Universität des Saarlandes
FR Informatik

Kurt Mehlhorn und Corinna Coupette

WiSe 2020/21

Übungen zu Ideen der Informatik

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter20/ideen/

Blatt 10 Abgabeschluss: 18. 1. 2020

Aufgabe 1 (*10 Punkte*) In der Vorlesung habe ich behauptet, dass der Geheimtext beim One-Time-Pad ein zufälliges Wort ist und keinerlei Information über den Klartext enthält. In dieser Aufgabe sollen Sie genauer verstehen, was damit gemeint ist. 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). Wir nehmen weiter an, wir hätten einen perfekten Würfel mit 27 Seiten (beschriftet mit den Zahlen von 0 bis 26).

(a) (4Punkte) Was meint man mit einem perfekten Würfel?

Hinweis: Sie sollten etwas über den Ausgang einen einzelnen Wurfs sagen und etwas über die Ausgänge mehrere Würfe.

Lösung: Ein perfekter Würfel hat zwei Eigenschaften:

- Bei jedem einzelnen Wurf sind alle Ergebnisse gleichwahrscheinlich. Bei einem Würfel mit 27 Seiten erhält man also jedes Ergebnis mit Wahrscheinlichkeit $1/27$.
- Die Ergebnisse verschiedener Würfe sind voneinander unabhängig. Wenn wir etwa zwei Würfel benutzen, dann sind alle Ergebnispaare (y_1, y_2) mit $y_1, y_2 \in \{0, 26\}$ gleichwahrscheinlich.
  Alternativ können Sie sagen: Die bedingte Wahrscheinlichkeit, dass der zweite Wurf ein bestimmtes Ergebnis hat unter der Voraussetzung das das Ergebnis des ersten Wurfs bekannt ist, ist $1/27$.
- Vorsicht: Die erste Eigenschaft allein reicht nicht. Sie wäre etwa erfüllt, wenn der Würfel beim ersten Wurf ein zufälliges Ergebnis liefert und dann bei jedem weiteren Wurf das gleiche Ergebnis wie beim ersten Wurf.

(b) Im Caesar-Verfahren ist der Schlüssel dann auch eine Zahl $k \in \{0, 26\}$ und die Verschlüsselung erfolgt wie folgt.

Schlüssel $k = 0$: $0 \mapsto 0, 1 \mapsto 1, \ldots, 26 \mapsto 26$
Schlüssel $k = 1$: $0 \mapsto 1, 1 \mapsto 2, \ldots, 26 \mapsto 0$
Schlüssel $k = 4$: $0 \mapsto 4, 1 \mapsto 5, \ldots, 26 \mapsto 3$

Das kann man auch knapper schreiben als $x \mapsto (x + k) \bmod 27$. Man addiert x und k und falls das Resultat größer ist als 26, dann zieht man 27 ab, um wieder in den Bereich 0 bis 26 zu kommen.

(a) (3 Punkte) Nehmen Sie an, wir würden den Schlüssel k mit unserem Würfel bestimmen. Mit welcher Wahrscheinlichkeit erhalten sie einen bestimmten Wert y, wenn Sie ein festes x mit diesem gewürfelten k verschlüsseln.

Falls Ihnen diese Formulierung zu abstrakt ist, dann beantworten Sie stattdessen folgende Frage. Verschlüsselt wird der Wert 17. Mit welcher Wahrscheinlichkeit erhalten sie die Geheimnachricht 8? Mit welcher Wahrscheinlichkeit die Geheimnachricht 9?

Schließen Sie daraus, dass für jeden Klartext x die Geheimnachricht eine zufällige Zahl in $\{0, 26\}$ ist. Der Geheimtext enthällt also keinerlei Information über den Klartext.

Lösung: Die 17 wird in die 8 verschlüsselt, genau wenn der Schlüssel k die Gleichung $8 = 17 + k - 27$ erfüllt, d.h., wenn $k = 18$ ist. Also ist die Wahrscheinlichkeit für diese Verschlüsselung gleich $1/27$. Das gleich gilt auch für den Geheimtext 9.

Allgemein wird x als y verschlüsselt, wenn $k = \begin{cases} y - x & \text{falls } y \geq x \\ y - x + 27 & \text{falls } y < x. \end{cases}$, d.h., es gibt genau einen Wert für k. Die Wahrscheinlichkeit ist demnach $1/27$.

Also ist der Geheimtext eine zufällige Zahl in $\{0, 26\}$.

(b) (3 Punkte) Wir verschlüsseln nun ein Wort x_1x_2 der Länge zwei, indem wir zwei Schlüssel k_1 und k_2 würfeln und dann x_1 mit k_1 und x_2 mit k_2 verschlüsseln. Mit welcher Wahrscheinlichkeit erhalten Sie einen bestimmte Geheimnachricht y_1y_2?

Wiederum als konkrete Formulierung. Verschlüsselt wird 15 3. Mit welcher Wahrscheinlichkeit erhält man 22 7? Mit welcher Wahrscheinlichkeit 4 9 oder irgendein anderes Paar?

Schließen Sie daraus, dass für jeden Klartext x_1x_2 der Geheimtext aus zwei zufälligen Zahlen besteht. Der Geheimtext entält also keinerlei Information über den Klartext.

Lösung: Man erhält 22 7 aus 15 3 genau wenn $k_1 = 7$ und $k_2 = 4$. Die Wahrscheinlichkeit dafür ist $1/27 \cdot 1/27$.

Allgemein muss die Gleichung aus dem ersten Item erfüllt sein für x_1, y_1 und k_1 und auch für x_2, y_2, und k_2. Es gibt also jeweils nur einen Wert für k_1 und k_2. Die Wahrscheinlichkeit ist demnach $1/27 \cdot 1/27$.

Also ist der Geheimtext eine Folge von zwei zufälligen Zahlen.

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

hfme tqjfmu lfjof spmmf

(a) (6 Punkte) Entschlüsseln Sie den Text und beschreiben Sie Ihr Vorgehen.

(b) (4 Punkte) 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: Die Aufgabe wurde von einem der Übungsgruppenleiter einer früheren Ausgabe dieser Vorlesung formuliert.

KM hat zur Lösung zunächst die Häufigkeit der vorkommenden Buchstaben bestimmt, sich dabei aber verzählt, und m als den häufigsten Buchstaben im Geheimtext bestimmt. Ich nahm dann 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.

Wenn man richtig zählt, ist f der häufigste Buchstabe im Geheimtext. Probiert man dann $e \mapsto f$, kommt man gleich auf die Lösung.

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? Man wirft also eine Münze und legt sich auf das Ergebnis fest. Man muss man der anderen Person etwas geben, was Ihr die Sicherheit gibt, dass man sich festgelegt hat, ohne mitzuteilen, auf was man sich festgelegt hat.

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) Invertieren ist schwer: Zu einem Bitstring c ist es (praktisch) unmöglich ein m zu bestimmen, so dass $h(m) = c$ gilt.

b) Eine Kollission zu finden ist schwer: 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 $c = h(t)$.

c) Sie legen sich dann auf das Bit $d \oplus e'$ fest, wobei e' das letzte Bit von t ist.

Beachte: e ist das Bit, das Bob gewählt hat. Das letzte Bit e' 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 und $c = h(m)$ in Schritt 1 geschickt hat, dann akzeptiert Alice und wir haben $e' = e$.

Die einzige Art für Bob zu schwindeln ist, dass er zwei Bitstrings m und t kennt, die sich im letzten Bit unterscheiden und für die $h(m) = h(t)$ gilt. Dann könnte er nach dem er das Bit d von Alice erhalten hat, seine Antwort davon abhängig machen, welchen Ausgang er sich für das Protokoll wünscht. Die Kenntnis eines solchen Paars ist aber unmöglich nach Eigenschaft 2).

Es ist wichtig, dass Bob sein Bit um einen zufälligen String auf 128 Bits erweitert. Er darf nicht mit einem bekannten String auffüllen, den Alice kennt oder erraten kann, etwa mit lauter Nullen. Denn dann bräuchte Alice nach dem Empfang von c nur $0 \ldots 00$ und $0 \ldots 01$ auszuprobieren.

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

Lösung: Bei GMX steht: GMX setzt als deutscher E-Mail-Anbieter und Gründungsmitglied des Sicherheitsverbunds E-Mail made in Germany höchste Maßstäbe bei den Sicherheits- und Datenschutzstandards: Innerhalb des Verbunds sind die Übertragungswege automatisch verschlüsselt und Ihre E-Mails werden garantiert nur in sicheren deutschen Rechenzentren gespeichert.

Vielleicht haben Sie beim Mailen in speziellen Fällen den Wunsch nach zusätzlichem Schutz: Wenn Sie beispielsweise sensible Inhalte wie Verträge oder Arztbriefe versenden möchten. Genau dafür bietet GMX mit der verschlüsselten Kommunikation ein geprüftes, kostenloses und auch leicht zu bedienendes Sicherheitsverfahren, das Sie auch mobil nutzen können.

Ich habe für die Videos, die Nachbereitung und das Übungsblatt etwa ☐ Stunden gebraucht.

(Angelina fertigt aus diesen Zahlen eine Statistik an. Kurt und Corinna sehen nur diese Statistik. Wir möchten wissen, ob der Schwierigkeitsgrad in etwa richtig ist.)

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