Master programme on
"Mathematics and Applications"
Department of Mathematics (UAM)
Academic Year 2010-2011

Cryptography
Tutor: Fernando Chamizo

Scope and Objectives

In this course we present some of the mathematical techniques employed in public-key cryptography. We consider specially elliptic curve cryptography that is one of the most serious competitors to RSA cryptosystem and deeper from the mathematical point of view.
The syllabus follows the lines of former editions of the course. The main topics are based on the chapters 1, 2, 3 and 5 of [**?**]. On the other hand the complementary topics cover some other parts of this monography.
The programming projects are a fundamental part of the course. Taking into account that the course is devoted to mathematical aspects of cryptography, the purpose of these projects will be to understand the theoretical basis rather that to design actual efficient applications. Regarding to programming languages an interesting and simple option is to employ Python through the impressive mathematical package SAGE. Another possibility is C with some arbitrary precision library to manage large numbers. In any case the softare will be open source and freely available.
We assume as a prerequisite for this course a basic proficiency in elementary number theory and group theory. Some results will be recalled in the course. In general any knowledge of discrete mathematics is wellcome. For the programming projects it is assumed a prior experience with computers.

Contents

3. The RSA cryptosystem

3.1 Algorithm, examples and cautions

3.2 Primality tests and factorization algorithms

3.3 Introduction to the number field sieve

4. Elliptic curve cryptography

4.1 Elliptic curves and group law

4.2 Elliptic curves and factorization

4.3 The elliptic version of the discrete logarithm problem

5. Complementary topics

5.1 Digital signatures

5.2 The algorithm DES

5.3 Knapsack cryptosystems

5.4 Lattices and cryptography

Bibliography

1. Ho-Pi-Si Hoffstein, J.; Pipher, J.; Silverman, J.H. An introduction to mathematical cryptography. Undergraduate Texts in Mathematics. Springer, New York, 2008.

2. Stein, W. Elementary number theory: primes, congruences, and secrets. A computational approach. Undergraduate Texts in Mathematics. Springer, New York, 2009.

3. Blake, I. F.; Seroussi, G.; Smart, N.P. Elliptic curves in cryptography. Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000.

4. Koblitz, N. A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994.

5. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. With a foreword by Ronald L. Rivest. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.

6. Buchmann, J. Introduction to cryptography. Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2004.