EINDHOVEN UNIVERSITY OF TECHNOLOGY

Homework #6

Student name: *Chengqi Liu (1954148), Maitraiyi Dandekar (1990136), Zakariae Jabbour (2039702)*

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *October 17th, 2023*

1.

The conditions are:

$$\begin{aligned} n =& pq = 7684607040813031964568123727442263397500506224420545927139570285341 \\ p =& a + r \\ a =& 38555870766972380837014983346749 44 \\ r <& 2^{36} \end{aligned}$$

Let $F(r) = (r + a)$, then r is a solution of $F(r) \equiv 0 \mod p$. Let $X = 2^{36}$. $r < X$. Construct the lattice:

$$B = \begin{bmatrix} n & 0 & 0 & 0 \\ a & X & 0 & 0 \\ 0 & aX & aX^2 & 0 \\ 0 & 0 & aX^2 & aX^3 \end{bmatrix}$$

You can find our codes in "LLL.py".
Run our codes and get the outputs.
(The matrix after LLL reduction is too large so we omit it here. You can run our program to find it.)
The function of r is:

$$\begin{aligned} F(r) =& -96555903568429351669384558377410 + 29495551758403475725598669039206 4r \\ &+ 60298211352416430157901672218624r^2 + 0r^3 \end{aligned}$$

Solve $F(r)$ by Newton's method and check whether $n \equiv 0 \mod a + r$. The outputs are:
r is: 21163420865
The answer is correct.
Then, find $p = a + r$ and $q = n/(a + r)$:
p is: 38555870766972380837015194980958 09

q is: 1993109450765095312123565166297088

2.

(In case of symbol confusion, we use $N = pq$ in this part.)

The Howgrawe-Graham Theorem is: There is some x_0 such that $|x_0| \leq X$ and$F(x_0) \equiv 0$ mod M. $b_F = (a_0, a_1X, ..., a_dX^d)$. If $||b_F|| < \frac{M}{\sqrt{d+1}}$, then $F(x_0) = 0$.

And, by the property of LLL lattice basis reduction, we have

$$||b_F|| \leq 2^{\frac{n-1}{4}} \det(B)^{\frac{1}{n}}$$

So, we can solve r if

$$2^{\frac{n-1}{4}} \det(B)^{\frac{1}{n}} < \frac{M}{\sqrt{d+1}}$$

We can construct the Lattice with $N^h, N^{h-1}F(x), ..., F^h(x), xF^h(x), x^2F^h(x), ..., x^{k-h}F^h(x)$. where $n = k, d = k-1, \det(B) = N^{\frac{(h+1)h}{2}} X^{\frac{(k+1)k}{2}}, M = p^h$.

$$\begin{aligned} 2^{\frac{n-1}{4}} \det(B)^{\frac{1}{n}} &< \frac{M}{\sqrt{d+1}} \\ \Leftrightarrow 2^{\frac{k-1}{4}} (N^{\frac{(h+1)h}{2}} X^{\frac{(k+1)k}{2}})^{\frac{1}{k}} &< \frac{p^h}{\sqrt{k}} \\ \Leftrightarrow X &< (\frac{p^h}{\sqrt{k}} 2^{-\frac{k-1}{4}} N^{-\frac{(h+1)h}{2k}})^{\frac{2}{k+1}} \end{aligned}$$

We can just let $h = 4, k = 8 = 2^3$, then it becomes

$$X < (p^4 2^{-\frac{13}{4}} N^{-\frac{5}{4}})^{\frac{2}{9}}$$

In the previous exercise, we have

$$\begin{aligned} X = 2^{36} &= 68719476736 \\ (p^4 2^{-\frac{13}{4}} N^{-\frac{5}{4}})^{\frac{2}{9}} &\approx 114170204032 \end{aligned}$$

So, $X < (p^4 2^{-\frac{13}{4}} N^{-\frac{5}{4}})^{\frac{2}{9}}$ is correct, which means r is small enough. We can solve r and factor N in polynomial time.

(Note that we didn't use the very complicated Lattice with $h = 4$ $k = 8$, because $||b_F|| \leq 2^{\frac{n-1}{4}} \det(B)^{\frac{1}{n}}$ only gives an extreme worst-case, and the Lattice with $h = 4$ $k = 8$ is very hard to compute. Usually a simpler Lattice can also give a correct result.)