**华北电力大学2024年博士生入学考试初试科目考试大纲**

科目名称：密码学与网络安全

**一、 考试总体要求**

《密码学与网络安全》包括密码编码学与网络安全的基本原理与应用技术, 是信息安全学科的基础。掌握密码编码学的基本原理、算法模型和应用技术；能够用对称密码、公钥密码体制解决信息系统数据的保密性、完整性、真实性等数据层的安全问题；能够用密码算法解决无线网络安全、电子邮件安全、IP安全以及Web安全等网络协议层的安全问题。

**二、 考试内容**

1. 古典密码学：包括代换密码、仿射密码、维吉尼亚密码、Hill密码、置换密码等。

2. 密码学的数学基础：有限域等近世代数基础；费马和欧拉定理、中国剩余定理和离散对数等数论基础。

3. 对称密码学：传统加密技术和原理；分组密码与数据加密标准(DES)；高级加密标准AES；多重加密与三重DES算法；分组密码的工作模式；流密码和RC4算法。

4. 公钥密码学：公钥密码体制的基本原理；RSA算法；椭圆曲线算术与椭圆曲线密码学；消息认证和Hash函数；安全散列算法；数字签名和认证协议。

5. 密钥分配和管理体制：随机数的产生与密钥分配；密钥管理和分发。

6. 网络安全与安全协议：Kerberos与X.509认证服务；PKI公开密钥基础设施；电子邮件的安全协议(PGP、S/MIME)；IP安全体系结构；Web安全(安全套接层和传输层的安全)；云安全；无线网络安全；安全电子交易。

**三、 考试题型**

简答题、画图设计题、计算题、综合分析题。

**四、 参考书目**

1．William Stallings（美），王后珍等译，《密码编码学与网络安全—原理与实践（第七版）》，电子工业出版社， 2018.