MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Hardness of least-significant discrete logarithm bit). *Let $\mathbb{G} = \langle g \rangle$ be a finite group of an order q generated by the powers of an element g. Then the Least Significant Discrete Logarithm Bit (LSB-DL) problem is following. For any element $y \in \mathbb{G}$ find a bit b such that such that $g^{2x+b} = y$ for $0 \leq x < q/2$.*

1. *Show that if q is even number then LSB-DL is easy.*
2. *Show that if q is odd number and algorithm that always solves LSB-DL then the DL problem is easy.*

HINT. *As the order of g is q, the equality $g^x = g^y$ implies $x \equiv y \pmod{q}$.*
HINT. *Define a simple algorithm for finding square roots if q is odd.*

Solution.