Cryptology, homework sheet 6

Due 17 October 2023, 13:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.
For this exercise you can use Sage. Hand in your Sage code along withe answers.

1. This exercise is about factoring with known bits of p. Alice uses RSA key $(n, e) = (768460704081303196456812372744226339750050622442054592713957028534 1, 65537)$ and you know that factors p and q have 112 bits. You also learn that the top part of p, more precisely $p = a + r$ for $r < 2^{36}$ and $a = 385558707669723808370149833467 4944$.

   Use Coppersmith's method to factor n. | 7 points

2. Use theorem by Howgrawe-Graham and the concrete sizes in the previous exercise to explain why the unknown part r is small enough so that this method had to work for factoring n. | 8 points