Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 1 / 12. Oktober 2010 / Abgabe 25. Oktober, 16:00 Uhr, Kasten NA 02

AUFGABE 1. Vigenère-Variante. (5 Punkte)
Betrachten Sie eine verbesserte Vigenère-Chiffre, in der die Verschiebechiffren durch monoalphabetische Substitutionen ersetzt werden, d.h. zum Parameter t besteht der geheime Schlüssel nun aus t Permutationen $\pi_1, \ldots, \pi_t$ und die Klartextsymbole an den Stellen $i, t+i, 2t+i, \ldots$ werden mit der i-ten Permutation π_i verschlüsselt.

Konstruieren Sie einen Angreifer $\mathcal{A}$, der mit *einer* CPA-Anfragen den geheimen Schlüssel $\pi_1, \ldots, \pi_t$ berechnen kann! Gehen Sie hierbei davon aus, dass dem Angreifer t bekannt ist.

AUFGABE 2. Verschieben verschieden. (5 Punkte)
Betrachten Sie folgende Varianten der Verschiebechiffre aus der Vorlesung und untersuchen Sie diese in Bezug auf perfekte Sicherheit.

a) Beweisen Sie: Wird nur ein einziger Buchstabe mit der Verschiebechiffre mit Schlüsselraum $\mathbb{Z}_{26}$ verschlüsselt, so ist dies ein perfekt sicheres Verfahren.

b) Gilt die Aussage auch noch, wenn wir zwei Buchstaben verschlüsseln, d.h. wenn wir für $k \in_R \mathbb{Z}_{26}$ eine Nachricht $(x_1, x_2) \in \mathbb{Z}_{26}^2$ mit

$$\langle x_1 + k \bmod 26, x_2 + k \bmod 26 \rangle$$

verschlüsseln?

Hinweis: Hier ist die Charakterisierung von perfekter Sicherheit aus dem Satz "Ununterscheidbarkeit von Verschlüsselungen" hilfreich.

AUFGABE 3. Perfekte Sicherheit. (5 Punkte)
Betrachten Sie folgende Tabelle.

	m_1	m_2	m_3
k_1	c_1	c_3	c_1
k_2	c_2	c_1	c_3
k_3	c_3	c_2	c_2

Diese gibt an, auf welchen Chiffretext c_i eine Nachricht m_j bei Verschlüsselung mit k_l abgebildet wird. Nehmen Sie an, dass die Schlüssel k_i zufällig gleichverteilt gewählt sind.

a) Ist das durch diese Tabelle definierte Verfahren ein gültiges Verschlüsselungsverfahren?

b) Modifizieren Sie die Tabelle, so dass ein perfekt sicheres Verfahren entsteht. Beweisen Sie die perfekte Sicherheit, indem Sie den Satz von Shannon benutzen!

AUFGABE 4. Entschlüsselungsfehler. (5 Punkte)
Wir erlauben einem Verschlüsselungsverfahren $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ bei der Entschlüsselung mit einer gewissen Wahrscheinlichkeit falsch zu liegen, d.h. wir fordern lediglich

$$\mathbf{Pr}\left[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m\right] \geq 2^{-t}$$

anstelle von $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$. Zeigen Sie, dass für $t \geq 1$ Verfahren existieren, die perfekt sicher sind und $|\mathcal{K}| < |\mathcal{M}|$ erfüllen.

Hinweis: Versuchen Sie, für Nachrichten $m \in \{0,1\}^{\ell+t}$ den vorderen Teil mit einem One-Time Pad zu verschlüsseln und für den hinteren Teil auszunutzen, dass Entschlüsselungsfehler erlaubt sind.