查看成绩

期中考试（二）

题目编号及标记说明

正确 错误 主观题

一、选择题

1 2 3 4 5

二、填空题

1 2 3 4

三、简答题

1

四、计算题

1

测验得分: **84.0** 分

期中考试（二）_2025

试卷描述 期中考试（三）

总题数: 11

总分: 100.0

第一部分: 选择题（共5道题）

1.下面（）不是Hash函数的常用的提法 ✓

A.压缩信息函数

B.哈希函数

C.单向散列函数

D.杂凑函数

2.加密算法（如AES）与散列函数算法（如SHA）的最大的不同是（） ✓

A.分组

B.迭代

C.非线性

D.可逆

3.Alice有一个消息M通过密钥K和MAC算法生成一个MAC为C（K，M），Alice将这个MAC附加在消息M后面发送给Bob，Bob用密钥K和消息M计算MAC并进行比较，这个过程可以提供什么安全服务？( ) ✓

A.仅提供保密性

B.不可否认性

C.仅提供消息认证

D.保密性和消息认证

4.1. SHA256函数的迭代结构称之为( )结构 ✓

A.SPN

B.DM

C.HMAC

D.MD

5.m序列本身是适宜的伪随机序列产生器，但只有在（）下，破译者才不能破解这个伪随机序列。 ✓

A.唯密文攻击

B.已知明文攻击

C.唯密文攻击

D.唯密文攻击

第二部分: 填空题（共4道题）

1.我国的商用hash函数标准是__算法

该生答案
SM3

教师反馈

请输入您对这道题的反馈信息...

2.序列密码结构可分为__部分和__部分两个主要组成部分

该生答案
驱动
，
非线性组合

教师反馈

请输入您对这道题的反馈信息...

3.序列密码的起源可以追溯到__密码算法

该生答案
Vernam

教师反馈

请输入您对这道题的反馈信息...

4.HMAC使用SHA-256作为其嵌入的散列函数，使用的密钥长度是120位，数据长度512位，则该HMAC的输出是__位。

该生答案
256

教师反馈

请输入您对这道题的反馈信息...

第三部分: 简答题（共1道题）

1.简要说明散列（哈希）函数的特点

该生答案

1.输入长度任意
2.输出长度定长
3.对任意输入，计算其哈希值比较容易
4.具有单向性，即给定哈希值无法通过计算找到其原象
5.具有抗弱碰撞性，即给定一个消息a无法通过计算找到消息b使得H(a)=H(b)
6.具有抗强碰撞性，即无法通过计算找到一个消息对(a,b)使得H(a)=H(b)

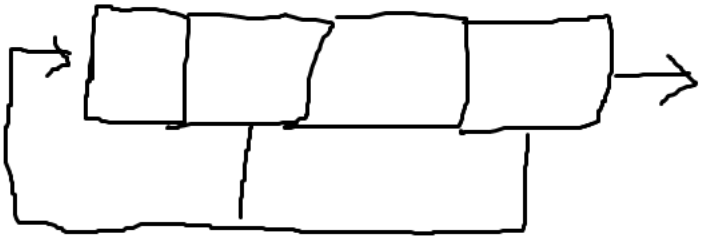
教师反馈

请输入您对这道题的反馈信息...

第四部分: 计算题（共1道题）

GF(2)上的级数是4的线性反馈移位寄存器，其输出序列满足$k_i = k_{i-2} + k_{i-4}$ ，
1.初始状态为0101，画出此线性反馈移位寄存器的示意图，写出输出状态变更过程和最终输出序列，并判断输出序列的周期。

该生答案



周期 12
最终输出序列 101000101000
状态
0101
0010 1
0001 0
1000 1
0100 0

教师反馈

请输入您对这道题的反馈信息...