《密码分析》

### 一．中英文简介

本课程讲解破解各类密码系统的（数学）原理和方法。学生需要有现代密码学和初等数论的背景。本课程涵盖证明安全理论导引、生日攻击原理、哈希与随机函数碰撞发现、分组密码的差分攻击、积分攻击与线性攻击、流密码的代数攻击、大整数分解方法、离散对数求解方法、格基规约分析方法、Grobner基攻击方法等。帮助学生了解密码学各分支的研究内容及密码学的新发展，方向以及培养学生在实践中解决问题的能力。

英文简介：

This course teaches the (mathematics) principles and methods of cracking various cryptographic systems. Students need to have a background in modern cryptography and elementary number theory. This course covers the introduction of proof security theory, birthday attack principle, hash and random function collision discovery, differential attack of block cipher, integral attack and linear attack, algebraic attack of stream cipher, large integer factorization method, discrete logarithm solving method, lattice based reduction method, Grobner basis method, etc. This course help students understand the research content of each branch of cryptography and the new development and direction of cryptography, and cultivate students' ability to solve problems in practice.