哈希函数章节密码学基础作业

姓名：郭子涵 学号：2312145 班级：信息安全、法学双学位班

1 习题 4.6

4.6 假定 $f:\{0,1\}^m \to \{0,1\}^m$ 是一个原像稳固的双射。定义 $h:\{0,1\}^{2m} \to \{0,1\}^m$ 如下：给定 $x \in \{0,1\}^{2m}$，记

$$x = x' \| x''$$

其中 $x', x'' \in \{0,1\}^m$，然后定义

$$h(x) = f(x' \oplus x'')$$

证明：h 不是第二原像稳固的。

证明:

已知 $x = x' \| x''$, 取任意非零$x_0 \in \{0,1\}^m$,

构造 $x_1' = x' \oplus x_0$ ， $x_1'' = x'' \oplus x_0$ ， $x_1 = x_1' \| x_1''$

验证：因为 $x_0 \neq 0$，所以$x_1' \neq x'$且$x_1'' \neq x''$, 所以 $x_1 \neq x$,

又因为， $h(x_1) = f(x_1' \oplus x_1'') = f((x' \oplus x_0) \oplus (x'' \oplus x_0)) = f(x' \oplus x'') = h(x)$

由此我们构造了$x_1 \neq x$，但是他们拥有相同的哈希值 $h(x_1) = h(x)$。因此h不是第二原像稳固的，证毕。

2 习题 4.9

4.9 假定 $h_1:\{0,1\}^{2m} \to \{0,1\}^m$ 是一个碰撞稳固的 Hash 函数。

(a) 定义 $h_2:\{0,1\}^{4m} \to \{0,1\}^m$ 如下：

1. 将 $x \in \{0,1\}^{4m}$ 记为 $x = x_1 \| x_2$，其中 $x_1, x_2 \in \{0,1\}^{2m}$。
2. 定义 $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$。

证明：h_2 是碰撞稳固的。

(b) 对整数 $i \geqslant 2$，从 h_{i-1} 递归定义 Hash 函数 $h_i:\{0,1\}^{2^i m} \to \{0,1\}^m$ 如下：

1. 将 $x \in \{0,1\}^{2^i m}$ 记为 $x = x_1 \| x_2$，其中 $x_1, x_2 \in \{0,1\}^{2^{i-1} m}$。
2. 定义 $h_i(x) = h_1(h_{i-1}(x_1) \| h_{i-1}(x_2))$。

证明：h_i 是碰撞稳固的。

2.1 (a) 证明:

假设有碰撞:

设$h_2(x) = h_2(x')$，其中 $x \neq x'$，记为$x = x_1 \| x_2$， $x' = x_1' \| x_2'$。

分析碰撞转化路径:

1. **第一种情况**：若$h_1(x_1) \neq h_1(x_1')$，那么$h_1(x_1)\|h_1(x_2) \neq h_1(x_1')\|h_1(x_2')$ ，
   且$h_2(x) = h_2(x')$ -> $h_1(h_1(x_1)\|h_1(x_2)) = h_1(h_1(x_1')\|h_1(x_2'))$
   这就意味着我们在h_1中找到了一个碰撞,与题设矛盾。
2. **第二种情况**：若$h_1(x_1) = h_1(x_1')$，但$h_1(x_2) \neq h_1(x_2')$，
   我们同样可以上述对称方式找出h_1的一个碰撞，与题设矛盾。
3. **第三种情况**：如果两个哈希值都相等：$h_1(x_1) = h_1(x_1')$，　$h_1(x_2) = h_1(x_2')$

但由于$x \neq x'$，说明$(x_1, x_2) \neq (x_1', x_2')$，所以必然存在 $x_1 \neq x_1'$或 $x_2 \neq x_2'$，

从而得出h_1有碰撞，与题设矛盾。

综上: 任意情况下，若h_2 有碰撞，就可以从中推导出h_1 的碰撞。但题设h_1是碰撞稳固的Hash函数 ⇒ 矛盾 ⇒ 所以h_2必然也是碰撞稳固的。

2.2 (b) 证明:

假设存在碰撞:
$h_i(x) = h_i(x')$，其中$x \neq x'$，记为$x = x_1\|x_2$，$x' = x_1'\|x_2'$

三种情况处理:

1. 若$h_{i-1}(x_1) \neq h_{i-1}(x_1')$：由$h_i(x) = h_i(x')$ ->
   $h_1(h_{i-1}(x_1)\|h_{i-1}(x_2)) = h_1(h_{i-1}(x_1')\|h_{i-1}(x_2'))$推出 h_1发生碰撞，与题设矛盾。
2. 若$h_{i-1}(x_2) \neq h_{i-1}(x_2')$：同理，由第一种情况推理方法，得到$h_1$发生碰撞，与题设矛盾。
3. 若$h_{i-1}(x_1) = h_{i-1}(x_1')$且$h_{i-1}(x_2) = h_{i-1}(x_2')$。

因为$x \neq x'$，说明$(x_1, x_2) \neq (x_1', x_2')$，所以必然存在 $x_1 \neq x_1'$或 $x_2 \neq x_2'$，

必然可以得到至少一个h_{i-1}的碰撞

综上: 如果h_i有碰撞 ，则必然存在 h_{i-1} 或h_1 的碰撞 ，若$i = 2$, $h1$碰撞必然存在，与题设矛盾。所以，若h_1抗碰撞 ⇒ 所有 h_i都抗碰撞,即h_i碰撞稳固。