24信息安全导论-试题回忆

编者	Egopposer（line2345）
日期	2024/12/27

0、前言及试题概览

为帮助软院同学正确考量考试难度，合理规划复习时间，预防应付考试复习冗余或者复习不足的情况，依照24年考试内容，制定本参考版试题回忆，帮助同学更好的制定复习计划。

莫得答案(ヽ∀･)

*斜体*为记忆模糊的题目，不保证可信度，**黑体**为我认为需要关注的点。

试题概览：（主观评价较多，仅供娱乐）

题量	中
难易度（软院专业课中）	5/10
送分题占比	50%
背诵记忆占比	0%（开卷）
21-23均分	
21-23平均满绩率	

整张卷子我只有两题想不起来，一道选择，一道填空((ゝ(*´ω`*)ノ))

1、选择题（2*10=20）

- 要求信息不被第三方窃取指的是信息的（）
  - 保密性
  - 完整性
  - 真实性
  - 防抵赖
- AES加密标准中的密钥长度不包括下列哪个选项（）
  - 128
  - 192
  - 256
  - 512
- AES解密算法每轮第一步操作为（）
  - 字节替换
  - 行移位
  - 列混淆
  - 轮密钥加
- 2-DES没有比DES保密性提高很多是因为（）的可行性

    - 中间人攻击
    - 中间相遇攻击
    - 重放
    - 生日攻击
- A使用私钥加密自己的信息，则不能提供下列哪一项安全机制（）
    - 信息加密
    - 消息认证
    - 用户认证
    - 数字签名
- 下列哪个密码体系不能被用于数字签名（）
    - D-H
    - RSA
    - ECC
    - ElGamal
- 安全哈希不能应用的场景为（）
    - 数字签名
    - 消息认证
    - 密钥交换
    - 恶意代码检测
- **国家保密标准**中对称密码使用的算法标准为（）
    - SM2
    - SM3
    - SM4
    - AES
- SSL应用在TCP/IP体系的（）
    - 应用层
    - 传输层
    - 网络层
    - 链路层

2、填空题（2*10=20）

- 香农提出密码系统设计中的两个重要准则分别是扩散和（）
- DES加密算法中一共使用了（）个S-box
- 公钥密码体制的主要应用包括：密钥封装、密钥交换和（）
- 在公钥分发的过程中，可信KDC分发的是（）密钥
- AES解密算法中，行移位中的第四行向左移动了（）位
- 假设一个密文的加密方式为$C = E(K_1, (D(K_2, E(K_3, P))))$，则解密方式为（）
- 假设CPC的密码加密方式为$C_i = E(K, (C_{i-1} \oplus P_i))$，则$P_{i-1}$的表达式为（）
- 欧拉函数$\phi(51) = ()$
- *Alice和Bob共同商定原根3和素数17，各自选定随机数4和2，则它他们之间的会话密钥为（）*

3、简答题（8*5=40）

- 解释密码学中雪崩效应的概念
- 简述公钥密码体系的要求
- 简述选用哈希函数需要具备的性质
- 简述安全哈希的性质和作用
- 简述第一代公钥密码和抗量子密码的主要区别

4、综合题（20）

假设A想向B发送一条消息，他使用**国家加密标准**进行加密。首先进行消息摘要和数字签名，再通过加密方式发送给B。

- 写出加密后密文的表达式（8分）
- 用流程图或者语句说明B收到密文后的解密和认证过程（8分）
- 这套加密方法提供了那些安全服务？能抵抗哪些安全攻击？（4分）