Aufgabe 5.1

Wir kommen zurück auf die Counter-Mode-Verschlüsselung auf Basis einer Blockchiffre E_K mit Blocklänge ℓ und Schlüsselmenge $\mathcal{K}$, wie wir sie in Aufgabe 2.3 betrachtet haben. Es sei also $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ das Verschlüsselungsschema für die Plaintextmenge $\mathcal{M} = \bigcup_{0 \le n \le 2^{\ell/2} \cdot \ell} \{0,1\}^n$ mit folgenden Algorithmen:

- $\mathcal{K}$ als Schlüsselgenerierungsalgorithmus gibt ein gleichverteilt zufälliges Element der gleichnamigen Menge $\mathcal{K}$ zurück.
- Der randomisierte Verschlüsselungsalgorithmus bestimmt $\mathcal{E}_K(m)$ wie folgt ($K \in \mathcal{K}$, $m \in \mathcal{M}$):
  1. Setze $iv \xleftarrow{\$} \{0,1\}^{\ell/2}$.
  2. Sei $g_K(iv, |m|)$ der Präfix der Länge $|m|$ von
  $$E_K(iv \,||\, 00\ldots0000) \,||\, E_K(iv \,||\, 00\ldots0001) \,||\, \ldots \,||\, E_K(iv \,||\, 11\ldots1111).$$
  3. Gib $iv \,||\, \big(m \oplus g_K(iv, |m|)\big)$ als Resultat der Verschlüsselung zurück.
- Der Entschlüsselungsalgorithmus bestimmt $\mathcal{D}_K(c)$ wie folgt:
  1. Ist $|c| < \ell/2$ oder $|c| > \ell/2 + 2^{\ell/2} \cdot \ell$, so gib $\perp$ zurück und brich den Entschlüsselungsvorgang ab.
  2. Sonst zerlege den Ciphertext in der Form $c = iv \,||\, C$ mit $|iv| = \ell/2$.
  3. Sei $g_K(iv, |C|)$ der Präfix der Länge $|C|$ von
  $$E_K(iv \,||\, 00\ldots0000) \,||\, E_K(iv \,||\, 00\ldots0001) \,||\, \ldots \,||\, E_K(iv \,||\, 11\ldots1111)$$
  4. Gib $C \oplus g_K(iv, |C|)$ als Resultat der Entschlüsselung zurück.

Wir wissen, dass dieses Verschlüsselungsschema RoR-OTCPA-sicher und sogar RoR-CPA-sicher ist, falls E_K PRP-sicher ist und der Umfang der verschlüsselten Daten im Rahmen bleibt.

Gesucht ist nun aber ein Angreifer $\boldsymbol{A}$ im RoR-OTCCA-Angriffsspiel (Real-or-Random, Einmalverschlüsselung, Chosen-Ciphertext-Attack) auf dieses Verschlüsselungsschema: Der Angreifer hat also ein Entschlüsselungsorakel nach den Regeln dieses Angriffsspieles zur Verfügung. Wie kann ein Angreifer vorgehen, um erfolgreich zu sein, um also einen Vorteil deutlich über Null zu erreichen?

Aufgabe 5.2

Bestimmen Sie den RoR-OTCCA-Vorteil des Angreifers, den Sie zu Aufgabe 5.1 beschrieben haben.

Aufgabe 5.3

Nun betrachten wir, weiterhin für eine Blockchiffer E_K mit Blocklänge ℓ und Schlüsselmenge $\mathcal{K}$, die Verschlüsselung mit CBC (Cipher Block Chaining); für die Entschlüsselung brauchen wir hier zusätzlich die Blockcipher-Entschlüsselung $D_K = E_K^{-1}$. Hier geht es also um das folgende Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ für die Plaintextmenge $\mathcal{M} = \bigcup_{0 \le i} \{0,1\}^{n \cdot \ell}$:

- $\mathcal{K}$ als Schlüsselgenerierungsalgorithmus gibt ein gleichverteilt zufälliges Element der gleichnamigen Menge $\mathcal{K}$ zurück.
- Der randomisierte Verschlüsselungsalgorithmus bestimmt $\mathcal{E}_K(m)$ wie folgt ($K \in \mathcal{K}$, $m \in \mathcal{M}$):
  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.
- Der Entschlüsselungsalgorithmus bestimmt $\mathcal{D}_K(c)$ wie folgt:
  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.

Wir wissen, dass dieses Verschlüsselungsschema LoR-OTCPA-sicher und LoR-CPA-sicher ist, falls E_K PRP-sicher ist und der Umfang der verschlüsselten Daten im Rahmen bleibt.

Gesucht ist hier ein Angreifer $\boldsymbol{A}$ im LoR-OTCCA-Angriffsspiel (Left-or-Right, Einmalverschlüsselung, Chosen-Ciphertext-Attack) auf dieses Verschlüsselungsschema. Wie kann ein Angreifer vorgehen, um erfolgreich zu sein?

Aufgabe 5.4

Bestimmen Sie den LoR-OTCCA-Vorteil des Angreifers, den Sie zu Aufgabe 5.3 beschrieben haben.