



## Übungen zu Ideen der Informatik

<https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter18/ideen/>

Blatt 7

Abgabeschluss: 10. 12. 2018

**Aufgabe 1** (10 Punkte) Für diese Aufgabe identifizieren wir die Buchstaben des Alphabets (einschließlich Zwischenraum) mit den Zahlen 0 bis 26. Ein Klartext ist dann einfach eine Folge von Zahlen. Jede Zahl der Folge liegt zwischen 0 und 26 (jeweils einschließlich). Im One-Time Pad ist der Schlüssel genauso lang wie der Text. Sei also  $m = m_1m_2 \dots m_L$  der Text und  $k = k_1k_2 \dots k_L$  der Schlüssel. Dann ist die verschlüsselte Nachricht  $c = c_1c_2 \dots c_L$ , wobei  $c_i = (m_i + k_i) \bmod 27$ . Die Operation mod ist die Restbildung bei der Division mit 27. Etwa  $29 = 1 \cdot 27 + 2$  und daher  $29 \bmod 27 = 2$  und  $6 = 0 \cdot 26 + 6$  und daher  $6 \bmod 27 = 6$ .

- Überzeugen Sie sich, dass dieses Verfahren für jede einzelne Stelle genau dem Caesar-Verfahren entspricht.
- Nehmen sie an, sie hätten einen perfekten Würfel mit 27 Seiten haben und bestimmen den Schlüssel  $k$  durch wiederholtes Würfeln. Was können Sie dann über die Nachricht sagen? Insbesondere, wie groß ist die Wahrscheinlichkeit, dass  $c_i$  einen bestimmten Wert annimmt? Besteht eine Abhängigkeit zwischen dem Wert von  $c_i$  und dem Wert von  $c_j$  für  $i \neq j$ ?

**Aufgabe 2** (10 Punkte) Betrachten Sie den folgenden mit dem Caesar-Verfahren verschlüsselten Text:

hfme tqjfm u lfjof spmmf

- Entschlüsseln Sie den Text.
- Nehmen Sie an, wir verwenden das One-Time Pad in einer etwas modifizierten Version. Statt einen Schlüssel mit derselben Länge wie der Ausgangstext zu verwenden, wählen wir einen Schlüssel, der viel kürzer ist als der Klartext (zum Beispiel 10 Zeichen lang) und setzen dann diesen Schlüssel immer wieder hintereinander. Wenn wir also XABZWCOPVE als Schlüssel wählen, dann benutzen wir

XABZWCOPVEXABZWCOPVEXABZWCOPVEXABZWCOPVEXABZWCOPVE...

im One-Time Pad. Im One-Time Pad wird jeder Buchstabe des Klartextes gemäß Caesar verschlüsselt.

Wie kann man so eine Verschlüsselung überwinden?

**Aufgabe 3** (5 Punkte) Spielen Sie Baby ElGamal mit folgenden konkreten Zahlen durch:  $p = 5793$ ,  $f = 5832$ ,  $m = 354834$ , und  $s = 457$ .

**Aufgabe 4** (10 Punkte) (Eine Münze werfen). Alice und Bob wollen eine Münze werfen. Allerdings sind Sie nicht im gleichen Raum, sondern sind nur über ein Telefon verbunden. Sie verabreden, dass jeder eine Münze wirft, und das Gesamtergebnis Kopf ist, wenn beide Münzwürfe das gleiche Ergebnis haben, und Zahl sonst. Wie können Sie sich das Ergebnis der Münzwürfe mitteilen und garantieren, dass keiner schummelt? Sie dürfen annehmen, dass Alice und Bob eine Funktion  $h$  kennen, die Bitstrings der Länge 128 in Bitstrings der Länge 128 abbildet und folgende Eigenschaften hat.

- Zu einem Bitstring  $c$  ist es (praktisch) unmöglich ein  $m$  zu bestimmen, so dass  $m$  von  $h$  auf  $c$  abgebildet wird.
- Es ist (praktisch) unmöglich ein  $m$  und ein  $t$  zu bestimmen, so dass  $m$  und  $t$  verschieden sind, aber von  $h$  auf den gleichen Wert abgebildet werden.

**Aufgabe 5** (*ohne Punkte*) Finden Sie heraus, wie Sie Ihre emails signieren und/oder verschlüsseln können.

*Kryptographie* war spannend  okay  langweilig   
schwierig  okay  einfach