**Aria Javani**

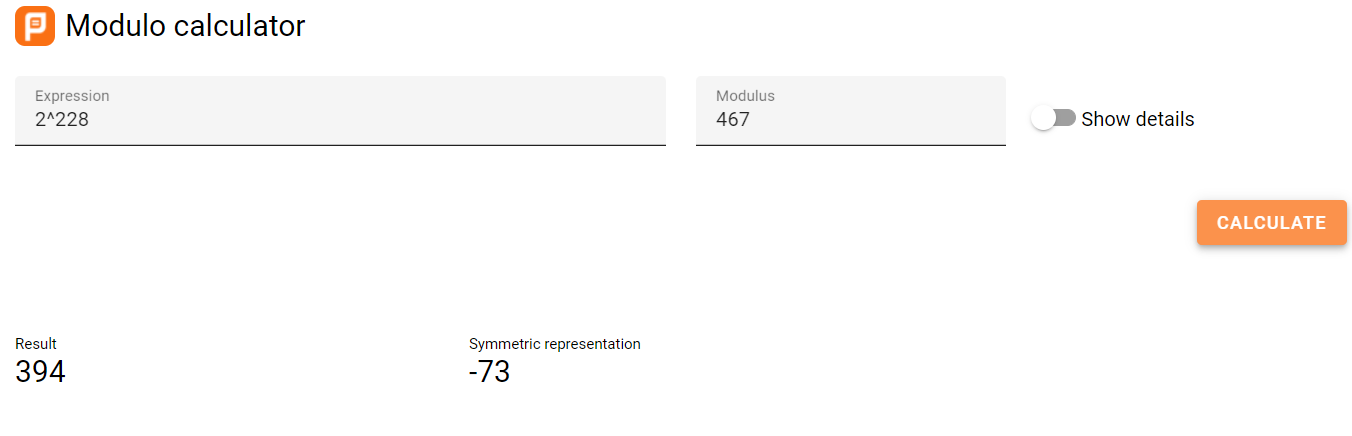
**9725303**

**1:**

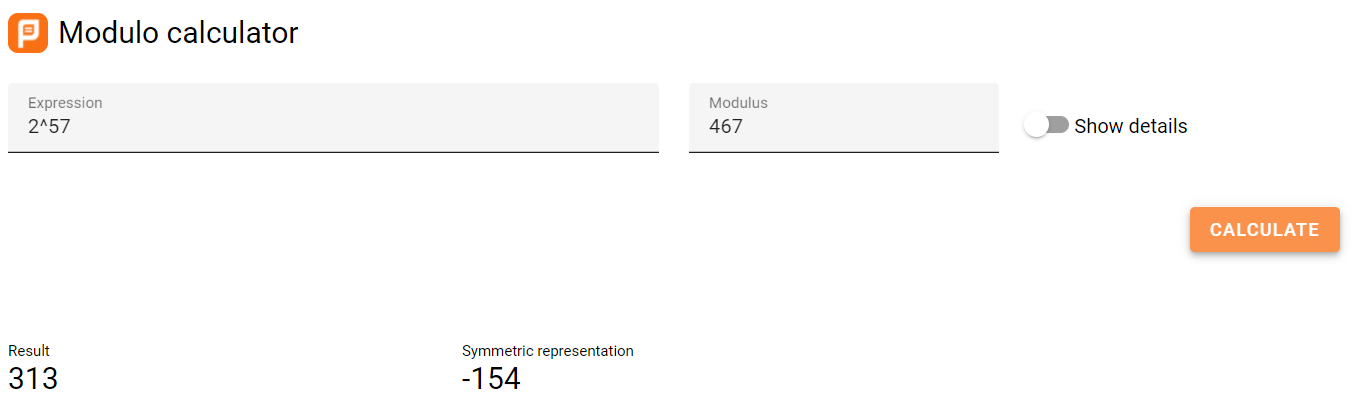
we have two answers

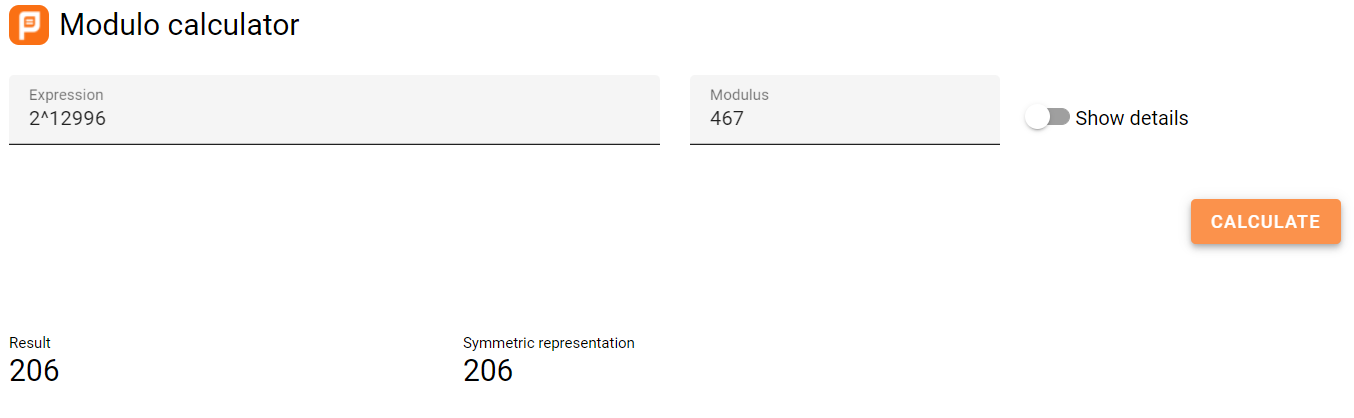
**2.1:**

mod 467

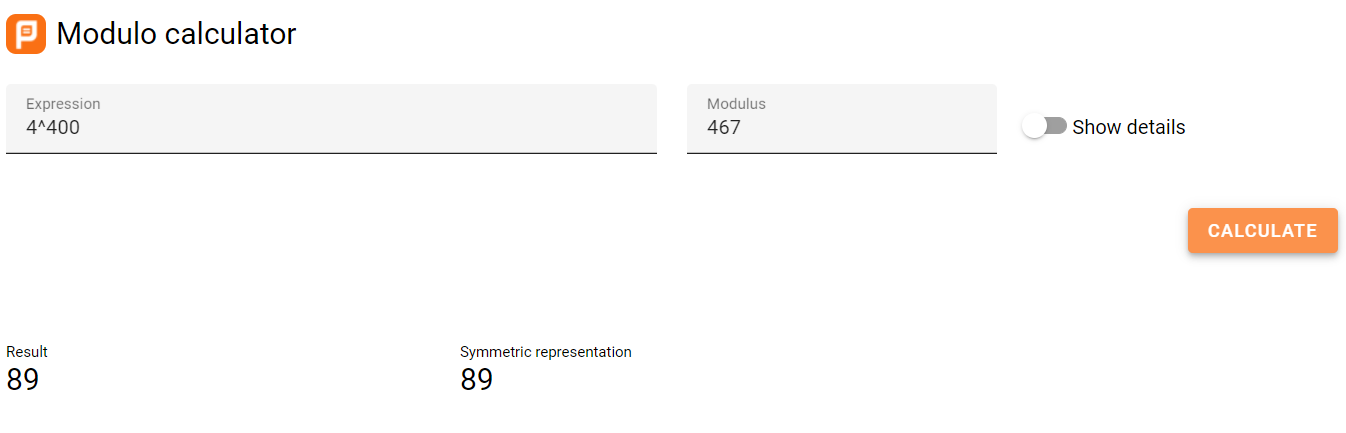


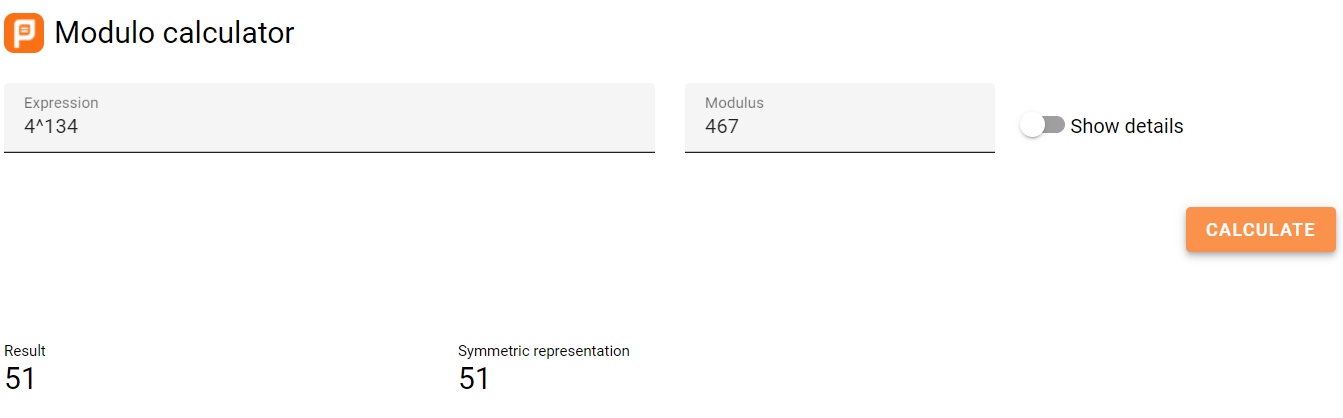
mod 467

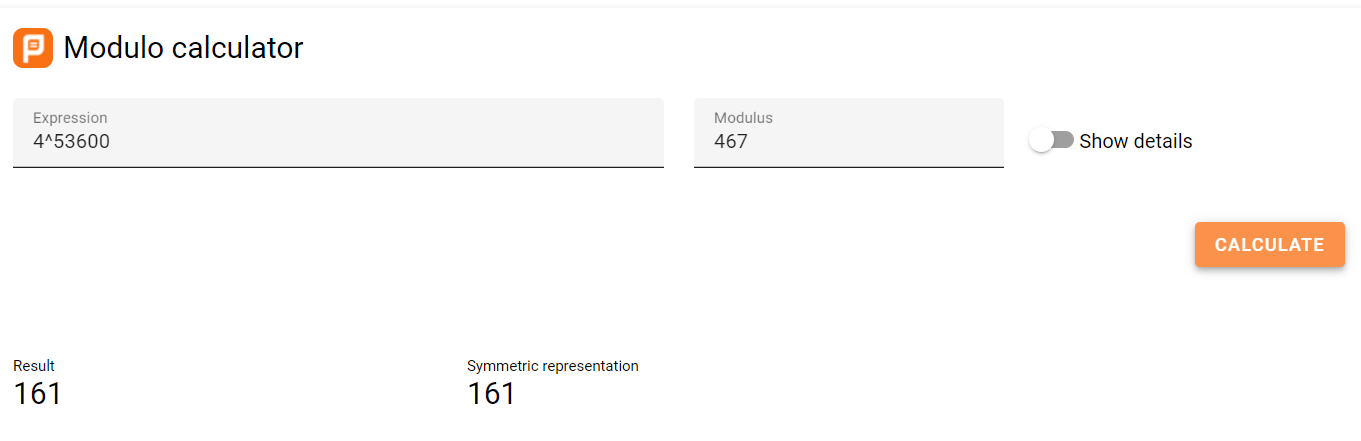
****

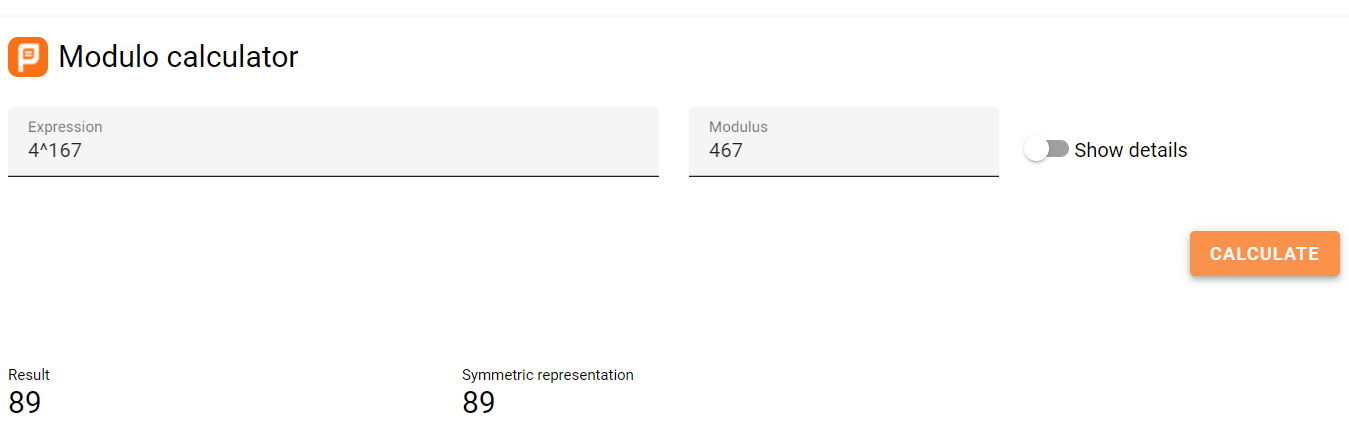
****

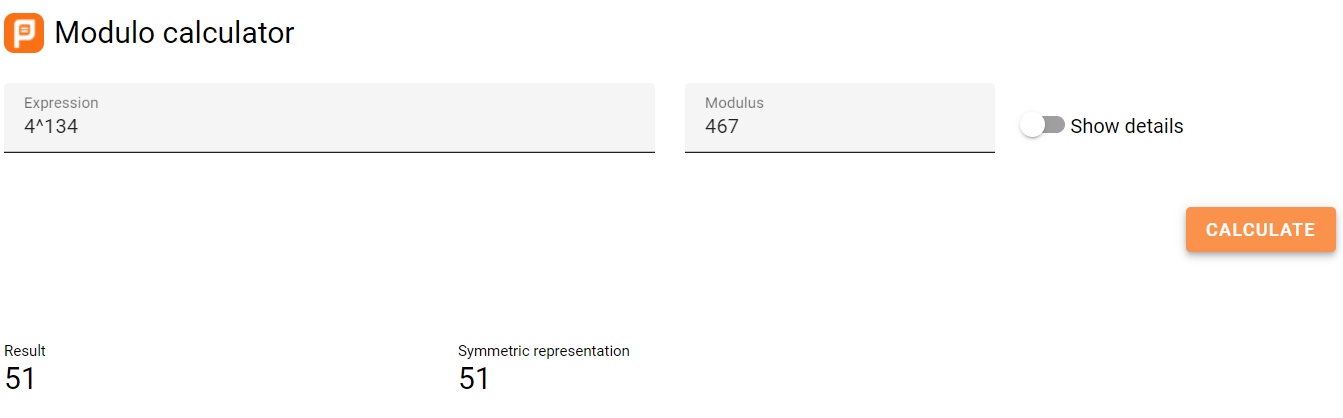
**2.2:**

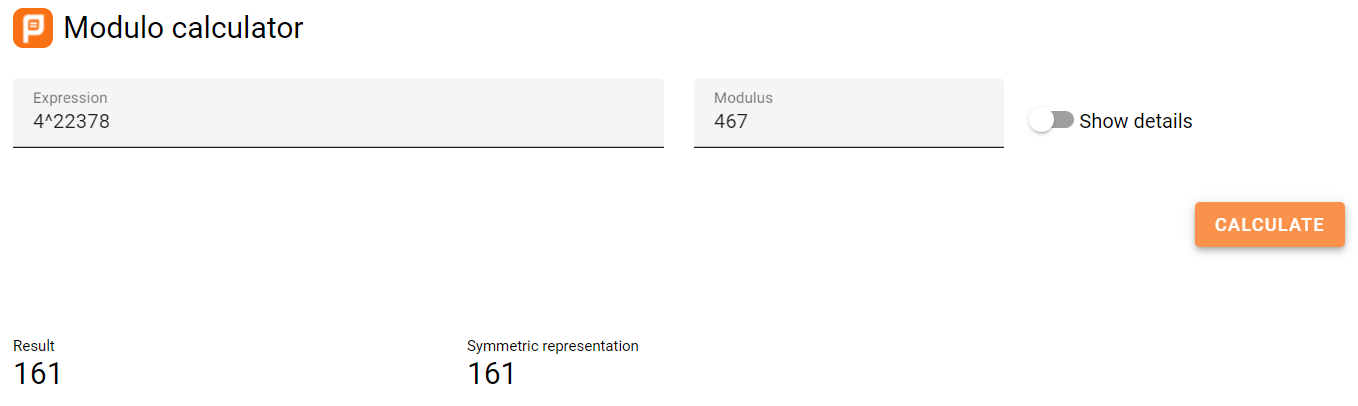


****

****



****

****

**2.3 :**

Order of our generator is 233 so 167 and 167+233=400 have the same result.

**3 :**

In this attack the attacker tries to send his own public key to Alice and Bob instead of letting them get each other public key. If he does this successfully in the next step Alice or Bob send their messages encrypted with attacker’s key so attacker can read them easily.

**4.1 :**

a primitive root of p is a number such that all of a powers generate all the number between 0 and p

**5 :**

encrypted message:

Bob sends

Alice decryption :

**6 :**

we try to show these problems are equivalent and how to convert each one to other.

in elgemal we find message and in diffie hellman we find the key.

next we need to find the common key in diffie helman

now suppose we want want to know the elgemal equivalence with diffie helman parameters

next we try to find elgemal message by having a algorithm that find diffie hellman key

by doing this exchanges we can put elgemal parameters in out diffie hellman algorithm.

**7 :**

if we choose 1 then public key is which allows attacker to find private key effortlessly.

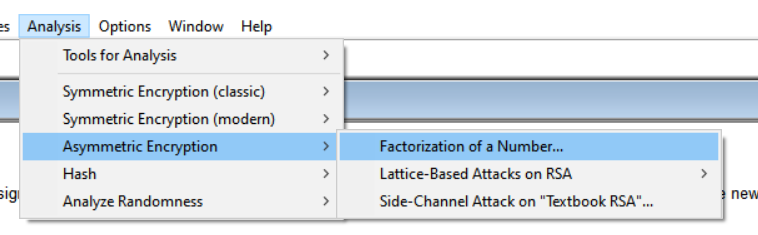
if we choose p-1 then public key is 1 which means our private key is p-1.

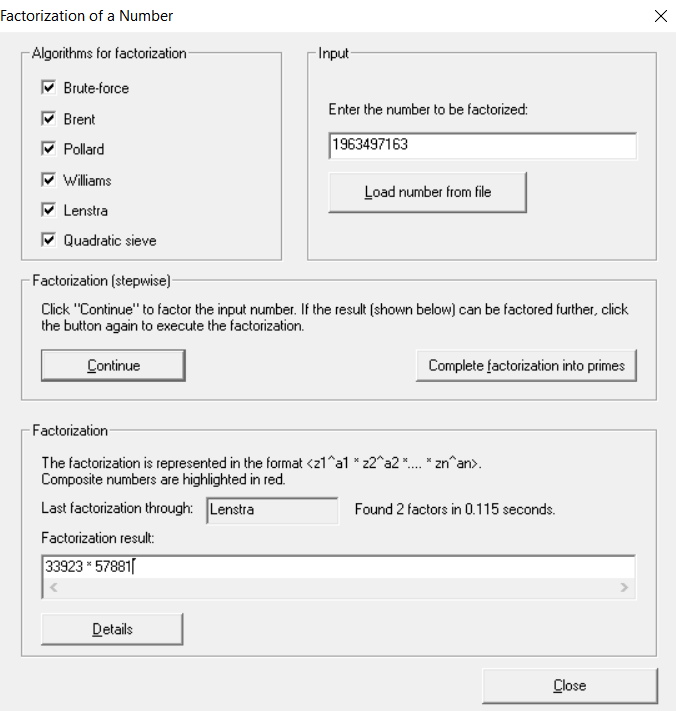
**8 :**

we’ve already proven this in homework 3 q7.2 :

first we assume a set of all possible strings of length p and a different characters possible for each string so the count of string will be . among all of these strings there are exactly a strings consisting of exactly one character. with the rest of them we make a necklace with each string then we consider all the strings with that have a same necklace with subset length of p in one group the reason we choose p as size is because a subset of length T should be chosen with the condition of T dividing length of whole string and since the length of strings is prim number of p we shall use p (also not 1 because it’s trivial) as the sub string length. so p divides and

**9 :**

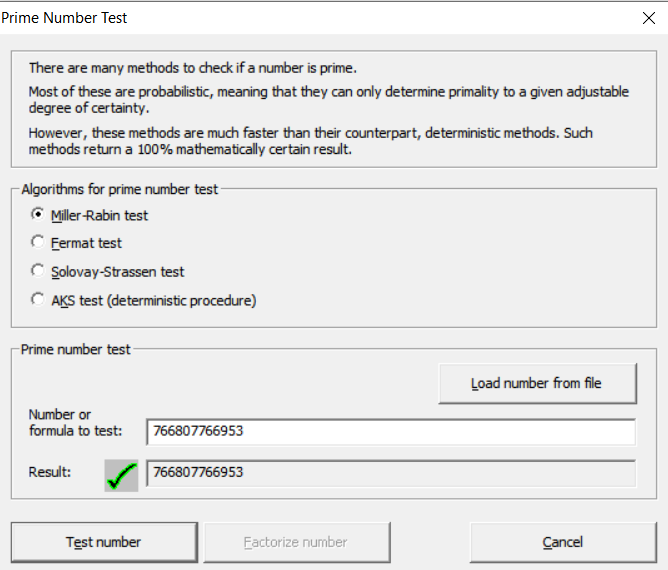


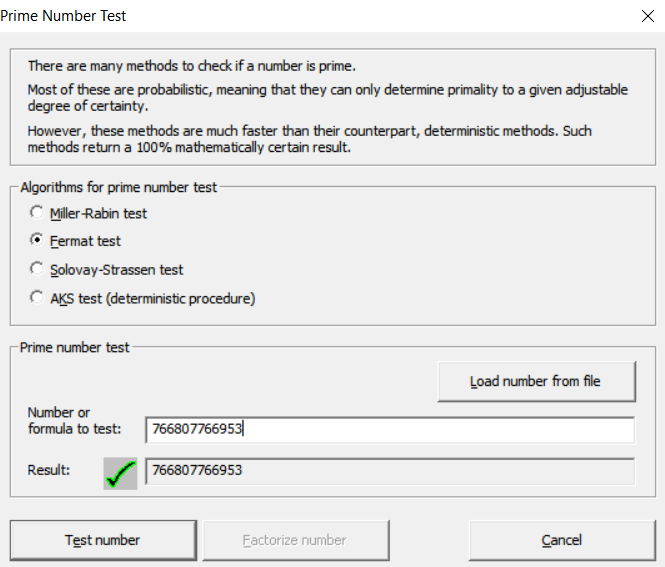


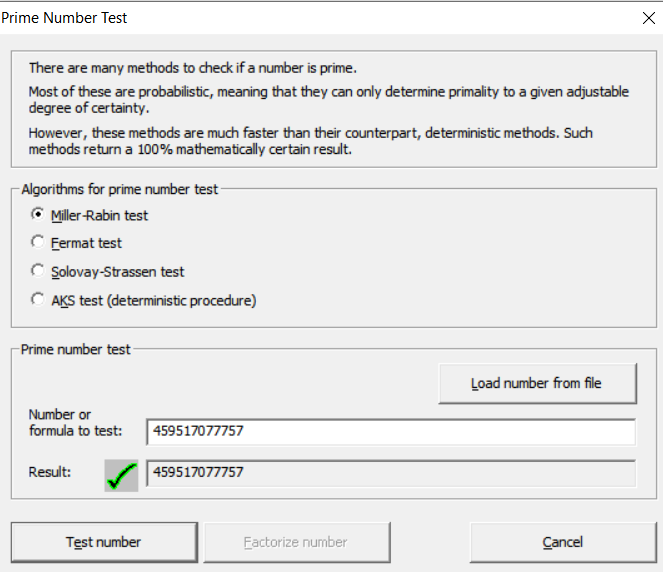
1. prime numbers : 766807766953, 459517077757, 26464987111

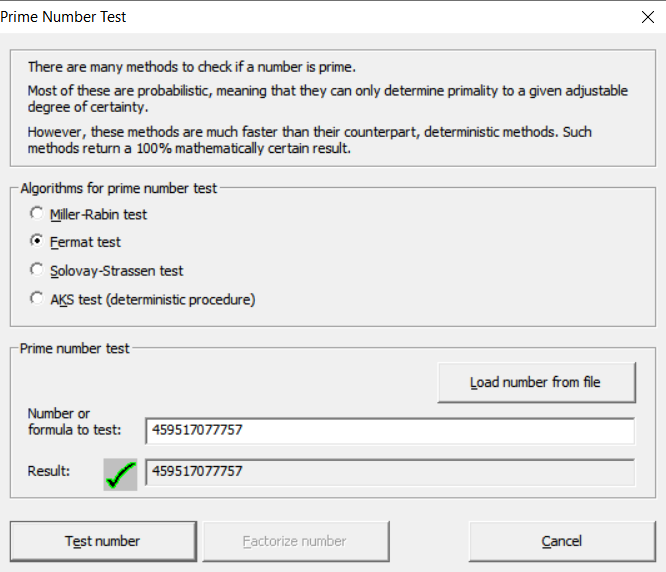
Carmichael numbers : 334153, 314821, 294409

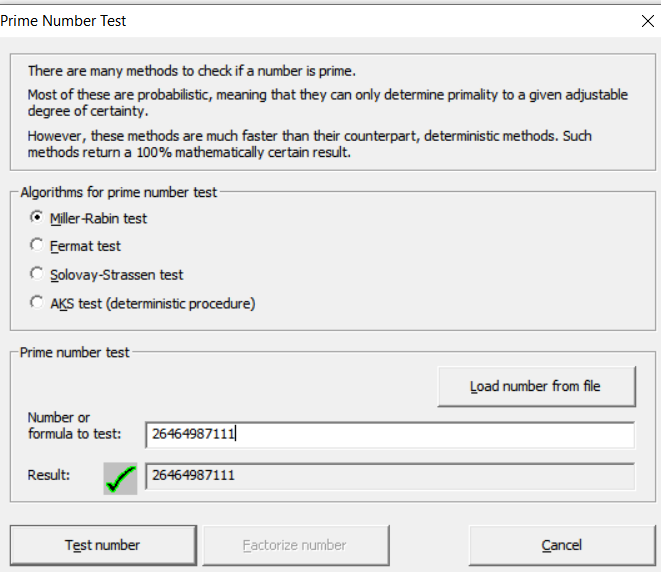
regular composite numbers : 111111111, 222222222, 33333333

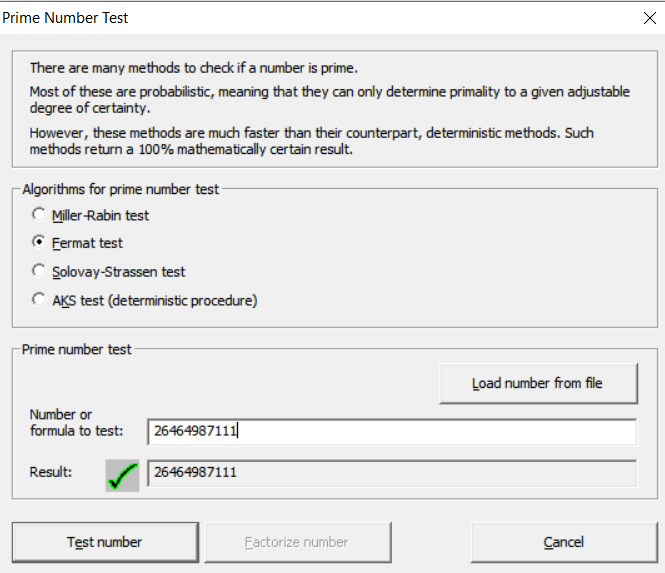


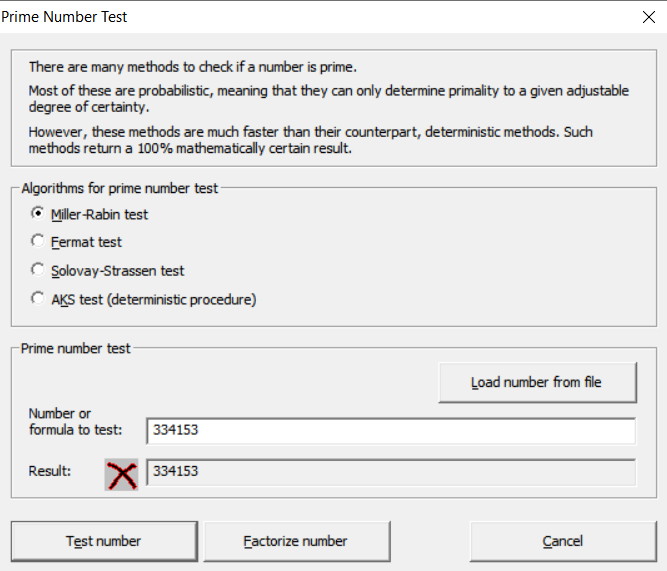


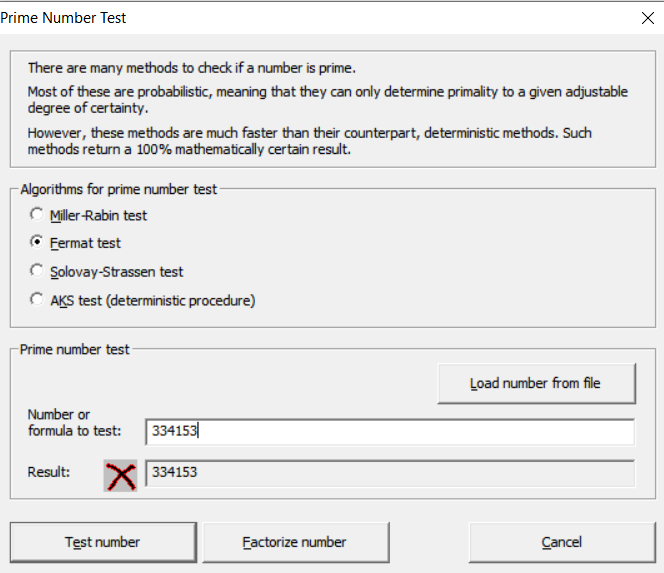


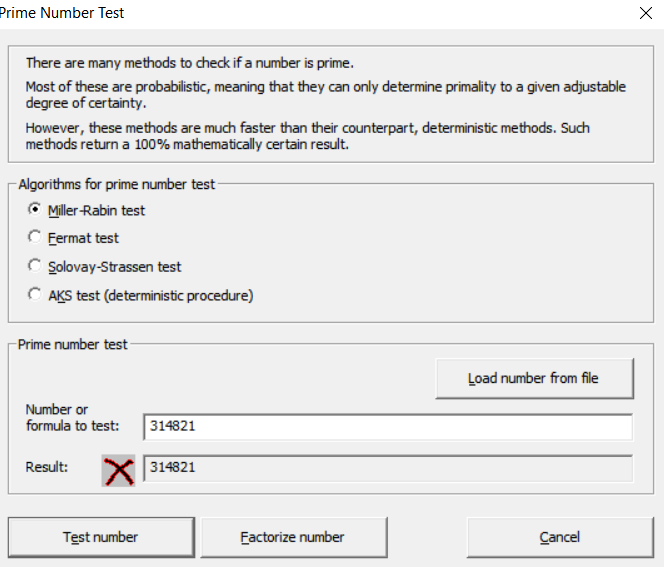


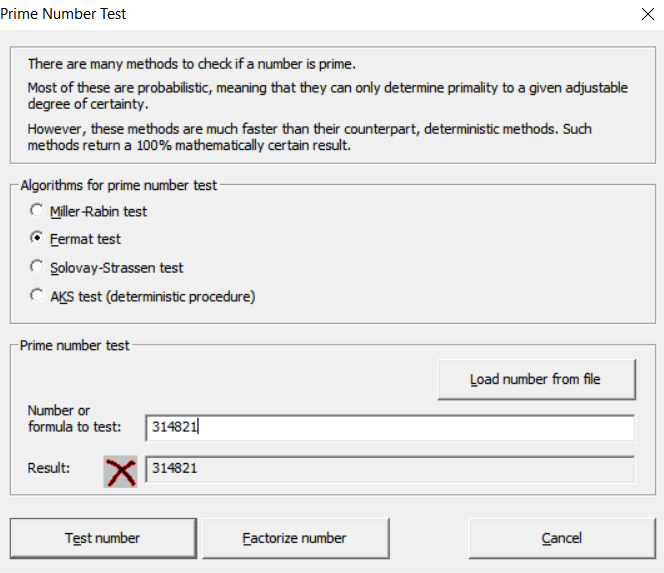


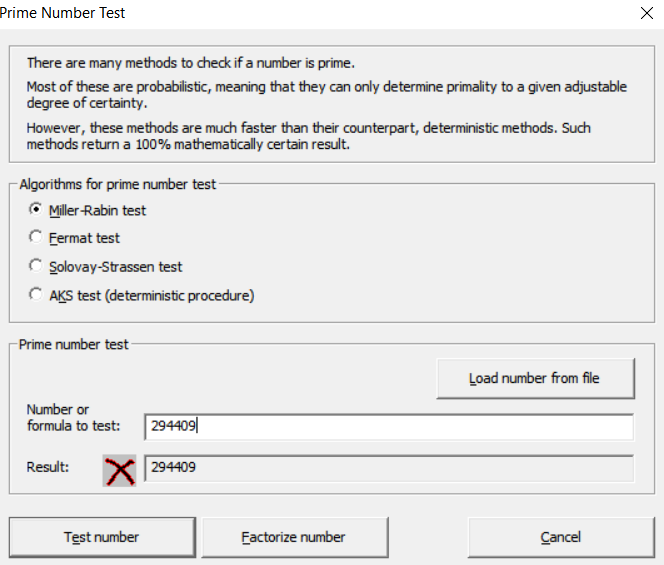


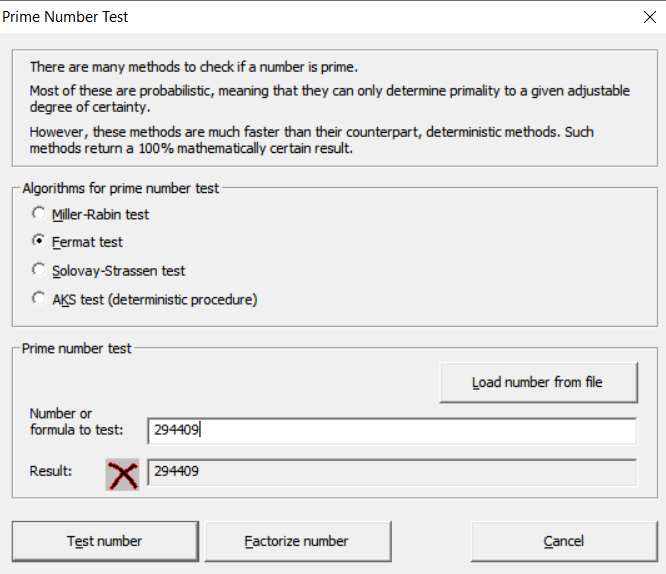


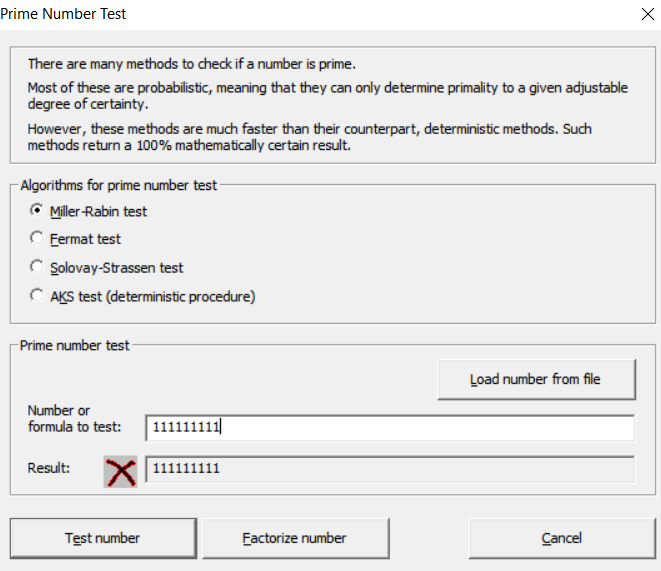


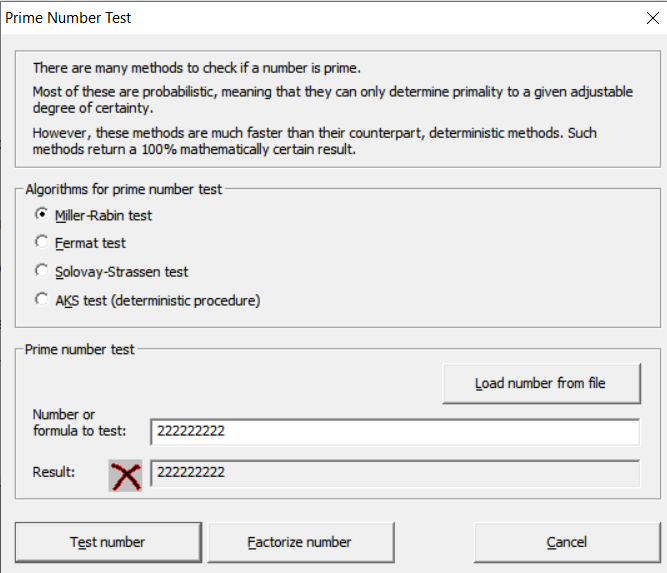


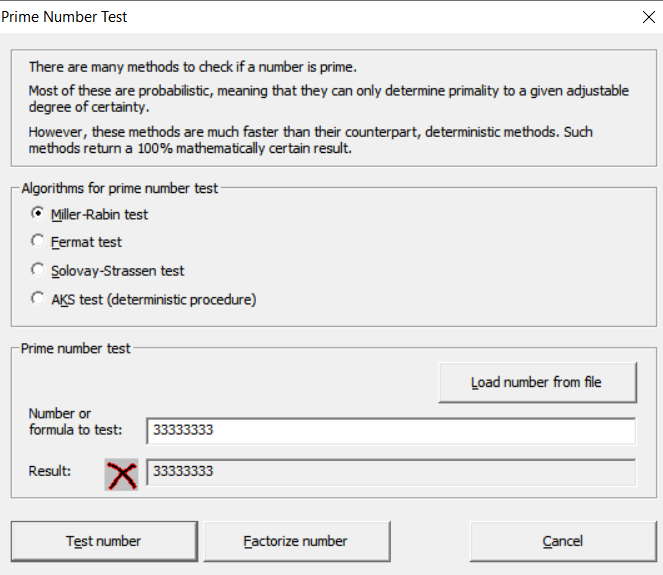




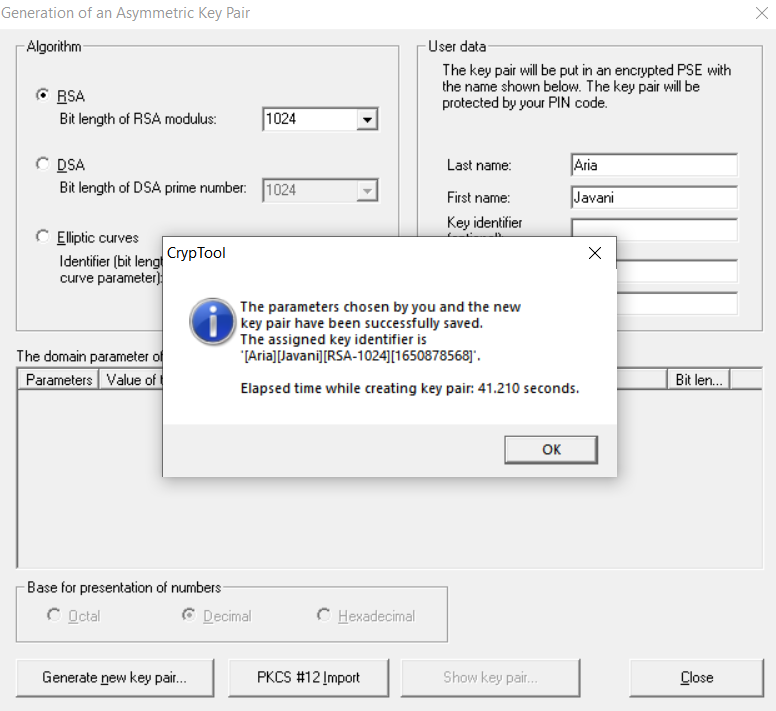




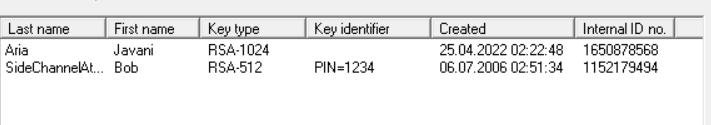


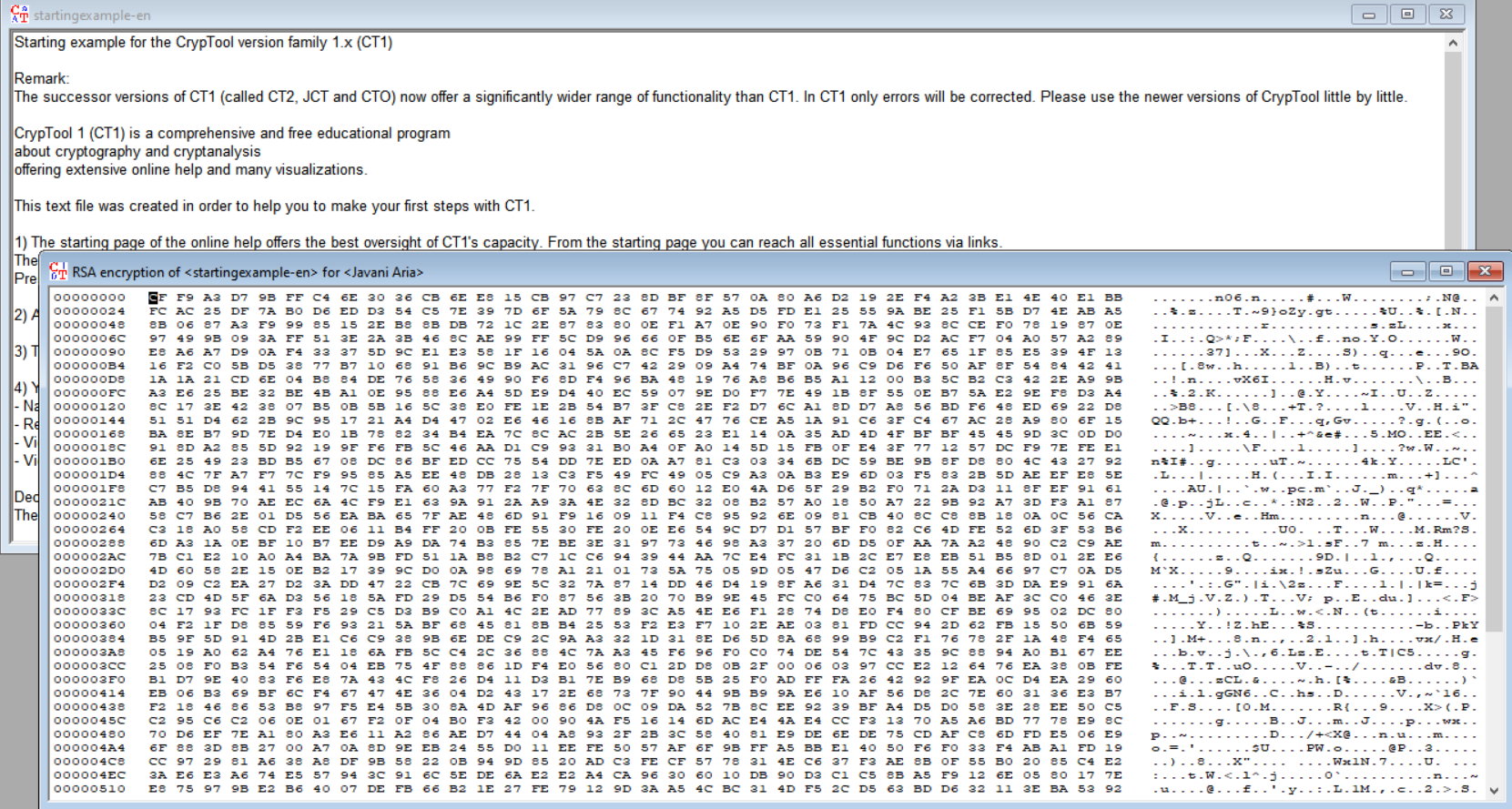


3)

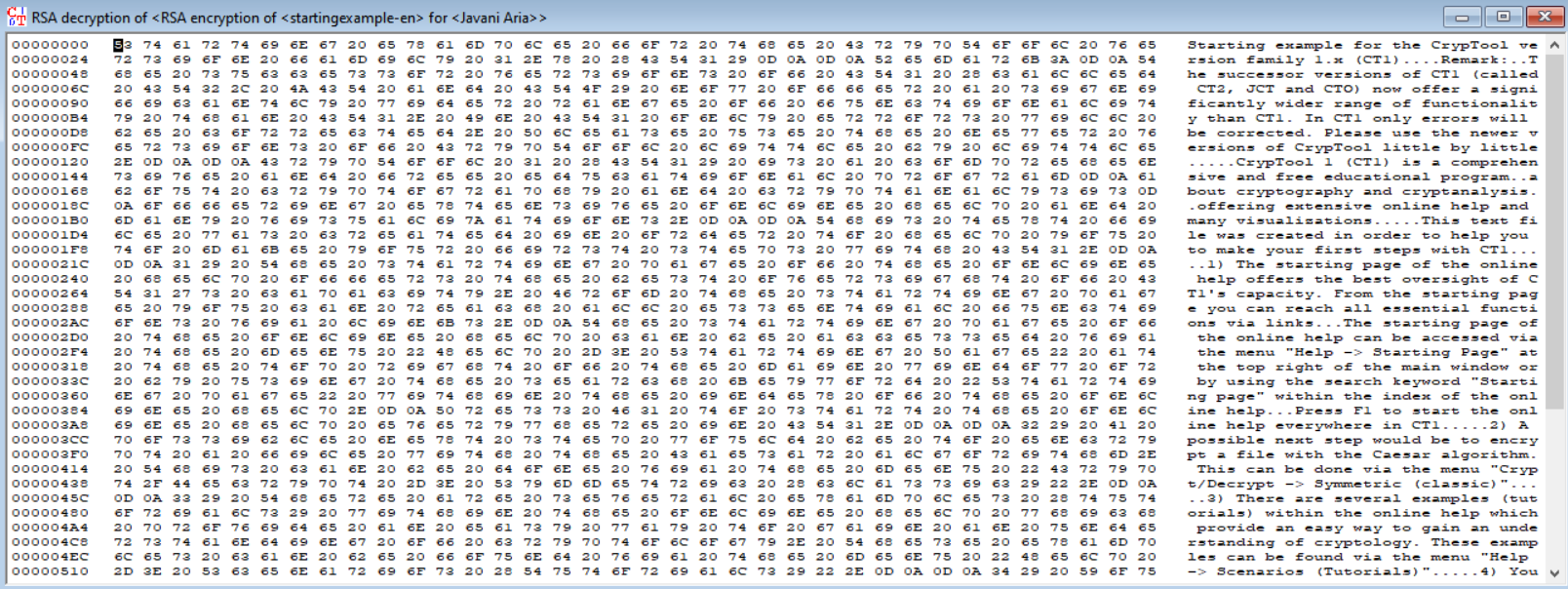


4)





encryption



decryption

5)

