Mandatory Assignment 2.
Cryptanalysis of RSA and factoring

The deadline is Tuesday, October 11 midnight. You have to hand in a short description of the algorithms you implemented, the implementation code as a collection of subroutines (functions), and computational results, all as one pdf file.

1. Let N, e be an RSA public key, where $ed \equiv 1 \bmod \phi(N)$ and d is the RSA secret exponent. One knows d is relatively small. The task is to factor $N = pq$ with continued fraction algorithm.

$$N = 109866760255573899735935560954501725544345148319543698135479176534163913565815620624219799211598999682972820305434711729 9$$

$$e = 41588400514977974310313095109794196879333674598330997130143265877576399624767718124304284023210653536725178246623372438 9$$

2. Factor the RSA number $N = 10862216162096506735513546937$ with ρ-method.

3. Factor the RSA number $N = 661643$ with Dixon's method (random squares). Choose smoothness bound $B = 20$. Give details as smooth squares you generated, a system of linear equations you solved and its solutions used for factoring.