密码学真题-2024夏-回忆版

选择（10 分）

1. 以下哪种密码体制可以抵抗统计分析
2. 以下哪个算法不是基于大整数分解困难问题
3. 以下哪个攻击条件最弱
4. 以下哪个不是 AES 可能的密钥长度
5. 对于输入 101010，请在下图 S 盒中找到其输出（二进制）
6. 对于密钥长度 256 比特的 AES，若以字节为元素采用状态矩阵，应有（）行（）列
7. DES 的拓展置换将 32bit 的输入转为（）bit 的输出
8. Hash 函数不能实现以下哪个功能
9. 以下哪些人提出了公钥密码体制
   ？（忘了）

填空（20 分）

1. 两类生日攻击的结论（2 空）
2. AES 四个基本变换（4 空）
3. 数字信封的作用（1 空）
4. n 级 LFSR 最大周期（1 空）
5. 分组密码的两大设计原则（2 空）
6. Hash 函数安全性质：单向性、（） （）（2 空）
7. 流密码根据是否与明文有关分为两类：（2 空）
8. Diffie-Hellman 密钥交换是基于（1 空）困难问题
   ？（忘了）

简答（30 分）

画图说明分组密码的两种迭代，举出对应的代表密码算法

说明 DSA 的工作过程；若采用相同的随机数 k，可能的攻击方式？

画图说明输出反馈型分组密码的加、解密过程和特点

计算（40 分）

计算 $A(x)+B(x), A(x)\cdot B(x) \quad mod\ p(x)$

Schnorr 数字签名

给出生成元 g、随机数 k、私钥 x、公钥 y、哈希结果 $h(r,m)$

1. 计算签名并验证
2. 以当前的计算能力，将 p 固定在 512 位是否安全？为什么

椭圆曲线

给出函数、质数 p、生成元坐标 $P(x,y)$、随机数 k、公钥 $Q=dP$

1. 计算 2g、3g
2. 给明文，计算密文并验证（未给出阶数、所有点）

Shamir 门限方案

给出分配份额数 n、恢复需要份额数 k、模数 p、分配后的份额对 (x,y)

1. 计算秘密

$-By$ 苏润洵