Die Lösungen zu den Aufgaben **2.1 und 2.2** werden als Teil der Prüfungsnote **bewertet**! Bitte mit Angabe von Name, Matrikelnummer, Studiengang und Fachsemester bei der Übung am 7. Mai abgeben (oder vorher per E-Mail an `bmoeller@crypto.rub.de`).

Aufgabe 2.1

Zeigen Sie: Die direkte AES-256-Blockverschlüsselung bietet für die Plaintextmenge $\{0,1\}^{128}$ sichere Einmalverschlüsselung im Sinne von RoR-OTCPA, wenn man AES-256 als PRP-sicher voraussetzt.

(Erläuterungen siehe Aufgabe 2.2!)

Aufgabe 2.2

Zeigen Sie: Die direkte blockweise AES-256-Verschlüsselung für eine Plaintextmenge $\{0,1\}^{n\cdot 128}$ mit $n \geq 2$ ist nicht sicher im Sinne von RoR-OTCPA.

Erläuterungen: Hier (und in Aufgabe 2.1) geht es um das folgende Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ für die Plaintextmenge $\mathcal{M} = \{0,1\}^{n\cdot 128}$ (mit $n = 1$ für Aufgabe 2.1):

- $\mathcal{K}$ erzeugt eine Gleichverteilung auf $\{0,1\}^{256}$.
- Der Verschlüsselungsalgorithmus berechnet $\mathcal{E}_K(m)$ für $m \in \mathcal{M}$ als

  $$E_K(m_1) \parallel E_K(m_2) \parallel \ldots \parallel E_K(m_n),$$

  wobei $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ mit $m_i \in \{0,1\}^{128}$.
- Der Entschlüsselungsalgorithmus berechnet $\mathcal{D}_K(c)$ für $c \in \{0,1\}^{n\cdot 128}$ als

  $$D_K(c_1) \parallel D_K(c_2) \parallel \ldots \parallel D_K(c_n),$$

  wobei $c = c_1 \parallel c_2 \parallel \ldots \parallel c_n$ mit $c_i \in \{0,1\}^{128}$. Ist $c \notin \{0,1\}^{n\cdot 128}$, so dass sich keine solche Zerlegung vornehmen lässt, lautet das Resultat $\perp$.

Dabei bezeichnen E_K und D_K die Blockverschlüsselung bzw. Blockentschlüsselung mit AES-256 unter einem Schlüssel K:

$$E_K, D_K : \{0,1\}^{128} \to \{0,1\}^{128} \quad \text{für } K \in \{0,1\}^{256}.$$

Das hier betrachtete Verschlüsselungsschema auf Basis einer beliebigen Blockchiffre nennt sich “Electronic Codebook Mode” (ECB).

Aufgabe 2.3

Beschreiben Sie den Counter Mode einer Blockchiffre wie auf Vorlesungsfolie 4.21 skizziert als Verschlüsselungsverfahren $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ mit einer Plaintextmenge $\mathcal{M}$, ausgehend von einer Blockchiffre E_K mit einer Schlüsselmenge $\mathcal{K}$ und einer geraden Blocklänge ℓ. Der Schlüsselgenerierungsalgorithmus $\mathcal{K}$ erzeugt einfach eine Gleichverteilung auf der gleichnamigen Menge $\mathcal{K}$. Aber wie würden Sie $\mathcal{M}$ festlegen? Wie sollten die Algorithmen $\mathcal{E}$ zur Verschlüsselung und $\mathcal{D}$ zur Entschlüsselung aussehen?

(Hinweis: Bei einigen Details kann man sich hier mehr oder weniger willkürlich entscheiden.)

Aufgabe 2.4

Hier betrachten wir die Counter-Mode-Verschlüsselung (Aufgabe 2.3) als Einmalverschlüsselung für bis zu $q \cdot \ell$ Bits. Wir gehen davon aus, dass q recht klein ist. Geben Sie eine Ungleichung an, die ausgehend von der PRP-Sicherheit der verwendeten Blockchiffre die RoR-OTCPA-Sicherheit zeigt.

Bei dieser Aufgabe geht es darum, bekannte Resultate aus der Vorlesung und vom Übungsblatt 1 richtig zusammenzufügen: PRP (Blockchiffre) als PRF ("PRP/PRF Switching Lemma"), PRF zur Konstruktion eines PRG, PRG zur Einmalverschlüsselung.

Aufgabe 2.5

Machen Sie eine Aussage über die Sicherheit der Counter-Mode-Verschlüsselung (Aufgabe 2.3) für Mehrfachverschlüsselung, ausgehend von der PRP-Sicherheit der verwendeten Blockchiffre!

Gesucht ist eine Ungleichung zu RoR-CPA-Vorteil und PRP-Vorteil, die die folgenden Parameter zu den Anfragen des Angreifers an das Verschlüsselungsorakel berücksichtigen sollte:

- Die maximale Anzahl $q_\#$ der Anfragen;
- die jeweilige Maximallänge q_B pro Anfrage, gerechnet in Blocks zu ℓ Bits.