

## 【1】考试过程

信息安全工程师考试已结束，QQ 群平静了很多。自入群后，一直潜水，从未冒泡，只想说一句“风物长宜放眼量”。

作为一名 IT 近 20 年的老司机，为以考促学，自 2015 年开始陆续考了项目管理师、系统架构师、系统分析师（论文没过）。两个高级在手，感觉也没啥区别，还是照样辅导孩子功课、洗碗洗衣。

这次考信息安全工程师，还是中级，都不好意思跟家人说起。原计划在 11 月开始突击看下视频，免得看早了，对知识点映像不深。但计划没有变化快，要赶工写一个部门年初报的课题论文，导致视频一点没看。

周 4，打印了准考证，一看地点在下沙了，城西到城东，路上要一小时，整个人都不高兴了，本已经在犹豫要不要去考，这下更不想去了，周 4 晚上看个科幻片《钢铁骑士》。周 5 上班，纠结后决定去捧个人场，报名的银子不能白交，去看个试题也成，万一过了呢！周 5 晚上，才告知老婆，周六小儿的兴趣班让她接送，自己去下沙考个试。因平日没铺垫，老婆没心理准备，不乐意了，一听还是中级，叫我别去了，对她来说，周 6 睡个懒觉比我考试重要。我说“信息安全只有中级，不管有用没用，学习的心不能变，给孩子做个榜样”，这才沟通好，答应了。

正式备考，2B 铅笔、水笔、橡皮等，干粮就不准备去买了。上班事情多，中午也没小睡，晚饭后已感觉脑子不在状态，就先睡觉了。晚上 9 点多，被儿子叫醒，说饭桌要收拾。只好起床，等洗完碗后，人已清醒，时间已是晚上 10 点。打开笔记本，直接看冲刺视频了，按视频把要点记了下，看完已是 12 日凌晨 2 点了。对考题的范围有了个大概了解，感觉冲刺视频内容还是挺多的，含金量挺高，这点要感谢群主上传。现在仍记得有 IC 卡 COS 包含的模块、SHA 哈希算法明文的分组长度等，上午试题中刚好有对应的两题，遗憾的是没记住视频细节，都答错了。可能太困，第一个 6:20 的闹钟没有醒来，第二个 7:20 闹钟才醒来，大惊，赶紧穿衣起床，7:30 开车上路，路上买上大饼油条，直接向下沙飞奔。8:30 顺利到达考点，时间还有多，在考场外看群友共享的文件“[2016 下半年信息安全工程师综合知识考前密卷答案 0101527.pdf](#)”，熟悉下题型。考前进场，找不到放身份证的钱包了，想起买早餐时直接放副驾驶座上了，一路小跑到停车位置拿回，幸好还没迟到。不认真准备还真是不行，状况不断。

后面考试就基本正常了，下午考完后就打道回府了。

## 【2】上午答案

考试交卷前，把选择题的答案超载了准考证上（提前打印了 2 张）。

2016/11/14 16:30:04															信管网网友
CCDDO	ADADC	DBDAD	ADCB	BOCB	ADDB	BCDAD	CCBAA	DBBDA	CBDDC	CDDBB	DBCAD	ADDC	DCDAC	DABCA	My
CCDDO	ADADC	BBBAA	CDCA	BABCA	ADDC	DOCAA	CCDCA	DBDD	DABDC	CDCAA	DBCD	ADDC	BADAB	DACCA	
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
			5		10				20		25			30	45分
2016/11/15 0:03:36															我的标准答案
CCDDO	ADADC	BBBAA	CDCA	BABCA	ADDC	DOCAA	CCDCA	DBDD	DABDC	CDCAA	DBCD	ADDC	BCACC	DACBA	My的答题卡
CCDDO	ADADC	BBBAA	CDCA	BABCA	ADDC	DOCAA	CCDCA	DBDD	DABDC	CDCAA	DBCD	ADDC	BADAB	DACCA	
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
			5		10			15					20		55分

参考信管网网友答案，自己只得了 45 分，随时可能不合格，太悬了。昨天晚上，花了 3 小时，自己重新参考网上各种资料，制作了标准答案（群友可以放心采用，误差 3 分之内），重新核对，分数瞬间提高到了 55 分，再次感叹掌握规则的重要性。

对答案如有疑问，可以 QQ 联系，400892@qq.com

我的标准答案：

CCDDD ADADC BBDAD CDCBD BABBB CDBCD DDCBA CCBCA DBBDA DBDDC CDBBA DBCCB  
ADDCC BCACC DACBA

有几道题稍微解释下：

【26】

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

果该S盒的输入110011，则其二进制输出为 (26) 。

A. 0110      B. 1001      C. 0100      D. 0101

自己选了【A】      110011      11----3      0011----3      第三行、第三列 6 → 0110

标准答案是【C】

110011, b1b6=3      b2b3b4b5=1001=9      对应是 4 → 0100

当输入为 101011 时, b1b6=11=3, b2b3b4b5=0101=5, 看 3 行 5 列为 15, 则 s2 盒的输出为 1111.

当输入为 110100 时, b1b6=10=2, b2b3b4b5=1010=6, 看 2 行 6 列为 13, 则 s2 盒的输出为 1101.

【66】、设在 RSA 的公钥密码体制中，公钥为  $(c, n) = (13, 35)$ ，则私钥为 ( )

- A、11
- B、13
- C、15
- D、17

答案是【B】，靠猜是绝对不会选 13 了，估计这个要错一大片了。

$e=13$     $N=35=5*7$     $l=(5-1)*(7-1)=24$

答案中，只有  $13*13 \bmod 24 === 1$

【69】、67mod119 的逆元是 ( )

- A、52
- B、67
- C、16
- D、19

自己选了【B】，不知逆元为何物，直接  $119 \bmod 67$  进行计算。

答案是【C】

4. 用推广的 Euclid 算法求  $67 \bmod 119$  的逆元。

解:

$q$	$g$	$u$	$v$
$\sim$	119	1	0
$\sim$	67	0	1
1	52	1	-1
1	15	-1	2
3	7	4	-7
2	1	-9	16

所以  $67^{-1} \bmod 119 = 16$

【74】

steganography today, however, is significantly more (4) than the example about suggest, allowing a user to hide large amounts of information within image and audio.

(4) A、powerful

B、sophisticated

C、advanced

D、easy

讲了信息隐藏。在 B 和 C 两个 ed 之间反复调了多次。最后选了【C】

答案是【B】

下午最后一题考点是缓冲区溢出。

作为老司机，看到类似的代码 BUG 太多了

第二问写了 2 个问题

1. 代码中的密码是 Secret 字符串，直接在源程序中；通过执行程序的静态分析，就能得到该字符串密码。可以保持为 Secret 的 md5 结果，并对输入串计算 md5，再比较。
2. 使用指定长度的安全输入函数，避免使用 gets

【3】工作积累

这次考试，考试教程和视频基本没看。但因平时工作中积累较多，主管 IT 项目管理工作，负责了加密平台、IC 卡等项目，对 RSA、证书、3DES、MD5、安全编程等都有一定的了解。另推荐一本书，记得群友也推荐过。这里再推荐下，入门比较适宜。

考试教程和视频还是应该多看。



2016/11/15

Chenj

QQ: 400892