Universität des Saarlandes
FR Informatik

Kurt Mehlhorn und Antonios Antoniadis **WiSe 2019/20**

Übungen zu Ideen der Informatik

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter19/ideen/

Blatt 10 Abgabeschluss: 6. 1. 2020

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 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 $6 \bmod 27 = 6$.

a) Überzeugen Sie sich, dass dieses Verfahren für jede einzelne Stelle genau dem Caesar-Verfahren entspricht.

b) 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 $i \neq j$?

Lösung:

a) Der Wert von k gibt an, um wie viele Buchstaben die beiden Ringe gegeneinander verschoben werden sollen. Also $k = 0$, $a \mapsto a$, $k = 1$, $a \mapsto b$, und so weiter.

b) Die Wahrscheinlichkeit das c_i einen bestimmten Wert annimmt, ist $1/27$, da es genau einen Schlüsselwert gibt, der m_i nach c_i abbildet.

Es besteht keine Abhängigkeit, da die Schlüssel für die verschiedenen Stellen unabhängig voneinander gewählt werden. Die Wahrscheinlichkeit, dass m_i nach c_i und m_j nach c_j abgebildet wird, ist $1/27 \cdot 1/27$.

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 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?

Lösung: Im Geheimtext ist der Buchstabe m besonders häufig. Wir nehmen daher an, dass m einen der häufigen Buchstaben in deutschen Texten kodiert. Die häufigsten Buchstaben sind e, n, i, s, ...
Ich habe $e \mapsto m$ und $n \mapsto m$ und $i \mapsto m$ ohne Erfolg ausprobiert.

Dann habe ich nochmals nachgedacht. Im verschlüsselten Text kommt mm vor. Also steht m für einen Buchstaben, der als Doppelbuchstabe vorkommen kann. Doppelbuchstaben sind ee, nn, ll, mm. Die ersten beiden haben wir schon probiert. Die Möglichkeit l $\mapsto$ m, das heißt jeder Buchstabe wird durch seinen Folgebuchstaben ersetzt, ergibt es Klartext

geld spielt keine Rolle.

Für den zweiten Teil zerlegen wir den Schlüsseltext in 10 Teilfolgen. Die erste Teilfolge besteht aus dem 1ten, 11ten, 21ten, und so weiter Buchstaben. Ähnlich für die anderen Teilfolgen. Auf jede Teilfolge wenden wir das Verfahren unter a) an.

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

Lösung: Der Empfänger berechnet $P = pf$ und veröffentlicht f und P. Um m zu schicken, wählt der Sender s und schickt $m + sP$ und sf. Der Empfänger berechnet $p \cdot (sf) = s \cdot P$ und dann m. Konkret bedeutet das.

- Der Empfänger berechnet $P = 5793 \cdot 5832 = 33.784.776$ und veröffentlicht 5832 und $33.784.776$.
- Der Sender berechnet $m + sP = 354834 + 457 \cdot 33.784.776 = 15.439.997.466$ und $sf = 457 \cdot 5832 = 2.665.224$ und schickt beide Zahlen.
- Der Empfänger berechnet $p(sf) = 5793 \cdot 2.665.224 = 15.439.642.632$ und dann $m = 15.439.997.466 - 15.439.642.632 = 354834$.

Aufgabe 4 (*5 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 Einschaften hat.

a) Zu einem Bitstring c ist es (praktisch) unmöglich ein m zu bestimmen, so dass m von h auf c abgebildet wird.

b) 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.

Eine solche Funktion nennt man *kryptographische Hashfunktion*.

Lösung: Bob und Alice sprechen sich ab, dass Kopf = 0 und Zahl = 1.

a) Bob wählt einen zufälligen Bitstring s der Länge 127 und hängt das Ergebnis e seines Münzwurfs hinten dran. Sei $m = se$ der Bitstring, den er so erhält. Er schickt dann $c = h(m)$ an Alice.

b) Alice verkündet ihren Münzwurf, etwa d. Bob schickt einen Bitstring t der Länge 128 an Alice und behauptet, dass das letzte Bit davon das Ergebnis seines Wurfes ist. Alice berechnet $h(t)$ und akzeptiert, wenn $c = h(t)$.

Beachte: e ist das Bit, das Bob gewählt hat. Das letzte Bit von t ist das Bit, von dem Bob behauptet, dass es das Ergebnis seines Wurfes ist.
Alice kann m aus c nicht berechnen (Eigenschaft 1). Daher kennt sie e nicht, wenn sie ihr Bit wählt. Daher kann Bob sicher sein, dass Alice nicht schummelt.
Wenn Bob $m = se$ in Schritt 2 schickt, dann akzeptiert Alice. Nehmen wir umgekehrt an, dass Alice akzeptiert. Dann ist $h(m) = h(t)$. Nach Eigenschaft 2) muss dann $m = t$ sein. Also kann sich Alice sicher sein, dass Bob nicht schummelt.

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

Lösung: Bei GMX steht: Nachrichten über digitale Überwachung und Missbrauch per E-Mail wecken den Wunsch nach Sicherheit in der persönlichen Kommunikation. GMX bietet mit der verschlüsselten Kommunikation ein geprüftes Sicherheitsverfahren, um bei Bedarf die Inhalte Ihrer E-Mails zu verschlüsseln - nur lesbar für Absender und Empfänger. Der einfache Einrichtungsassistent hilft Ihnen, die E-Mail-Verschlüsselung schnell einzurichten. Das Verfahren ist komplett kostenlos und auch auf mobilen Geräten nutzbar.

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