密码论心得

朱志儒 16337341

很荣幸听张方国教授的密码学简介讲座，他介绍了密码学的由来，研究密码学的原因，密码学的历史和现代密码学的研究及应用。听了他的讲座，我受益匪浅，让我对密码学有了很大的兴趣。

他介绍道：密码学的英文是 Cryptography，是由希腊语 kryptós“隐藏的”，和 gráphein“书写”派生而来的，是研究如何隐密地传递信息的学科！也就是说，密码学是第三方存在下的安全通信技术的研究与实践。他还例举了电视剧《潜伏》和电影《风语者》中运用到的密码学。他向我们解释密码学的基本概念，明文通过加密密钥进行加密形成密文，再传输，接着通过解密算法用解密密钥解密还原成明文。密码体制分为：单钥、私钥、对称密码体制；双钥、公钥、非对称密码体制。

他说研究密码学的原因是：保密，自古以来就被非常重视：“事成于密，而败于泄”，“知己知彼，百战不殆”；密码在古代就被用于传递秘密消息；在近代和现代战争中，传递情报和指挥战争均离不开密码，外交斗争中也离不开密码；并且密码已经从军事走向日常生活：电子邮件、接入控制、电子银行、软件保护、版权保护等等。信息化社会中，Internet 一方面成为人们离不开的信息工具，同时它也成为公开的攻击对象目标和便利的工具。信息社会环境下的安全威胁有：信息泄露、破坏信息的完整性、拒绝服务、非法使用(非授权访问)、窃听、业务流分析、假冒、旁路控制、木马、抵赖、重放等等。信息安全的基本要求有：信息的保密性（保证信息不泄漏给未经授权的人）、信息的完整性（防止信息被未经授权的篡改或破坏）、认证性（对某一实体所声称的身份提供证实的行动）。

张方国教授详细地向我们讲述了密码学的研究历史，1976 年前的古典（传统）密码：远古密码，手工密码，机械密码，电子机械密码。至少 4000 多年前古埃及人在金字塔中加密象形文字就是典型的远古密码；公元前 500 年的古希腊人发明的 Scytale 密码就是手工密码；1790 年代的杰弗逊圆盘和 1860 年代 Wheatstone disc 均是机械密码；电子机械密码又称转轮密码，用一组转轮或接线编码轮所组成的机器，用以实现长周期的多表代换密码，最有名的代表有 Enigma 和 Purple（紫密）。公钥密码学的提出和美国数据加密标准 DES 的颁布使密码学成为了一门科学，研究从军事和外交走向了公开，也形成了现代密码学。

教授讲到现代密码学研究有：可证明安全、全同态加密、Hash 函数的设计与分析、格密码、多线性映射密码、后量子密码体制（量子密码学）、区块链及其应用、侧信道攻击（抗密钥泄露的密码体制）、轻量级密码的设计、密码软硬件的实现。

然后张教授向我们介绍了区块链与比特币，区块链是比特币的底层技术，但先比特币，后区块链。然后他讲解了哈希链和哈希函数。哈希函数是将任意长度的消息映射成一个较短的定长输出消息的函数。它的安全性有：单向性或原像稳固；抗第二原像或弱抗攻击性；抗碰撞或强抗攻击性。

最后张教授简单的说了密码的新应用：任何一个新兴的网络，或一个新兴的社会需求，只要需要安全性或隐私性，密码工具就能用上去，从而成为密码学应用研究领域的一个研究热点。