Universität des Saarlandes
FR Informatik

Kurt Mehlhorn und Corinna Coupette

WiSe 2021/22

Übungen zu Ideen der Informatik

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter21/ideen/

Blatt 10 Abgabeschluss: 17. 1. 2022

Aufgabe 1 (*5 Punkte*) Schauen Sie Sich die Videos zu Kryptographie an und beantworten Sie dann die folgenden Fragen zunächst, ohne nochmals auf den Folien nachzusehen. Dann können Sie gern zu den Folien zurückgehen und ihre Antworten gegebenenfalls korrigieren. Es gibt 1,25 Punkte pro Frage.

1) Welche der folgenden Analogien entspricht der symmetrischen Verschlüsselung, welche der asymetrischen Verschlüsselung?
   a) Alice kauft sich viele Bügelschlösser. Sie behält alle Schlüssel und verteilt die offenen Schlösser über die Stadt. Wenn Bob ihr eine Nachricht schicken will, legt er die Nachricht in eine Kiste und verschließt sie mit einem der Bügelschlösser. Dann lässt man die Kiste zum Empfänger transportieren.
   b) Alice und Bob kaufen sich ein Bügelschloss mit zwei Schlüsseln. Jeder bekommt einen der Schlüssel. Um der jeweils andern Person eine Nachricht zu schicken, legt man die Nachricht in eine Kiste und verschließt sie mit dem Bügelschloss. Dann lässt man die Kiste zum Empfänger transportieren.
2) Wie können zwei Parteien einen Schlüssel für ein symmetrisches Verfahren vereinbaren?
   a) Eine Partei teilt der anderen Partei den Schlüssel in einer E-Mail mit.
   b) Bei einem Treffen der beiden Parteien.
   c) Durch Verwendung von asymmetrischer Kryptographie.
3) Worauf beruht die Sicherheit des Verfahrens von Adelman, Rivest und Shamir?
   a) 1000-stellige Primzahlen zu finden ist sehr aufwendig.
   b) Multiplizieren von 1000-stelligen Zahlen ist sehr aufwendig.
   c) Faktorisieren von 1000-stelligen Zahlen ist sehr aufwendig.
4) Sei m die Nachricht, die unterschrieben werden soll, und sei $s = D(m)$. Was ist die unterschriebene Nachricht m.
   a) Der Text s.
   b) Das Paar (m, s).
   c) Der Text m.

Lösung: 1a ist asymmetrisch, 1b ist symmetrisch. 2b und 2c sind richtig, 3c und 4b.

Aufgabe 2 (*5 Punkte*) Bob möchte die Nachricht m verschlüsselt und signiert an Alice schicken. Beide benutzen Public Key Kryptographie. Die Verschlüsselungsfunktionen E_{Bob} und E_{Alice} sind allgemein bekannt. Wie geht Bob vor? Wie verifiziert Alice die Unterschrift?

Lösung:

1) Bob signiert m indem er das Paar (m, s) erzeugt, wobei $s \leftarrow D_{\text{Bob}}(m)$. Sei $\#$ ein Buchstabe, der sonst nicht benutzt wird.

2) Bob schickt $c \leftarrow E_{\text{Alice}}(m\#s)$ an Alice.

3) Alice entschlüsselt und berechnet $m\#s \leftarrow D_{\text{Alice}}(c)$.

4) Sie verifiziert $m = E_{\text{Bob}}(s)$. Falls keine Gleichheit besteht, bricht Alice ab. Andernfalls akzeptiert sie.

Aufgabe 3 (*5 Punkte*) Bob möchte die Nachricht m verschlüsselt und signiert an Alice schicken. Beide benutzen Public Key Kryptographie. Die Verschlüsselungsfunktionen E_{Bob} und E_{Alice} sind allgemein bekannt.

Hier sind zwei mögliche Protokolle.

1) Bob erzeugt das Paar (m, s), wobei $s \leftarrow D_{\text{Bob}}(m)$. Das Paar (s, m) ist die von Bob unterschriebene Nachricht m. Die Gleichheit $m = E_{\text{Bob}}(s)$ beweist, dass Bob die Nachricht unterschrieben hat. Sei $\#$ ein Buchstabe, der sonst nicht benutzt wird.

2) Bob schickt $c \leftarrow E_{\text{Alice}}(m\#s)$ an Alice.

3) Alice entschlüsselt und berechnet $m\#s \leftarrow D_{\text{Alice}}(c)$.

4) Sie verifiziert $m = E_{\text{Bob}}(s)$. Falls keine Gleichheit besteht, bricht Alice ab. Andernfalls akzeptiert sie.

Oder

1) Bob verschüsselt m mit dem öffentlichen Schlüssel von Alice, sei $c \leftarrow E_{\text{Alice}}(m)$.

2) Bob signiert c und erzeugt das Paar (c, s), wobei $s \leftarrow D_{\text{Bob}}(c)$.

3) Bob schickt das Paar (c, s) an Alice.

4) Alice benutzt E_{Bob} und verifiziert $c = E_{\text{Bob}}(s)$. Falls keine Gleichheit besteht, bricht Alice ab.

5) Alice berechnet $D_{\text{Alice}}(c)$ und bekommt m zurück.

Bob streitet ab, dass er das Dokument m unterschrieben hat. Es kommt zum Rechtsstreit. Wie argumentiert Alice, dass Bob unterschrieben haben muss? Bei dem ersten Protokoll? Bei dem zweiten Protokoll?

Jeder Kryptoexperte wird vor Gericht bezeugen, dass nur Bob zu einer Nachricht m eine Unterschrift s mit der Unterschriftseigenschaft $m = E_{\text{Bob}}(s)$ erzeugen kann.

Lösung:

Beim ersten Protokoll: Alice kommt mit dem Paar (m, s) zum Gericht und bittet den Richter, zunächst $E_{\text{Bob}}(s)$ zu berechnen und dann die Gleichheit $m = E_{\text{Bob}}(s)$ zu verifizieren. Dann ruft sie den Kryptoexperten also Zeugen auf.

Beim zweiten Protokoll: Alice kommt mit dem Paar (c, s) und der Nachricht m zu Gericht. Sie kann vor Gericht beweisen, dass nur Bob aus c das Paar (c, s) erzeugen kann. Sie kann also beweisen, dass Bob das c unterschrieben hat. Dann rechnet sie vor, dass $c = E_{\text{Alice}}(m)$. Sie kann aber nicht beweisen, dass Bob das c aus m berechnet hat. Bob könnte zum Beispiel behaupten, dass ihm jemand beigebracht hat, wie man digital unterzeichnet, und er das an dem Unsinnstext c erproben sollte.

Aufgabe 4 (*5 Punkte*) Betrachten Sie den folgenden mit dem Caesar-Verfahren verschlüsselten Text:

Glh Yruohvxqj lvw ulfkwlj lqwhuhvvdqw

Entschlüsseln Sie den Text und beschreiben Sie Ihr Vorgehen. Beachten Sie, dass wir den Wortzwischenraum als Wortzwischenraum verschlüsselt haben.

Lösung: Im Geheimtext kommt l fünfmal vor, h dreimal vor, v viermal vor, ... Ich vermute, dass e auf einen dieser Buchstaben abgebildet wird.

Ich probiere $e \mapsto \ell$ für die Verschlüsselung und bekomme zea Rknhaoqjc eop neYdpec ejpanaooWjp. Das ist es wohl nicht.

Ich probiere $e \mapsto v$ für die Verschlüsselung und bekomme Unsinn.

Ich probiere $e \mapsto h$ und bekomme "*Die Vorlesung ist richtig interessant*".

Aufgabe 5 (*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 6 (*5 Punkte*) (Eine Münze werfen, wenn die Teilnehmer nicht im gleichen Raum sind). 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 ihrer Münzwürfe mitteilen und garantieren, dass keiner schummelt? Man wirft also eine Münze und legt sich auf das Ergebnis fest. Dann 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. Zumindest eine der beiden Seiten muss das machen.

Überlegen Sie sich zunächst eine analoge Lösung mit Kisten und Bügelschloss. Bob hat eine Kiste und ein Bügelschloss mit einem Schlüssel. Er ...

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: Zuerst die analoge Lösung. Bob wirft seine Münze, schreibt das Ergebnis auf einen Zettel, legt den Zettel in die Kiste, verschließt die Kiste und schickt die Kiste an Alice. *Er behält den Schlüssel.* Nun hat sich Bob festgelegt. Da Alice die Kiste nicht öffnen kann, weiß sie nur, dass Bob sich festgelegt hat, aber nicht auf was.

Nun wirft Alice ihre Münze und teilt Bob das Ergebnis mit.

Nachdem Bob das Ergebnis erhalten hat, schickt er Alice den Schlüssel. Alice öffnet die Kiste und kennt nun Bobs Münzwurf.

Und nun die digitale 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 7 (*Zusatzaufgabe, 5 Punkte*) Finden Sie heraus, wie Sie Ihre emails signieren und/oder verschlüsseln können und schicken Sie KM oder CC eine signierte Email. Die 5 Punkte gibt es, für das Verschicken einer signierten email.

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.

(Ann-Sophie 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 ☐