953 密码学复习指导

写在前面的话：953 是今年改考的，加了死亡密码学，难度也说不准，只能按照越全面越好的准则去复习。对于数据结构，目标得分在 50 分，对于计网，目标得分在 52 分（不要觉得计网得分要求太高了，实际上等你们真的做真题了，会发现 952 真的很简单）。对于密码学，只要前两门复习的好，稍微舍弃一部分知识点，应试能拿 25 分就很棒了。

改考是机遇也是风险，但是合理评估自己公共课水平，专业课是很难拉开分的！

复习规划：

第一轮复习：7-8 月底。每天两小时

可以跟着王道视频，把计算机网络与数据结构第一遍结束，并把王道的选择题全部做一遍。每天 2 小时，三天一个循环，比如第一天数据结构，第二天计算机网络，第三天做王道，

计网：应该看一遍黑书，对于整个知识框架应该有个简单的了解了，比如至少能说出来寻址的过程，差错控制、访问控制、流量控制、拥塞控制等内容。

数据结构：应将王道选择题与荣政教材课后题做完，对于缩小规模算法应该已能记住。

第二轮复习：9 月中至 10 月底。每天 2-3 小时

计网部分：应再看一遍黑书，重新做一遍王道选择题，并将大题做一遍。此阶段应已清晰计网的考点，能够自己梳理一遍知识点。**如果时间充裕可以选择做一遍期末题，但是如果时间紧张，不需要做计网期末题！以王道题为主多做训练！**

数据结构部分：

1) 先利用王道复习每一章的知识点，并且将第一轮选择题练习的错题重新做一遍；
2) 对于王道的经典算法代码，应该要记住关键步骤，且能尽量做到默写，比如：

合并有序链表等；

3) 荣政书上的例题应该再看一遍，能够完成树、图、排序、查找的手动模拟题，掌握缩小规模算法。

4) 完成资料中的期末题

密码学：密码学的前置课程为**网安数学基础**。重点需要掌握：

1、同余；2、扩展欧几里得算法，求逆元；3、模重复平方法，减少计算量；4、孙子定理，求解同余方程组；5、二次剩余。掌握了以上五点，应该可以较好的做出计算题。针对群环域部分，仅需了解概念，包括生成元，以及每个代数系统是由何种运算组成。

数论我将老师的 PPT，截出重点部分，打印在本资料后面。以及之前期末考试复习的一些重点，也附在资料后面，在学习的时候，可以参考那些重点进行针对性学习。能记住结论，在学习密码学能反应出来用了这些知识就好。**这些内容可以用一周半时间，与计网和数据结构并行学习**

密码学：

密码学学习最劝退的应该是第二章的内容，这一块概念较多，公式较多，偏硬件，很容易一看 ppt 就会放弃，**但是请坚持住第二章，实在觉得不会，就放弃这一章内容！如果放弃第二章，则需要加倍努力学习三四五六章，对于每一道计算题都不能出错。**在资料里面有一份去年复习的重点笔记，第二章的内容当时任课老师讲的也比较少（但是考试考了）。

第一章是文字题；

第二章流密码需要掌握线性反馈移位寄存器是如何运作的，可能会出那种看图写生成式的题；包括后面的 m 序列破译，也应该掌握；

第三章是分组密码，我个人觉得只需要掌握 DES 和 AES，DES 每个部分都应该会，AES 可以只掌握各个部件的组成；

第四章是公钥密码，这一章主要会出计算题，需要掌握 RSA、背包、rabin、Elgamal 与椭圆曲线五种加密算法，并且能够自己默写出来。其中背包和 RSA 可以出计算题；

第五章是签名，签名需要掌握几种不同的签名方法。指的是能够默写出如何签名，以及如何验证签名；

第六章则是几种应用，对于秘密共享应该重点掌握，此处可以出计算题（通过数论的孙子定理）；
第七章稍微看一下就行了，主要考文字题；

在学习完数论的基础上，此时可以开始密码学的正式学习，同样与计网和数据结构并行开始。可以每两天一章，做完一章之后可以重点将课后题完成。此过程应在十月中旬之前完成。在该阶段，可以不要求能够背诵各个加密算法的加解密过程，只需要看到之后能反应出其加密名称即可。

然后剩下半个月，开始练习本资料后面的题目。实在不会做的直接跳吧

第三轮复习：11 月初到考前。

数据结构的缩小规模算法一定要认真学习，仅仅记住特征与应用场合是不够的的。

951 和 952 总共 10 套真题。每天任选一套，其中数据结构计算量偏大，可能需要花三小时才能做完并订正一套；但 952 比较简单，正常来说 80 分钟能做完一套，加上订正的时间，也不到两小时。可考虑一天做两套 952 的题目。直到考前，**951 和 952 的真题应该至少做三遍**（其实第三遍开始就是看一眼就能得出答案了）。**王道也应该重头到位再做一遍**。至此，王道的每一道题应该可以做到看题马上反应答案了。

密码学没有真题，我们会努力回想去年我们密码学考试的题目。此阶段密码学的复习主要以背诵加密算法，签名与验签算法，以及流密码里面的各种公式为主，务必做到倒背如流。**可以通过本资料后面的空白默写版进行一个自我检测。**