CS 5823/4823 Cryptography Midterm Project

Due March 22, 2017, 11:59pm

This project intends to help you understand the concept of smoothness in cryptoanalysis. A monic polynomial $f(x)$ over a field is b-smooth if all its irreducible factors have degree less than or equal to b. For example, over $\mathbf{F}_2$, $x^{15}+x^3+1$ is 6-smooth since

$$(x^{15}+x^3+1) = (x^3+x+1) * (x^6+x^3+1) * (x^6+x^4+x^2+x+1).$$

An integer is s-smooth if all the prime factors are less than or equal to s. For example, 47711592 is 101-smooth since

$$47711592 = 2^3 * 3^{10} * 101.$$

You are allowed to work in a group of $g \leq 4$ students. Let

$$p = 837583943092107483758343358937591.$$

To complete the project, you or your group should submit an integer A and a sequence of integers $a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_l$ so that

1. $2^{400} \leq A \leq 2^{410}$.
2. The first $9g$ decimal digits of A are concatenation of student ID numbers in the group.
3. It holds that in $\mathbf{F}_p[x]$

$$a_1 a_2 \cdots a_k (x+b_1)(x+b_2)\cdots(x+b_l) \equiv (x^5+2)^A \pmod{x^6+x-44}. \quad (1)$$

Note that both x^5+2 and x^6+x-44 are irreducible in $\mathbf{F}_p[x]$.

You earn half of the credit if all of the above requirements hold. The other half will depend on how smooth the left-hand side of (1) is, namely, you should minimize

$$\max\{|a_i|, |b_j| : 1 \leq i \leq k, 1 \leq j \leq l\}.$$

The smaller the smoothness is, the higher points you will earn.

Note: Sage/Python is slower than C/C++. You may want to use NTL/GMP for efficiency. Sage provides an interface to the NTL C++ library. The computation is done on polynomials with few terms, hence you may find a way to take advantage of the special forms.

For the convenience of grading, please sort the sequence a_i and b_j, and put them into a Sage expression with A, following the format of (1). Please submit your source code and a summary of running time and search space. Only one member in a group needs to submit. Please include the member names in the submission. Every member in the same group receives the same grade. No two groups can have overlapping memberships. Please be warned that if you decide to work in a group rather than work individually, you have a smaller search space.