23年秋《密码学原理》期末考试

姓名_____ 学号 _____ 得分 _____

Problem 1. (10 points) Hash function.

Let $H : \mathcal{M} \to \mathcal{T}$ be a collision resistant hash where $\mathcal{M} = \{0,1\}^\ell$ and $\mathcal{T} = \{0,1\}^n$. For each of the following, explain why it is collision resistant, or describe an efficient way to find collisions:
假设 $H : \mathcal{M} \to \mathcal{T}$ 是一个抗碰撞哈希, 其中 $\mathcal{M} = \{0,1\}^\ell$ 且 $\mathcal{T} = \{0,1\}^n$. 对于以下每个情况, 请解释为什么它具有抗碰撞性质, 或者描述一种有效的寻找碰撞的方法：

(1) For a fixed $0^\ell \neq \Delta \in \mathcal{M}$, define $H_1(m) := H(m) \oplus H(m \oplus \Delta)$.
对于固定的 $0^\ell \neq \Delta \in \mathcal{M}$, 定义 $H_1(m) := H(m) \oplus H(m \oplus \Delta)$.

(2) For a fixed $0^n \neq \Delta \in \mathcal{T}$, define $H_2(m) := H(m) \oplus \Delta$.
对于固定的 $0^n \neq \Delta \in \mathcal{T}$, 定义 $H_2(m) := H(m) \oplus \Delta$.

Problem 2. (10 points) Euler theorem.

Let p be a prime with $p = 2 \bmod 3$. Show an efficient algorithm that takes $\alpha \in \mathbb{Z}_p^*$ as input and outputs the cube root of α in $\mathbb{Z}_p$. That is, show how to efficiently solve the equation $x^3 - \alpha = 0$ in $\mathbb{Z}_p$.
设 p 是一个满足 $p = 2 \bmod 3$ 的质数. 请给出一个高效的算法, 该算法以 $\alpha \in \mathbb{Z}_p^*$ 为输入, 并输出 $\mathbb{Z}_p$ 中的 α 的立方根. 也就是说, 在 $\mathbb{Z}_p$ 中高效求解方程 $x^3 - \alpha = 0$.

Hint: Euler theorem shows that $x^{p-1} = 1 \bmod p$.
提示： 欧拉定理表明 $x^{p-1} = 1 \bmod p$.

Problem 3. (20 points) Chinese remainder theorem.

The number of students in a school is unknown. If we group them into groups of 9, there are 6 students left. If we group them into groups of 7, there are 2 students left. If we group them into groups of 5, there are 3 students left. What is the minimum number of students in the school? (please provide detailed calculations)

某学校的学生人数未知, 按每组9人进行分组, 剩下6人. 每组7人, 剩下2人. 每组5人, 剩下3人. 请问这个学校至少有多少学生? (请给出详细的计算过程)

Problem 4. (20 points) RSA encryption.

In the RSA encryption scheme, the public key is $\langle N, e\rangle$. Can e equal 2 in practice? Explain your answer.
在RSA加密方案中, 公钥为 $\langle N, e\rangle$. 在实际应用中, e 是否可以等于 2? 请解释你的判断.

Problem 5. (20 points) ElGamal encryption.

Given a public key $pk = \langle \mathbb{G}, q, g, h \rangle$, a ciphertext $c_A = \langle g^y, h^y \cdot g^a \rangle$, where y is uniformly chosen from $\mathbb{Z}_q$ and a is uniformly chosen from $\{0, 1\}$.
给定公钥 $pk = \langle \mathbb{G}, q, g, h \rangle$ 和密文 $c_A = \langle g^y, h^y \cdot g^a \rangle$, 其中 y 从 $\mathbb{Z}_q$ 中均匀选择, a 从 $\{0, 1\}$ 中均匀选择.
(Please note that you only know $c_A = \langle g^y, h^y \cdot g^a \rangle$, not y and a)
(请注意, 你只知道 $c_A = \langle g^y, h^y \cdot g^a \rangle$, 而不知道 y 和 a)

(1) Can you efficiently construct such a cipher text $c_B (\neq c_A)$ such that c_B is the encryption of g^b, where $b \in \{0, 1\}$ and $a \oplus b = 0$? If yes, please construct it.

你能否有效构造这样一个密文 $c_B (\neq c_A)$, 使得 c_B 是 g^b 的加密结果, 其中 $b \in \{0, 1\}$ 且 $a \oplus b = 0$? 如果可以, 请给出构造过程.

(2) Can you efficiently construct such a cipher text $c_B (\neq c_A)$ such that c_B is the encryption of g^b, where $b \in \{0, 1\}$ and $a \oplus b = 1$? If yes, please construct it.

你能否有效构造这样一个密文 $c_B (\neq c_A)$, 使得 c_B 是 g^b 的加密结果, 其中 $b \in \{0, 1\}$ 且 $a \oplus b = 1$? 如果可以, 请给出构造过程.

Problem 6. (20 points) Signature scheme.

Let (G, S, V) be a secure signature scheme with message space $\{0,1\}^{\ell(n)}$. Generate two signing / verification key pairs $(pk_0, sk_0) \leftarrow G(1^n)$ and $(pk_1, sk_1) \leftarrow G(1^n)$. Which of the following are secure signature schemes? Show an attack or explain why it is secure briefly.
设 (G, S, V) 是一个消息空间为 $\{0,1\}^{\ell(n)}$ 的安全签名方案. 生成两对签名/验证密钥 $(pk_0, sk_0) \leftarrow G(1^n)$ 和 $(pk_1, sk_1) \leftarrow G(1^n)$. 以下的签名方案是否安全? 请展示一种攻击或简要解释为何是安全的.

(1) Accept one valid: This scheme accepts a signature if at least one of the two signatures is valid.
该方案在两个签名中至少有一个有效时接受签名.

$$S_1((sk_0, sk_1), m) := (S(sk_0, m), S(sk_1, m)) = (\sigma_0, \sigma_1)$$

$$V_1((pk_0, pk_1), m, (\sigma_0, \sigma_1)) = 1 \Leftrightarrow [V(pk_0, m, \sigma_0) = 1 \text{ or } V(pk_1, m, \sigma_1) = 1]$$

(2) Sign halves: This scheme signs the left and right halves of the message separately with the respective private keys and verifies each signature.
该方案使用两个签名私钥对消息的左半部分和右半部分分别进行签名, 并验证每个签名.

$$S_2((sk_0, sk_1), (m_L, m_R)) := S(sk_0, m_L), S(sk_1, m_R) = (\sigma_0, \sigma_1)$$

$$V_2((pk_0, pk_1), (m_L, m_R), (\sigma_0, \sigma_1)) = 1 \Leftrightarrow V(pk_0, m_L, \sigma_0) = V(pk_1, m_R, \sigma_1) = 1$$

(3) Sign with randomness: In this scheme, the message m is XORed with a random value r. Verification checks the validity of the signatures with the modified message $m \oplus r$ and the random value r.
在该方案中, 消息 m 与一个随机值 r 进行异或, 并对修改后消息 $m \oplus r$ 和随机值 r 分别签名.

$$S_3(sk_0, m) := [r \xleftarrow{\$} \{0,1\}^{\ell(n)}, \text{ output } (r, S(sk_0, m \oplus r), S(sk_0, r))]$$

$$V_3(pk_0, m, (r, \sigma_0, \sigma_1)) = 1 \Leftrightarrow V(pk_0, m \oplus r, \sigma_0) = V(pk_0, r, \sigma_1) = 1$$