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.

(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.

(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.

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?

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

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*.

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