密码学原理期末考试答案

姓名 ______________ 学号 ______________ 得分 ______________

1. 计算题

(1) 73

(2) q = 16, hA = 6, k = 14(xB = 7)

(3) h = 15, c = <2, 1> , m = 7

(4) 不是, 第二空 $\sigma^7 = m$ 即可, 推荐做法为选择一个 $a \in Z_N^*, m' = 2 * a^e, \sigma' = a * \sigma$

2. (1) Gen: $(G, q, g) \leftarrow \mathcal{G}(1^n)$, $x \leftarrow Z_q$, $pk = (G, q, g, g^x), sk = (G, q, g, x)$.

(2) Dec: input $\langle c1, c2 \rangle$, $b = (c_1^x == c_2)$

错误情况为加密 b=0 时选择的 z=xy.

(3) Let $p_{b,b'} = Pr[\mathcal{A}(G, q, g, h = g^x, Enc_x(c)) = b' | c = b]$.

We have $Pr[PubK_{\mathcal{A},\Pi}^{CPA}(n) = 1] = (p_{00} + p_{11})/2 = \frac{1}{2} + (p_{11} - p_{01})/2$.

If Π is not CPA-secure, then $Pr[PubK_{\mathcal{A},\Pi}^{CPA}(n) = 1] > \epsilon(n)$.

So $p_{11} - p_{01} > 2\epsilon(n)$. This implies $Pr[\mathcal{A}(G, q, g, h = g^x, g^y, g^{xy}) = 1] - Pr[\mathcal{A}(G, q, g, h = g^x, g^y, g^z) = 1] > 2\epsilon(n)$, which conflicts with DDH is hard.

3. $l = 1$:

$sk = (x_0, x_1), pk = (y_0, y_1)$, where x_0, x_1 are chosen uniformly from $\{0,1\}^n$, $y_0 = H(x_0), y_1 = H(x_1)$. $Sign_{sk}(b) = x_b$.

If it is not on-time secure, then $\exists \mathcal{A}$ that $Pr[Sig-forge_{\mathcal{A},\Pi}^{1-time}(n) = 1] > \epsilon(n)$.

We can construct $\mathcal{A}'$ which invokes $\mathcal{A}$, and try to invert H as follows:

Given a y, $\mathcal{A}'$ needs to return a $x \in \{0,1\}^n$ that $H(x) = y$.

$\mathcal{A}'$ firstly choose a uniform $b' \in \{0,1\}$ and a uniform $x' \in \{0,1\}^n$. Then he publishes his public key $pk = (y_{b'} = H(x'), y_{1-b'} = y)$ to $\mathcal{A}$. After that, if $\mathcal{A}$ queries $b = 1 - b'$, $\mathcal{A}'$ aborts. Otherwise if $\mathcal{A}$ queries $b = b'$, $\mathcal{A}'$ answers him with x'.

At last, $\mathcal{A}$ will returns the signature $\sigma = x$ of $1 - b'$, ans he succeeds if $H(x) = y$.
So $Pr[\mathcal{A}' \ inverts \ H] = Pr[\mathcal{A} \ forges \wedge b = b']$.
For that y is also a image on a uniformly chosen x, the view of $\mathcal{A}$ is same with its view in the 1-time signature experiment. So its output is independent with b'. This implies $Pr[b = b'] = 1/2$ and $Pr[\mathcal{A} \ forges] = Pr[Sig-forge^{1-time}_{\mathcal{A},\Pi}(n) = 1]$. For $l \neq 1$, refer to the text book P463.

4. (1) For $x, y \in G$, $\exists x', y' \in Z_p^*$ that $x'^2 = x, y'^2 = y$, so $xy = (x'y')^2 \in G$.
$|G| = |Z_p^*|/2 = q$. For that $x^2 = (-x)^2$ and $x! = -x \mod p$.
(2) If $h \in G$, then $\exists x \in Z_p^*, x^2 = h$. So $h^q = x^{2q} = x^{p-1} = 1$.
For the oher side, $h = g^x$ for some x and a generator g. And $h^q = g^{xq} = 1$. For that Z_p^* is a cyclic group, so $xq = 0 \mod (p-1)$. This is impossible is x if odd. If x is even, $h = (g^{x/2})^2$.
(3) If at least x, y is even, $g^{xy} \in G$. So we can construct D to distinguish $h = g^{xy}$ and $h = g^z$. If $(g^x \in G \vee g^y \in G) \wedge h \in G$, it outputs 1. Otherwise it outputs 0.
$Pr[D(g^x, g^y, g^{xy}) = 1] = Pr[x \ is \ even \ \vee \ y \ is \ even] = 3/4$.
$Pr[D(g^x, g^y, g^z) = 1] = Pr[(x \ is \ even \ \vee \ y \ is \ even) \wedge \ z \ is \ even] = 3/8$.
5. If not, $\exists c \forall N \exists n > N, l(n) \leq clog(n)$. Construct $\mathcal{A}$ as follows:
Given $c = Enc(b)$, he use encryption oracle to get $c' = Enc(0)$. If $c = c'$, then he outputs $b' = 0$, otherwise outputs a uniform bit $b' \in 0, 1$.
$Pr[\mathcal{A} \ succeeds] = Pr[b = b'] = Pr[b = 1 \wedge b' = 1] + Pr[b = 0 \wedge b' = 0 \wedge c = c'] + Pr[b = 0 \wedge b' = 0 \wedge c \neq c']$.
Without loss of generality, we can assume that when $b = 0$, the ciphertexts are of equal possibility. So $Pr[b = 0 \wedge b' = 0 \wedge c = c'] \geq 1/2^{l(n)} \geq 1/n^c$.
Such that $Pr[\mathcal{A} \ succeeds] \geq 1/2 + 1/n^c$.