密码学 2024 级期末考试回忆版

张方国 现代密码学

填空

1.ELGGAML,p=11,$\alpha = 2$,a=8,计算β

2.线性同余生成器$s \mapsto 3s + 5$，初始种子 s=8，计算前 6 个随机数

3.AES 密钥长度可以为(3 个)

4.评价密码安全性(3 个)

5.数字签名攻击者的 3 种攻击目标

判断

1.Miller-Rabin 算法是一个对于质数问题偏否的 Monte Carlo 算法。

2.RSA 是由 Diffie-Hellman 两人在 1976 年提出的

3.SHA-1 的摘要长度是 256bit

4.Rabin 体制能防御选择明文攻击

5.BBS 伪随机数生成器是基于二次剩余的困难问题

单选

1.AES 中哪个不是线性代换?

A.字节替换 B.行移位 C.列混合 D.轮密钥加

2.一个骰子掷两次，已知前一次比后一次的点数小，问得到了多少信息量()

A.lb(12/5) B.lb(3) C.lb(6) D.lb(36/5)

3.凯撒密码加密后的密文求原文（jd 开头的）

4.线性分析是什么攻击() A. 选择密文攻击 B.唯密文攻击 C.选择明文攻击 D.已知明文攻击

5.公钥密码体制中最强的攻击手段是()

A. 选择密文攻击 B.唯密文攻击 C.选择明文攻击 D.已知明文攻击

多选

1.分组密码工作模式包括()

A. 电码本模式 B. 密文反馈模式 C. 密文分组链接模式 D. 输出反馈模式 E. 计数器模式

2.以下哪些是对的()

A.DSA160 位消息有 80 位摘 要

B.dsa 在处理消息前要压缩

C.当 sita=0 时，需要重新选择随机数 k

D.DSA 是基于 ElGamal 算法的基础的

E.ECDSA 是利用了椭圆曲线的性质。

3.下面哪个算法在大整数分解被解决后不安全了

A.ElGamal B.Robin C.RSA D.AES

4.离散对数问题的算法有

A.Shanks 算法 B.Pollard ρ 离散对数算法 C.Pohlig-Hellman 算法 D.指数演算法 E.凯撒测试法

5.哪些是公钥密码体制

ElGamal RSA Robin Hill DES

简答（名词解释）

1.完善保密性

2.SPN

3.DDH

4.可识别密文

5.Lamport 方案

计算

1

(1)对于 GF(2),判断x^3+x^2+x+1,x^3+1,x^3+x+1是不是不可约的

(2)对于上述不可约的项，列出 GF(2^3)模这个项的有限域的元素，并计算x^{2024}

(3)计算在这个有限域的x^2+x的乘法逆元

2

(1)计算欧拉函数$\Phi(2024)$

(2)对于 RSA,n=91,e=5,计算解密指数 d

综合

1. 假设函数 h_1 是抗碰撞的,$\{0,1\}^{2m}\to\{0,1\}^m$; 定义 $x=x_1\parallel x_2$,$h_2=h_1(h_1(x_1)\parallel h_1(x_2))$, $\{0,1\}^{4m}\to\{0,1\}^m$ 证明 h2 是碰撞稳固的。
2. 介绍选择密文攻击;为什么教科书式的 RSA 在选择密文攻击的条件下不安全?
3. 介绍一个密码学的实际应用,说明用了什么密码方案,作用是什么。