Universität Duisburg-Essen **SS 2019**
Ingenieurwissenschaften / Informatik **17. April 2019**
Dozent: Prof. Dr. Barbara König **Übungsblatt 1**
Übungsleitung: Richard Eggert **Abgabe: -**

Formale Aspekte der Softwaresicherheit und Kryptographie

Hinweis: Dies ist kein Testatblatt; reichen Sie bitte keine Lösungen ein!
Dieses Übungsblatt wird am 02.05 besprochen.

Aufgabe 1 Entschlüsselung

Entschlüsseln Sie den Text unter

`www.ti.inf.uni-due.de/fileadmin/public/teaching/ssk/misc/krypto-2.txt`,

der – wie der Text in der Vorlesung – mit monoalphabetischer Verschlüsselung verschlüsselt wurde.

Aufgabe 2 Produkt von Kryptosystemen

Es sollen zwei gegebene Kryptosysteme (Kryptosystem 1 und Kryptosystem 2) zu einem neuen Kryptosystem kombiniert werden. Dabei soll die Verschlüsselung in dem neuen System so erfolgen, dass zuerst mit Kryptosystem 1 und anschließend mit Kryptosystem 2 verschlüsselt wird.

- Welche Bedingungen müssen zwei Kryptosysteme erfüllen, damit sie kombiniert werden können?
- Wie sehen die Komponenten des neuen Kryptosystems aus? (Definieren Sie möglichst genau die einzelnen Komponenten: Menge der Nachrichten, Menge der verschlüsselten Nachrichten, Schlüsselpaare, Ver- und Entschlüsselungsfunktion).
- Weisen Sie nach, dass das von Ihnen definierte neue Kryptosystem korrekt ist. (D.h., Verschlüsselung, gefolgt von Entschlüsselung, ergibt wieder die ursprüngliche Nachricht.)

Aufgabe 3 Wahrscheinlichkeitstheorie

Wir betrachten den Wahrscheinlichkeitsraum $\Omega = \{0,1\}^n$ (Menge aller Nachrichten der Länge n), wobei die Wahrscheinlichkeiten aller Elementarereignisse gleich sind, d.h., $P(x) = \frac{1}{|\Omega|}$ für jedes $x \in \Omega$.

(a) Was ist die Wahrscheinlichkeit eines Elementarereignisses?

(b) Wie groß ist die Wahrscheinlichkeit, dass eine Nachricht genau zwei Einsen enthält?

(c) Wie groß ist die Wahrscheinlichkeit, dass eine Nachricht mindestens zwei Einsen enthält?

(d) Wie groß ist die Wahrscheinlichkeit, dass eine Nachricht mit m Einsen beginnt und das Zeichen an der Stelle $m+1$ eine Null ist?

(Diese Frage macht natürlich nur dann Sinn, wenn $n > m$ gilt.)

(e) Wie groß ist die Wahrscheinlichkeit, dass eine Nachricht mit gerade vielen Einsen beginnt und das jeweils nächste Zeichen eine Null ist?

(f) Was ist die Wahrscheinlichkeit, dass eine Nachricht mindestens eine Eins enthält, vorausgesetzt dass sie mit genau einer Eins, gefolgt von einer Null, beginnt?

Wie groß ist die Wahrscheinlichkeit, dass eine Nachricht mit genau einer Eins, gefolgt von einer Null, beginnt, vorausgesetzt dass sie mindestens eine Eins enthält?

Beschreiben Sie die Ereignisse auch mit Hilfe einer Zufallsvariable.

Aufgabe 4 AES

Für folgende Bytes läßt sich das dazugehörige Byte in der S-Box von AES relativ einfach berechnen. Berechnen Sie jeweils das Byte, das für b substituiert werden muss.

(a) $b = 00000001$

(b) $b = 10001101$

Hinweis: Schreiben Sie dieses Byte als Polynom $p(x)$ und vergleichen Sie es mit $m(x)$. Mit welchem Polynom $q(x)$ muss man $p(x)$ multiplizieren, so dass $p(x) \cdot q(x) \bmod m(x) = 1$ gilt? Dabei ist $m(x) = x^8 + x^4 + x^3 + x + 1$.