**Tutor :**

Nuno Ricardo Barroso de Freitas

https://www.icmat.es/miembros/nfreitas/

**Method :**

Online meetings.

**Language :**

English, Spanish or Portuguese

**Project Title :**

# Public key cryptography with elliptic curves

**Summary :**

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir, and Adleman in 1978 are watershed events in the long history of secret communications. It is hard to overestimate the importance of public key cryptosystems in the modern world of computers and the Internet. Over last three or four decades, elliptic curves have been playing an increasingly important role in applications. For example, in the 1980s, elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization and primality testing. A reason for using elliptic curves in cryptographic situations is that they provide security equivalent to classical systems while using fewer bits. For example, it is estimated that a key size of 4096 bits for RSA gives the same level of security as 313 bits in an elliptic curve system.

In this project the student will explore the basic theory of elliptic curves with a view towards public key cryptography.