《密码学原理》期末考试

姓名 ______________ 学号 ______________ 得分 ______________

1. 计算题 (20 分)

(1) $N = 7 * 13$, $a = 5$, $a^{-1} \mod N =$ ______(a 模 N 的乘法逆元).

(2) 在 Diff-Hellman 密钥交换协议中, Alice 和 Bob 默认在模 N 的乘法群中交换密钥. Alice 生成的群为 $N = 17$, $g = 5$, 她的秘密 $x = 3$, 那么她送给 Bob 的信息为 ($N = 17, q =$ ______, $g = 5, h_A =$ ______). 之后她收到 Bob 发回的信息为 $h_B = 10$, 那么他们最终得到的密钥 $k =$ ______.

(3) 在 ElGamal 加密系统中, 设 G 为模 $P = 19$ 的乘法群, 生成元 $g = 3$, 若私钥中的 $x = 5$, 公钥中的 $h =$ ______. 若加密 $m = 3$ 时的随机数 $y = 7$, 那么对应的密文 $c =$ ______. 若密文 $c = \langle 5, 6 \rangle$, 那么密文 $m =$ ______.

(4) 在 plain RSA 签名中, 令 N = 299, 公钥 e = 7, 请问 $\sigma = 5$ 是对 $m = 5$ 的签名么?______. 已知 $\sigma = 141$ 是对 $m = 2$ 的签名, 请再给出一对合法的签名 $m' =$ ______$(m' \neq 2), \sigma' =$ ______

2. 基于 ElGama 加密系统的密钥生成算法 Gen, 构造了如下一个新的 1-bit 加密方法: 若公钥为 (G, q, g, h), 私钥为 x. 对于明文 $b \in \{0, 1\}$

(1) 若 b = 0, 则等概率选取相互独立的随机数 $y, z \in Z_q$, 并计算 $c_1 := g^y, c_2 := g^z$. 密文为 $\langle c_1, c_2 \rangle$.

(2) 若 b = 1, 则等概率选取一个随机数 $y \in Z_q$, 并计算 $c_1 := g^y, c_2 := h^y$. 密文为 $\langle c_1, c_2 \rangle$.

请回答以下问题 (20 分):

(1) 写出 ElGama 加密系统的密钥生成算法 Gen, 其中群生成算法为 $\mathcal{G}$.

(2) 写出该加密算法的解密算法. 在什么情况下 $Dec_{sk}(Enc_{pk}(b))! = b$ 可能发生?

(3) 证明若 DDH 问题关于 $\mathcal{G}$(Gen 中的群生成算法) 是困难的, 那么该加密系统是 CPA 安全的.

(hard relative to 可以参照以下定义)

The discrete-logarithm experiment $\mathsf{DLog}_{\mathcal{A},\mathcal{G}}$

1. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group of order q (with $|q| = n$), and g is a generator of $\mathbb{G}$.
2. Choosen a uniform $h \in \mathbb{G}$.
3. $\mathcal{A}$ is given $\mathbb{G}, q, g, h$, and outputs $x \in Z_q$.
4. The output of the experiment is defined to be 1 if $g^x = h$, and 0 otherwsie.

DEFINITION 8.62

We say that **the discrete-logarithm problem is hard relative to** $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function *negl* such that

$$Pr[\mathsf{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1] \leq negl(n).$$

3. 单次安全签名系统的定义如下

The one-time signature experiment $\mathsf{Sig\text{-}forge}^{\mathsf{1\text{-}time}}_{\mathcal{A},\Pi}(n)$**:**

1. $\mathsf{Gen}(1^n)$ *is run to obtain keys* (pk, sk).
2. *Adversary* $\mathcal{A}$ *is given* pk *and asks a* single *query* m' *to its oracle* $\mathsf{Sign}_{sk}(\cdot)$. $\mathcal{A}$ *then outputs* (m, σ) *with* $m \neq m'$.
3. *The output of the experiment is defined to be 1 if and only if* $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$.

DEFINITION 12.14 *Signature scheme* $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *is* existentially unforgeable under a single-message attack, *or is a* one-time-secure signature scheme, *if for all probabilistic polynomial-time adversaries* $\mathcal{A}$, *there exists a negligible function* negl *such that:*

$$\Pr\left[\mathsf{Sig\text{-}forge}^{\mathsf{1\text{-}time}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \mathsf{negl}(n).$$

请证明若 H 是单向函数 (one-way function), 那么如下构造的签名系统是单次安全的 (20 分, 若只考虑 $l = 1$ 的情况可以得到一部分分数):

CONSTRUCTION 12.15

Let $H : \{0,1\}^* \to \{0,1\}^*$ be a function. Construct a signature scheme for messages of length $\ell = \ell(n)$ as follows:

- Gen: on input 1^n, proceed as follows for $i \in \{1, \ldots, \ell\}$:
  1. Choose uniform $x_{i,0}, x_{i,1} \in \{0,1\}^n$.
  2. Compute $y_{i,0} := H(x_{i,0})$ and $y_{i,1} := H(x_{i,1})$.

  The public key pk and the private key sk are

$$pk = \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{\ell,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{\ell,1} \end{pmatrix} \quad sk = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{\ell,1} \end{pmatrix}.$$

- Sign: on input a private key sk as above and a message $m \in \{0,1\}^\ell$ with $m = m_1 \cdots m_\ell$, output the signature $(x_{1,m_1}, \ldots, x_{\ell,m_\ell})$.
- Vrfy: on input a public key pk as above, a message $m \in \{0,1\}^\ell$ with $m = m_1 \cdots m_\ell$, and a signature $\sigma = (x_1, \ldots, x_\ell)$, output 1 if and only if $H(x_i) = y_{i,m_i}$ for all $1 \leq i \leq \ell$.

4. 考虑模 p 的乘法群 Z_p^*, 其中 $p = 2q + 1$ 且 p, q 都是素数. 令集合 $G = \{x \in Z_p^* : \exists y \in Z_p^*, y^2 = x\}$(25 分).

(1) 请证明 G 在模 p 乘法下也构成群, 计算集合 G 的大小 $|G|$.

(2) 证明对 $h \in Z_p^*$, $h \in G$ 等价于 $h^q = 1 \mod p$.

(3) 请证明 decisional Diffie-Hellman 假设在 Z_p^* 中不成立.

5. 设加密系统 Π 是一个加密 1-bit 信息的公钥加密系统, 设当其密钥生成函数 Gen 输入安全参数为 1^n 时, 该加密算法的密文长度为 $l(n)$. 请证明 (15 分):
若 Π 是 CPA 安全的, 则对任意常数 c, 存在自然数 N, 对所有 $n > N, l(n) > c \log n$.