假期准备学习工作总结——第二周

本周的主要学习内容是对于《经典密码学与现代密码学》和《密码编码学与网络安全》这两本书的阅读。

这是第一次接触到密码学的相关内容，通过一周的学习了解到了密码学的历史和现代发展。主要的学习内容是密码学概论和**经典加密法**中的单码加密法和多码加密法。结合了之前学习的内容，在学习对称加密（传统加密）的过程中比较顺利，根据书籍中所提到的经典加密方法发现，经典的加密法基本上是不要求计算机来实现，很多经典加密法都在CAP软件中实现了，但是考虑到刚刚入门密码学，所以还是先打好基础，毕竟一些经典加密法的本质和特点还有待研究。学习这些经典加密法的过程比较有趣，比如学习**关键词加密法**的时候，就对密码学的学科交互性有了深刻理解，做好密码分析的工作不单要有强大的逻辑思维，还要具备一定的生活工作常识，像英文字母频率这种看似无关紧要的数据，对于解密有时候会有相当大的帮助。此外还学习到了**Hill密码**、**Vigenere密码**和**Vernam密码**。Hill密码就结合了**线性代数**中的知识，即将m个连续的明文字母替换成m个密文字母，并且由m个线性方程决定。Hill密码就完全隐蔽了之前关键词加密法中提到的单字母频率特性。

$$\boldsymbol{C} = \mathrm{E}(\boldsymbol{K}, \boldsymbol{P}) = \boldsymbol{PK} \bmod 26$$
$$\boldsymbol{P} = \mathrm{D}(\boldsymbol{K}, \boldsymbol{C}) = \boldsymbol{CK}^{-1} \bmod 26 = \boldsymbol{PKK}^{-1} = \boldsymbol{P}$$

图1.1 Hill密码系统线性代数表示

多表代替密码中的基础则是Vigenere密码，其代替规则集是由26个**Caesar密码**的代替表组成。这种操作跟Alberti的加密转盘差别不是很大，就是用密钥字母确定表的行，明文字母确定表的列，表中行列交叉处的字母就是用来替换明文字母的密文字母，在学习时发现，在进行密码分析时，数学统计相关知识对于密码分析也相当有帮助。比如IC（一致性索引）基于凹凸度量理念，根据IC值我们便可大致判断使用到的加密法类型。

密钥长度	IC值	密钥长度	IC值
1	0.0660	7	0.0420
2	0.0520	8	0.0415
3	0.0473	9	0.0411
4	0.0450	10	0.0408
5	0.0436	11	0.0405
6	0.0427	12	0.0403

图1.2密钥长度与IC值

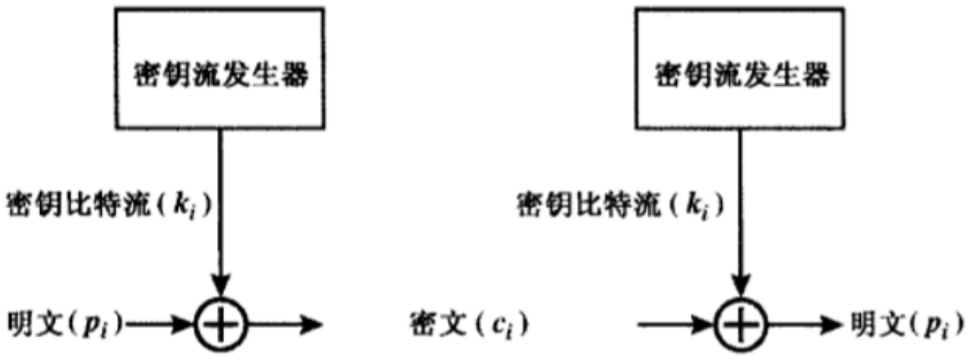

图1.3 Vernam密码

传统加密技术还包含了**置换技术**、**转轮机**、**隐写术**等，这些传统的技术虽然已经跟不上时代的步伐了，但其中所蕴含的思想是十分宝贵的。这一周的学习更像是一次科普，了解到的大多技术跟区块链技术中使用的hash、数字签名相差甚远，不过也是为了接下来更深入的研究做好准备，或多或少会有帮助。在学习密码学的同时也延续了区块链的学习，通过看网课，了解了Block Chain使用到的Merkle Tree这种数据结构的核心优势，对于区块链技术中的collision resistance、hiding、puzzle friendly这三个性质有了进一步的认识。