

Question 1.

Marks: 5.0

Let f be a length-preserving OWF. Is $g(x) : f(f(x))$ necessarily one-way? Give reasoning or explain with an example.

Question 2.

Marks: 5.0

Let f be length preserving OWF. Let $bit(i, x) := x_i$, the i th bit of x (defined for $1 \leq i \leq |x|$). Prove that the function $f'(x) = f(x) || bit(1, x) || 1$ is a one-way function. Explain why the predicate $bit(1, \cdot) : \{0, 1\}^* \rightarrow \{0, 1\}$ is not hard-core for f' .