

## 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  $N = 63978486879527143858831415041$  (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

$n = 63978486879527143858831415041$

**Factorization of a Number**

Algorithms for factorization:

- ☒ Brute-force
- ☒ Brent
- ☒ Pollard
- ☒ Williams
- ☒ Lenstra
- ☒ Quadratic sieve

Input:

Enter the number to be factorized:

63978486879527143858831415041

Load number from file

Factorization (stepwise):

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

Continue Complete factorization into primes

Factorization:

The factorization is represented in the format  $\langle z_1^{a_1} * z_2^{a_2} * \dots * z_n^{a_n} \rangle$ . Composite numbers are highlighted in red.

Last factorization through: Quadratic sieve Found 2 factors in 0.357 seconds.

Factorization result:

145295143558111 \* 440334654777631

Details

Close

$n = 351573870816322547022741576341143304183$

Factorization of a Number

Algorithms for factorization

☒ Brute-force

☒ Brent

☒ Pollard

☒ Williams

☒ Lenstra

☒ Quadratic sieve

Input

Enter the number to be factorized:

351573870816322547022741576341143304183

Load number from file

Factorization (stepwise)

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

Continue

Complete factorization into primes

Factorization

The factorization is represented in the format  $\langle z1^{a1} * z2^{a2} * \dots * zn^{an} \rangle$ .  
Composite numbers are highlighted in red.

Last factorization through: Quadratic sieve Found 2 factors in 1.014 seconds.

Factorization result:

12764787846358441471 \* 27542476619900900873

Details

Close