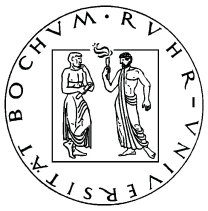
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May



Hausübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 1 / 16. Oktober 2009 / Abgabe 26. Oktober 2009, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Betrachten Sie eine verbesserte Vigenère-Chiffre, in der die Verschiebechiffren durch monoalphabetische Substitutionen ersetzt werden.
Dies bedeutet, dass der Schlüssel aus t Zufallspermutationen des Alphabets besteht. Die Klartextsymbole an der Stelle $i, t+i, 2t+i, \ldots$ werden mit der i-ten Permuation verschlüsselt. Beschreiben Sie einen Algorithmus, der im CPA-Modell den Schlüssel mit höchstens t gewählten Plaintexten extrahiert.

AUFGABE 2 (5 Punkte)**:**

1. Beweisen Sie, dass wenn nur ein einziger Buchstabe verschlüsselt wird, die Verschiebechiffre mit dem Schlüsselraum $\mathbb{Z}_{26}$ perfekt sicher ist (2 Punkte)
2. Warum ist die Verschiebechiffre, so wie sie in der Vorlesung definiert wurde, für keine Nachrichtenlänge perfekt sicher ? (1 Punkt)
3. Beweisen Sie, dass die Vigenère-Chiffre perfekt sicher ist, wenn sie genau ein Wort der Länge t verschlüsselt. (2 Punkte)

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie die folgende Definition perfekter Sicherheit für Nachrichtenpaare:
Ein Verschlüsselungsschema $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ über einem Nachrichtenraum $\mathcal{M}$ ist *perfekt sicher für zwei Nachrichten* wenn für jede Verteilung über $\mathcal{M}$, jedes nach dieser Verteilung unabhängig gewählte Paar $m, m' \in \mathcal{M}$, und jedes $c, c' \in \mathcal{C}$ mit $\mathsf{Pr}[C = c \wedge C' = c] > 0$ gilt:

$$\mathsf{Pr}[M = m \wedge M' = m' | C = c \wedge C' = c'] = \mathsf{Pr}[M = m \wedge M' = m']$$

Beweisen Sie: *Kein* Verschlüsselungsverfahren erfüllt diese Definition.

AUFGABE 4 (5 Punkte)**:**
Beweisen oder widerlegen Sie: Jedes Verschlüsselungschema bei dem die Kardinalität des Schlüsselraums gleich der Kardinalität des Nachrichtenraums ist und bei dem der Schlüssel unabhängig gleichverteilt aus dem Schlüsselraum gezogen wird, ist perfekt sicher.