1) So, $h : (Z_2)^7 \to (Z_2)^4$ & from table we get,

$$X_1 + X_2 + X_3 + X_4 = 0 \quad \ldots (1)$$
$$X_2 + X_3 + X_4 + X_5 = 1 \quad \ldots (2)$$
$$X_3 + X_4 + X_5 + X_6 = 0 \quad \ldots (3)$$
$$X_4 + X_5 + X_6 + X_7 = 1 \quad \ldots (4)$$

→ Putting $X_4 = X_1 + X_2 + X_3$ in eq^n 2, 3, & 4, we get

$$X_5 = X_1 + 1 \quad \ldots (b)$$
$$X_6 = X_2 + 1 \quad \ldots (c)$$
$$X_7 = X_3 + 1 \quad \ldots (d)$$

∴ From eq^n (a), (b), (c) & (d), we get all pre-images of (0, 1, 0, 1) as

X_1	X_2	X_3	X_4	X_5	X_6	X_7
0	0	0	0	1	1	1
0	0	1	1	1	1	0
0	1	0	1	1	0	1
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	0	1	0	0	1	0
1	1	0	0	0	0	1
1	1	1	1	0	0	0

2] $h : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$

a) $n = m > 1$ & $h(x) = x^2 + ax + b \pmod 2$

-> If $\exists\ g(x)$, such that $h(g(x)) = h(x)$ & $g(x) \neq x$, then it is usually easy to solve Second Pre-image while $g(x)$ is linear.

Case 1:- If a ~~guess~~ is even, Assume $g(x) = x'$

$= x + 2^{m-1} \bmod 2^m$

Now, $g(x) \neq x$ as $2^{m-1} \bmod 2^m \neq 0$

$\therefore h(g(x)) = h(x') = (x + 2^{m-1})^2 + a(x + 2^{m-1}) + b \pmod{2^m}$

$= x^2 + 2^m x + 2^{2m-2} + ax + a2^{m-1} + b \pmod{2^m}$

$= (x^2 + ax + b) \pmod{2^m} + (2^m x + 2^{2m-2} + a2^{m-1}) \bmod 2^m$

As $m > 1$; $2^{2m-2} \bmod 2^m = 0$

$\therefore h(g(x)) = x^2 + ax + b$, $h(g(x)) = h(x)$ & $g(x)$ is linear.

Case 2:- If a is odd, let $g(x) = x'$

Let $x' = x \quad \therefore (-x-a) = x \pmod{2^m}$

$\Rightarrow (2x+a) = 0 \pmod{2^m}$ is false as a is odd.

$\therefore g(x) = x' \neq x$

$\therefore h(g(x)) = g(x)(g(x)+a) + b \pmod{2^m}$

$= (-x-a)(-x-a+a) + b \pmod{2^m}$

$= (-x-a)(-x) + b \pmod{2^m}$

$= x^2 + ax + b \pmod{2^m}$

$\therefore h(g(x)) = h(x)$ if $g(x)$ is linear. Hence Proved.

b) $n > m$

$$h(x) = \sum_{i=0}^{d} (a_i x) \pmod{2^m}$$

Let $g(x) = x' = x + k2^m \; ; k \in \mathbb{Z}$

$\therefore h(x_i) = [a_0 + a_1 x + a_2 x^2 + \ldots + a_x x^x] \pmod{2^m}$

$\therefore h(g(x)) = [a_0 + a_1 (x + k2^m) + a_2 (x + k2^m)^2 \ldots]$

$\pmod{2^m}$

→ Without loss of generality, let take $k=1$

$$h(g(x)) = [a_0 + a_1 x + \ldots + a_\alpha x^{\alpha} 2^{2m}] \bmod 2^m$$

$$h(g(x)) = [a_0 + a_1 x + \ldots + a_\alpha x^{\alpha}] \bmod 2^m + 2^m (S) \bmod 2^m$$

$$\Rightarrow 0$$

Where S is series of remaining terms in eqn,

$\therefore h(g(x)) = h(x)$. Hence Proved

3] As $X = X' \| X''$ & $h(x) = f(X' \oplus X'')$

Now, let $X_1 \neq X'$; & So let compute $X_2 = X' \oplus X'' \oplus X_1$.

$\therefore X_2 \oplus X_1 = X' \oplus X''$ & So,

$f(X_2 \oplus X_1) = f(X' \oplus X'')$

$\therefore \bar{X} = X_1 \| X_2$ is the second pre-image of $f(X' \oplus X'')$

→ Therefore, h is not second pre-image resistant

4)

a) let there be a collision on h_2.
i.e $X \neq X'$ & $h_2(X) = h_2(X')$, where $X = X_1 || X_2$ & $X' = X_1' || X_2'$.

$h_2(X) = h_2(X') \Rightarrow h_1(h_1(X_1) || h_1(X_2)) = h_1(h_1(X_1') || h_1(X''))$

$\Rightarrow$ Now, Since h_1 is collision resistant ...

$X_1 = X_1'$ & $X_2 = X_2'$ which contradicts assumption of $X \neq X'$.

$\therefore$ h_2 is collision resistant.

b) Now, let us suppose a collision on h_i, that $X \neq X'$ & $h_i(X) = h_i(X')$ where $X = X_1 || X_2$ & $X' = X_1' || X_2'$

$\therefore h_i(X) = h_i(X') \Rightarrow h_1(h_{i-1}(X_1) || h_{i-1}(X_2)) = h_1(h_{i-1}(X') || h_{i-1}(X''))$

Since h_1 is collision resistant

$\therefore h_{i-1}(X_1) = h_{i-1}(X_1')$ & $h_{i-1}(X_2) = h_{i-1}(X_2')$

$\therefore h_1(h_{i-2}(X_{11}) || h_{i-2}(X_{12})) = h_1(h_{i-2}(X_{11}') || h_{i-2}(X_{12}'))$

-> Similarly, as h_1 is collision resistant.

Finally, we have

$\therefore h_1(X_{111\cdots1}) = h_1(X'_{111\cdots1}) ; h_1(X_{21\cdots22}) = h_1(X'_{21\cdots12})$

-> For X & X' are the as $X = X_{111\cdots111} || X_{111\cdots12} || X_{21\cdots111} || X_{22\cdots2}$

$X' = X'_{111\cdots111} || X'_{111\cdots12} || X'_{21\cdots111} || X_{22\cdots2}$

=> Since h_1 is collision resistent so $X = X'$, which contradicts our assumption.