Cryptography 2011

Instructor: Fernando Chamizo.
Office: Faculty of Sciences M-17 (formerly C-XV) 307.
Email: fernando.chamizo@uam.es. Web: www.uam.es/fernando.chamizo

Contents: We intend to cover the most of the topics in 1-4 and perhaps some of the topics in 5.

1. **Historical introduction.** Motivation and examples. Elementary group theory and number theory. Finite fields. Simple encryption algorithms.
2. **The discrete logarithm problem.** Statement and examples. Basic attacks. Diffie-Hellman key exchange. The ElGamal cryptosystem.
3. **The RSA cryptosystem.** Algorithm, examples and cautions. Primality tests and factorization algorithms. Introduction to the number field sieve.
4. **Elliptic curve cryptography.** Elliptic curves and group law. Elliptic curves and factorization. The elliptic version of the discrete logarithm problem.
5. **Complementary topics.** Digital signatures. The algorithm DES. Knapsack cryptosystems. Lattices and cryptography.

Schedule of the lectures: Tuesday and Thursday from 5:30 pm to 7:00 pm. The classroom is 320 in the Math Department (M17).

Biblography: The main topics are based on the chapters 1, 2, 3 and 5 of

[1] Hoffstein, J.; Pipher, J.; Silverman, J.H. An introduction to mathematical cryptography. Undergraduate Texts in Mathematics. Springer, New York, 2008.

The complementary topics cover some other parts of this monography. Other recommended texts are

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

Grading:

1. Final exam or final project: 40%.
2. Exercises and homework assignments: 40%.
3. Quizzes, in-class exercises, participation : 20%.