23.02.2021

Dr. Felix Heuer
fheuer.lba@fh-salzburg.ac.at

Kryptographie und Mediensicherheit

Sommersemester 2021

Übungszettel 1

Abgabe: 09.03.2021 vor der Vorlesung

Bitte lassen Sie sich nie von schlimm klingenden Aufgaben abschrecken. Zum Beispiel brauchen Sie keine Angst vor "Zeigen Sie, dass..." Aufgaben zu haben. In der Regel müssen Sie hier nichts beweisen, sondern nur Dinge nachrechen, oder dürfen selbst mal Angreifer spielen. ;-)

1 Aufgabe (10 Punkte)

Zeigen Sie, dass die Vigenère Chiffre korrekt ist.

2 Aufgabe (10 Punkte)

Wir definieren das folgende symmetrische Verschlüsselungsverfahren für Nachrichten aus $\mathcal{M} = \mathbb{Z}_{26}^{\ell}$ für $\ell \in \mathbb{N}$, das eine leichte Verallgemeinerung der Caesar Chiffre ist. Es sei $\mathcal{K} = \mathbb{Z}_{26}$ und $\mathcal{C} = \mathcal{M}$. Wir identifizieren Buchstaben wie bisher mit ihrer Position im Alphabet ($A \equiv 0, \ldots, Z \equiv 25$).

Gen: Setze $k \leftarrow \mathcal{K}$. Gib k aus.

Enc: Für $k \in \mathcal{K}$ und $m = m_0 \ldots m_{\ell-1}$ setze $c_i = (m_i + k) \bmod 26$. Gib $c = c_0 \ldots c_{\ell-1}$ aus.

a) Geben Sie einen Dec Algorithmus an und zeigen Sie, dass das gesamte Verfahren damit korrekt ist.

b) Entschlüsseln Sie den folgenden Ciphertext mit einem C# Programm.

```
20,17,9,24,17,10,20,5,19,24,23,17,4,16,23,11,10,23,21,1,2,17,6,6,10 .
```

3 Aufgabe 4 (10 Punkte)

In der Unterlagen zur Vorlesung finden Sie einen Text, der mit der Vigenère Chiffre verschlüsselt wurde (`ciphertext.txt`). Das Alphabet finden Sie in `alphabet.txt`. Es hat Größe 47 (26 Kleinbuchstaben, Satz- und einige Sonderzeichen). Der Schlüssel besteht aus 20 zufälligen Zeichen dieses Alphabets.

a) Einer der stärksten Supercomputer im Jahre 2019 würde ca. 10^{15} Schlüssel pro Sekunde testen können. Wie lange bräuchte dieser Supercomputer, um alle möglichen Schlüssel der Länge 20 durchzuprobieren?

   Nehmen wir an, die schnellsten 10.000 Supercomputer der Welt wäre alle genau so stark. Wie lange bräuchte der Verbund dieser Rechner, um alle Schlüssel auszuprobieren?

b) Entschlüsseln Sie den hochgeladenen Text mit einem C# Programm.

Hinweis: Erinnern Sie sich daran, wie wir Varianten von Caesar gebrochen haben. Stellen Sie sich zunächst vor, wie Sie den Angriff bei einem Schlüssel der Länge 1 durchführen würden. Wie können Sie nun den Angriff auf Schlüssel der Länge 2,3,. . . , 20 anwenden?

4 Aufgabe (10 Punkte)

Hinweis: KPA Sicherheit behandeln wir erst in der zweiten Vorlesung/Übung.

Zeigen Sie, dass die Vigenère Chiffre nicht KPA-sicher ist.