SageMath for Cryptographers

Jaime Gutierrez, University of Cantabria

Introduction to SageMath

SageMath (previously Sage or SAGE, System for Algebra and Geometry Experimentation) is a mathematical software with features covering many aspects of mathematics, including algebra, number theory, calculus and plotting, combinatorics, algebraic geometry, numerical mathematics, etc. and applications to coding theory, cryptography, etc.

SageMath is an open-source software system based on the Python language programming. SageMath is developed by an international community of hundreds of teachers and researchers, whose aim is to provide an alternative to the commercial products Magma, Maple, Mathematica and Matlab. To reach this goal, SageMath relies on several open-source programs, including GAP, Maxima, R, PARI and various scientific libraries for Python, to which thousands of new functions are added. SageMath is freely available and is supported by all modern operating systems.

In this lecture we shall an introduction to SageMath and to SageMath programming: lists, tuples, dictionaries, sets, iterators, loops, control statements and comparisons, objects and classes in Python and functional programming for mathematicians.

Algebraic techniques for cryptology with SageMath

In this lecture we introduce three SageMath algebraic tools for cryptology and we illustrate those to analyze some cryptographic protocols.

1. Elliptic and Hyperellitic Curves over a finite field. The discrete logarithm problem based on elliptic and hyperelliptic curves has gained a lot of popularity as a cryptographic primitive. One of the reason is that no subexponential algorithm for computing discrete

logarithms on small genus curves is currently available and curve-based cryptosystems require much smaller key sizes than RSA to attain the same security level.

2. Gröbner Basis. *"Breaking a good cipher should require as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type." Claude Shannon (1949): A mathematical theory of communication.* The theory of Gröbner Bases is an important tool for solving polynomial system of equations.

3. Lattices. One important interaction between algorithmic mathematics and cryptology is the so called Lenstra, Lenstra, and Lovász (LLL) lattice basis reduction algorithm, it was a key ingredient to solve a computer algebra problem, namely factoring polynomials over the rational numbers; since then, it was used in numerous attacks in cryptology and to constructions of cryptographic primitives.