Universität des Saarlandes
FR 6.2 Informatik

Prof. Dr. Kurt Mehlhorn
Michael Dirnberger

WiSe 2015/16

Übungen zu Ideen der Informatik

http://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter15/ideen/

Blatt 7 Abgabeschluss: 14.12.2015

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 $m = m_1 m_2 \dots m_L$ der Text und $k = k_1 k_2 \dots k_L$ der Schlüssel. Dann ist die verschlüsselte Nachricht $c = c_1 c_2 \dots c_L$, wobei $c_i = (m_i + k_i) \bmod 27$. Die Operation $\bmod$ ist die Restbildung modulo 27. Etwa $29 = 1 \cdot 27 + 2$ und daher $29 \bmod 27 = 2$ und $6 = 0 \cdot 26 + 6$ und daher $6 \bmod 27 = 6$.

a) Überzeugen Sie sich, dass dieses Verfahren genau dem Caesar-Verfahren entspricht.

b) Nehmen sie an, dass sie einen perfekten Würfel mit 27 Seiten haben und den Schlüssel k durch wiederholtes Würfeln bestimmen. 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 tqjfmu lfjof spmmf

a) Entschlüsseln Sie den Text.

b) 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 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*) (Aus wenig gutem Zufall guten Zufall machen). Eine perfekte Münze liefert in 50% der Würfe Kopf. Die Ergebnisse verschiedener Würfe sind voneinander unabhängig.
Nehmen Sie an, dass sie nur eine unfaire Münze haben, die mit Wahrscheinlichkeit 0.9 Kopf liefert. Verschiedene Würfe sind aber unabhängig. Sie werfen die Münze n-mal und erklären Kopf, wenn die Münze eine ungerade Anzahl von Köpfen geliefert hat. Sei p_n die Wahrscheinlichkeit, dass sie Kopf erklären. Berechnen Sie p_1, p_2 und p_3 und geben sie eine Formel für p_n an.

Kryptographie war	spannend ☐	okay ☐	langweilig ☐
	schwierig ☐	okay ☐	einfach ☐