4.6. $\forall x \in \{0,1\}^{2m}$

将 x 的所有bit由1转为0，由0转为1得到的bit串定义为 $\neg x$.

则 $\neg x = \neg x' || \neg x''$，由异或的性质知

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

故 h 不是第二原像稳固的

4.9 a) 若然，假设可找到 $x \neq x'$ 使得 $h_2(x) = h_2(x')$，接下来找 h_1 的碰撞.

记 $x = x_1 || x_2$，$x' = x_1' || x_2'$

① $x_1 \neq x_1'$

则 $h_1(x_1) \neq h_1(x_1')$，若不然，h_1 碰撞不稳固

故 $h_1(x_1) || h_1(x_2) \neq h_1(x_1') || h_1(x_2')$

而 $h_1(h_1(x_1) || h_1(x_2)) = h_2(x) = h_2(x') = h_1(h_1(x_1') || h_1(x_2'))$

故 h_1 碰撞不稳固。

② $x_1 = x_1'$，但 $x_2 \neq x_2'$

则 $h_1(x_2) \neq h_1(x_2')$，若不然，h_1 碰撞不稳固；

类似①，可推出 h_1 碰撞不稳固。

与 h_1 碰撞稳固矛盾，故 h_2 碰撞稳固。

b) 数学归纳①: $i=2$ 时，结论成立

②: 设 $i=2,3,\cdots k-1$ 时，结论都成立，则 $i=k$ 时，

反证：若 h_k 不是碰撞稳固的，即 $\exists x' \neq x$，s.t. $h_k(x)=h_k(x')$

记 $x=x_1\|x_2$，$x'=x_1'\|x_2'$，

① $x_1 \neq x_1'$，

$h_{k-1}(x_1) \neq h_{k-1}(x_1')$，若不然则 h_{k-1} 不是碰撞稳固的。

则 $h_{k-1}(x_1)\|h_{k-1}(x_2) \neq h_{k-1}(x_1')\|h_{k-1}(x_2')$，

而 $h_1(h_{k-1}(x_1)\|h_{k-1}(x_2))=h_k(x)=h_k(x')$

$=h_1(h_{k-1}(x_1')\|h_{k-1}(x_2'))$，故 h_1 不是碰撞稳固的，矛盾，

② $x_1=x_1'$，但 $x_2 \neq x_2'$

类似①，要么 h_{k-1} 不是碰撞稳固的，要么 h_1 不是，矛盾。

故 h_k 是碰撞稳固的

③ 从而 $\forall i \geq 2$，结论成立，即 h_i 是碰撞稳固的。