2013 年陕西科技大学硕士研究生理学院招生专业课考试大纲

（2012 年 9 月修订）

《944 密码学》

考试要求：要求考生系统地掌握密码学的基本概念与应用原理，并能灵活运用，具有较强的分析问题与解决问题的能力。要求考生对国内外密码学的新进展和重大事件有所了解。

考试内容：

1．现代密码学的基本问题
2．古典密码学
3．密码学的信息论基础
4．密码学的计算复杂性理论基础
5．单向函数
6．伪随机序列生成器
7．序列密码
8．分组密码
9．公钥密码
10．数字签名
11．杂凑函数
12．身份识别方案
13．密钥管理
14．零知识证明
15．密码学的新进展