Laboratorul 9

# Exercitiul 1

Se consideră cheia publică RSA cu modulul pe 128 biți: N=234841136411758273000763594354834942653

e=65537

N = p\*q, p si q prime;

N este produsul a doua numere prime.

Prin factorizare pe un calculator online, obtinem:

N = a^2 + b^2

A = 13455261125040573138

B = 7334649580500091147

Cu urmatorii divizori:

1

14086963408384851001

16670813262138239653

234841136411758273000763594354834942653

234841136411758273000763594354834942653 = 14086963408384851001 \* 16670813262138239653

p= 14086963408384851001

q = 16670813262138239653

phi(N) = (p-1)\*(q-1) = 14086963408384851000 \* 16670813262138239652 = 234841136411758272970005817684311852000  
d=e^−1modφ(N)

In calculatorul Wolfram Alpha, cu operatia x^y mod z, am obtinut:

131139372709478882400526464589358085473