专业课试题

0x01 前言

《密码学与网络空间安全基础》《数据结构与 c 语言程序设计》两门课二选一，毫无疑问肯定密码学喽，既是根据成绩，也是根据爱好。

《密码学与网络空间安全基础》涉及范围广，包括我大二大三的先修课程，如：密码学（92），信息论与编码（91），无线网络安全（91），网络安全基础（81），操作系统安全（85），计算机网络（84），差不多就这些，融合起来的一门课。平时自己也瞎折腾，对这方面的了解相比于数据结构还是比较多的。

《数据结构与 c 语言程序设计》，刚发下卷子大概浏览了一下，果真和我考前预测的一模一样。我在考前就跟舍友说，这门考试如果没有密码学方向的题目，那我会觉得这些老师很失败。结果如我所料，考纲没有写需要掌握密码学知识，但是出了两道简单的密码学编程题。跨考的，非信安的，呃呃呃，估计自求多福了吧。

啰嗦这么多，就到这儿吧，我主要做了《密码学与网络空间安全基础》，下面分享我的考试题目（PS：考完晚上和同学出去吃饭，不可避免地吸收了一点 C2H5OH，忘了一点东西，我想起来再补充）

0x02

最重要的写在前面，认真跟着考纲复习，基础打牢，永远是最重要的，不要试图投机取巧，我专业课，书从头看到尾，从尾看到头，自我感觉看了 7 遍+

题目全部源于考纲，没有一题是超纲的。十一道大题？记不清了，反正自开考后，手就没停，一刻也没停，题量相当大，差点没做完。

一、填空题（40 分）

总共四十个空，涉及到的能记得题目，我写题目，忘了题目的，写知识点。

1.信息安全最基本的三个目标（3 分）

2.渗入威胁的三种方式（3 分）

3.安全攻击的两种类型（2 分）

4.OSI 七层参考模型，按底层到高层，写出来（7 分）

5.TCP/IP 四层参考，按底层到高层，写出来（4 分）

6.密码学常用的两种加密方式（这是考置换，代换 2 分）

7.IPv4 多少位？IPv6 多少位（2 分）

8.HTTP,SMTP,DNS,POP3 端口号（好像是四个 4 分，记不清了）

9.AES 多少分组长度多少位？密钥长度多少位？MD5 输出多少位？SHA-1 多少位？（4 分）

10.四种网络加密方式分别是？（4 分）

11.ARP 把啥地址转成啥地址？（2 分）

总共 37 分，应该都是比较确定的考题。想不起来了 23333333

二、判断题（10 分）

这个题目有错有对，我只说我理解的知识点，也就是正确的该是啥。

1.柯克霍夫原则，就是密码系统的保密性，应该取决于密钥的保密性，而不是加密或解密算法的保密性。也就是说，算法细节是可以公开的。

2.加密轮数越多越安全？肯定不是，单钥密码算法，如 des，aes 哪个超过 20 轮了，双钥密码算法加密轮数增加，还存在迭代攻击，因为密钥处于一个域中，存在循环问题。

3.多个密码算法串联加密，一定更安全？考虑一下两个 des 串联？

4.ELGamal 可以看作分组密码的一种？公钥密码算法都是分组密码

5.关于公钥密码学加密的，A，B 想通信，A 用谁的什么加密给 B 发的消息？B 用谁的什么把消息解密？

6.签名，A,B 之间签名，A 用谁的什么给文件签名？B 用谁的什么验证签名？

7.PKI 的，最后的那个，ca 给数字证书签名的过程。

忘了。

三、忘了几分了，后面都是大题

X.800 中的 5 类安全服务

X.800 中的 8 种安全机制

相互之间的关系，可以列表说明

四、分组密码

分组密码的五种工作模式，要求写出各种模式的名字，并且画出图说明

五、消息认证

MDC 是啥？定义？

MAC 是啥？定义？

他们之间的区别

然后画了一个图，就是既有签名，哈希函数，单钥加密，然后让你分析，为啥能完成，数字签名，消息认证，加密传输的功能

六、RSA

此题巨坑无比，有密码学基础的都知道，RSA 肯定要用计算器算的，手算算到啥时候，是，有模重复平方法，但是也是要用计算器的啊，结果准考证上写，“所有科目都不得使用计算器“。没有密码学基础的，可以试试计算下面的这个式子。73^13（mod 77），如果这个可以借助计算器计算出来的话（应该是不行的），来，再来一个，75^37（mod 77），这可算不出来了吧。。。。这就是考试题，需要使用模重复平方，不停降幂次数。除此之外，还考了扩展欧几里得算法，p=7，q=11，e=13，求私钥 d

七.diffie-hellman 协议进行中间人攻击，数学表达式

八.diffie-hellman 协议的密钥交换的中间人攻击，数学表达式

九.PKI

X.509v3 证书格式画出来，说明 ca 给证书签名过程，用户验证证书真实性的 过程

十.无线网络安全

GSM 通信的缺陷

rand 能否是一个常数？有什么影响?

十一、安全协议

设计一个协议，既能完成双方之间的身份认证，又能完成密钥交换，进行安全通信

大体就这样，想起来会继续补充的，嘻嘻嘻，码了好长时间字了，全凭随意，没有要求，祝大家顺利。