Possible M.Sc./M.Sci. projects

R. A. Wilson

2007–8

Most of these projects can be adjusted to be suitable either as a (shorter) M.Sci. project or a (longer) M.Sc. project.

Projects in cryptography

The Data Encryption Standard

The DES is a standard method for encryption of digital data using a symmetric key. You will find out in detail how it works, and explain this in your own words. Evaluate its effectiveness, for example by analysing the difficulty of various attacks. Discuss possible improvements, etc.

Prerequisite: MAS335 Cryptography

Elliptic curve cryptography

An elliptic curve is a cubic curve of the form $y^2 = ax^3 + bx^2 + cx + d$. It can be made into an abelian group in such a way that three points sum to zero if and only if they lie on a straight line. (The associative law is quite tricky to prove!) It is possible to design a public-key cryptosystem analogous to RSA, using elliptic curves over finite fields in place of modular arithmetic. Find out about this and explain it in your own words.

Prerequisites: MAS335 Cryptography, MAS201 Algebraic structures I

Projects in group theory

Classical groups

The general linear group $GL(n, F)$ consists of all invertible $n \times n$ matrices over the field F. It has a normal subgroup $SL(n, F)$ consisting of the matrices of determinant 1. Also $SL(n, F)$ has a normal subgroup consisting of scalar matrices. The quotient by this normal subgroup is $PSL(n, F)$, which is (usually) a simple group. Find out about this, and explain in your own words. The other classical groups are subgroups defined by the property that they fix certain ‘forms’ (like inner products): see how far you can get with proving analogous properties of these groups.

Prerequisites: MAS305 Algebraic structures II