BJUT 密码学学期总结

Curious;

2020 年 1 月 25 日

密码学在刚刚入学时往往会被认为是难度较大的一科，但考试感觉来说可以说是大三上学期最简单的科目之一，在考试剩 40 分钟以上时我就基本完成了作答，而操作系统、数据库等基本都是卡线写完甚至时间不够，所以至少相对于这两科来说，密码学难度不高。

密码学也是分理论和实验两个部分，接下来将分为这两个部分再加上对期末的总结和部分题目的概述详细的进行说明。此外还要说明因为信息安全技术日新月异，题目和学习的东西都会随不同时间而变化，预计在未来几年对于密码学新方向，例如量子密码等会有更多的介绍。

目录

1 密码学理论学习

密码学在最开始讲解的是古典密码，单表代换，多表代换，还有密码分析等，这些跟着听基本都能搞定，都是一些简单的套路操作。像凯撒密码一些估计大家在以前多少都听说过，但其实有些很有意思的古典加密算法在课上也会为大家讲解，例如福尔摩斯”跳舞的小人“案，把密码字符条缠绕在棍子上书写之后再取下……

真正的难点从对称密码体制开始，这块来说因为都是老师讲，没办法自己模拟一个完整的加密解密过程，所以会比较混乱。这块我的建议是先跟着能听懂多少就听懂多少，有时间自己稍微模拟模拟试试，但要注意建议一个完整的过程讲完后，例如完整的讲完 DES 算法后，再自己稍微的进行一个尝试，明白每个步骤都在干什么。这里最关键的是 DES 算法，其他基本做一个简单的了解即可。

之后的公钥密码，数字签名可以看做基本上就是一些数学概念的理解，在这里开始阶段恐怕不好理解这句话的意思:” 公钥密码加密流程是用公钥加密，解密流程是用私钥解密；数字签名是利用公钥密码体制，使用私钥进行签名，再使用公钥进行验证。“如果能理解了这句话，基本说明对这一部分有了初步的理解。如果说对称密码体制是建立在 SP 网络的混乱和扩散，来增加解密时的计算量，公钥密码体制主要是建立在复杂的数学问题基础上。RSA，离散对数 ElGamal，椭圆曲线 ECC。公钥密码的学习主要就是数学的学习方式，刷题，然后理解数学思想，加密解密。

公钥密码数字签名之后比较重要的内容是密码协议，其中有一些”新奇“的密码学思路。当时在学习完这一部分后，感觉密码学真的是一门十分高深而且有意思的科目，值得深入研究，公平掷币协议、比特承诺等，还有零知识证明，这些方法都很巧妙的利用到了数学思想。

2 密码学实验

实验就是让用图形化界面实现几个加解密算法，我们这年是单表代换，凯撒，RSA, DES。

这个实验其实本来不是很难，难就难在这个实验安排在的周数正好是事情最多，好几个事情聚在一起的时候。老师比较倾向使用 C/C++ 进行实现，其他语言跟老师提前打个招呼，应该也是可以。这个因为数据结构课设用了图形化界面，所以只需要弄好算法，稍微包装一下。

单表代换和凯撒的难度是可以预见的比较简单；RSA 要支持大位数也就是高精度，网上应该能够找到一些工具。（在这里我不得不吐槽一句数据结构课设，这个等说到数据结构课设时候再详细说了）；DES 的实现也是可以预见的难，我自己实现过程中一个比较印象深刻的是可以把替换的操作弄成一个函数，其他的函数中调用这个函数一层一层模块化会好很多。如果能趁此机会把 DES 的过程完全弄明白，基本也帮助了课内的学习。

3 密码学期末

密码学期末找不到之前的试卷，好像唯一能找到的一套和现在的密码学考试方向已经变化很多了。密码学课程在 2015 年后修改了教学大纲，这一篇也是针对 2015 年教学大纲来说的，猜测在不远的几年内一定会再次修改。

期末前如果课时没有受到什么挤压的话，老师会带着大家进行一次串讲，这次老师会明确哪些地方比较关键，哪些地方相对要求没那么高，这次课一定要加倍集中注意力，如果最后因为其他课程占据了太多复习时间（因为在我们这年密码学是最后一门科目，前边的课程大多难度非常高会占据很长的复习时间。）最后考试前争取把老师课上说的重点弄一下。需要注意的是 PPT 中每一个用方框什么的画的流程图，示意图一定要弄明白，并且记住这个图是怎么画的，考试中会有类似的题目。

前边的填空选择题基本是送分，在复习结束后再看一看书上后边的选择填空，选择题和书上的选择题非常像，填空题也有部分和书上相似，但是只看书上的肯定不够，还是对着 PPT 复习，记住出现的每个【数字】，例如 DES 的加密是多少轮啊这些的。

简答题也还好，记忆中写字的不是很多，因为密码学中基本的概念还不是很抽象，不像操作系统和数据库动不动就是野指针满天飞。主要还是流程图一定要重视，流程图真的是随便出一个就能考。

剩下的一些计算大题基本就是作业那几个，密码学本身也不留几次作业，每个题也都比较套路，弄懂了就好。

说几个让我印象比较深的题或者复习中的点（不分先后了，想到什么就说什么了）：

1) 密码协议一章中（具体这个问题的名字有些忘记了）：机构要统计一家公司中的工资平均数，但是每个人又不想让别人包括这家机构知道自己的工资具体值。这个算法要求画流程图，并说明解释这个流程。

2) ECC 算法作业中基本是算加法，但是一定要注意 ECC 的减法，

$$(x_1, y_1) - (x_2, y_2) = (x_1, y_1) + (x_2, -y_2) \tag{3.1}$$

这个我自己在考试前几周的时候是推过一次，主要还是利用椭圆曲线的性质，但如果临近考试的话就没必要了，考试也不会考这个怎么推，明白怎么把减法转化成加法，然后套用那几个老师课上给的公式就可以了。

3) 最后大题中有一个 2 分题问 RSA 算法应用在数字签名技术中中安全性有关的问题，问 RSA 为什么要在数字签名之前进行一次 hash，然后签名签名在这个 hash 生成的值 $h(m)$ 上。好像问的是如果不这么操作会引起什么安全问题，就

是比如直接利用消息进行签名会怎么样。这个题我现在也不是很确定，可以聚在一起讨论一下或者直接问问老师。

4) 考到了有一个周期最长的序列那个题，给你一个初始序列，让你写几轮然后最后问是否达到了 m 序列。

5) 考到了 DES 算法中 SP 网络中混乱（代换）操作，给你一个 6 位的二进制数字，然后问你换完了是多少，就是 S 盒对着查表转化那个。印象中这个题就是这么一个普通的转换分值设置了 8 分，估计如果到时候还是类似的题要把步骤写的稍微清楚一点吧。

6) 考到了比特承诺的思想和整个流程的描述。

4 备注部分

密码学在我们这一届的考试中是最后一科，而且本年来说难度不大，如果能保持对之前其他科目的的复习认真度，相信看到密码学试卷后不会感到很大压力，应该可以比较顺利的完成。

书写文档的过程也是我对 LaTex 学习的过程，希望看到此篇的人能够加上自己对所写这一门课程的看法，继续完善此总结。