Eidgenössische
Technische Hochschule
Zürich
Institut für Verhaltenswissenschaft
Departement Informatik

Einführung in die (kryptografischen) Wahlprotokolle (e-Voting)

Ein Leitprogramm in Informatik

Fach	Angewandte Kryptografie
Schultyp	Fachhochschule
Adressaten	Informatikstudenten ab dem 5. Semester
Voraussetzungen	Klassische, Moderne und Public Key Kryptografie, sowie vertiefte Kenntnisse der Zahlentheorie
Bearbeitungsdauer	8 Lektionen
Autor	Giovanni Serafini
Betreuer	Prof. Dr. Juraj Hromkovic
Fassung vom	27. September 2005
Schulerprobung	Erfolgt, am 7. und am 14. September 2005

"It's not the voting that's democracy, it's the counting."

Tom Stoppard, Britischer Dramatiker, 1972

Einführung und Motivation

Sie sind es als Stimmberechtigter wahrscheinlich gewohnt, Ihren Wahlzettel direkt und persönlich in die Urne im Wahlbüro zu legen. Diese Form der Stimmabgabe ist die älteste, die noch heute praktiziert wird und ist oft ein Zeichen eines gewissen Missvertrauens gegenüber den Behörden. Sie möchten ja nicht, dass jemand Ihren Stimmzettel sieht und Ihre politischen Präferenzen erfährt...

Wenn Sie unserer Behörden besonders vertrauen, stellen Sie Ihren Wahlzette in einem Wahlcouvert direkt der Gemeinde- oder Stadtkanzlei per Post zu.

Egal ob Sie per Post abstimmen oder ob Sie den Weg zum Wahlbüro wählen, Sie möchten Ihre Stimme abgeben und sicherstellen, dass „alles reibungslos" abläuft. Hinter dem Ausdruck „alles reibungslos" verstecken sich präzis regulierte Interaktionen zwischen dem Wähler und den Beamten. Alle diese Interaktionen definieren ein sogenanntes Protokoll – Sie kennen ja viele Protokolle aus der Kryptografie oder aus der Netzwerktechnik. Und da es um ein Protokoll geht, das mit Wahlen zu tun hat, nennen wir es **Wahlprotokoll**.

Warum sind Wahlprotokolle überhaupt wichtig?

Wir leben im 21. Jahrhundert, in der Gesellschaft der Information und der Globalisierung. Wir sind es gewohnt, bequem von zu Hause aus unsere Bücher zu bestellen oder unsere Zahlungen am Monatsende via e-Banking zu erledigen. Dem Internet sei Dank. Wenn wir schon so viel Zeit vor unserem PC verbringen, warum sollen wir nicht auch unsere Pflichten als Bürger (sprich unsere Stimme abgeben) wann und wo wir wollen wahrnehmen.?

Das Zauberwort in diesem Kontext heisst Electronic-Voting (kurz e-Voting).

Möglicherweise würde die erhöhte Flexibilität bei der Abgabe der eigenen Stimme via e-Voting der schweizer Demokratie neuen Schwung verleihen. Die Frage, ob die Gleichung „e-Voting = more voters" überhaupt stimmt wird uns wohl die unmittelbare Zukunft beantworten.

Falls Sie auch gerne Ihre Stimme übers Internet abgeben würden und mehr über die dahinter verstecken Protokolle erfahren möchten, sollten Sie unbedingt dieses Leitprogramm in Angriff nehmen.

Worum geht es in diesem Leitprogramm?

Mit der Hilfe dieses Leitprogrammes werden Sie eine Einführung in das Gebiet der „kryptografischen Wahlprotokolle" *selbstständig* erarbeiten.

Was wissen Sie schon?

Im Laufen des Semesters haben Sie viele Grundlagen aus der Kryptografie und aus der Mathematik erarbeitet.

Sie haben gelernt, dass die Kryptografie mit einer besonderen Branche der Mathematik eng verknüpft ist – die Rede ist von der Zahlentheorie.

Sie kennen die Anatomie des Data Encrytion Standards (DES) und wissen, dass der DES auf der „geschickten Kombination" von Permutation, Substitution und XOR-Verknüpfung von Bits basiert. Alle modernen Verschlüsselungsverfahren weisen dieses Merkmal auf!

Die Verschlüsselung mit nur einem (symmetrischen) Schlüssel ist Ihnen also vertraut!

Sie kennen die Definition von Public Key Kryptosystem und können die wichtigsten asymmetrischen Verfahren zur Verschlüssung und zur Signierung anwenden. Der mathematische Hintergrund dieser Verfahren wurde sorgfältig analysiert und die Sicherheit, bzw. einige Angriffsmöglichkeiten auf das Verfahren wurden aufgeführt und begründet.

Was werden Sie nach der Bearbeitung des Leitprogrammes können?

In diesem Leitprogramm werden Sie lernen, wie dank dem Einsatz kryptografischer Massnahmen Protokolle für Wahlen in einer offenen IT-Infrastruktur (z.B. im Internet) entwickelt werden können, so dass trotz der latenten Bedrohungslage die elementaren Sicherheitanforderungen erfüllt werden.

Was genau mit dem Begriff „elementare Sicherheitsanforderungen" verstanden wird, wird auf den kommenden Seiten aufgeführt.

Inhaltsverzeichnis

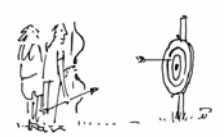
Verzeichnis der Abbildungen

Arbeitsanleitung

Wie sind die einzelnen Kapitel organisiert?

Das Leitprogramm besteht aus vier Kapitel, welche immer die gleiche Struktur aufweisen:

Übersicht
Welches Thema wird in diesem Kapitel behandelt?



Lernziele
Was werden Sie nach der Bearbeitung dieses Kapitels können?

:=	i		
Definition	**Information**	**Wissenssicherung**	**Aufgabe**

Lernkontrolle
Hier können Sie überprüfen, ob Sie alles verstanden haben. Haben Sie alles verstanden? Falls ja, können Sie ruhig weiter zum Kapiteltest beim Dozenten oder beim Tutor gehen.

Lösungen
Die Musterlösungen zu allen vorgestellten Übungsaufgaben.

Kapiteltest
Nachdem Sie einen Kapitel bearbeitet haben, müssen Sie zum Dozenten (oder zu einem Tutor) gehen und die Testfragen holen. Wenn Sie die Testfragen beantworten können, werden Sie dann mit dem Studium des folgenden Kapitels starten können.

Und was tun, falls man etwas nicht versteht?

Wenn Sie mit einem Abschnitt richtig Mühe haben oder wenn Sie ein Kapitel schon mehrmals gelesen haben, aber Sie nicht fortwärts kommen, dann ist es empfehlenswert, dass Sie eine Kollegin oder einen Kollegen um Hilfe bitten.

Wenn auch zu Zweit die Zweifel nicht verschwinden, dann dürfen Sie zum Dozenten gehen.

Kapitel 1: Die Ursprünge der Stimmabgabe

One man shall have one vote.
John Cartwright, 1780

Übersicht

Worum geht es in diesem Kapitel?

Das Bedürfnis, der Gesellschaft eine Struktur zu geben ist fast so als wie die Menschheit. Die griechischen Philosophen Aristoteles und Plato haben sich schon 400 Jahre vor Christus mit der sogenannten „politischen Philosophie" auseinandergesetzt: diese Philosophen haben sich u.a. die Frage gestellt, wie man die Verteter des Volkes – falls solche überhaupt nötig waren – zu wählen sind. Die Frage nach geeigneten Wahlprotokollen ist also alles andere als neu.

In diesem Kapitel werden Sie Ihre Reise durch die Wahlprotokolle anhand eines kuriosen Exkurses aus der Geschichte anfangen: Sie werden nicht bis zu den alten Griechen zurückkehren müssen, sondern nur bis ins 18. Jahrhundert, in die USA.

Was wissen Sie schon?

Sie, als Schweizer Bürger oder Schweizer Einwohner, kennen sich in den Belangen der Wahlen und Abstimmungen sehr gut aus – nicht umsonst ist in der Schweizer direkten Demokratie der Bürger verpflichtet mehrmals im Jahr seine Meinung auf einen Stimmzettel abzugeben.

Und dass eine Stimme geheim und unverfälscht bleiben soll ist Ihnen klar.

Was werden Sie neu lernen?

Wussten Sie auch, dass in dem 19. Jahrhundert in Missouri Abstimmungen und Wahlen nach dem so genannten „Voice-Voting" Prinzip stattgefunden haben? Falls Sie die Geschichte der USA nicht so im Detail kennen – es ging mir übrigens auch so – werden Sie in diesem Kapitel die Gelegenheit bekommen, diese Lücke zu schliessen.

Sie werden erfahren, wie man es gewohnt war, im Jahre 1846 in Missouri seine Stimme abzugeben. Und Sie werden selber feststellen können, dass dieses Abstimmungsprozedere viele Gefahren in sich birgt.

Übrigens: falls Sie sich für Kunst interessieren, werden Sie auch eine Abbildung eines schönen Gemaldes einer der Abstimmungen in Missouri im Folgenden betrachten können.

Sie werden – ausgehend von dem Voice-Voting – einige der wichtigsten Begriffe der Kryptografie (wie z.B. Vertraulichkeit) wiederholen. Nicht nur das, Sie werden auch spezifische Anforderungen im Bezug auf die Sicherheit von Wahlprotokolle erfahren, bzw. formulieren können.

Lernziele

Das erste Kapitel ist auf die Sicherheitsanforderungen an Wahlprotokolle fokussiert. Nach der Bearbeitung dieses Kapitels werden Sie...

- ∅ die drei allgemeinen Anforderungen „Vertraulichkeit", „Authentizität" und „Integrität" nennen und charakterisieren können. Sie werden auch in der Lage sein, die Bedeutung dieser Anforderungen anhand konkreter Beispiele aufzuführen können.
- ∅ vier zusätztliche Anforderungen an ein Protokoll für Wahlen nennen, sowie ihre Bedeutung anhand von Beispielen aufführen können.
- ∅ den Begriff „Voice Voting" kennen und dessen Ablauf, samt Sicherheitsproblemen, erklären können.

Ablauf des Kapitels

Auf den kommenden Seiten werden Sie zuerst eine Abbildung aus dem Jahre 1846 finden. Ihnen wird erklärt worum es auf der abgebildeten Versammlung geht, dies kompakt, auf einer halben Seite.

Sie werden sich danach mit drei Beispielsituationen aus der Abbildung beschäftigen. Ausgehend von jedem Beispiel werden Sie die Gelegenheit haben, eine Definition zu erfahren und eine Aufgabe zu lösen.

Das gerade Erlernte wird in einer besonderen Übung („Wissensicherung") gefestigt, so dass Sie dann mit dem zweiten Beispiel-Block starten können. Und auch in diesem Fall werden Sie zu jedem Beispiel eine Definition lernen können.

Im Anschluss werden Sie beim Dozenten oder beim Tutor testen können, ob Sie alles korrekt verstanden haben.

Alles klar? Jetzt können Sie endlich loslegen!

Voice-Voting in Missouri, 1846

Eine Einführung

Die Art und Weise eine Abstimmung zu führen hat sich in den letzten 200 Jahren massiv verändert: die Bedeutung dieser Evolution lässt sich am besten anhand eines Gemäldes von George Caleb Bingham zeigen. Die Abbildung 1 zeigt einen Ausschnitt des angesprochenen Bildes (das vollständige Bild ist im Anhang 5 beigelegt), dessen Titel „*The County Election*" ist und aus dem Jahre 1846 stammt.

Im Gemälde wird eine Abstimmung veranschaulicht, welche vor dem Gerichtshaus von Saline County in dem Bundestat Missouri stattfindet: in der Mitte des Bildes befindet sich einen Richter, der vor einem Wähler steht. Der Wähler schwört vor dem Richter, Hand auf der Bibel, dass er stimmberechtigt ist, und dass er seine Stimme noch nicht abgegeben hat.

Da kein Wahlregister vorhanden ist, ist es Aufgabe des Richters (oder von jemanden, der dem Richter und dem Wähler nahe ist) zu überprüfen, ob jemand mehr als einmal gestimmt hat. Der Schwur auf die Bibel sollte auf jedem Fall allfällige Betrüger entmutigen.

Es war kein Recht auf eine geheime Stimme vorhanden: der Wähler musste einfach seine Stimme dem Beamten hinter dem Richter quasi „hinschreien". Jeder Beamte hat die Aufgabe, den Namen des Wählers, sowie seine Stimme auf einem Wahlheft festzuhalten. Obwohl es aus der Abbildung nicht ersichtlicht ist, ermöglicht der Einsatz von mehereren Beamten, allfällige Fehler im Wahlheft zu entdecken.

Abbildung 1: The County Election (Detail), George Caleb Bingham (aus der Quelle [1])

Auf dem Gemälde sind mehrere Menschen dargestellt, die einen Zettel in der Hand haben: diese Zettel sind keine Stimmzettel (wie man vermuten würde), da es uns bekannt ist, dass Missouri bis 1863 „Voice-Voting" angewendet hat. Wir können davon ausgehen, dass die Wähler Ihre Wahlpreferenzen sicherheitshalber notiert und mitgenommen haben.

Eine Wahlkampagne direkt beim improvisierten Wahlbüro war damals legal und üblich. Der Mann in blau mit dem Zylinder hinter dem Wähler ist einer der Kandidaten dieses Wahlganges, ein gewisser Herr E.D. Sappington – er verlor die Wahl (übrigens gegen dem Maler dieses Gemäldes) genau um eine Stimme! Sappington zeigt eine Karte mit seinem Namen, so dass die Wähler lesen können wie er heisst und für ihn wählen können.

„Voice-Voting" bietet bescheidenen Schutz gegen eine betrügerische Manipulation der Stimmenzählung: ein Beobachter hatte die Möglichkeit eine unabhängige Zählung der Stimmen zu führen – dies auf völlig legale Art und Weise, da keine Urne vorhanden ist. Auf der anderen Seite kann das Fehlen der Privacy dazu führen, dass z.B. ein Arbeitsgeber von seinen Mitarbeiern fordern kann, dass Sie abstimmen, wie er will. Ein Gauner könnte sogar Stimmen abkaufen... (Quelle [1]).

Die ersten drei Anforderungen an Voice-Voting

Das Beispiel von "Voice-Voting" ist eine ideale Ausgangslage, um genau zu definieren, welche elementaren Anforderungen an ein Wahlprotokoll gestellt werden müssen.

Eine erste Tranche von Anforderungen, die Ihnen sicher schon aus der Kryptografie bekannt sind, wird im Folgenden vorgestellt:

:=

Definition 1.1: Vertraulichkeit

Mit dem Begriff der Vertraulichkeit wird die Geheimhaltung des Inhaltes einer Nachricht verstanden, dies für alle ausser den berechtigten Ansprechpartnern.

Wird in „Voice-Voting" die Vertraulichkeit während der Stimmabgabe gewährleistet? Die Antwort ist klar – nein! Alle können zuhören, für wen der Wähler sich entschieden hat, da er seine Stimmen dem Beamten hinschreien muss.

Aufgabe 1.1

Sie haben gerade die Definition von Vertraulichkeit gelernt. Die Vertraulichkeit ist eine wichtige Anforderung an ein Wahlprotokoll.

In dieser Aufgabe geht darum, zwei Beispielszenarien aus Ihrem Studenten-Alltag zu nennen und kurz zu beschreiben, in welchen die Vertraulichkeit eine besondere Rolle spielt.

:=

Definition 1.2: Integrität

Der Begriff der Integrität bezieht sich in der IT-Sicherheit auf die unerwünschte, externe Änderung an Daten durch einen Unbefugten, z.B. während einer Übermittlung vom Sender zum Empfänger.

Die zu schützende Nachricht im Wahlprotokoll von 1846 in Missouri ist nichts anderes als das, was der Wähler dem Beamten sagt. Der Beamte hat aber die Möglichkeit, die abgegebenen Stimmen zu fälschen, indem er auf dem Wahlheft andere Stimmen notiert als diejenigen, die ihm vorgesagt wurden.

Aufgabe 1.2

Die Integrität eines Stimmzettels besagt, dass der Inhalt eines Stimmzettels nach der Stimmabgabe durch den Stimmberechtigten nicht mehr geändert werden darf.

Gibt es andere Bereiche (z.B. in der Netzwerktechnik oder im Bankwesen), in welchen die Integrität einer Nachricht besonders wichtig ist? Nennen Sie bitte zwei Beispiele, die Sie auch stichwortartig dokumentieren.

:=

Definition 1.3: Authentizität

Mit dem Begriff der Authentizität wird die Echtheit eines Benutzers, eines Rechners oder z.B eines Web-Services verstanden. Diese Echtheit ist für die betroffenen Ansprechpartner überprüfbar.

In dem obigen Wahlprotokoll ist es für ein Wähler nicht allzu schwierig sich für jemand anderen auszugeben, da keine effektive Überprüfung dessen Identität durchgeführt wird. Der Schwur auf die Bibel reicht bei Weitem nicht aus.

Aufgabe 1.3

Die Authentizität einer Person kann überall eine Rolle spielen. Wie wird an eine schriftliche Prüfung bei uns an der Fachhochschule festgestellt, dass der Kandidat tatsächlich derjenigen ist, für den er sich ausgibt? Ist diese Methode überhaupt sicher? Begründen Sie Ihre Antwort.

Sie haben sich in dem ersten Teil dieses Kapitels mit drei elementaren Anforderungen an Wahlprotokolle auseinandergesetzt. Es ist jetzt Zeit, bevor Sie die folgenden Anforderungen in Angriff nehmen, dass Sie Ihr Wissen festigen, bzw. dass Sie überprüfen, ob Sie alles korrekt verstanden haben.

Wissensicherung

In dieser Aufgabe werden Sie die drei Anforderungen Vertraulichkeit, Authentizität und Integrität anhand einer Beispielsituation wiederholen können.

Sie sind alle schon einmal zu einer Bank gegangen und haben am Schalter Geld von Ihrem Konto abgehoben. Versuchen Sie den Prozess des Geldabhebens stichwortartig zu dokumentieren und identifizieren sich wo (und wie) jene drei oben aufgeführten Anforderungen erfüllt werden.

Vier weitere wichtige Sicherheitsanforderungen

In diesem Abschnitt werden Sie vier andere Anforderungen kennenlernen, welche an Wahlprotokolle gestellt werden. Bei drei der vier folgenden Anforderungen geht es um Bedingungen, welche einen direkteren Bezug auf Wahprotokolle haben. Die Vierte ist eher allgemeiner Natur.

Definition 1.4: Autorisierung

Mit dem Begriff „Autorisierung" wird die Berechtigung gemeint, auf eine Ressource zuzugreifen oder sich an einem Prozess zu beteiligen.

In dem vorgeführten „Voice-Voting"-Prozess wird von jedem Wähler direkt bestätigt, dass er einen Recht hat, eine Stimme abzugeben. Da kein Wahlregister vorhanden ist, ist es auch unmöglich zu bestimmen, ob ihm diesen Recht tatsächlich zusteht.

Aufgabe 1.4

Um sicherzustellen, dass jemand tatsächlich einen Anspruch auf die Stimmabgabe hat, kann man sich viele Massnahmen überlegen. Wie wird das Problem gelöst, wenn Sie bei Ihrer Gemeinde ins Wahlbüro gehen und Ihre Stimme in die Urne legen wollen?

:=

Definition 1.5: Vermeidung der mehrfachen Stimmabgabe

Jeder Stimmberechtigter hat das Recht, seine Stimme genau einmal abzugeben.

Ist es beim „Voice-Voting" möglich, mehrmals abzustimmen? Grundsätzlich schon, da der Wähler sich selber zugelässt, vor dem Richter auf die Bibel zu schwören, dass er „noch nicht gewählt hat".

Aufgabe 1.5

Was könnte der Wahlbeamte beim "Voice-Voting" unternehmen, um sicherzustellen, dass ein Wähler nicht mehr als einmal seine Stimme abgibt? Formulieren Sie eine Massnahme und beurteilen Sie, ob diese Massnahme tatsächlich umsetzbar ist.

:=

Definition 6: Sichere Aufbewahrung der eingegangen Stimmen

Alle abgegeben Stimmen müssen so aufbewahrt werden, dass weder die Vertraulichkeit, noch die Integrität der Stimme beeinträchtigt werden können.

Im (oder besser gesagt vor) dem Gerichtshaus von Saline County war es wahrscheinlich unmöglich, die Stimmen sicher aufzubewahren: wo wird das Wahlheft nach der Abstimmung aufbewahrt? Darüber haben wir leider keine Information.

Aufgabe 1.6

Eine Urne samt Wahlzettel sicher aufzubewahren ist nicht so einfach. Schliesslich ist eine Urne nicht so klein... Überlegen Sie sich eine einfache Massnahme, um eine Urne im Gemeindehaus sicher aufzubewahren.

:=

Definition 7: Möglichkeit der Reproduktion des Wahlergebnisses

Aus der Definition 6 wissen wir, dass alle abgegeben Stimmen sicher aufbewahrt werden müssen. Durch die aufbewahrten Stimmen muss es dann möglich sein, die Zählung der Stimmen zu wiederholen – z.B. im Fall eines Rekurses.

Konnte man in Missouri im Jahre 1846 die Zählung der Stimmen wiederholen? Grundsätzlich ja, wenn das Wahlheft sicher aufbewahren wurde.

Wen wir uns auf die Schweiz und Ihre Gesetzeslage beziehen, werden die aufgeführten Sicherheitsanforderungen an Wahlprotokolle in dem Bundesgesetz über die politischen Rechte (BPR) und dessen Verordnung festgehalten

Der Vollständigkeit halber muss ich hier erwähnen, dass ich aus der Gesetzgebung ausschliesslich die sieben technischen Anforderungen zitiere, welche im Rahmen eines Wahlprotokolles tatsächlich erfüllbar sind. Andere drei Anforderungen werden hier „nicht weiter diskutiert, da deren Gewährleistung ein grundsätzliches, verfahrensunabhängiges Problem darstellt" (Quelle [3]).

Zusammenfassung

Ihr Selbstudium der Wahlprotokolle anhand dieses Leitprogrammes wird in wenigen Augenblicken mit der Lernkontrolle fortgesetzt. Ich möchte aber vorher die sieben Sicherheitsanforderungen an Wahlprotokolle zusammenfassen, die Sie bisher gelernt haben.

Damit eine sichere Durchführung eines Wahlprotokolles möglich ist, muss das Wahlprotokoll…

- die **Vertraulichkeit** der abgegeben Stimme garantieren
- die **Integrität** des Stimmzettels gewährleisten
- von **einem authentischen** Wähler durchgeführt werden
- von einem Stimmberechtiger (**Autorisierung**)
- die **mehrfache Stimmabgabe** vermeiden
- die **Stimmzettel sicher aufbewahren**
- und eine **Reproduktion** der Stimmergebnisse ermöglichen.

Weiter kennen Sie den Begriff „Voice-Voting" und sind Sie in der Lage, über die Einhaltung (oder nicht) der sieben Anforderung umfangreich zu argumentieren.

Die letzte Aufgabe, die Sie vor dem Kapiteltest in Angriff nehmen müssen, ist die Lernkontrolle: diese erste Überprüfung des Erlernten wird von Ihnen selbständig absolviert, ohne die Interaktion mit dem Dozenten oder mit dem Tutor. Sie machen alles alleine: zuerst müssen Sie die folgende Aufgabe lösen, danach können Sie in den Musterlösungen am Ende des Kapitel selber kontrollieren, ob Ihre Antwort korrekt ist. Falls Sie das Gefühl haben, dass Sie etwas nicht verstanden haben, lesen Sie die Abschnitte noch einmal, die für Sie kritisch waren.

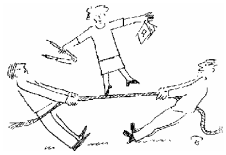
Lernkontrolle

Alle Anforderungen, welche in den vorherigen Abschnitten erläutert wurden, wurden anhand eines Beispieles (das „Voice-Voting") aus dem Jahre 1846 dargelegt.

Ihre Aufgabe besteht jetzt darin, alle Schritte der Stimmabgabe per Post zu analysieren und jeweils festzulegen, mittels welcher Massnahme jede der sieben Anforderungen gewährleistet wird.

Kapiteltest

Wenn Sie alle aufgeführten Aufgaben lösen konnten und keine offene Frage mehr haben, können Sie sich an den Dozenten oder an den Tutor wenden, um den Kapiteltest zu holen.



Lösungen zum Kapitel 1: Die Ursprünge der Stimmabgabe

Lösung zur Aufgabe 1.1

Wie Sie sich vorstellen können, sind mehrere Szenarien denkbar. Ich führe hier zwei auf, die Ihnen bei der Analyse Ihrer Lösungen hilfreich sein könnten.

1. Die Noten, welche von den Dozenten im Rahmen von Tests und Prüfungen gegeben werden, dürfen gemäss dem Datenschutzgesetzt der Allgemeinheit nicht zugänglich sein. In diesem Sinne, sollten die Dozenten und die Administration bei der Übermittlung von Noten per E-Mail Verschlüsselungsmechanismen anwenden. Die Noten sind vertraulich!
2. Studenten, welche aus Gesundheitsgründe eine Vorlesung verpassen werden aufgefordet, ein Arztzeugnis vorzuweisen. Die Arztzeugnisse müssen an einem für Unbefugte nicht zugänglichen Ort aufbewahrt werden. Auch in diesem Fall, sind die betroffenen Daten vertraulich.

Lösung zur Aufgabe 1.2

Wie bei der Aufgabe 1.1 ist auch hier möglich, die verschiedensten Lösungen zu generieren.

Als Denkanstoss stelle ich meine Lösungen vor:

1. Im Bankwesen ist es selbstverständlich, dass bei einer Geldabhebung der richtige Betrag vom Konto abgebucht wird.
2. Stellen Sie sich vor: Sie bestellen sich eine Kopie des Buches „The Da Vinci Code" bei Amazon und bekommen drei davon. Was ist mit Ihrer Bestellung passiert? Wurde Ihre Bestellung von einem Betrüger absichtlich manipuliert? Oder durch einen Übertragungsfehler zwischen der Online-Datenbank von Amazon und dem Lager wurde Ihre Bestellung unabsichtlich aufgestockt?

Lösung zur Aufgabe 1.3

Bei uns an der Hochschule für Technik Zürich gibt es keine Studentenausweise. An den mündlichen Prüfungen werden die Studenten direkt vom Dozenten identifiziert. Die Klassen sind ja klein, und der Dozent hat während des Semesters die Möglichkeit, sich zu merken, wer wer ist.

Diese Methode ist sehr pragmatisch und sicher, da die Klassen an der HSZ-T klein sind. Wie wäre es aber, wenn die Klassen aus 50 oder 60 Studenten bestehen würden?

Lösung zur Wissenssicherung

Ich werde versuchen, eine Standardsituation zu beschreiben.

1. Sie kommen in die Bank hinein und bewegen sich zum Schalter.
2. Am Schalter geben Sie Ihre Bankomat-Karte ab. Sie tippen ein PIN ein. Nur der legitimierte Besitzer der Karte kennt den PIN. Damit beweisen Sie, dass Sie tatsächlich der Besitzer der Karte sind (Authentizität). Es ist durchhaus möglich, dass Sie anstatt Ihre Bankomat-Karte, einen Ausweis vorweisen müssen. Im Extremfall könnte es sogar sein, dass der Kassenmitarbeiter Sie persönlich kennt und direkt authentifiziert.
3. Sie teilen dem Schaltermitarbeiter den Betrag mit, den Sie abheben möchten. Niemand rund um Sie hört zu. Der Mitarbeiter darf auch niemandem erzählen, dass Sie so und soviel Geld abgehoben haben (Vertraulichkeit).
4. Sie bekommen das Geld und eine Quittung und stellen fest, dass Sie tatsächlich den Betrag bekommen haben, den Sie wollten (Integrität). Und wenn auf der Quittung sowohl der alte, als auch der neue Saldo aufgeführt wird, können Sie direkt berechnent, ob die Bank den von Ihnen gewollten Betrag abgebucht hat.

Lösung zur Aufgabe 1.4

Im Wahlbüro wird von Ihnen verlagt, dass Sie einen Stimmausweis vorlegen. Sie haben in der Regel den Stimmausweis per Post bekommen. Die Echtheit des Stimmausweises wird (oberflächig) von den Wahlbeamten überprüft. Der Bestitz des Stimmausweises autorisiert Sie eine Stimme abzugeben.

In manchen Kantonen werden keine Stimmausweise im Voraus verteilt – in diesem Fall erfolgt die Autorisierung dank eines herkömmlichen Personalausweises; der Wahlbeamte sucht Ihren Name in dem Wahlregister, direkt vor der Urne. Sind Sie im Wahlregister eingetragen, werden Sie zur Wahl zugelassen.

Lösung zur Aufgabe 1.5

Mehrere Massnahmen sind denkbar. Aus meiner Sicht, könnte der Wahlbeamte – wenn er eine Stimme auf den Wahlheft notiert – durch die ganze Liste der Einträge gehen, um zu überprüfen, dass der jetzige Wähler noch nicht gewählt hat.

Diese Massnahme ist sinnvoll, jedoch kaum umsetzbar, wenn hunderte von Wähler ihre Stimme abgeben – die Überprüfung der ganzen Liste würde zu lange dauern, und wäre sicher fehleranfällig.

Zweiter Vorschlag: jeder der schon gewählt hat bekommt einen Stempel – siehe Diskos – oder so etwas, dass zwar nicht lange hält, aber zumindest den Wahltag übersteht, d.h. etwas, das jeder sehen kann und somit eine doppelte Stimmabgabe verunmöglicht. Dieses Vorgehen wurde z.B. bei den ersten Wahlen nach der Wende in Afghanistan anwendet - da hat es allerdings nicht funktioniert, da die Wähler diese Marke irgendwie löschen konnten.

Lösung zur Aufgabe 1.6

In der Regel wir eine Urne bei einem Wahlgang in der Schweiz von Wahlbeamten beobachtet. Verteter der Polizei sind auch dabei. Wenn das Wahlbüro geschlossen ist (z.B. in der Nacht vom Samstag auf dem Sonntag) wird die Urne in einem geschlossenen Raum (mit Sicherheitstür) aufbewahren. Der Schlüssel ist bei einem Wahlbeamten.

Lösung zur Lernkontrolle

Die Stimmabgabe per Post beschränkt sich auf die folgenden Schritte:

a. Sie bekommen einen Stimmrechtsausweis, sowie den Stimmzettel, per Post, eventuell eingeschrieben.

b. Sie füllen Ihren Stimmzettel aus, und legen es in ein Kuvert.

c. Sie unterschreiben den Stimmrechtsausweis und legen diesen zusammen mit dem Kuvert, in welchen sich der Stimmzettel befindet in ein anderes Kuvert. Sie schicken der Stadt- oder Gemeindekanzlei dieses Kuvert.

d. Die Stadt- oder Gemeindekanzlei bekommt das Kuvert, überprüft den Stimmrechtsausweis und legt das geklebte Kuvert (mit dem Stimmzettel) in die Wahlurne.

e. Nach dem Ablauf der Abstimmung wird die Urne geöffnet, alle Kuvert aufgemacht und die Stimmen gezählt.

f. Die Stimmzettel werden wieder in die Urne gelegt und die Urne (bis zum Ablauf der gesetzlichen Rekursfriste) sicher (z.B. in einem Safe) aufbewahren.

Werden die sieben Anforderungen erfüllt?

1. Vertraulichkeit: das Kuvert mit dem Stimmzettel wird **ungeöffnet** in die Urne gelegt. Diese Massnahme ermöglicht die Gewährleistung der Vertraulichkeit der Stimme.
2. Integrität: die Post, sowie die Wahlbeamten sind gesetzlich verpflichtet, Stimmzettel nicht aufzumachen. Es ist eine organisatorische Massnahme zur Einhaltung der Integrität (nicht nur, wie oben gesehen) der Stimme, welche gesetzlich verankert ist.
3. Authentizität: der Wähler bekommt einen Stimmrechtsausweis per Post. Auch in diesem Fall, garantiert die Post, dass alle Wähler ihre Stimmrechtsausweise bekommen. Und die Unterschrift auf dem Stimmrechtsausweis darf auch nicht gefälscht werden. Auch in diesem Fall geht es um eine organisatorisch und gesetzlich verankerte Massnahme, zur Einhaltung der Authentizität des Wählers.
4. Autorisierung: nur Stimmberechtige bekommen den Stimmrechtsausweis.
5. Mehrfache Stimmabgabe: zusammen mit dem Stimmzettel wird der Stadt- oder Gemeindekanzlei der Stimmrechtsausweis zugestellt. Ohne diesen, kann der Wähler keine Stimme mehr abgeben.

Weiterhin wird bei der Überprüfung des Stimmrechtsausweises ein Eintrag in das Wahlregister für den betroffenen Wähler gemacht, so dass er keine Stimme mehr abgeben kann.

6. Sichere Aufbewahrung der Stimmzettel: die Stimmzettel werden in der Regel in einem geschlossenen Raum, sogar in einem Safe aufbewahren.
7. Reproduzierbarkeit der Ergebnisse: da alle Stimmzettel bis zum Fristablauf sicher aufbewahren werden, ist es bis zum diesem Zeitpunkt möglich, die Stimme nochmals zu zählen.

Kapitel 2: Blinde Signaturen

You won the election, but I won the count.
Anastasio Somoza, Dictator, 1977

Übersicht

Worum geht es in diesem Kapitel?

Sie haben in dem ersten Kapitel sieben wichtige Anforderungen an ein Wahlprotokoll kennengelernt. In diesem neuen Kapitel werden wir wieder in die uns vertraute Welt der Mathematik zurückkehren und werden uns erstmals in dem vorgelegten Leitprogramm um kryptografische Verfahren kümmern. Und dass Krypto-Verfahren spannend sein können, konnten Sie bereits erleben!

Was wissen Sie schon?

Im zweiten Modul der Vorlesung Angewandte Kryptografie konnten Sie lernen, was ein Public-Key-Kryptosystem ist: Begriffe, bzw. Verfahren wie RSA, ElGamal und der Schlüsselaustausch nach Diffie und Hellman sind Ihnen vertraut.

Sie wissen, dass eine digitale Signatur keine eingescannte Unterschrift ist – Sie können eine Definition für eine digitale Unterschrift mühelos geben und können – dank den oben erwähnten Verfahren – digitale Unterschriften berechnen; weiterhin ist es Ihnen bewusst, dass eine digitale Signatur ein hervorragender Schutz gegenüber Fälschungsversuche von Nachrichten, sowie eine effektive Massnahme ist, um die Identität eines Kommunikationsteilnehmers zu gewährleisten.

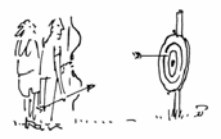
Anders gesagt, eine digitale Unterschrift ermöglicht die Einhaltung der **Integrität** und der **Authentizität** einer Nachricht.

Was werden Sie neu lernen?

In dem bevorstehenden Abschnitten werden wir den Begriff der digitalen Signatur erweitern: Sie werden lernen dass es für Alice, dank eines ausgeklügelten Vorgehens, möglich ist, von Bob eine Nachricht unterschreiben zu lassen, ohne dass Bob selber die Nachricht kennen muss.

Es mag komisch scheinen, etwas zu unterschreiben, das man nicht selber lesen oder anschauen kann, aber die praktischen Anwendungen dieses Vorgehens sind mehrere, nicht nur im Rahmen von Wahlprotokollen. Diese besondere Art von Unterzeichnung einer

Nachricht, die nicht gekannt wird, heisst übrigens „blinde Unterschrift".



Lernziele

Das zweite Kapitel des Leitprogrammes konzentriert sich auf digitale Signaturen. Nach der Bearbeitung des Kapitels werden Sie...

- ∅ den Begriff der „blinden Unterschrift" charakterisieren können, sowie den Unterschied zwischen einer blinden Signatur und einer herkömmlichen digitalen Signatur aufführen können.
- ∅ eine einfache Methode anwenden können, um eine blinde Signatur dank einem Blaukuvert und einem Kugelschreiber zu erzeugen.
- ∅ das RSA-Public-Key-Kryptosystem anwenden können, um blinde Unterschriften zu berechnen.
- ∅ wissen, was ein Blendungsfaktor ist und wie man einen Blendungsfaktor auswählt.
- ∅ erklären können, warum man eine blinde Signatur nicht fälschen kann.

Ablauf des Kapitels

In diesem Kapitel werden Sie auf den Begriff der digitalen Signatur bauen: als Erstes wird Ihnen eine Definition von blinder Unterschrift vermittelt. Danach werden Sie mit dem beigelegten Büromaterial ein Vorgehen in Angriff nehmen, um auf einfache Art und Weise blinde Signaturen zu generieren.

Sie werden dann blinde Unterschriften mathematisch charakterisieren und in einigen Übungen erfahren, wie man eine Nachricht blind unterschreibt, verifiziert und eventuell fälschen könnte.

Am Anfang war die digitale Signatur

Bevor Sie sich mit dem Hauptthema dieses Kapitels auseinandersetzen, möchte ich noch betonen, dass es sehr wichtig ist, dass Sie ganz genau wissen, wie eine digitale Signatur aufgebaut ist und wie sie berechnet wird. Dies um sicherzustellen, dass Sie dann im Folgenden die Ähnlichkeiten und die Unterschiede zwischen einer „herkömmlichen" digitalen Signatur und einer „blinden" Signatur erkennen.

Ich werde hier bewusst keine Definition von digitaler Unterschrift aufführen, da Sie sich schon lange im Rahmen dieser Vorlesung damit beschäftigen. Falls Sie diesbezüglich jedoch noch Zweifel haben würden, können Sie die Unterlagen aus der Wochen 10, 11 und 12 anschauen.

Übrigens: die Begriffe „Signatur" und „Unterschrift" sind synonym. Ich werde im Folgenden beide Begriffe benutzen – lassen Sie sich davon nicht verwirren...

Das Szenario

Das Szenario, das wir hier betrachten, ist das in der Kryptografie übliche Dreieck bestehend aus Alice, Bob und Mallory, wobei Alice und Bob die „Guten" sind (möchten miteinander sicher kommunizieren) und Mallory der „Bösewicht", der die Kommunikation abhören und möglicherweise abändern will.

:=

Definition 2.1: Blinde Signatur

Mit dem Begriff der „blinden Signatur" wird eine digitale Unterschrift bezeichnet, die Bob auf einer von Alice vorgelegten Nachricht hinzufügt, ohne den Inhalt der Nachricht zu kennen.

Die erste, wichtige Feststellung, die Sie machen sollte ist: **eine blinde Signatur ist eine digitale Signatur**. Auch wenn Sie auf einer für uns unüblichen Art und Weise generiert wird.

Blind ist eigentlich nicht die Unterschrift selber, sondern das Signaturverfahren.

Eine Frage, die Sie sich spontan stellen ist sicher die Folgende: warum soll Bob eine Nachricht unterschreiben, ohne dessen Inhalt überhaupt zu kennen? Im realen Leben würde kaum jemand von Hand ein Vertrag unterschreiben, ohne diesen zuerst durchgelesen zu haben...

Das Konzept der blinden Unterschrift – auch wenn es ein Paradoxon zu sein scheint – hat viele praktische und sehr nützliche Anwendungen – davon werden Sie sich spätestens nachdem Sie alle Kapitel des Leitprogrammes bearbeitet haben, werden selbst überzeugen. Also, noch ein bisschen Geduld!

Digitale Signaturen mit einem Blaukuvert und einem Kugelschreiber

Sie können ohne Mühe eine digitale Signatur auf einer Nachricht berechnen, dies z.B. mit dem RSA- oder mit dem ElGamal-Public-Key-Kryptosystem. Mathematisch gesehen, sind für Sie digitale Signaturen interessant, aber nicht besonders schwierig zu verstehen.

Um den Begriff der „blinden" Signatur zu verstehen, möchte ich zuerst einen kleinen Exkurs machen: wir werden zuerst veranschaulichen, wie man überhaupt eine blinde Signatur ohne der Hilfe der Kryptografie erzeugen kann.

Krimmer (Quelle [6]) führt auf einer sehr verständlichen Art und Weise auf, wie man eine blinde Signatur auf einfache Weise erzeugen kann:

> „Ursprünglich wurde dieses System von David Chaum 1982 basierend auf dem RSA Algorithmus entwickelt (...), um digitales Geld zu ermöglichen. Dieses besitzt die Eigenschaft, dass (i) jeder Geldschein, jede Münze auf die Notenbank zurückzuführen ist, die sie ausgibt, aber (ii) kein Konnex vom Geld zu seinem Besitzer herstellbar ist.
>
> Um sein Verfahren zu erklären, verwendet Chaum die Analogie zu einem Blaupapierkuvert. Man gibt das zu signierende Dokument in dieses Blaupapierkuvert, dessen Inhalt der Signierende nicht kennen darf, und lässt ihn auf dem Kuvert unterschreiben. Die Unterschrift drückt sich eins zu eins auf den Dokumentinhalt durch und man erhält ein unterschriebenes Dokument ohne dass der Signierende es je gesehen hat."

Alles klar? Dann versuchen Sie selber in der folgenden Übungsaufgabe eine blinde Unterschrift zu generieren!

Aufgabe 2.1:

In dem vorherigen Abschnitt konnten Sie erfahren, wie man mit Hilfe eines Blaukuverts und eines Kugelschreibers eine blinde Signatur einer Nachricht hinzufügen kann.

Jetzt sind Sie dran! In der Beilage zu diesem Leitprogramm werden Sie einen Blaukuvert und einen Zettel (mit einem Satz) finden.

Auf der Basis der obigen Anleitung lassen Sie eine blinde Signatur von Ihrem Tischnachbarn erzeugen.

Und mathematisch?

Sie wissen jetzt, wie man auf einfache und nachvollziehbare Art und Weise eine blinde Signatur erzeugen kann. Das Vorgehen, das oben beschrieben wurde ist einfach, aber selbstverständlich ungeeignet, um in einem Wahlprotokoll eingebunden zu werden.

Wir brauchen ja ein Vorgehen, das sich mathematisch darstellen lässt. Und ein solches Vorgehen sollte möglicherweise auf unseren bereits vorhanden Kentnissen bezüglich digitalen Signaturen beruhen.

Digitale Signaturen erfordern nicht unbedingt höhere mathematische Kenntnisse. Sie wissen schon, dass mit dem RSA- oder mit dem ElGamal-Verfahren eine digitale Signature mit nicht allzu viele Berechungen berechnet werden kann.

Eine blinde Signatur lässt sich auch – und diese ist für uns eine sehr erfreulich Nachricht - mit dem RSA-Verfahren berechnen.

Studieren Sie kurz das folgende Protokoll, dass auf dem RSA-Verfahren basiert:

Protokoll zur Berechung einer blinden Signatur mit dem RSA-Verfahren

Gegeben:

- ✓ $n = p \cdot q$, mit zwei grossen Primzahlen p und q
- ✓ (e, n) öffentlicher Schlüssel von Bob
- ✓ d privater Schlüssel von Bob
- ✓ M geheime Nachricht von Alice.

Zusammenfassung:

- ✓ Alice erhält von Bob eine blinde Signatur S auf die Nachricht M.
- ✓ Jeder Kommunikationsteilnehmer kann die Signatur S auf der Nachricht M selbstständig verifizieren.

1. Alice wählt einen Blendungsfaktor $k \in Z_n^*$.
   ($k \in Z_n^*$ weil später der Inverse von k benötigt wird; dieses Invers existiert nur wenn $k \in Z_n^*$)
2. Alice berechnet die geblendete Nachricht:
   $M' = M \cdot k^e \bmod n$
   und sendet sie an Bob.
3. Bob signiert M' durch
   $S' = (M')^d \bmod n$
   und sendet S' an Alice.
4. Alice entfernt die Blendung auf S' durch Berechnung von
   $S = k^{-1} \cdot S' \bmod n$
   Bobs Signatur auf M ist S.

Das Protokoll wurde aus der Quelle [4] entnommen.

Aufgabe 2.2a:

Jetzt wissen Sie, wie man das RSA-Verfahren leicht anpassen muss, damit man blinde Signaturen berechnen kann. Es ist Zeit, dass Sie es selber einmal ausprobieren.

Betrachten Sie das folgende Szenario: Bob soll eine Nachricht `M` für Alice blind unterschreiben.

Dabei betrachten Sie die folgenden Parameter:

- ✓ der Private-Key von Bob ist `d = 91`.
- ✓ sein Public-Key ist `(e,n) = (19,221)`.
- ✓ die zu unterschreibende Nachicht ist `M = 11`.
- ✓ als Blendungsfaktor wählen Sie `k = 23`.

Berechnen Sie die blinde Signatur `S`, mithilfe des oben aufgeführten Protokolles.

Aufgabe 2.2b:

Berechnen Sie jetzt die digitale Signatur von Bob auf der Nachicht `M`, mit denselben Parametern aus der Aufgabe 2.2a, dies mit dem herkömmlichen Protokoll zur Berechung digitaler Unterschriften.

Bekommen Sie diesselbe digitale Unterschrift wie bei der Aufgabe 2.2a heraus?

Warum bekommt man zwei gleiche Unterschriften?

Sie haben es in der Aufgaben 2.2a und 2.2b selber erleben können. Aus der Signatur `S'` der geblendeten Nachricht `M'` lässt sich tatsächlich eine gültige digitale Unterschrift `S` für die Nachricht `M` herleiten. Egal ob Sie die digitale Unterschrift `S` mit dem „herkömmlichen Verfahren" oder mit dem „blinden" Verfahren berechnen, kommen Sie immer auf denselben Wert.

Warum? Kann man diese Tatsache auch mathematisch begründen?

Die Antwort auf diese letzte Frage ist positiv: aus der Unterschrift `S'` der geblendeten Nachricht `M'` eine gültige digitale Unterschrift hergeleitet werden kann ist kein Zufall.

Studieren Sie den folgenden Beweis:

- ✓ Die geblendete Nachricht ist $M' = M \cdot k^e \bmod n$
- ✓ Bob signiert die geblendte Nachricht M' durch
  $S' = (M')^d \bmod n = (M \cdot k^e)^d = M^d k^{ed} \bmod n$
- ✓ Da $e \cdot d \bmod \varphi(n) = 1$ ist $k^{ed} \bmod n = k^1 \bmod n = k \bmod n$
- ✓ Damit ist $S' = M^d \cdot k \bmod n$
- ✓ Alice berechnet $k^{-1} \cdot S' \bmod n = k^{-1} \cdot M^d \cdot k \bmod n = k^{-1}\ k\ M^d \bmod n = M^d \bmod n$
- ✓ Und $M^d \bmod n$ ist nichts anders als das S, das Sie suchen.

Sind Sie überzeugt? Eigentlich haben Sie diesen Beweis schon in der Aufgabe 2.2a durchgespielt, mit konkreten Zahlen anstatt rein algebraisch.

Verifizierung einer blinden Unterschrift

Jetzt sollten alle Alarmglocken bei Ihnen läuten: Sie haben gerade gelernt, dass die herkömmliche Unterschrift und die blinde Unterschrift von Bob für dieselbe Nachricht M absolut gleich sind. Die Unterschrift ist gleich, der Signierungsprozess ist jedoch unterschiedlich.

Lässt sich die berechnete Signatur S überhaupt verifizieren wenn sie blind berechnet wurde? Die Antwort ist ja.

Warum?

Um die digitale Signatur von Bob auf einer Nachricht M zu verifizieren, geht man bekanntlich wie folgt vor:

Protokoll zur Verifizierung einer herkömmlichen Signatur mit dem RSA-Verfahren

Gegeben:

- ✓ $n = p \cdot q$, mit zwei grossen Primzahlen p und q
- ✓ (e,n) öffentlicher Schlüssel
- ✓ d privater Schlüssel von Bob
- ✓ M geheime Nachricht von Alice.
- ✓ S digitale Signatur von Bob auf der Nachricht M, $S = M^d \bmod n$.

Zusammenfassung:

- ✓ Alice verifiziert die Signatur von Bob auf M.

1. Alice verifiziert die Signatur von Bob auf der Nachricht M indem sie
   $S^e \bmod n = (M^d)^e \bmod = M^{d \cdot e} \bmod n = M$
   berechnet.
2. Alice vergleicht die Nachricht M, die sie aus der digitalen Signatur berechnet, mit der Nachricht M, die Sie Bob unterbreitet hat.
   Wenn beide gleich sind, dann ist die Signatur gültig. Ansonsten nicht.

Aufgabe 2.3a:

Ihre Aufgabe besteht jetzt darin, eine „herkömmliche" digitale Unterschrift zu verifizieren, nach dem obigen Protokoll.

Verwenden Sie dabei die folgenden Parameter:

- ✓ $n = 13 \cdot 17 = 221$ mit zwei grossen Primzahlen $p = 13$ und $q = 17$.
- ✓ $(e,n) = (11,221)$ öffentlicher Schlüssel
- ✓ und $d = 35$ privater Schlüssel von Bob
- ✓ $M = 8$ geheime Nachricht von Alice.
- ✓ $S = 70$ digitale Signatur von Bob auf der Nachricht M, $(S = 8^{35} \bmod 221 = 70)$.

Und wie verifiziert man eine blinde Unterschrift?

Protokoll zur Verifizierung einer blinden Signatur mit dem RSA-Verfahren

Gegeben:

- ✓ $n = p \cdot q$, mit zwei grossen Primzahlen p und q
- ✓ (e,n) öffentlicher
- ✓ d privater Schlüssel von Bob
- ✓ M geheime Nachricht von Alice.
- ✓ S digitale Signatur von Bob auf der Nachricht M.

Zusammenfassung:

- ✓ Alice verifiziert die Signatur von Bob auf M.

1. Alice verifiziert die Signatur von Bob auf der Nachricht M indem sie

   $S^e \bmod n = (k^{-1} \cdot S')^e \bmod n = (k^{-1})^e \cdot (S')^e \bmod n =$
   $= (k^e)^{-1} \cdot ((M')^d)^e \bmod n = (k^e)^{-1} \cdot M' \bmod n =$
   $= (k^e)^{-1} \cdot M \cdot k^e \bmod n = M$

   berechnet.

3. Alice vergleicht die Nachricht M, die sie aus der digitalen Signatur berechnet, mit der Nachricht M, die Sie Bob unterbreitet hat.

   Wenn beide gleich sind, dann ist die Signatur gültig. Ansonsten nicht.

Aufgabe 2.3b:

Ihre Aufgabe besteht jetzt darin, eine „blinde" digitale Unterschrift zu verifizieren, nach dem obigen Protokoll.

Verwenden Sie dabei die folgenden Parameter:

- ✓ $n = 13 \cdot 17 = 221$ mit zwei grossen Primzahlen $p = 13$ und $q = 17$.
- ✓ $(e, n) = (11, 221)$ öffentlicher Schlüssel
- ✓ und $d = 35$ privater Schlüssel von Bob
- ✓ $M = 8$ geheime Nachricht von Alice.
- ✓ $k = 12$ der Blendungsfaktor
- ✓ und $k^{-1} = 129$ das Invers des Blendungsfaktors
- ✓ $M' = 8 \cdot 12^{11} \bmod 221 = 8 \cdot 142 \bmod 221 = 31$ die geblendete Nachricht
- ✓ $S' = (M')^d \bmod 221 = 31^{35} \bmod 221 = 177$ die Signatur auf die geblendete Nachricht $M' = 31$.
- ✓ $S = 70$ digitale Signatur von Bob auf der Nachricht M, blind berechnet ($S = k^{-1} \cdot S' \bmod n = 129 \cdot 177 \bmod 221 = 70$).

Kann man blinde Unterschriften fälschen?

Sie wissen ja schon, dass eine herkömmliche, digitale Unterschrift, die z.B. mit dem RSA-Verfahren berechnet wird, kaum zu fälschen ist. Anders gesagt, ein Bösewicht Mallory kann sich nicht für Bob ausgeben, und anstelle von ihm eine Nachricht digital unterschreiben, ohne unentdeckt zu bleiben. Gilt dasselbe auch für blinde Unterschriften?

Schauen Sie das Protokoll zur Berechnung einer blinden Unterschrift, das oben aufgeführt wird an: es wird Ihnen sofort auffallen, dass, um eine blinde Unterschrift zu berechnen, der Private-Key vom Signierende benötigt wird. Und falls Mallory sich für Bob ausgeben will und

an seiner Stelle eine Nachricht blind unterschreiben will, muss sie unbedingt den Private Key von Bob kennen...

Aufgabe 2.4:

Blinde Unterschriften, genau so wie, herkömmliche, digitale Unterschriften lassen sich nicht fälschen. Sie haben es gerade gelernt.

In dieser Aufgabe geht es darum, dass Sie ein Szenario durchspielen, um zu sehen was passiert, falls Mallory (der Bösewicht) versucht, eine Nachricht `M` anstelle von Bob blind zu signieren.

Dabei gehen Sie folgendermassen vor:

1. Alice möchte die Nachricht `M = 10` von Bob blind unterschreiben lassen.
2. Mallory möchte eine blinde Unterschrift anstelle von Bob ausgeben; sie gibt sich bei Alice als Bob aus und berechnet die entsprechende digitalte Unterschrift `S`.
3. Alice versucht, die Unterschfit `S` mit dem Public Key von Bob zu verifizieren. Was passiert?

Dabei betrachten Sie die folgenden Paramter:

- ✓ der Private-Key von Bob ist: `d = 91`.
- ✓ sein Public-Key ist `(e,n) = (19,221)`.
- ✓ die zu unterschreibende Nachicht ist `M = 10`.
- ✓ als Blendungsfaktor wählen Sie `k = 23`.
- ✓ der Private-Key von Mallory ist `d = 29`.
- ✓ ihr Public-Key ist `(e,n) = (41,437)`

Zusammenfassung

Was haben Sie in diesem Kapitel gelernt? Ihre Arbeit hat die erhofften Früchte getragen, wenn Sie wissen, dass...

- ∅ blinde Signaturen digitale Signaturen sind, welche jedoch auf Nachrichten berechnet werden, deren Inhalt der Signierende nicht kennt.
- ∅ um eine blinde Signatur zu erzeugen, einen Blaukuvert und ein Kugelschreiber reichen. Selbstverständlich wissen Sie auch, wie man diese zwei Werkzeuge einsetzt.
- ∅ sich blinde Signaturen mit dem RSA-Verfahren berechnen lassen. Weiterhin kennen Sie das Protokoll, welches angewendet wird, um eine Nachricht blind zu unterschreiben.
- ∅ um eine blinde Signatur zu verifizieren, das übliche Verfahren zur Verifizierung digitaler Unterschriften angewendet werden kann.
- ∅ einen Blendungsfaktor (k) die Nachricht für den Signierenden Bob unlesbar macht.

Die letzte Aufgabe, die Sie vor dem Kapiteltest in Angriff nehmen müssen, ist die Lernkontrolle: diese erste Überprüfung des Erlernten wird von Ihnen selbständig absolviert, ohne die Interaktion mit dem Dozenten oder mit dem Tutor. Sie machen alles alleine: zuerst müssen Sie die folgende Aufgabe lösen, danach können Sie in den Musterlösungen am Ende des Kapitel selber kontrollieren, ob Ihre Antwort korrekt ist. Falls Sie das Gefühl haben, dass Sie etwas nicht verstanden haben, lesen Sie die Abschnitte noch einmal, die für Sie kritisch waren. Ansonsten machen Sie mit dem Kapiteltest weiter.

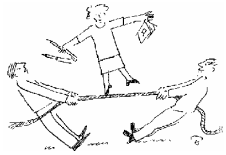
Lernkontrolle

Sie haben gelernt, dass „blinde Unterschriften" herkömmliche „digitale Unterschriften" sind, die aber ein bisschen anders berechnet werden.

Erklären Sie mit eigenen Wörter, woraus dieser Unterschied in der Berechnung der Unterschrift besteht und führen Sie auf, welche Massnahme die Erreichung dieses Zieles überhaupt möglich macht.

Kapiteltest

Wenn Sie alle aufgeführten Aufgaben lösen konnten und keine offene Frage mehr haben, können Sie sich an den Dozenten oder an den Tutor wenden, um den Kapiteltest zu holen.



Lösungen zum Kapitel 2: Blinde Signaturen

Lösung zur Aufgabe 2.1:

Die Lösung zu dieser Aufgabe lässt sich direkt aus der Beschreibung von Krimmer (Seite 28) entnehmen.

Lösung zur Aufgabe 2.2a:

1. Alice wählt als Blendungsfaktor $k = 23$ (wurde von mir vorgegeben).
2. Alice berechnet die geblendete Nachricht:
   $M' = M \cdot k^e \bmod n = 11 \cdot 23^{19} \bmod 221 =$
   $= 11 \cdot 114 \bmod 221 = 149$
   und sendet $M' = 149$ an Bob
3. Bob signiert $M' = 149$ indem er
   $S' = (M')^d \bmod n = 149^{91} \bmod 221 = 72$
   berechnet. Er sendet $S' = 72$ an Alice.
4. Alice entfernt die Blendung auf S' durch Berechnung von
   $S = k^{-1} \cdot S' \bmod n = 173 \cdot 72 \bmod 221 = 80$

Lösung zur Aufgabe 2.2b:

Bob signiert $M = 11 \bmod 221$ indem er
$S = M^d \bmod n = 11^{91} \bmod 221 = 80$
berechnet. Er sendet $S = 80$ an Alice.

Wie zu erwarten war, sind die Signaturen aus den Aufgaben 2.2a und 2.2b gleich. Die eine wurde „blind", die andere mittels des „herkömmlichen" Verfahren berechnet.

Lösung zur Aufgabe 2.3a:

- ✓ $n = 13 \cdot 17 = 221$ mit zwei grossen Primzahlen $p = 13$ und $q = 17$.
- ✓ $(e,n) = (11,221)$ öffentlicher Schlüssel
- ✓ $d = 35$ privater Schlüssel von Bob
- ✓ $M = 8$ geheime Nachricht von Alice.
- ✓ $S = 70$ digitale Signatur von Bob auf der Nachricht $M = 8$.

1. Alice verifiziert die Signatur von Bob auf der Nachricht M indem sie

   $S^e \bmod n = 70^{11} \bmod 221 = 8 = M$

   berechnet.
2. Alice vergleicht die Nachricht M, die sie aus der digitalen Signatur berechnet, mit der Nachricht M, die Sie Bob unterbreitet hat.

   Sie sind gleich, dann ist die Signatur gültig.

Lösung zur Aufgabe 2.3b:

- ✓ $n = 13 \cdot 17 = 221$ mit zwei grossen Primzahlen $p = 13$ und $q = 17$.
- ✓ $(e,n) = (11,221)$ öffentlicher Schlüssel
- ✓ und $d = 35$ privater Schlüssel von Bob
- ✓ $M = 8$ geheime Nachricht von Alice.
- ✓ $k = 12$ der Blendungsfaktor
- ✓ und $k^{-1} = 129$ das Invers des Blendungsfaktors
- ✓ $M' = 8 \cdot 12^{11} \bmod 221 = 8 \cdot 142 \bmod 221 = 31$ die geblendete Nachricht
- ✓ $S' = (M')^d \bmod 221 = 31^{35} \bmod 221 = 177$ die Signatur auf die geblendete Nachricht $M' = 31$.
- ✓ $S = 70$ digitale Signatur von Bob auf der Nachricht M,

  blind berechnet $(S = k^{-1} \cdot S' \bmod n = 129 \cdot 177 \bmod 221 = 70)$.

1. Alice verifiziert die Signatur von Bob auf der Nachricht M indem sie

   $Se \bmod n = (k^{-1} \cdot S')^e \bmod n = (129 \cdot 177)^{11} \bmod 221 = 70^{11} \bmod 221 = 8 = M$

   berechnet.
2. Alice vergleicht die Nachricht M, die sie aus der digitalen Signatur berechnet, mit der Nachricht M, die Sie Bob unterbreitet hat.

   Sind Sie gleich, dann ist die Signatur gültig.

Merken Sie sich, dass um dieses Vorgehen anzuwenden, man k^{-1} (d.h. k) kennen muss. Ab dem blau markierten Schritt ist aber die Kenntnis von k und k-1 nicht mehr nötig. Anders gesagt, ab dem blau markierten Schritt sind die Verifizierungsprotokolle der Aufgaben 2.3a und 2.3b gleich.

Lösung zur Aufgabe 2.4:

1. Alice wählt als Blendungsfaktor $k = 23$ (wurde von mir vorgegeben).
2. Alice berechnet die geblendete Nachricht mit dem Public-Key von Bob:
   $M' = M \cdot k^e \bmod n = 10 \cdot 23^{19} \bmod 221 =$
   $= 10 \cdot 114 \bmod 221 = 35 \bmod 221$
   und sendet $M' = 35$ an Mallory (die sich für Bob ausgibt)
3. Mallory signiert $M' = 35$ indem sie
   $S' = (M')^d \bmod n = 35^{41} \bmod 437 = 113 \bmod 347$
   berechnet. Er sendet $S' = 113$ an Alice.
4. Alice entfernt die Blendung auf S' durch Berechnung von
   $S = k^{-1} \cdot S' \bmod n = 173 \cdot 113 \bmod 221 = 101$
5. Alice verfiziert die Signatur von Bob auf der Nachricht $M = 10$ indem Sie $S^e \bmod n$ berechnet:
   $S^e \bmod n = 101^{19} \bmod 221 = 101$ (es ist ein Zufall)
6. Das Resultat aus der obigen Berechung ist 101. M war 10. Die Signatur wird weggeworfen.

Lösung zur Lernkontrolle

Eine blinde Unterschrift ist eine herkömmliche digitale Unterschrift.

Bei der Berechnung einer digitalen Unterschrift sieht der Signierende die Nachricht, die er zu unterschreiben hat. Dagegen, bei der Berechung einer blinden Unterschrift, sieht der Signierender nur eine geblendete Version der Nachicht, die er unterschreiben muss.

Die Nachricht, die Alice von Bob blind unterschreiben lassen will, wird mit einem Blendungsfaktor (k) „manipuliert", so dass Bob diese Nachricht nicht erkennen kann.

Alice ist die einzige Person, in der Lage ist, aus der blinden Signatur S' die Signatur S aus der Nachricht M zu entnehmen, da Sie im Besitz des geheimen Blendungsfaktors k ist.

Kapitel 3: Einfache Wahlprotokolle

Man kann das ganze Volk eine Zeit lang täuschen und man kann einen Teil des Volkes die ganze Zeit täuschen, aber man kann nicht das ganze Volk die ganze Zeit täuschen.

Abraham Lincoln

Übersicht

Worum geht es in diesem Kapitel?

In diesem Kapitel werden Sie sich mit zwei einfachen Wahlprotokollen auseinandersetzen. Die vorgestellten Wahlprotokolle wurde übrigens weltweit in verschiedenen Variationen implementiert und getestet.

Was wissen Sie schon?

Sie haben die ersten zwei Kapitel des vorgelegten Leitprogrammes bearbeitet. Dabei haben Sie gelernt, welche (sieben) Anforderungen man an ein Wahlprotkoll stellen kann. Weiter wissen Sie, wie man so genannten blinden Signaturen berechnet.

Im Grundstudium haben Sie gerlent, mit UML[1] zu arbeiten. Sie wissen was ein Sequenzdiagramm ist und können einfache Sequenzdiagramme ohne grosse Mühe vorbereiten.

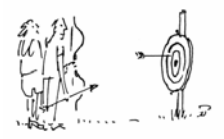
Um dieses Kapitel zu verstehen brauchen Sie eigentlich nichts mehr.

Was werden Sie neu lernen?

In diesem Kapitel werden Sie sich mit zwei Wahlprotokollen beschäftigen: Sie werden die daran beteiligten Akteure kennenlernen, sowie ihre Aufgaben untersuchen. Weiterhin werden Sie Grundsatzaussagen über die Sicherheit der Protokolle herleiten, bzw. wahrnehmen.

Parallel dazu wird Ihnen einen Gefühl für die Schwierigkeit der Überprüfung der sieben Sicherheitsanforderungen vermittelt.

[1] UML: Unified Modeling Language; eine standardisierte Beschreibungssprache für Strukturen und Abläufe in objektorientierten Programmsystemen (aus wikipedia.de).



Lernziele

In dem dritten Kapitel dieses Leitprogrammes werden Sie zwei einfache Wahlprotokolle lernen. Am Ende des Kapitels werden Sie in der Lage sein,...

- ∅ die drei Akteure in den behandelten Wahlprotokollen zu nennen, sowie ihre Aufgaben zu beschreiben.
- ∅ ein naives Wahlprotokoll durchzuführen, sowie die Gründe seiner Unsicherheit zu beschreiben.
- ∅ ein zweites Wahlprotokoll aufzuführen, das die Mängel des naiven Wahlprotokolls behebt, aber trotzdem für Angriffe anfällig bleibt. Sie werden auch wissen, welche konkrete Art von Bedrohung die Sicherheit des Protokolles beeinflusst.
- ∅ für das zweite Wahlprotokoll zu erklären, warum eine Wählerin Eve nicht erfahren kann, wie ihre Kollegin Alice gewählt hat.
- ∅ aufzuführen, dass der Administrator und das Zählsystem vertrauenswürdig sein müssen.

Ablauf des Kapitels

Dieses Kapitel ist in zwei Bereiche aufgeteilt, in welchen je ein Wahlprotokoll beschrieben wird. Sie werden zu jedem Wahlprotokoll einen Theorieblock, sowie einige Übungsaufgaben absolvieren müssen.

Ein naives Wahlprotokoll

Ich werde Ihnen zuerst ein naives Wahlprotokoll erklären, das leider die Ansprüche einer realen Wahl nicht erfüllt.- dies sollte Ihnen von Anfang an klar sein. Dank diesem Protokoll werden Sie aber die (drei) Akteure in einem Wahlprokoll kennenlernen! Übrigens, in diesem Wahlprotokoll kommen Sie ohne den Einsatz der Kryptografie an Ihr Ziel.

Die folgende Abbildung stellt die drei Schritte einer Wahl nach diesem „naiven" Protokoll dar – betrachten Sie kurz, was gemacht wird.

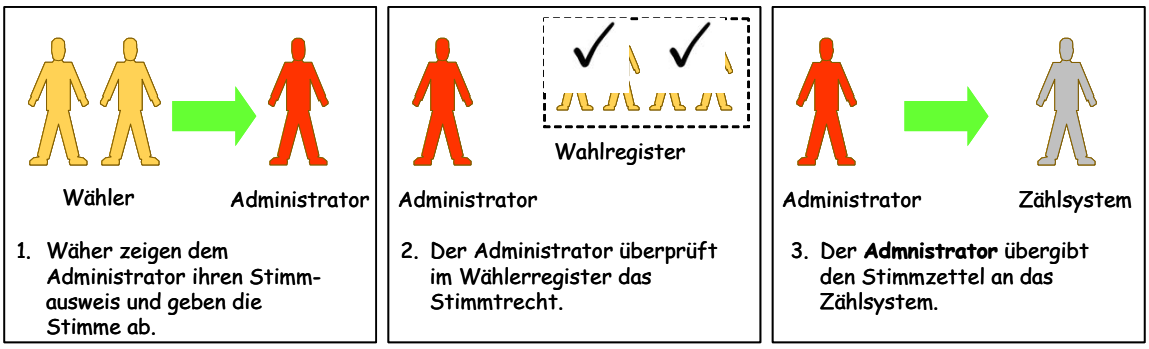


Abbildung 2: Ein naives Wahlprotokoll

Welche drei Aktuere werden benötigt, um ein Wahlprotokoll durchzuführen?

1. Der Wähler („the voter"): Sie sind damit gemeint. Sie möchten eine Stimme abgeben, um einen neuen Präsident zu wählen oder eine Gesetzesvorlage anzunehmen.
2. Der Administrator („the Validator"): damit ist die Instanz gemeint, die überprüfen muss, ob Sie überhaupt einen Recht haben, an der Abstimmung (als Wähler) teilzunehmen.
3. Das Zählsystem („the tailler"): die elektronische Urne, samt dem Programm, das die Stimmen zählt.

Aufgabe 3.1:

Diese Übungsaufgabe erfordert von Ihnen, dass Sie die drei Akteure im naiven Wahlprotokoll mit Figuren aus dem Gemälde von Bingham (siehe Kapitel 1, bzw. Anhang 4) assozieren.

Wer im Gemälde von Bingham der Wähler ist, ist eindeutig und muss nicht weiter ergeforscht werden.

a. Wer stellt aber den Administrator („the Validator") im Gemälde dar?

b. Und wer ist das Zählsystem („the Tailler")?

Aufgabe 3.2:

In dieser Übungsaufgabe werden Sie sich Gedanken über das gerade vorgestellte, naive Wahlprotokoll machen. Genauer gesagt, werden Sie drei der sieben Sicherheitsanforderungen im Bezug auf das Wahlprotoll untersuchen.

Beantworten Sie stichwortartig die folgenden Fragen:

a. Ist die Vertraulichkeit der Stimme garantiert?
b. Ist es für irgendeinen Akteur möglich einen Stimmzettel zu fälschen?
c. Kann jemand für jemand anderen eine Stimme abgeben?

Spätestens nach der Bearbeitung der ersten Übungsaufgabe ist es Ihnen klar, dass dieses naives Wahlprotokoll nie umgesetzt werden kann.

Bevor Sie die nächste Aufgabe in Angriff nehmen, möchte ich hier einige Gedanken über die sichere Aufbewahrung der Stimmzettel, sowie über die Möglichkeit der Reproduktion der Ergebnisse loswerden:

∅ Auf Grund der Angaben im gerade vorgestellten Wahlprotokoll, verfügen Sie über zu wenige Informationen, um selber zu entscheiden, ob die Stimmzettel sicher aufbewahren werden können. Sie können aber davon ausgehen, dass unverschlüsselte Stimmzettel (wie es hier der Fall ist) nicht sicher aufbewahren werden können. Das Gefahr einer Manipulation ist ja gross.

∅ Können die Ergebnisse (sprich das Resultat der Abstimmung) reproduziert werden? In der Regel, nachdem die Ergebnisse einer Abstimmung der Öffentlichkeit bekannt gegeben werden, wird ein Frist gegeben, um Rekurs einzulegen. Nach dem Ablauf der Frist werden die Wahlergebnisse genehmigt. In dem vorgestellten Protokoll könnte man grundsätzlich die Zählung der Stimmzettel wiederholen. Das Problem ist aber hier, wie oben gesehen, dass diese Stimmzettel nicht sicher aufbewahren werden können.

Aufgabe 3.3:

In der Aufgabe 3.2 haben Sie die drei ersten Sicherheits-anforderungen im Bezug auf das naive Wahlprotokoll analysiert. Jetzt wird von Ihnen erwartet, dass Sie weitere zwei betrachten.

Beantworten Sie stichwortartig die folgenden Fragen:

a. Ist es für jemand der keine Stimmberechtigung hat möglich, seine Stimme abzugeben?
b. Ist es für ein Wähler möglich mehrmals seine Stimme abzugeben?

Eine Verbesserung: das „Two Agency Protocol"

Sie werden jetzt ein Wahlprotokoll kennenlernen, das die meisten Probleme des naiven Wahlprotokolls löst. Dieses neue Protokoll setzt auch kryptografische Massnahmen um.

Gehen wir einen Schritt nach dem anderen vor! Ich möchte Ihnen zuerst alle Schritte (es sind insgesamt sechs) einer Wahl nach diesem neuen Protokoll vorführen:

1. Der Administrator verteilt eine Liste von anonymen Tags an jeden Stimmberechtigten, vor dem Beginn der Abstimmung.

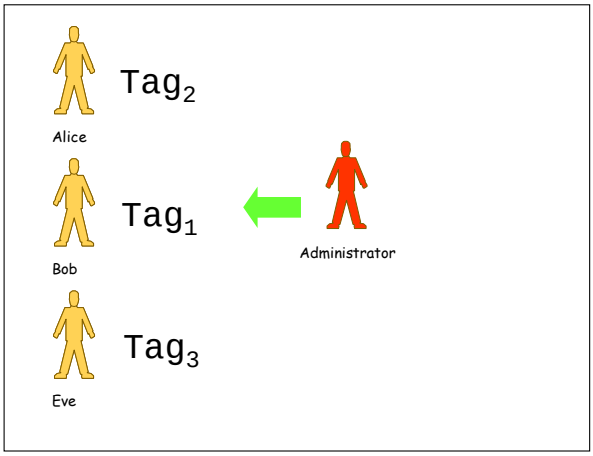


Abbildung 3: Verteilung der anonymen Tags

Information 3.1:

Mit dem Begriff Tag wird eine Art „Primary Key" gemeint, der natürlich eindeutig sein muss.

In den folgenden Aufgaben gehen wir davon aus, dass die drei Wähler Alice, Bob und Eve einen Tag vom Administrator bekommen haben. Als Tags stehen die Werte `10`, `01`, `11` zur Verfügung.

Um die kommenden Aufgaben zu lösen, müssen Sie zuerst notieren, dass Alice den Tag `10`, Bob den Tag `01` und Eve den Tag `11` bekommen haben.

Am besten können Sie die folgenden Aufgaben lösen, indem Sie die vorgeschlagenen Werten für Tags und Stimmen in die generischen Abbildungen, die Sie auf den folgenden Seiten finden einfügen.

Mit einem Begriff aus der objektorientierten Programmierung könnte man sagen, dass Sie die Abbildungen mit den vorgeschlagenen Daten „instanzieren" müssen.

2. Der Administrator lässt dem Zählsystem die Liste der verteilten, anonymen Tags zukommen.

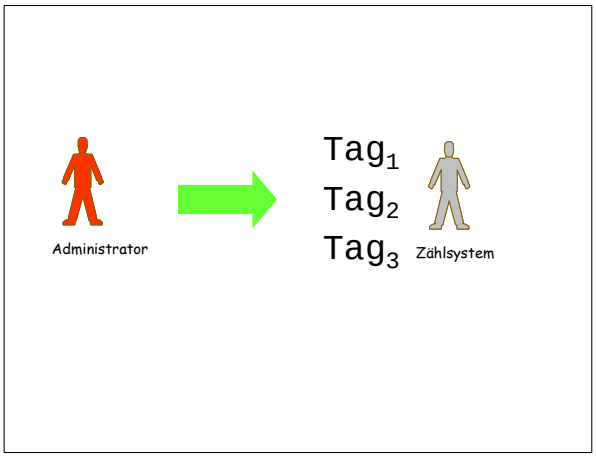


Abbildung 4: Anonyme Tags

Aufgabe 3.4:

Führen Sie die Liste der Tags auf, die das Zählsystem (auf Grund der Angaben bei der Information 3.1) vom Administrator bekommt.

3. Wenn das Abstimmungszeitfenster anfängt, schickt jeder Wähler dem Zählsystem ein Paket bestehend aus der (zusammen) verschüsselten Stimme und dem Tag, sowie dem unverschlüsselten Tag. Die Verschlüsselung erfolgt mit einer **symmetrischen Chiffre**, mit Schlüssel K. Der Schlüssel bleibt geheim.

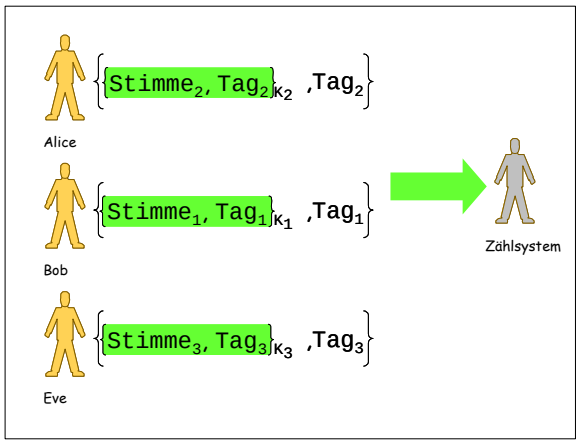


Abbildung 5: Stimmabgabe

Aufgabe 3.5:

Nehmen Sie an, dass Alice „Ja" stimmt und Bob und Alice hingegen beide „Nein" stimmen. Welche Information schickt Alice dem Zählsystem? Anders gesagt, wie sieht ihr „Paket" aus? Und Bobs? Und Eves?

4. Das Zählsystem veröffentlicht eine Liste aller anonymen Tags, samt verschlüsselten Stimmzettel, so dass jeder Wähler selber überprüfen kann, ob sein Stimmzettel dabei ist.

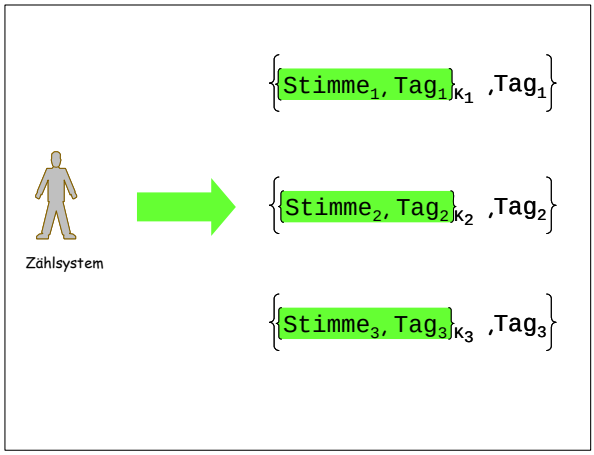


Abbildung 6: Veröffentlichung der Stimmzettel

Aufgabe 3.6:

Das Zählsystem veröffentlicht die Liste der anonymen Tags, samt verschüsselten Stimmzetteln. Führen Sie diese Liste auf für das Beispiel aus den Aufgaben 3.3 und 3.4.

5. Jeder Wähler schickt dem Zählsystem seinen symmetrischen Schlüssel. Das Zählsystem kann anhand des Schlüssels den Stimmzettel (samt Tag) enschlüsseln. Das Zählsystem hat jetzt zwei Versionen des Tags für jeden Stimmzettel: falls die zwei Tags gleich sind, wird die Stimme gezählt.

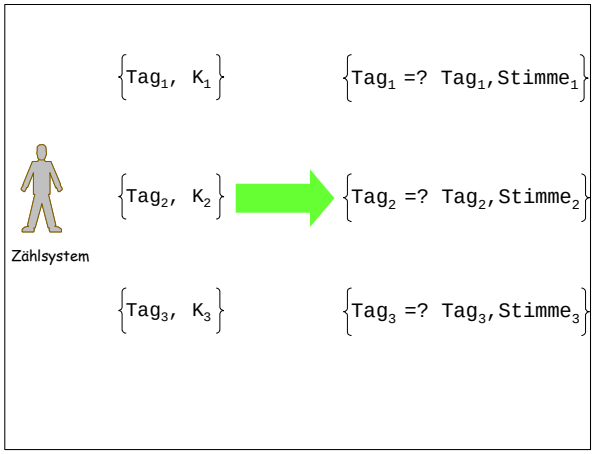


Abbildung 7: Veröffentlichung der Stimmen

Aufgabe 3.7:

Ausgehend von den Ergebnissne der Aufgabe 3.5 breiten Sie die Liste, der Tags und der Stimmen vor, die das Zählsystem veröffentlicht.

Können Alice, Bob und Eve ihre Stimmen finden?

6. Wenn die Abstimmung vorbei ist, publiziert das Zählsystem eine Liste der Stimmzettel (in Klartext), samt verschlüsselten Stimmzettel. Der Wähler kann jetzt überprüfen, ob seine Stimme geändert wurde.

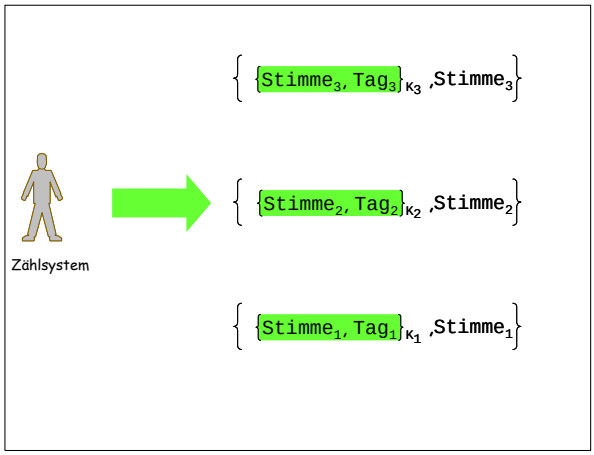


Abbildung 8: Stimmzettel und Stimmen

Aufgabe 3.8:

Ausgehend von den Ergebnissen der Aufgabe 3.7 bereiten Sie die Liste aus der obigen Abbildung vor.

Können Alice, Bob und Eve ihre Stimmen finden? Wurden Ihre Stimmen geändert?

Wissensicherung

Sie haben gerade gelernt, wie das „Two-Agency-Protocol" aufgebaut ist. Sie werden jetzt eine Möglichkeit bekommen, um Ihre Vision des Protokolles zu überprüfen.

Ich gehe davon aus, dass Sie die Sequenzdiagrammen kennen. Sie haben im Grundstudium UML gelernt und in diesem Kontext Sequenzdiagrammen geübt.

Ihre Aufgabe besteht darin, den Ablauf des Wahlprotokolles in dem folgenden Sequenzdiagramm zu vervollständigen.

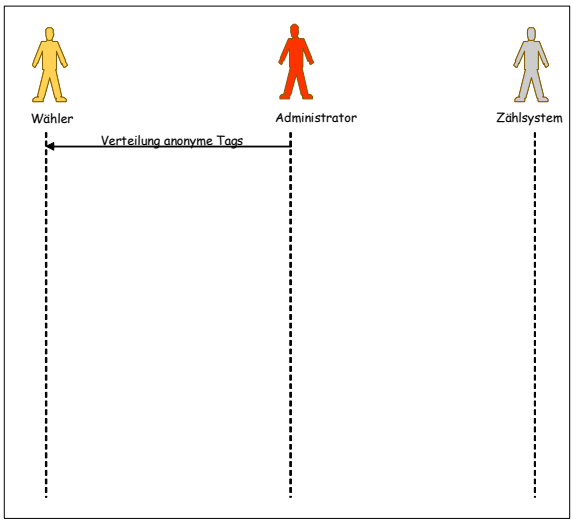


Abbildung 9: Wissensicherung Two-Agency-Protokoll

Erfüllt das vorgestellte Wahlprotokoll alle sieben Sicherheits-anforderungen?

Eine vollständige Analyse der Einhaltung der sieben Sicherheitsanforderungen erfordert eine sehr umfangreich Arbeit. Fleiss reicht aber nicht – wenn man eine formale Analyse eines Sicherheitsprotokolls durchführen möchte, werden Methoden benötigt, welche systematisch nur von einem Rechner durchgespielt werden können und dessen Aufwand (leider) in der Regel subexponentiell ist.

Wer mehr davon wissen möchten, kann einen Blich auf die Home-Page des „Zürcher Information Security Center"[2] werfen und das Projekt „AVISPA" suchen.

Für unser Leitprogramm hat diese Tatsache eine klare Bedeutung: anstatt formal nach Schwachstellen in dem gerade aufgeführten Protokoll zu suchen, werden wir „makroskopische" Angriffsmöglichkeit erforschern – es ist in diesen Rahmen sehr wichtig, dass ein Gefühl für die Sicherheit des Verfahrens entwickeln können.

Zu dem „Two-Agency-Protocol" lässt sich eigentlich nicht viel sagen oder schreiben: viele der Probleme des naiven Wahlprotokolls von vorher werden hier behoben. Die einzige, grosse Angriffsfläche wird vom Administrator und vom Zählsystem geboten: was passiert, wenn die beide komplottieren?

Aufgabe 3.9:

In der Aufgabe betrachten wir die zwei Wählerinnen Alice und Eve. Am Ende des Two-Agency-Wahlprotokolls möchte Eve ermitteln, wie Alice gewählt hat. Kann Sie es? Begründen Sie Ihre Antwort.

Aufgabe 3.10:

Gehen Sie davon aus, dass der Admnistrator die Wahl manipulieren möchten. Er ist, sozusagen, ein Bösewichte.

Entwerfen Sie einen Angriff auf die Vertraulichkeit der Stimme, die Alice abgibt. Anders gesagt, Ihre Arbeit besteht darin, einen Angriff vorzubereiten, in welchem der Administrator die Stimme von Alice erfährt.

Sie lösen die Aufgabe am besten, wenn Sie ein Sequenzdiagramm zeichnen.

[2] Zürich Information Security Center: http://www.zisc.ethz.ch/

Aufgabe 3.11:

In dieser Aufgabe gehen Sie davon aus, dass der Administrator und das Zählsystem eine Stimme abgeben möchten, dies anstelle des legitimierten Wählers Bob. Bob nimmt am Wahlgang nicht teil.

Entwerfen Sie ein Szenario, welches diesen Angriff umsetzt.

Sie lösen die Aufgabe am besten, wenn Sie ein Sequenzdiagramm zeichnen.

Die letzte Aufgabe, die Sie vor dem Kapiteltest in Angriff nehmen müssen, ist die Lernkontrolle: diese erste Überprüfung des Erlerntes wird von Ihnen selbständig absolviert, ohne die Interaktion mit dem Dozenten oder mit dem Tutor. Sie machen alles alleine: zuerst müssen Sie die folgende Aufgabe lösen, danach können Sie in de Musterlösungen am Ende des Kapitel selber kontrollieren, ob Ihre Antwort korrekt ist. Falls Sie das Gefühl haben, dass Sie etwas nicht verstanden haben, lesen Sie die Abschnitte noch einmal, die für Sie kritisch waren. Ansonsten, falls alles reibungslos gelaufen ist, machen Sie mit dem Kapiteltest weiter.

Lernkontrolle

In dieser Aufgabe werden Sie ein Sequenzdiagramm entwerfen müssen, auf der Basis des bereits in der Lernkontrolle Vorbereiteten.

Hier betrachten wir einen Auschnitt der gesamten Landschaft der Stimmberechtigen, der aus der Wählerin Alice besteht.

Alice bekommt vom Administrator den Tag `101` und entscheidt sich, „`Ja`“ zu stimmen.

Ihre Aufgabe besteht darin, das Sequenzdiagramm für die Stimmabgabe von Alice anhand des Two-Agency-Wahlprotokolls zu zeichnen.

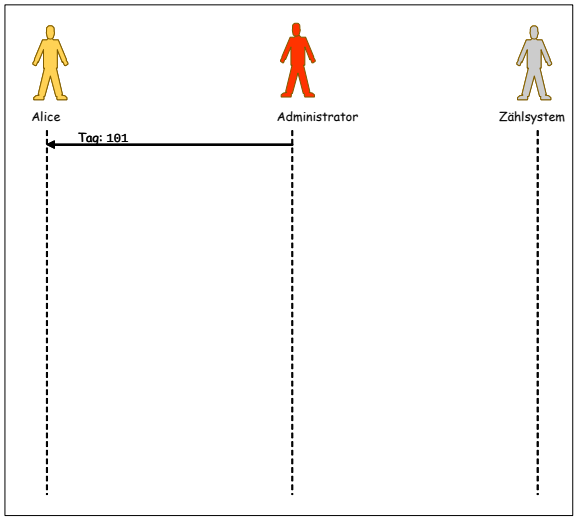
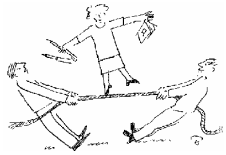


Abbildung 10: Lernkontrolle Kapitel 3

Kapiteltest

Wenn Sie alle aufgeführten Aufgaben lösen konnten und keine offene Frage mehr haben, können Sie sich an den Dozenten oder an den Tutor wenden, um den Kapiteltest zu holen..



Lösungen zum Kapitel 3: Einfache Wahlprotokolle

Lösung zur Aufgabe 3.1:

a. Der generisch aufgeführten Administrator im naiven Wahlprotokoll entspricht dem Richter im Gemälde von Bingham.

b. Das Zählsystem im naiven Wahlprotokoll könnte dem Beamten entsprechen. Ich schreibe „könnte", da es in der Literatur nicht explizit erwähnt wird, wer die Aufgabe, die Stimmen zu zählen, übernommen hat.

Lösung zur Aufgabe 3.2:

a. Die Vertraulichkeit der abgegeben Stimme ist nicht garantiert: der Administrator nimmt den Stimmzettel entgegen und leitet diesen dem Zählsystem weiter. Er kann ohne Mühe die Stimme lesen.

b. Der Administrator, noch einmal er, hat die Möglichkeit einen entgegengenommenen Stimmzettel mit einem eigenen zu ersetzten. Die Integrität der Stimme ist nicht garantiert.

c. Grundsätzlich kann kein Wähler für jemand anderen eine Stimme abgeben, da die Stimmausweise vom Administrator überprüft werden. In der Praxis kann aber der Administrator selber eine Stimme abgeben, dies für jemanden der an der Wahl nicht teilgenommen hat, eventuell kurz vor der Schliessung der Urne – der Administrator hält ja im Wahlregister fest, wer gestimmt hat und wer nicht. Die Authentizität des Wählers ist nicht gewährleistet.

Lösung zur Aufgabe 3.3:

a. Nur Wähler sind berechtigt eine Stimme abzugeben. Der Stimmausweis authorisiert sie dazu. Wie aber diese Stimmausweise (und ob sie fälschungssicher sind) ist im Protokoll nicht festgehalten. Der Admnistrator könnte sich das Recht nehmen, wie in der vorherigen Aufgabe gelernt, eine Stimme für einen stimmberechtigten Wähler abzugeben.

b. Da ein Wahlregister geführt wird, kann man davon ausgehen, dass ein Versuch, eine Stimme mehrmals abzugeben entdeckt werden

würde.

Lösung zur Aufgabe 3.4:

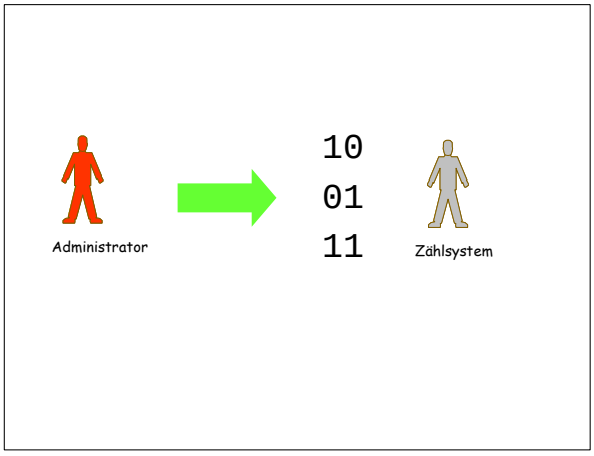


Abbildung 11: Lösung Aufgabe 3.4

Lösung zur Aufgabe 3.5:

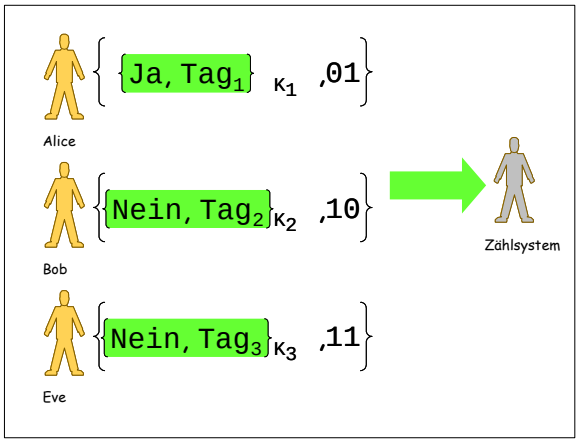


Abbildung 12: Lösung Aufgabe 3.5

Lösung zur Aufgabe 3.6:

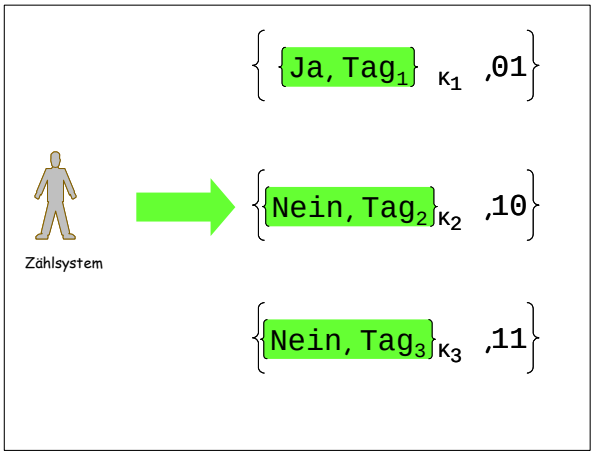


Abbildung 13: Lösung Aufgabe 3.6

Lösung zur Aufgabe 3.7:

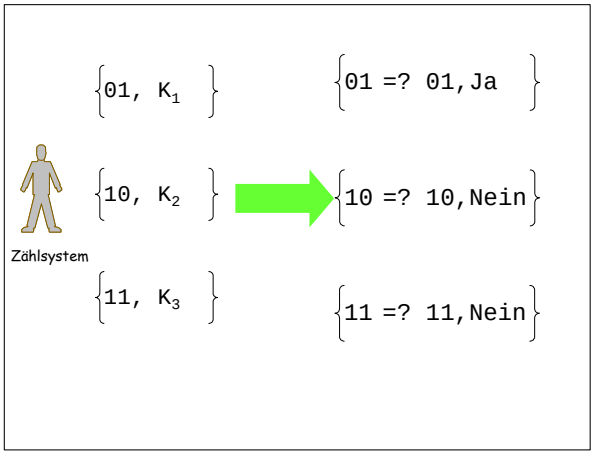


Abbildung 14: Lösung Aufgabe 3.7

Lösung zur Aufgabe 3.8:

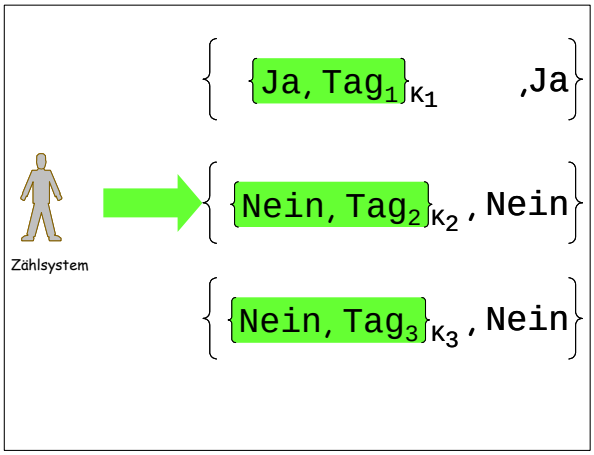


Abbildung 15: Lösung Aufgabe 3.8

Lösung zur Aufgabe 3.9:

Eve kann die Stimme von Alice nicht sehen. Eve, wie alle Wähler, hat Zugriff zur Liste mit den Tags und den jeweiligen Stimmen. Eve kennt aber nicht welcher Wähler sich hinter welchem Tag versteckt.

Die Vertraulichkeit der Stimme von Alice ist in diesem Fall gewährleistet.

Lösung zur Aufgabe 3.10:

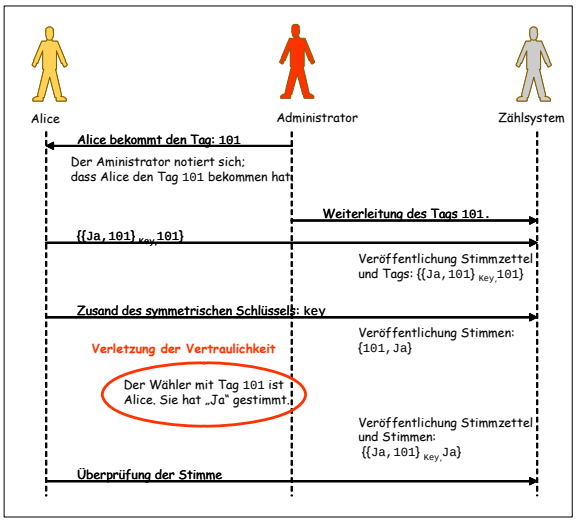


Abbildung 16: Lösung Aufgabe 3.9

Aus diesem Angriff können Sie entnehmen, dass die Rolle des Administrators in einem Wahlprotokoll sehr wichtig ist. Der Administrator darf nicht alles machen, was er will. Er muss **vertrauenswürdig** sein – an Möglichkeiten zu betrügen (in dem Two-Agency-Wahlprotokoll) fehlt es nicht!

Lösung zur Aufgabe 3.11:

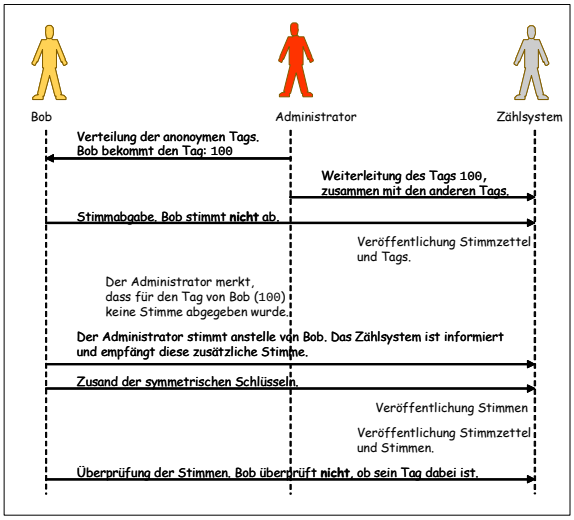


Abbildung 17: Lösung Aufgabe 3.10

Damit der Angriff erfolgreich sein kann, muss Bob seine Stimme nicht abgeben. Er soll auch nicht überprüfen wollen (im letzten Schritt), ob eine Stimme mit seinem Tag abgegeben wurde. Wenn aber Bob kein Interesse für die Wahl zeigt (er schickt seine Stimme nicht ab), wird er vermutlich auch nicht überprüfen, ob jemanden mit seinem Tag gewählt hat.

Wenn Sie nicht wählen gehen, fragen Sie auch nicht bei der Gemeinde nach, ob jemand für Sie gewählt hat?

Was lernen wir aus diesem Angriffsszenario? Sowohl der Administrator, als auch das Zählsystem müssen **vertrauenswürdig** sein.

Lösung zur Wissenssicherung:

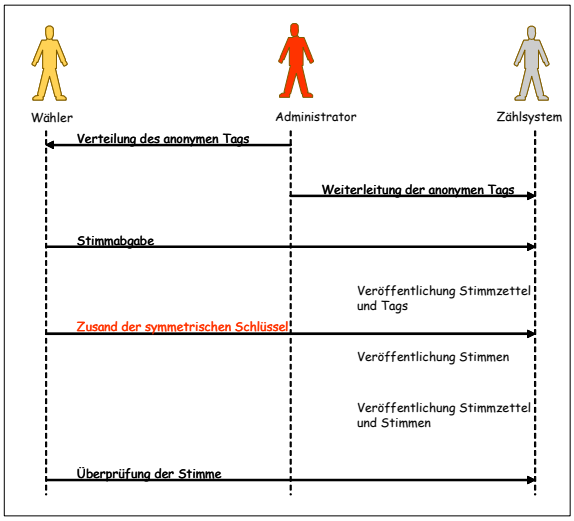


Abbildung 18: Lösung zur Wissensicherung Kapitel 3

Lösung zur Lernkontrolle

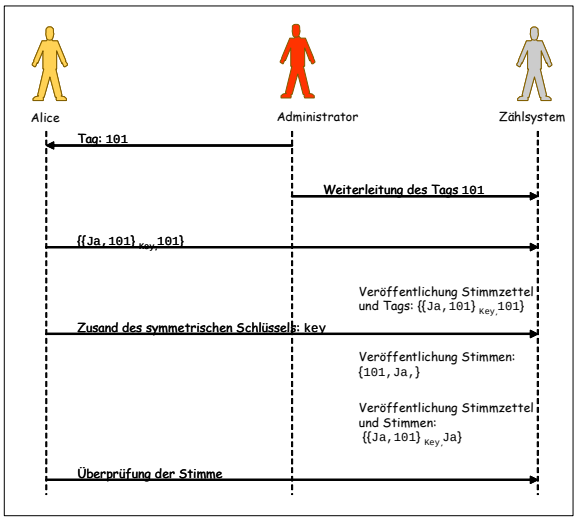


Abbildung 19: Lösung zur Lernkontrolle Kapitel 3

Kapitel 4: Blind-Signature Voting Protocol

Der Staat ist für die Menschen,
nicht die Menschen für den Staat.
Albert Einstein

Übersicht

Worum geht es in diesem Kapitel?

In diesem Kapitel werden Sie sich mit einem Wahlprotokoll beschäftigen, das auf blinde Signaturen beruht.

Was wissen Sie schon?

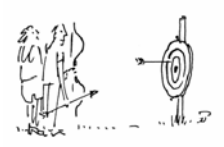
In den ersten drei Kapiteln des Leitprogrammes haben Sie gelernt, welche (sieben) Sicherheitsanforderungen an ein Wahlprotokoll gestellt werden. Sie haben diese Anforderungen im Bezug auf zwei Wahlprotokolle untersucht (jedoch nicht rein formel – das wäre fast unmöglich) und haben dabei verstanden, dass es gar nicht so einfach ist, ein Wahlprotokoll zu entwickeln, dass tatsächlich die vorgegeben Anforderungen erfüllt.

Sie können für ein Wahlprotokoll –auf Grund der Erfahrung, die Sie im Kapitel 3 des Leitprogrammes gesammelt haben – selbständig eruieren, ob eine bestimmte Sicherheitsanforderung eingehalten wird oder nicht. Dies auf der Ebene der makroskopischen Angriffsmöglichkeiten.

Blinde Signaturen sind für Sie kein Geheimnis – Sie haben im Kapitel 2 geübt, wie man sie mit dem RSA-Verfahren auf eine sehr effiziente und effektive Art und Weise berechnen kann.

Was werden Sie neu lernen?

In diesem letzten Kapitel werden Sie ein Wahlprotokoll kennenlernen, das auf blinde Signaturen beruht. Sie werden verstehen, wie blinde Signaturen bei der Gestaltung eines Wahlprotokolls hilfreich sein können und werden selber in der Lage sein, einige Runden des vorgestellten Wahlprotokolles auf Papier durchzuspielen.



Lernziele

Nach der Bearbeitung dieses Kapitels werden Sie über das folgende Know-how verfügen:

- ∅ Sie werden ein generisches Wahlprotokoll erklären können, das auf blinden Signaturen basiert.
- ∅ Sie werden den Grund des Einsatzes blinder Signaturen nennen können.
- ∅ Sie werden wissen, dass der Administrator alleine den Inhalt eines Stimmzettels nicht erfahren kann.
- ∅ Sie werden das Wahlprotokoll mit dem Einsatz des RSA-Verfahrens durchspielen können.

Ablauf des Kapitels

In dem bevorstehenden Kapitel werden Sie zuerst einen neues Wahlprotokoll kennenlernen. Sie werden sich Gedanken über einige Angriffsmöglichkeiten machen. Dann werden Sie eine konkrete Umsetzung des Wahlprotokolls kennenlernen, .die auf dem RSA-Verfahren basiert. Zu diesem Protokoll werden Sie einige numerische Beispiele durchspielen.

Ein Wahlprotokoll basierend auf blinden Signaturen

Ich werde Ihnen jetzt ein Wahlprotokoll – Schritt für Schritt, wie im vorherigen Kapitel – vorstellen, das auf blinde Unterschriften beruht:

1. Der Wähler verschlüsselt seine Stimme (mit einem symmetrischen Schlüssel K, den er geheim hält) und blendet es. Der Wähler signiert die geblendete Stimme. Danach schickt er die geblendete Stimme, sowie die Signatur dem Administrator.
2. Der Administrator überprüft die Gültigkeit der Signatur. Falls die Signatur authentisch ist und der Wähler tatsächlich stimmberechtigt ist, unterschreibt der Administrator die vom Wähler signierte, geblendete Stimme und schickt sie dem Wähler zurück.
3. Der Wähler entfernt den Blendungsfaktor und bekommt eine gültige Signatur vom Administrator auf der ürsprünglichen, ungeblendeten Stimme.
4. Der Wähler stellt dem Zählsystem seine verschüsselte Stimme samt digitaler Signatur des Administrators zu.
5. Das Zählsystem sammelt die Stimmen aller Wähler und veröffentlicht die Liste der verschlüsselten Stimmen, so dass jeder Wähler überprüfen kann, ob seine Stimme dabei ist. Dabei prüft es, ob die digitale Unterschrift auf dem Stimmzettel diejenige des Administrators ist. Falls ja, darf der jeweilige Wähler seine Stimme abgeben. Falls nein, wird die Stimme weggeworfen.
6. Der Wähler schickt dem Zählsystem sein Schlüssel K; der Wähler entschlüsselt den Stimmzettel und berechten die Ergebnisse der Wahl.
7. Das Zählsystem veröffentlicht die Liste der verschlüsselten Stimmen (samt Schlüssel), so dass jeder Wähler die Ergebnisse der Wahl selber reproduzieren kann.

Aufgabe 4.1:

Sie haben gerade gelernt, wie das „Blind-Signature Voting Protocol" aufgebaut ist. Sie werden jetzt eine Möglichkeit bekommen, um Ihre Vision des Protokolles zu überprüfen.

Ihre Aufgabe besteht darin, den Ablauf des Wahlprotokolles in dem folgenden Sequenzdiagramm zu vervollständigen.

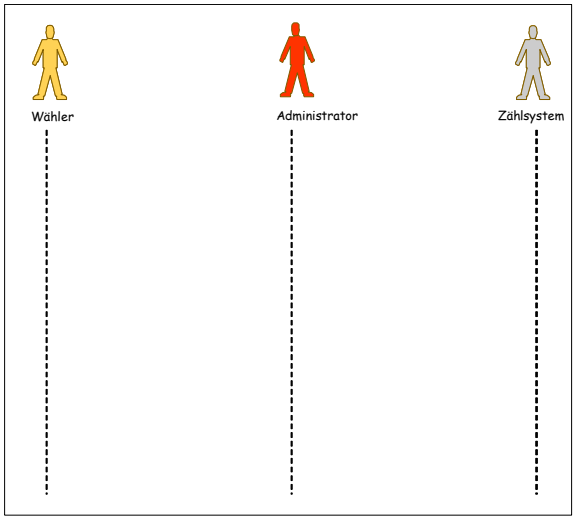


Abbildung 20: Sequenzdiagramm für das Blind-Signature Voting Protocol

Warum werden blinden Unterschriften eingesetzt?

In dem gerade vorgestellen Wahlprotokoll werden (und dies ist für uns neu) blinde Unterschriften eingesetzt. Genauer gesagt, ganz am Anfang des Protokolles. Die Wählerin Alice verschlüsselt ihre Stimme, blendet sie und signiert anschliessend das Ganze.

Welchen Beitrag leisten blinde Unterschriften zur Sicherheit des Protokolles?

Erinnern Sie sich an das Two-Agency-Protokoll aus Kapitel 3? Ganz am Anfang des Protokolles musste der Admnnistrator allen Wahlberechtigen Tags verteilen. Aus der Summe dieser anonymen Tags war es einer Dritteperson unmöglich, für ein abgegeben Stimme den dazugehörigen Wähler zu bestimmen.

In dem Blind-Signature Voting Protocol werden keine Tags verteilt. Die Vertraulichkeit der abgegeben Stimme wird dank der blinden Unterschrift des Administrators auf die verschlüsselte, geblendete Stimme gewährleistet.

Der Wähler bekommt vom Administrator eine gültige digitale Signatur auf die Stimme, eine Signatur die aber blind berechnet wurde. Der Administrator weiss, dass er die Stimme von Alice unterschrieben hat, kann aber dessen Inhalt nicht erfahren.

Aufgabe 4.2:

In dieser Aufgabe betrachten wir die zwei Wählerinnen Alice und Eve. Am Ende des Blind-Signatur Voting Protocol möchte Eve ermitteln, wie Alice gewählt hat. Kann Sie es? Begründen Sie Ihre Antwort.

	**Aufgabe 4.3:** Gehen Sie davon aus, dass der Administrator die Wahl manipulieren möchten. Er ist, sozusagen, ein Bösewicht. Analysieren Sie den Angriff auf die Vertraulichkeit der Stimme, den Sie in der Aufgabe 3.10 für das Two-Agency-Protokoll entworfen haben. Ist dieser Angriff auch beim Blind-Signatur Voting Protocol erfolgreich? Begründen Sie Ihre Antwort.
	**Aufgabe 4.4:** In dieser Aufgabe gehen Sie davon aus, dass der Administrator und das Zählsystem eine Stimme abgeben möchten, dies anstelle des legitimierten Wählers Bob. Bob nimmt am Wahlgang nicht teil. Entwerfen Sie ein Szenario, das diesen Angriff umsetzt. Sie lösen die Aufgabe am besten, wenn Sie ein Sequenzdiagramm zeichnen.

Sie haben gerade gelernt, dass digitale Signaturen ein mächtiges Werkzeug sind, die die Gewährleistung der Vertraulichkeit einer Stimme ermöglichen.

Das Blind-Signature Voting Protocol mit dem RSA-Verfahren

Sie konnten im vorherigen Abschnitt lernen, wie das Blind-Signature Voting Protocol strukturiert ist; die Bestandteile des Protocols sind Ihnen bekannt und daher sollte es Ihnen nicht schwer fallen, die folgende, konkrete Beschreibung desselben Protokolls zu verstehen.

Als Public-Key-Kryptosystem für die Berechnung der digitalen und der blinden Unterschriften wird hier RSA gebraucht. Als symmetrische Chiffre könnte man sich vorstellen, AES oder Triple-DES einzusetzen. In den folgenden Abschnitten, auf jedem Fall, werden wir die symmetrische Chiffre einfach mit $E(M,K)$ notieren, wobei M die zu signierende Nachricht, und K der symmetrische Schlüssel ist.

- ∅ Der Wähler verschlüsselt seine Stimme M mit dem Schlüssel K:
  $V = E(M,K)$.
- ∅ Der Wähler blendet seine verschlüsselte Stimme mit einem Blendungsfaktor k:
  $V' = k^{e_A} \cdot V \bmod n_A$
- ∅ Der Wähler unterschreibt seine eigene, geblendete Stimme: $S_w = (V')^{d_w} \bmod n_w$
- ∅ Der Wähler schickt dem Administrator die geblendete Stimme, sowie seine Signatur(V', S_w).

Aufgabe 4.5:

Führen Sie den ersten Schritt des Blind-Signature Voting Protocol durch. Dabei beachten Sie folgenden Parametern:

- ✓ Stimme $M = 10$.
- ✓ Symmetrischer Schlüssel $K = 5$.
- ✓ Sei $E(10,5) = 11$ (Sie können ja die symmetrische Chiffre nicht von Hand duchrechnen!).
- ✓ Der Private-Key vom Wähler sei $d_w = 11$. Der Public-Key sei $(e_w, n_w) = (35, 119)$.
- ✓ Der Private-Key vom Administrator sei $d_A = 37$. Der Public-Key sei $(e_A, n_A) = (109, 221)$.
- ✓ Sei der Blendungsfaktor $k = 11$.

Sie haben jetzt sicher verstanden, wie man vorgehen soll, um das RSA-Verfahren beim Blind-Signature Voting Protocol einsetzen zu können. Die Notation mag umständlich sein, die Berechungen sind aber – wie gewöhnlich nicht allzu schwer.

Wissenssicherung:

Ihre Aufgabe besteht jetzt darin, die Aufgabe 4.2 fortszusetzen. Führen Sie die Schritte 2. bis 7. des Blind-Signature-Protocol durch.

Alle Parameter, die Sie dazu benötigen, sind in der Aufgabenstellung der Aufgabe 4.2 angegeben.

Werden die sieben Sicherheitsanforderungen eingehalten?

Auch hier, wie im Kapitel 3, gilt das Prinzip, dass eine formale Analyse der Einhaltung der sieben Sicherheitsanforderungen kaum möglich ist. Aus diesem Grund wird hier verzichtet, eine klare Stellungsnahme aufzuführen.

Das vorgestellte Protokoll wurde implementiert und angewendet in Princeton (siehe Quelle [3]). Es hat sich herausgestellt, dass der ganze Abstimmungsablauf in wenig Zeit abgeschlossen werden konnte, dies trotz der Komplexität des Wahlprotokolles und trotz dem Einsatz der (langsamen) Public-Key-Kryptografie. Farrel Lifson (siehe Quelle [5]) berichtet, dass das ganze Wahlprotokoll eine einzige Interaktion mit dem Wähler erfordert, nämlich bei der Abgabe der Stimme. Alle andere Prozesse werden vollautomatisch von der elektronischen Wahlplattform absolviert.

Die Frage, die man sich stellen kann ist aber... Kann man der Software überhaupt vertrauen?

Lernkontrolle

Haben Sie verstanden, wie das Blind-Signature Voting Protocol funktioniert? Wenn Sie die Aufgaben 4.2 und 4.3 gelöst haben, werden Sie keine Mühe haben, diese neue Aufgabe zu bewältigen!

Ihre Aufgabe besteht darin, den Ablauf des Wahlprotokolles in dem folgenden Sequenzdiagramm zu vervollständigen – diesmal aber mit den konkreten Zahlen (und Parameter) aus den Aufgaben 4.2 und 4.3.

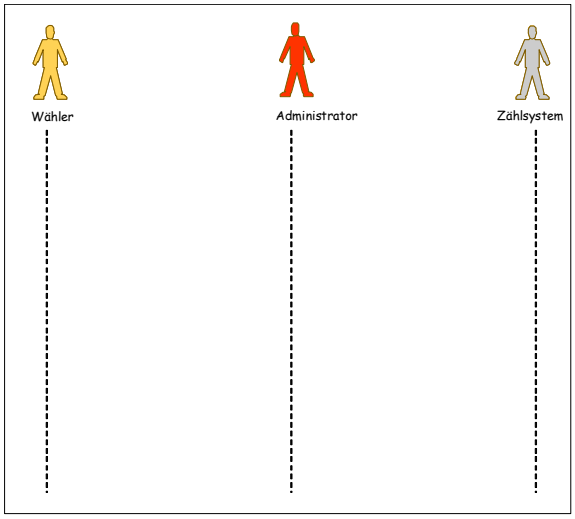
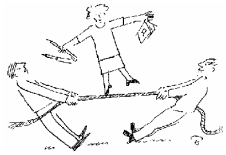


Abbildung 21: Lernkontrolle Kapitel 4

Kapiteltest

Wenn Sie alle aufgeführten Aufgaben lösen konnten und keine offene Frage mehr haben, können Sie sich an den Dozenten oder an den Tutor wenden, um den Kapiteltest zu holen.



Lösungen zum Kapitel 4: Blind-Signature Voting Protocol

Lösung zur Aufgabe 4.1:

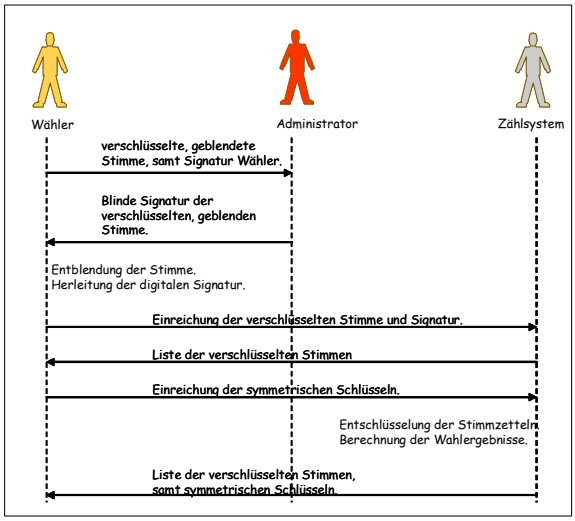


Abbildung 22: Sequenzdiagramm Aufgabe 4.1

Lösung zur Aufgabe 4.2:

Am Ende des Wahlprotokolls werden vom Zählsystem alle Stimmen (in verschlüsselter Form), sowie die dazugehörigen symmetrischen Schlüssel bekannt gegeben.

Eve hat die Möglichkeit, alle Stimmen korrekt zu entschlüsseln, dadurch auch diejenige von Alice. Dass aber genau diese Stimme Alice gehört, bleibt Eve verheimlicht, da die Stimme selber und der symmetrische Schlüssel keinen Hinweis auf die Identität von Alice geben.

Lösung zur Aufgabe 4.3:

In dem Agriff auf dasTwo-Agency-Protokoll notierte sich der Administrator wem er welchen Tag gegeben hat.

Beim Blind-Signatur Voting Protocol werden keine Tags verteilt. Der Administrator muss lediglich eine verschlüsselte, geblendete Stimme

unterschreiben. Er erfährt den Inhalt der Stimme nicht. Und die Verifizierung seiner gültigen digitalen Unterschrift auf einer Stimme, ermöglicht ihm nicht die Identität des Wählers zu eruieren.

Lösung zur Aufgabe 4.4:

Diese Aufgabe entspricht der Aufgabe 3.11. Dieselbe Antwort, mit denselben Gedanken gilt auch hier.

Lösung zur Aufgabe 4.5:

∅ Der Wähler verschlüsselt seine Stimme $M = 10$ mit dem Schlüssel $K = 5$:

$V = E(10,5) = 11$ (vorgegeben).

∅ Der Wähler blendet seine verschlüsselte Stimme mit einem Blendungsfaktor $k = 13$:

$$V' = k^{e_A} \cdot V \bmod n_A = 11^{109} \cdot 11 \bmod 221 =$$
$$= 24 \cdot 11 \bmod 221 = 43$$

∅ Der Wähler unterschreibt seine eigene, geblendete Stimme:

$$S_W = (V')^{d_W} \bmod n_W = 43^{11} \bmod 119 = 15$$

Der Wähler schickt dem Administrator die geblendete Stimme, sowie seine Signatur$(43,15)$.

Lösung zur Wissenssicherung:

1. Der Administrator überprüft die Gültigkeit der Signatur.
   $M' = S_W^{e_W} \bmod n_W = 15^{35} \bmod 119 = 43$ $(M = 43!)$
   Falls die Signatur authentisch ist und der Wähler tatsächlich stimmberechtigt ist, unterschreibt der Administrator die vom Wähler signierte, geblendete Stimme und schickt sie dem Wähler zurück.
   $S'_A = (V')^{d_A} \bmod n_A = 43^{37} \bmod 221 = 212$
2. Der Wähler entfernt den Blendungsfaktor und bekommt eine gültige Signatur vom Administrator auf der ürsprünglichen Stimme:
   $S_A = k^{-1} \cdot S'_A \bmod n_A = 201 \cdot 212 \bmod 221 = 180$
3. Der Wähler stellt dem Zählsystem seine verschüsselte Stimme, samt digitaler Signatur des Administrators zu.
   $(V, S_A) = (11,180)$
4. Das Zählsystem sammelt die Stimmen aller Wähler; er veröffentlicht die Liste der verschlüsselten Stimmen, so dass jeder Wähler überprüfen kann, ob seine Stimme dabei ist.
   $(V, S_A) = (11,180)$ ist dabei
   Das Zählsystem prüft, ob das Unterschrift auf der verschlüsselten Stimme diejenige des Administrators ist:

$V^{dA} \bmod n_A = 180^{109} \bmod 221 = 11 \; (= V!)$

5. Der Wähler schickt dem Zählsystem sein Schlüssel K; der Wähler entschlüsselt den Stimmzettel und berechten die Ergebnisse der Wahl.

   $D(V,K) = D(11,5) = 10 = M$ (die Stimme)

6. Das Zählsystem veröffentlicht die Liste der verschlüsselten Stimmen (samt Schlüssel), so dass jeder Wähler die Ergebnisse der Wahl selber reproduzieren kann.

   $(V,K) = (11,5)$

Lösung zur Lernkontrolle:

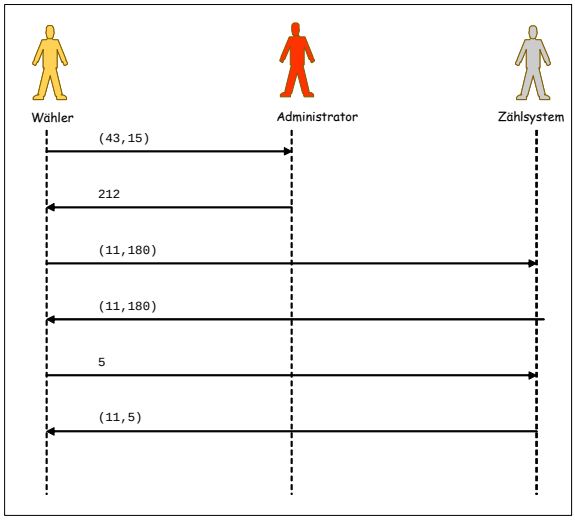


Abbildung 23: Sequenzdiagramm zur Lösung zur Lernkontrolle

Anhang 1: Kapitel-Tests für die Tutoren

Testaufgaben zum Kapitel 1

	**Testaufgabe 1.1 (K1)** Was ist mit dem Ausdruck „Vertraulichkeit einer Stimme" gemeint?
	**Testaufgabe 1.2 (K2)** Erklären Sie den Unterschied zwischen „Autorisierung" und „Authentizität". Dabei können Sie sich mit einem Beispiel helfen.
	**Testaufgabe 1.3 (K2)** Erklären Sie den Unterschied zwischen „Vertraulichkeit" und „Authentizität". Dabei können Sie sich mit einem Beispiel helfen.
	**Testaufgabe 1.4 (K2)** Erklären Sie den Unterschied zwischen „Autorisierung" und „Integrität". Dabei können Sie sich mit einem Beispiel helfen.

Testaufgaben zum Kapitel 2

Testaufgabe 2.1 (K2)

Erklären Sie woraus der Hauptunterschied zwischen einer herkömmlichen Signatur und einer blinden Signatur besteht.

Testaufgabe 2.2 (K3)

Betrachten Sie das folgende Szenario, das Sie übrigens aus den Übungsaufgaben schon kennen: Bob soll eine Nachricht `M` für Alice blind unterschreiben.

Dabei betrachten Sie die folgenden Paramter:

- ✓ der Private-Key von Bob ist: `d = 283`.
- ✓ sein Public-Key ist `(e,n) = (19,377)`.
- ✓ die zu unterschreibende Nachricht ist `M = 10`.
- ✓ als Blendungsfaktor wählen Sie `k = 17`.

Berechnen Sie (blind) die Signatur `S`.

Testaufgabe 2.3 (K3)

Betrachten Sie das folgende Szenario, das Sie übrigens aus den Übungsaufgaben schon kennen: Bob soll eine Nachricht `M` für Alice blind unterschreiben.

Dabei betrachten Sie die folgenden Paramter:

- ✓ der Private-Key von Bob ist: `d = 283`.
- ✓ sein Public-Key ist `(e,n) = (19,377)`.
- ✓ die zu unterschreibende Nachricht ist `M = 10`.
- ✓ als Blendungsfaktor wählen Sie `k = 17`.

Die Signatur von Bob auf der Nachricht `M = 10` ist `S = 101`.

Verifizieren Sie die Signatur `S`.

Testaufgabe 2.4 (K2)

Gibt es Unterschiede in der Verfizierung einer herkömmlichen Unterschrift im Vergleich zur Verifizierung einer blinden Unterschrift? Begründen Sie Ihre Antwort.

Testaufgaben zum Kapitel 3

Testaufgabe 3.1 (K2)

Sie haben gelernt, wie das „Naives Wahlprotokoll" aufgebaut ist. Sie werden jetzt eine Möglichkeit bekommen, um Ihre Vision des Protokolles zu überprüfen.

Ihre Aufgabe besteht darin, den Ablauf des Wahlprotokolles in dem folgenden Sequenzdiagramm zu vervollständigen.

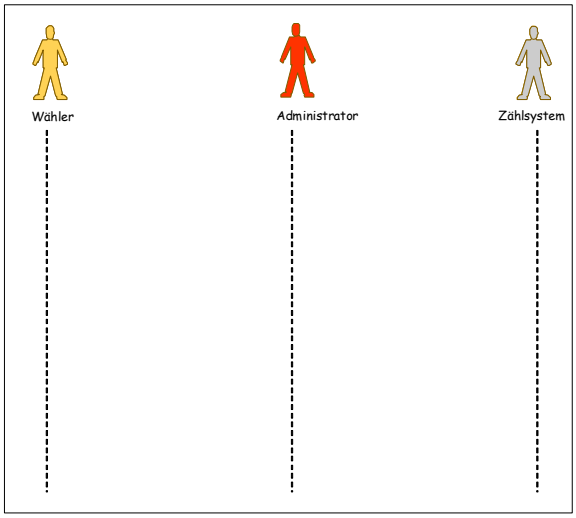


Abbildung 24: Sequenzdiagramm für das naives Wahlprotokoll

Testaufgabe 3.2 (K2)

In dieser Aufgabe geht es darum, einen Auschnitt des „Two-Agency"-Wahlprotokolls zu betrachten. Studieren Sie zuerst die folgende Abbildung:

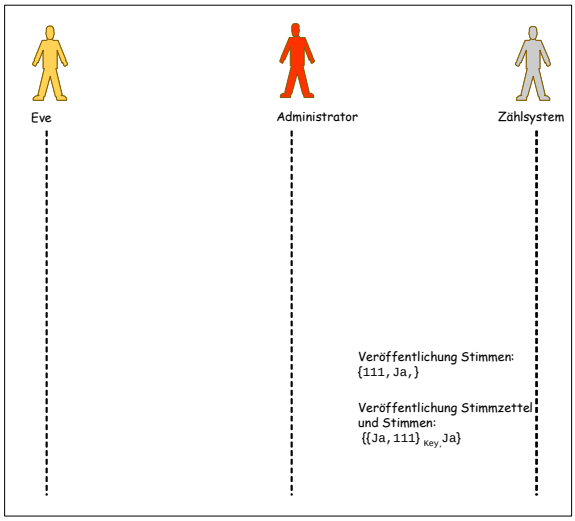


Abbildung 25: Testaufgabe 3.2

Die Wählerin Alice hat den Tag 111 bekommen und Ihre Stimme abgegeben. Erklären Sie...

a. woher das Zählsystem die Liste der Tags hat.
b. woher das Zählsystem die symmetrischen Schlüssel hat.
c. warum es für den Wähler Bob unmöglich ist zu erfahren, was Alice gestimmt hat.

Testaufgabe 3.3 (K1)

Erklären Sie wie Sie vorgehen würden, wenn Sie der Admnistrator wären und erfahren möchten, was Alice gewählt hat.

Testaufgabe 3.4 (K2)

In dieser Aufgabe werden Sie ein Sequenzdiagramm entwerfen müssen, auf der Basis des bereits in der Lernkontrolle Erlernten.

Hier betrachten wir einen Auschnitt der gesamten Landschaft der Stimmberechtigen, der aus der Wählerin Alice besteht.

Alice bekommt vom Administrator den Tag `101` und entscheidet sich, „`Ja`“ zu stimmen.

Ihre Aufgabe besteht darin, das Sequenzdiagramm für die Stimmabgabe von Alice anhand des Two-Agency-Wahlprotokolls zu zeichnen.

Testaufgaben zum Kapitel 4

Testaufgabe 4.1 (K3)

Führen Sie den ersten Schritt des Blind-Signature Voting Protocol durch. Dabei beachten Sie folgenden Parametern:

- ✓ Stimme $M = 8$.
- ✓ Symmetrischer Schlüssel $K = 3$.
- ✓ Sei $E(8,3) = 7$ (Sie können ja die symmetrische Chiffre nicht von Hand duchrechnen!).
- ✓ Der Private-Key vom Wähler sei $d_w = 13$. Der Public-Key sei $(e_w, n_w) = (37,119)$.
- ✓ Der Private-Key vom Administrator sei $d_A = 11$. Der Public-Key sei $(e_A, n_A) = (71,141)$.

Sei der Blendungsfaktor $k = 15$.

Testaufgabe 4.2 (K3)

Führen Sie den ersten Schritt des Blind-Signature Voting Protocol durch. Dabei beachten Sie folgenden Parametern:

- ✓ Stimme $M = 5$.
- ✓ Symmetrischer Schlüssel $K = 8$.
- ✓ Sei $E(5,8) = 2$ (Sie können ja die symmetrische Chiffre nicht von Hand duchrechnen!).
- ✓ Der Private-Key vom Wähler sei $d_w = 5$. Der Public-Key sei $(e_w, n_w) = (13,85)$.
- ✓ Der Private-Key vom Administrator sei $d_A = 19$. Der Public-Key sei $(e_A, n_A) = (7,161)$.

Sei der Blendungsfaktor $k = 11$.

Testaufgabe 4.3 (K3)

In dem „Two-Agency-Protokoll" werden gleich am Anfang des Wahlvorganges Tags verteilt. In dem „Blind-Signature Voting Protocol" stützt man sich auf blinde Unterschriften.

Erklären Sie den Vorteil der blinden Unterschriften im Vergleich zu den Tags.

Testaufgabe 4.4 (K2)

Gleich am Anfang des „Blind-Signature Voting Protocols" wird vom Wähler die Stimme verschlüsselt, geblendet und anschliessend digital unterschrieben.

Erklären Sie die Bedeutung dieser drei Operationen.

Lösungen zu den Testaufgaben des Kapitels 1

	**Lösung zur Testaufgabe 1.1** Mit dem Ausdruck „Vertraulichkeit einer Stimme" ist die Bedingung gemeint, die besagt, dass niemand erfahren darf, für wen (oder was) ein Wähler gestimmt hat.
	**Lösung zur Testaufgabe 1.2** Mit dem Begriff „Autorisierung" ist die Berechtigung gemeint, auf eine Ressource zuzugreifen oder sich an einem Prozess zu beteiligen. Mit dem Begriff der Authentizität ist die Echtheit eines Benutzers, eines Rechners oder z.B eines Web-Services verstanden. Diese Echtheit ist für die betroffenen Ansprechpartner überprüfbar. Die zwei Anforderungen sind komplementär.
	**Lösung zur Testaufgabe 1.3** Mit dem Begriff der Authentizität ist die Echtheit eines Benutzers, eines Rechners oder z.B eines Web-Services verstanden. Diese Echtheit ist für die betroffenen Ansprechpartner überprüfbar. Mit dem Ausdruck „Vertraulichkeit einer Stimme" ist die Bedingung gemeint, die besagt, dass niemand erfahren darf, für wen (oder was) ein Wähler gestimmt hat. Die zwei Anforderungen sind komplementär.
	**Lösung zur Testaufgabe 1.4** Mit dem Begriff „Autorisierung" ist die Berechtigung gemeint, auf eine Ressource zuzugreifen oder sich an einem Prozess zu beteiligen. Der Begriff der Integrität bezieht sich in der IT-Sicherheit auf die unerwünschte, externe Änderung an Daten während einer Übermittlung vom Sender zum Empfänger. Die zwei Anforderungen sind komplementär.

Lösungen zu den Testaufgaben des Kapitels 2

Lösung zur Testaufgabe 2.1

Der Hauptunterschied zwischen einer herkömmlichen, digitalen Signatur und einer blinden Signatur liegt in der Tatsache, dass im ersten Fall der Signierende genau sieht was er unterschreibt, während er im zweiten Fall eine geblendete Nachricht unterschreibt.

Lösung zur Testaufgabe 2.2

1. Alice wählt als Blendungsfaktor $k = 17$ (wurde von mir vorgegeben).
2. Alice berechnet die geblendete Nachricht:
   $$M' = M \cdot k^e \bmod n = 10 \cdot 17^{19} \bmod 377 =$$
   $$= 10 \cdot 186 \bmod 377 = 352$$
   und sendet $M'=352$ an Bob
3. Bob signiert $M' = 352$ indem er
   $$S' = (M')^d \bmod n = 352^{283} \bmod 377 = 209$$
   berechnet. Er sendet $S' = 209$ an Alice.

Alice entfernt die Blendung auf S' durch Berechnung von

$$S = k^{-1} \cdot S' \bmod n = 244 \cdot 209 = 101$$

Lösung zur Testaufgabe 2.3

1. Alice verifiziert die Signatur $S = 101$ von Bob auf der Nachricht $M = 10$ indem Sie $S^e \bmod n$ berechnet:
   $$S^e \bmod n = 101^{19} \bmod 377 = 10$$

Das Resultat aus der obigen Berechung ist 10. M war auch 10. Die Signatur wird angenommen.

Lösung zur Testaufgabe 2.4

Eine blinde Unterschrift ist eine herkömmliche Unterschrift. Der Unterschied zwichen den beiden liegt nicht in der Unterschrift selber, sondern in dem Verfahren, das angewendet wird, um sie zu bestimmen.

Lösungen zu den Testaufgaben des Kapitels 3

Lösung zur Testaufgabe 3.1

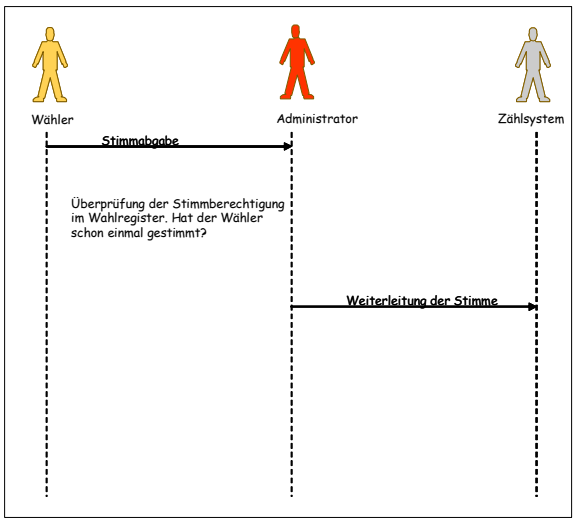


Abbildung 26: Lösung Testaufgabe 3.1

Lösung zur Testaufgabe 3.2

a. Das Zählsystem hat die Liste der Tags vom Administrator bekommen, nachdem der Administrator die Tags generiert und an die Wählern verteilt hat.

b. Die benötigten symmetrischen Schlüssel werden von den Wählern an das Zählsystem zugestellt, zusammen mit dem jeweiligen Tag. Das Zählsystem kann nicht eruieren, welchem Wähler, welcher Tag gehört.

c. Ein Wähler Bob sieht nur die Stimmen und die Tags. Er weiss aber nicht welchem Wähler welcher Tag gehört.

Lösung zur Testaufgabe 3.3

Dieser Angriff entspricht demjenigen in der Aufgabe 3.9.

Lösung zur Testaufgabe 3.4

Diese Aufgabe entspricht die Lernkontrolle des Kapitels 3:

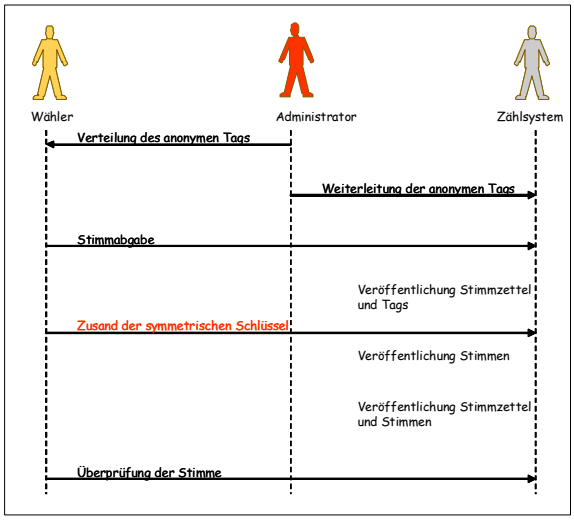


Abbildung 27: Lösung Testaufgabe 3.3

Lösungen zu den Testaufgaben des Kapitels 4

Lösung zur Testaufgabe 4.1

∅ Der Wähler verschlüsselt seine Stimme $M = 8$ mit dem Schlüssel $K = 3$:

$V = E(8,3) = 7$ (vorgegeben).

∅ Der Wähler blendet seine verschlüsselte Stimme mit einem Blendungsfaktor $k = 15$:

$$V' = k^{e_A} \cdot V \bmod n_A = 15^{71} \cdot 7 \bmod 141 =$$
$$= 57 \cdot 7 \bmod 141 = 117$$

∅ Der Wähler unterschreibt seine eigene, geblendete Stimme:

$$S_W = (V')^{d_W} \bmod n_W = 117^{13} \bmod 119 = 19$$

Der Wähler schickt dem Administrator die geblendete Stimme, sowie seine Signatur$(117,19)$.

Lösung zur Testaufgabe 4.2

∅ Der Wähler verschlüsselt seine Stimme $M = 5$ mit dem Schlüssel $K = 8$:

$V = E(5,8) = 2$ (vorgegeben).

∅ Der Wähler blendet seine verschlüsselte Stimme mit einem Blendungsfaktor $k = 15$:

$$V' = k^{e_A} \cdot V \bmod n_A = 11^{7} \cdot 2 \bmod 161 =$$
$$= 53 \cdot 2 \bmod 161 = 106$$

∅ Der Wähler unterschreibt seine eigene, geblendete Stimme:

$$S_W = (V')^{d_W} \bmod n_W = 106^{5} \bmod 85 = 21$$

Der Wähler schickt dem Administrator die geblendete Stimme, sowie seine Signatur$(106,21)$.

Lösung zur Testaufgabe 4.3

Die blinden Unterschriften in dem „Blind-Signature Voting Protocol" übernehmen diesselbe Funktion der Tags in dem „Two-Agency-Protokoll".

Ein unehrlicher Administrator kann sich aber notieren welcher Wähler welchen Tag bekommt und somit die Vertraulichkeit der Stimmen verletzten. Dank der blinden Unterschrift des Administrators auf dem verschlüsselten, geblendeten Stimmzettel kann der Wähler eine gültige digitale Unterschrift auf dem verschlüsselten Stimmzettel berechnen und somit beweisen, dass er einen Anspruch hat, an der Wahl

	teilzunehmen. Dies ohne dem Zählsystem seine Identität zu verraten.
	**Lösung zur Testaufgabe 4.4** o Die Verschlüsselung der Stimme dient zur Gewährleistung der Vertraulichkeit. Niemand (weder der Administrator, noch das Zählsystem, noch andere Wähler) dürfen erfahren wie die Wählerin Alice gestimmt hat. o Blendung der verschlüsselten Stimme: der Administrator muss seine digitale Unterschrift auf den verschlüsselten Stimmzettel hinzufügen, ohne dessen Inhalt zu kennen. Zu diesem Zweck wird der Stimmzettel so getarnt, dass er nicht mehr erkennen kann, was er überhaupt unterschreibt. o Signierung der verschlüsselten, geblendeten Stimme: der Wähler beweist mit seiner Unterschrift seine Identität. Der Administrator kann somit überprüfen, ob der Wähler überhaupt berechtigt ist seine Stimme abzugeben.

Anhang 2: Material

Blaukuvert für die Aufgabe 2.1.

Anhang 3: Quellen

Grundlagen

[1] Jones Douglas W.: A Brief Illustrated History of Voting. Available online from http://www.cs.uiowa.edu/~jones/voting/pictures/

[2] Wätjen D.: Kryptographie: Grundlagen, Algorithmen, Protokolle, Berlin, 2004 (Spektrum Akademischer Verlag GmbH Heidelberg).

[3] Davenport B., Newberger A., Woodard J: Creating a secure digital voting protocol for campus elections. Unpublished paper. 1995. Available online from http://www.princeton.edu/~bpd/voting/

Zitierte Quellen

[4] Wätjen D.: Kryptographie: Grundlagen, Algorithmen, Protokolle, Berlin, 2004 (Spektrum Akademischer Verlag GmbH Heidelberg), 190-191.

[5] Lifson F.: Blind Signature Protocol. Available online from http://people.cs.uct.ac.za/~flifson/things/security/node8.html

[6] Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen. Working Paper 05/2002 des Institut für Informationsverarbeitung und -wirtschaft, 2002, 42-43. Available online from http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01_3d6.pdf?ID=epub-wu-01_3d6

Anhang 4: Das Gemälde von Bingham

In dem Kapitel 1 des Leitprogrammes wird ein Ausschnitt aus dem folgenden Gemälde vorgestellt:

Abbildung 28: The County Election, George Caleb Bingham (aus der Quelle [1])