Aufgabe 6.1

Sei E_K eine Blockchiffre mit Blocklänge $\ell = 64$ und irgendeiner Schlüsselmenge $\mathcal{K}$. Die zugehörige Blockchiffre-Entschlüsselung sei $D_K = E_K^{-1}$ Wir betrachten wieder die Verschlüsselung mit CBC als Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ für die Plaintextmenge $\mathcal{M} = \bigcup_{0 \le i} \{0,1\}^{n \cdot \ell}$.

Wir verwenden also die folgenden Algorithmen:

- $\mathcal{K}$ gibt ein gleichverteilt zufälliges Element der gleichnamigen Menge $\mathcal{K}$ zurück.
- $\mathcal{E}_K(m)$ arbeit wie folgt (für $K \in \mathcal{K}$, $m \in \mathcal{M}$):
  1. Setze $n = |m|/\ell$.
  2. Zerlege m in der Form $m = m_1 \| m_2 \| \ldots \| m_n$ (mit $|m_i| = \ell$ für jedes i).
  3. Setze $c_0 \xleftarrow{\$} \{0,1\}^\ell$.
  4. Setze $c_i \leftarrow E_K(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$.
  5. Gib $c_0 \| c_1 \| c_2 \| \ldots \| c_n$ als Resultat der Verschlüsselung zurück.
- $\mathcal{D}_K(c)$ wird wie folgt bestimmt:
  1. Setze $n = |m|/\ell - 1$.
  2. Ist n keine ganze Zahl oder ist $n < 0$, so gib $\perp$ zurück und brich den Entschlüsselungsvorgang ab.
  3. Zerlege c in der Form $c = c_0 \| c_1 \| c_2 \| \ldots \| c_n$ (mit $|c_i| = \ell$ für jedes i).
  4. Setze $m_i \leftarrow c_{i-1} \oplus D_K(c_i)$ für $i = 1, \ldots, n$
  5. Gib $m_1 \| m_2 \| \ldots \| m_n$ als Resultat der Entschlüsselung zurück.

In diesem Szenario sei $\boldsymbol{A}$ ein INT-CTXT-Angreifer. $\boldsymbol{A}$ hat also Orakelzugriff auf ein Verschlüsselungsorakel $E(\cdot)$ und auf ein Entschlüsselungsorakel $D(\cdot)$; diese Orakel bieten $\mathcal{E}_K(\cdot)$ sowie $\mathcal{D}_K(\cdot)$ für ein festes K, das mit $\mathcal{K}$ erzeugt wurde.

Beschreiben Sie einen Angreifer $\boldsymbol{A}$, der einen Ciphertext findet, der dem 64 Bit langen Plaintext $m = 00\,01\,02\,03\,04\,05\,06\,07$ (hexadezimal) entspricht, der *dabei aber nie sein Verschlüsselungsorakel verwendet.*

($\boldsymbol{A}$ verwendet das Entschlüsselungsorakel. Das INT-CTXT-Angriffsspiel gewinnt $\boldsymbol{A}$ schon mit der ersten Anfrage an dieses Orakel, die mit etwas anderem als $\perp$ beantwortet wird. Bei dieser Aufgabe geht es aber nicht lediglich um einen erfolgreichen INT-CTXT-Angreifer, sondern um einen Angreifer, der ein *zusätzliches* Ziel erreicht.)