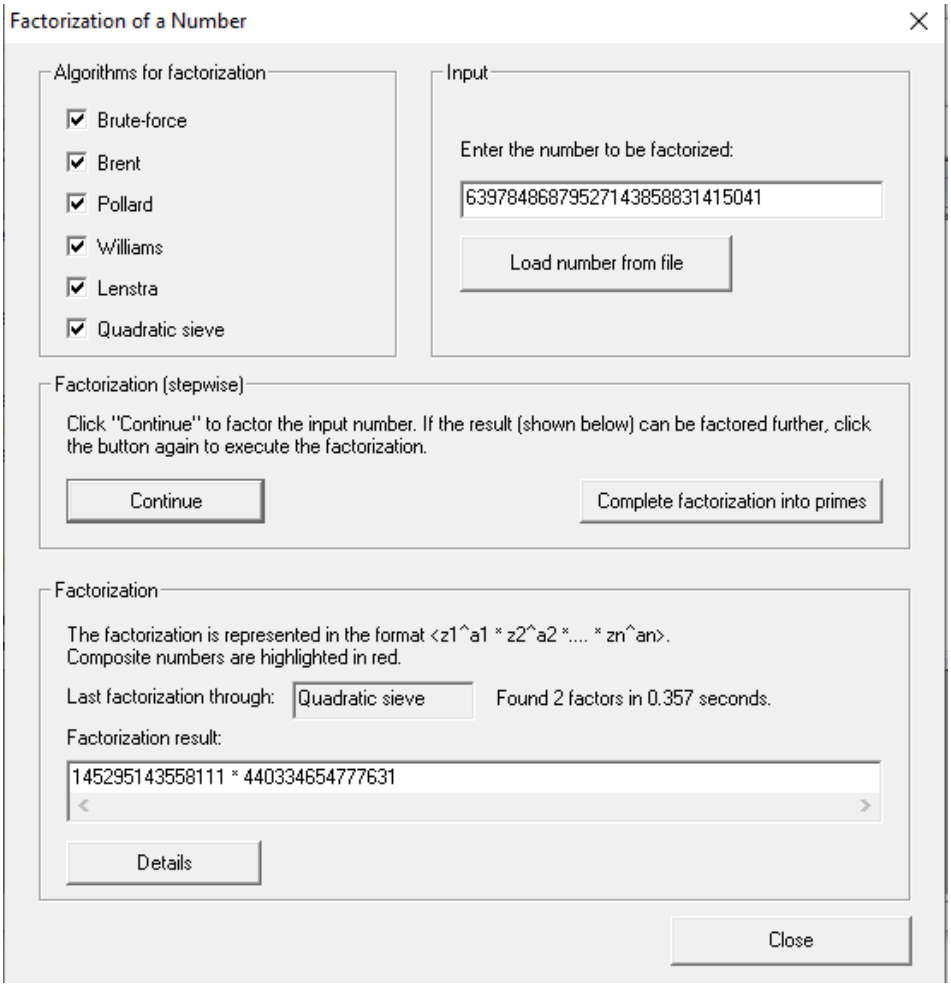
Kabeer Ahmed SE-19028

LAB 10

Exercise:

1. In RSA, practical difficulty of factoring the product of two large prime numbers is known as the factoring problem. This is what RSA is based on. The prime factors must be kept secret. If the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.
If we know N = 639784868795271438588314150 41 (95 bit, 29 decimal digits) and then try this number N = 351573870816322547022741576341143304183 (129 bit, 39 digit). Find the factors using cryptool by going in to Indiv. Procedures -> RSA Cryptosystem -> Factorization of a number. Then enter the number and find the factors. What does this tell you about the difficulty level of finding the factors in both cases?
What are the factors in both cases? What algorithm was used last to factorize in both cases? Show practical demonstration

n = 639784868795271438588314150 41



Kabeer Ahmed SE-19028

n = 351573870816322547022741576341143304183