假期准备学习工作总结——第三周

本周的主要学习内容是延续上周的**经典密码**部分的学习，同时也进行了**区块链理论**的学习。

针对王老师提出的学习方向，对于**古典密码的安全强度**进行了进一步的学习。经学习得知，对加密信息的攻击类型包含了以下几种：**1.唯密文攻击 2.已知明文攻击 3.选择明文攻击 4.选择密文攻击 5.选择文本攻击。**其中的唯密文攻击是相比之下最容易防范的，因为攻击者拥有的信息量最少，当分析者捕捉到的明文信息更多，且具有相对应的密文时，攻击类型也就变成了已知明文攻击，如果分析者能够获得信源系统，并在发送方发出的消息中插入自己所选的信息，那么选择明文攻击就有可能实现。

如王老师指出的Caesar密码的密钥空间大小仅为26，是远不够安全的，如果密文行可以是26个字母的任意代替，那么就有26！种可能的密钥，显然密钥空间比DES的密钥空间大了10个数量级，但并不是足够安全的（王老师也提到了这点，“**密钥空间足够大是密码应用的必要条件但不是充分条件**”），前面学习总结中有提到，如果密码分析者知道明文的属性，就可以利用语言的规律，即字母使用的相对频率。为减少代替密码里明文结构在密文中的残留度，多表代替密码是可行方法之一。前面所学习到的Hill密码完全隐蔽了单字母频率特性，另外一个3*3的Hill密码不仅隐藏了单字母频率特性，还隐藏了双字母的频率特性。对于**Hill密码的安全强度**，根据书中提到的**矩阵运算**的例子可以得知尽管Hill足以抵抗唯密文攻击，但它较易被已知明文攻击破解。Vigenere密码强度在于每个明文字母对应着多个密文字母，且每个密文字母使用唯一的密钥字母，相较于Hill密码而言，字母频率信息同样被隐蔽了，但并非所有的明文结构信息都被隐蔽了。

区块链理论的学习主要是基于bilibili上的《区块链技术与应用》公开课，结合着吕老师之前提供的资料，目前已经学习到了BTC的共识协议。其中学习到的一些知识点如下：**1**.数字货币和纸质货币区别是可以复制，叫作双花攻击 即double spending attack。**2**.比特币的产生基于mining（挖矿），mining就是不断地去试一个nonce，如果找到了一个H（block header）<=target则获得了记账权，且获得一定数量的BTC，目前一个区块奖励为12.5个BTC **3**.BTC交易时需要验证身份，比如A向B转账，A需要知道B的地址，B的地址是通过公钥求Hash得到的，此外B也需要知道A的公钥，因为要清楚转账人的身份，验证过程则是通过BitCoin Script（比特币脚本）来实现，验证交易的合法性，就需要把当前交易的输入脚本跟前面交易(提供币来源的交易)的输出脚本拼在一起，然后看看能不能顺利执行，如果能执行说明是合法的。**4**.如果把区块链比作一个帐本，在向账本内写入内容时，要取得distributed consensus（分布式共识），分布式共识的一个例子就是distributed hash table（哈希表）， 共识的内容则是哈希表中包含了哪些key value pair（键值对）。假如有人在自己电脑上插入一个键值对，那么别人在另一台读的时候也要能把这个读出来，这就叫一个全局的哈希表。此外还有一些分布式理论如FLP impossibility result 和 CAP Theorem。**5.** BTC系统要解决的一个问题是，系统中存在恶意节点，那么要如何取得共识？其解决方案是按照算力来决定membership，这种方式可以有效解决sybil attack（女巫攻击）。**6.** 区块链在正常情况下也可能出现几乎同时出现两个新区快的状况，这时就会出现两个等长的分叉，且都满足 longest valid chain（最长合法链）这一规则，此时要接受的链为在缺省情况下最早接收到的区块。**7.** 区块间存在竞争，当一个区块胜出后（成为了主链的一部分），另一个区块及之后的链都会作废。