Cryptography
CAS 762
An introduction to the mathematical aspects of cryptography
Instructor: Michael Soltys <soltys@mcmaster.ca>
Term 1, September–December 2010
http://www.cas.mcmaster.ca/~soltys/cas762-f10

Syllabus

This course is an introduction to the mathematical aspects of cryptography. We are going to review the classical public key cryptosystems: (i) based on the hardness of the discrete logarithm problem: Diffie-Hellman and ElGamal—as well as their counterparts in the context of the discrete logarithm problem for elliptic curves over finite fields; (ii) based on the hardness of factoring: RSA; (iii) the new cryptosystems based on the hardness of approximating solutions to the discrete lattice problems: the Ajtai-Dwork system, the GGH of Goldreich, Goldwasser & Halevi, and the NTRU system proposed by Hoffstein, Pipher and Silverman. It is the last family of cryptosystems, (iii), that is going to be examined most thoroughly. We shall assume no previous background in cryptography.

A more detailed course outline

The security of most public key cryptosystems is based on either the hardness of factoring large numbers (RSA) or the hardness of finding discrete logarithms in a finite group (ElGamal, in its classical version or in the context of elliptic curves). We refer here to the computational "hardness."

In the mid 1990s a new approach to public key cryptography was proposed, based on linear algebra and discrete lattices. That is, a cryptosystem based on the hardness of SVP (Shortest Vector Problem): given a lattice L, find a vector $w \in L$ with a minimal Euclidean norm, and CVP (Closest Vector Problem): given a lattice L and a vector v, find a vector $w \in L$ which minimizes the Euclidean norm of $v - w$.

There are numerous advantages to the new SVP/CVP-cryptosystems: they are faster than the traditional factorization or discrete logarithm based systems (the difference being roughly a "square" versus a "cube"). Further, they require only simple linear algebra operations, which are easy to implement in hardware & software. Finally, while factoring and discrete logarithm are hard in the "worst-case," SVP & CVP are hard on "average," a great asset from a security point of view. Both "worst-case" and "average-case" are complexity concepts that we shall define precisely in the course.

All these are substantial merits of SVP/CVP-cryptosystems. However, RSA & ElGamal are used in practice because they are well known and trusted; SVP/CVP-cryptosystems (such as the Ajtai-Dwork system, the GGH of Goldreich, Goldwasser & Halevi, and the NTRU system proposed by Hoffstein, Pipher and Silverman) are new, and their security analysis is weak.

One of the goals of this course is to examine the security of SVP/CVP-cryptosystems in depth. It is generally believed that SVP & CVP are computationally very hard problems (at least NP-hard, which can be shown for CVP without assumptions, and for SVP under the mild "randomized reduction hypothesis"), and so SVP/CVP-cryptosystems are built on robust foundations. Further, the speed of encryption & decryption is a strong argument in their favor.

Cryptography is now a mature field and concepts such as "encryption," "public key cryptosystem," "authentication versus strong authentication," "integrity testing," "non-repudiation," etc., are well understood. However, it is very difficult to give formal proofs of correctness (which

in the context of cryptography means "proof of security from given assumptions") unless these well-understood concepts are formally defined and derived, for a given cryptosystem, in a logical theory—we shall mention this briefly in the course.

Textbooks and background

We are going to follow this textbook fairly closely:

- *An introduction to mathematical cryptography*
  by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman,

and the following two textbooks provide some background, but, as far as the first one is concerned, any basic linear algebra textbook would do:

- *Linear Algebra Problem Book*
  by Paul Halmos, and
- *An introduction to the analysis of algorithms*
  by Michael Soltys.

The last textbook has a quick introduction for the required number theory background (Appendix A), as well as sections on the basics of Diffie-Hellman, ElGamal, RSA and the Rabin-Miller algorithm.

As a general rule, all the necessary background will be presented in class.

Grading

There will be no tests and no final exam, but there will be two take home assignments, worth each 20% of the final grade, as well as presentations. The number and length of the presentations will depend on the number of students taking the course for credit; many people find presenting in front of the class stressful—but you need to get the practice, if only to prepare for your master or PhD defense.

Web page

Please check the web page for this course regularly; the URL is given in the title of this document.