AN INTRODUCTION TO ELLIPTIC CURVES

Elliptic curves, aside from being interesting in and of themselves, are worth studying because they have applications ranging from cryptography to string theory. In the talk we will explore various properties of elliptic curves, and the group structure we can define on them. We will also see how we can exploit the difficulty of finding an integer \( n \), given points \( P \) and \( Q \), which satisfies \( nP=Q \) on an elliptic curve (this is known as the elliptic curve discrete logarithm problem) to implement a cryptosystem.