Universität des Saarlandes
FR 6.2 Informatik

Prof. Dr. Kurt Mehlhorn
Dr. Antonios Antoniadis
André Nusser

WiSe 2017/18

Übungen zu Ideen der Informatik

http://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/ideen/

Blatt 7 Abgabeschluss: 11.12.2017

Aufgabe 1 (*10 Punkte*) Für diese Aufgabe identifizieren wir die Buchstaben des Alphabets mit den Zahlen 0 bis 25 (0 = a, 1 = b, ...). Ein Klartext ist dann einfach eine Folge von Zahlen. Jede Zahl der Folge liegt zwischen 0 und 25 (jeweils einschließlich). Leerzeichen, Satzzeichen, etc. bleiben der Einfachheit halber gleich.
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 $c_i = (m_i + k_i) \bmod 26$. (Die Operation $\bmod$ ist die Restbildung bei der Division mit 26. Etwa $29 = 1 \cdot 26 + 3$ und daher $29 \bmod 26 = 3$ und $6 = 0 \cdot 26 + 6$ und daher $6 \bmod 26 = 6$).

a) Nehmen Sie an, dass $m_i = d$ für irgendein i zwischen 1 uns L. Was ist der dazugehörige Buchstabe c_i im verschlüsselten Text wenn $k_i = 2$? Wenn $k_i = 12$? Wenn $k_i = 24$?

b) Nehmen Sie an, Sie hätten einen perfekten Würfel mit 26 Seiten 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*)

a) Betrachten Sie den folgenden mit dem Caesar-Verfahren verschlüsselten Text:

ygt yknn hkpfgv ygig

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 3 Zeichen lang) und setzen dann diesen Schlüssel immer wieder hintereinander. Wenn also ZAO als Schlüssel wählen, dann verwenden wir

ZAOZAOZAOZAOZAOZAOZAOZAO...

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

Folgender Text wurde mit dem One Time Pad Verfahren verschlüsselt:

Ppa Acm Fxuq Eip vmtdmdi hg smz ewxnixepmqmfxaowmz Hcnhbuicfxwzhdqgnmwzqc, jqx lqcmz sqq tqzomxcmz Qcowafpjqc qz ymitqxh izsmdt Jgrpeiintv gboqlizsmxi eqglqc. Sqcvltqowvqclqh Uqgsypt ptz Qxvypthtzerpxjmehmxjvs xaf sqq tqzbixxoq Kmdlmzsczv mucme ocrpmxaqstv Erpxjmehmxh, lqg lut oxtqowm Xpmzvm ixm pxm lj dqgaowtgtaettzsm Zpktgqowb mjnitqei.

Der benutzte Schlüssel ist 3 Zeichen lang (und nicht ZAO!). Satzzeichen und Leerzeichen werden bei der Verschlüsselung ignoriert. Das heißt P wurde mit dem ersten Zeichen verschlüsselt, p mit dem zweiten, a mit dem dritten, A wieder mit dem ersten, c wieder mit dem zweiten, und so weiter. Großschreibung wurden beibehalten. Was sind die ersten vier Worte (Ppa Acm Fxuq Eip) in entschlüsselter Form? Was ist der Schlüssel?

Hinweis: Um den Schlüssel zu finden müssen Sie den gesamten Text betrachten. Der bei Weitem am häufigsten vorkommende Buchstabe in der deutschen Sprache ist „e“. Dadurch ergibt sich auch eine verschobene Häufigkeit der Buchstaben im verschlüsselten Text.

Aufgabe 3 (*5 Punkte*) Spielen Sie Baby ElGamal mit folgenden konkreten Zahlen durch: $p = 5973$, $f = 8532$, $m = 453438$, und $s = 413$.

Aufgabe 4 (*10 Punkte*) (Aus weniger gutem Zufall guten Zufall machen). Eine perfekte Münze liefert in 50% der Würfe Zahl. Die Ergebnisse verschiedener Würfe sind voneinander unabhängig.
Nehmen Sie an, dass Sie nur eine unfaire Münze haben die mit Wahrscheinlichkeit $p = 0.78$ Zahl 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 nach n Würfen. Berechnen Sie p_1, p_2 und p_3. Wie hängen p_n und p_{n-1} zusammen? Sei $q_n = p_n - 1/2$. Zeigen Sie, dass $q_n = 0.56 \cdot q_{n-1}$. Welchen Wert hat q_n für sehr großes n? Welchen Wert hat p_n für sehr großes n?

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

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