Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 06.11.2015 **Abgabe:** Mo. 16.11.2015 bis 14:45 Uhr

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 2

AUFGABE 1 (8 Punkte)**:**
Diskutieren Sie die Sicherheit der affin-linearen Caesar-Chiffre aus Aufgabe 1 der Heimübung H1.

a) Angenommen, Sie besitzen einen beliebigen Klartextbuchstaben m und einen dazugehörigen Chiffretextbuchstaben c. Können Sie aus diesem Klartext-Chiffretext-Paar etwas über den geheimen Schlüssel lernen?

b) Angenommen, Sie besitzen zwei Klartext-Chiffretext-Paare (m_1, c_1) und (m_2, c_2). Welche Anforderungen müssen diese erfüllen, damit Sie den Schlüssel eindeutig bestimmen können? Wie kann dieser dann bestimmt werden?

c) Angenommen, Sie wissen, dass die Chiffre verwendet wird, um deutsche Texte zu Verschlüsseln. Wie können Sie dann den geheimen Schlüssel aufdecken, ohne einfach komplett den gesammten Schlüsselraum $\mathcal{K}$ zu durchsuchen?

d) Sie fangen folgende Verschlüsselung eines deutschen Textes ab:
`CKDCSQDLQJEWJGFQIBQIIQDUQJJQJCQJJCKDQIJKGFNAWDRSAQJWSQDUQJJQJCOZZNQJ`
Wie lautet vermutlich der verwendete Schlüssel? Verifizieren Sie Ihre Vermutung an den letzten sieben Buchstaben.

AUFGABE 2 (8 Punkte)**:**
Wir wollen nun die Caesar-Chiffre $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ aus der Vorlesung verallgemeinern, um die Schwäche, die in Aufgabenteil c) und d) der vorherigen Aufgabe ausgenutzt wurde zu beheben. Dazu definieren wir die Vigenère-Chiffre informell folgendermaßen:

- Ein Schlüssel sei gegeben durch ein n-Tupel $(e_0, \ldots, e_{n-1}) \in \mathbb{Z}_{26}^n$.
- Eine gegebene Nachricht $m_0 m_1 m_2 \cdots \in \mathbb{Z}_{26}^*$ wird dadurch verschlüsselt, dass das i-te Zeichen m_i der Nachricht durch die Caesar-Chiffre mit dem Schlüssel $e_{i \bmod n}$ verschlüsselt wird:

$$m_0 m_1 m_2 \cdots m_{n-1} m_n \cdots \mapsto E_{e_0}(m_0) E_{e_1}(m_1) \cdots E_{e_{n-1}}(m_{n-1}) E_{e_0}(m_n) \cdots$$

a) Geben Sie die Vigenère-Chiffre formal als 5-Tupel $(\mathcal{P}', \mathcal{C}', \mathcal{K}', \mathcal{E}', \mathcal{D}')$ an.

b) Verschlüsseln Sie die Nachricht „Geheim“ für $n = 3$ mit dem Schlüssel $e = (4, 23, 5)$.

c) Zeigen Sie, dass das Problem aus Aufgabe 1 c) nicht gelöst wurde, indem Sie einen geeigneten Angriff auf die Vigenère-Chiffre beschreiben. Nehmen Sie dazu an, dass die Schlüssellänge n in der Spezifikation festgelegt wurde und Ihnen als Angreifer bekannt ist.

   Tipp: Zerlegen Sie die Nachricht geeignet und wenden Sie den Angriff aus Aufgabe 1 c) auf jeden dieser Teile separat an.

AUFGABE 3 (8 Punkte)**:**
Sie erhalten eine verschlüsselte Nachricht $c_0c_1c_2\cdots c_t$, wobei die einzelnen c_i mittels einer Blockchiffre mit $\mathcal{P} = \mathcal{C} = \{0,1\}^n$ erzeugt wurden. Angenommen es geschieht bei der Übertragung ein Fehler und Sie verlieren unbemerkt den Block c_i. Analysieren Sie, wie sich dieser Verlust auf die Entschlüsselung der restlichen Blöcke auswirkt, wenn die Nachrichten jeweils mit dem Verschlüsselungsmodus ECB, CBC, CFB oder OFB generiert wurden.

AUFGABE 4 (6 Punkte)**:**
Betrachten Sie die Elemente von $\{0,1\}^3$ als Binärdarstellung der Zahlen $\{0,1,\ldots,7\}$ und sei Abbildung f wie folgt definiert:

$$\begin{aligned} f \ : \ \{0,1\}^3 \times \{0,1\}^3 &\to \{0,1\}^2 \\ (a,b) &\mapsto \lceil a \cdot b \rceil_2 \end{aligned}$$

Dabei bezeichnet $\lceil a \cdot b \rceil_2$ die beiden höchstwertigen Bits der 6-Bit-Zahl, die das Produkt von a und b darstellt.
Angenommen, a, b werden unabhängig und gleichverteilt aus $\{0,1\}^3$ gewählt. Welche Wahrscheinlichkeitsverteilung ergibt sich dann für die Bilder $f(a,b) \in \{0,1\}^2$?