

- 3a) For public keys $X = g^x$ and $Y = g^y$, make a call to O_D under XY which would return m . Given $(c_0, c_1) = (g^r, m(g^{xy})^r)$, we can calculate g^{xy} by taking $\frac{c_1}{c_0 * m}$.
- 3b) Input the values $X = Z = g^z, Y = c_0 = g^r$ into O_{DH} . By querying this oracle, we obtain g^{zr} . Since $c_1 = m(g^z)^r$, we can compute $\frac{m(g^z)^{zr}}{g^{zr}}$ to obtain m .