LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / I & C
CH-1015 Lausanne
Phone: ++41 (0) 21 693 76 03
Fax: ++41 (0) 21 693 68 79
URL: http://lasecwww.epfl.ch

# 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 $\mathsf{E} : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher that encrypts a message $m \in \{0,1\}^n$ under the key $k \in \{0,1\}^\ell$ as $\mathsf{E}_k(m)$. Consider the following construction:

$$\begin{array}{rccc} f: & \{0,1\}^n \times \{0,1\}^\ell & \longrightarrow & \{0,1\}^n \\ & (x,y) & \longmapsto & \mathsf{E}_y(x) \oplus y. \end{array}$$

Show how to easily find a collision on $f$.
**Hint**: The block cipher $\mathsf{E}$ and the corresponding decryption algorithm $\mathsf{D}$ are known to the adversary.