Exercise S#3

The Davis-Meyer scheme shows how to build a good compression function from a block cipher. In this exercise, we study another construction and show that it is weak. Let $E: \{0, 1\}^\ell \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a block cipher that encrypts a message $m \in \{0, 1\}^n$ under the key $k \in \{0, 1\}^\ell$ as $E_k(m)$. Consider the following construction:

$$f: \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^n$$

$$(x, y) \mapsto E_y(x) \oplus y.$$

Show how to easily find a collision on $f$.

**Hint:** The block cipher $E$ and the corresponding decryption algorithm $D$ are known to the adversary.