Inhalt

Lerntätigkeiten der AdressatInnen im Vorfeld

Public Key Kryptologie

Im Vorfeld zu dieser Lektion beschäftigen sich die Studierenden mit dem grundlegenden Konzept der *Public Key Verfahren*. Die Studierenden haben das System kennengelernt und so stark verinnerlicht, dass sie es einem Laien in einem kurzen Vortrag erläutern können. Konkret wissen sie: Es gibt zwei strikte getrennte Schlüssel, den *Public* und den *Private Key*. Die Schlüssel sind praktisch unmöglich auseinander herleitbar. Mit Hilfe des Public Keys werden Dokumente verschlüsselt. Eine so verschlüsselte Botschaft kann in nützlicher Frist einzig und allein mit dem zugehörigen Private Key entschlüsselt werden. Aus diesem Grund kann der Public Key problemlos der ganzen Welt zur Verfügung gestellt werden. Auf der anderen Seite muss der Private Key unbedingt geheim bleiben. Von ihm hängt die Sicherheit des Systems ab.

Ein wichtiger Punkt für die Lernaufgabe

Ein Merkmal ist für die vorliegende Lernaufgabe von besonderer Bedeutung: Der Public und der Private Key bilden exakte Gegenstücke und sind grundsätzlich gleichwertig. Was mittels Public Key verschlüsselt wurde, kann praktisch ausschliesslich durch den Private Key wieder zugänglich gemacht werden. Diese Beziehung zwischen den Schlüsseln gilt auch in umgekehrter Richtung!

Vorschlag

Mit dem Thema der Public Key Kryptologie haben sich die Lernenden während mindestens 1-2 Stunden beschäftigt. Die grundlegende Idee mit den beiden getrennten Schlüsseln können die Studierenden selbständig erarbeiten. Die Lernaufgabe mit dem Titel "Public Key Kryptologie – Die Idee mit den beiden Schlüsseln" vom gleichen Autor im Rahmen dieser Sammlung macht dazu einen ausführlichen Vorschlag (Näf 1997).

Vorkenntnisse allgemeiner Art

Die folgenden Kenntnisse hängen nicht direkt mit dem Thema zusammen. Sie sind trotzdem unerlässlich für das Verständnis des Stoffes. Es handelt sich um Begriffe, die den Studierenden vertraut sein sollten. Die angegebene kurze Beschreibung genügt.

- Das **Internet** ist ein riesiges Netzwerk von TeilnehmerInnen. Alle TeilnehmerInnen können miteinander kommunizieren. Das Internet bietet immense Mengen an Information an, und der Informationsaustausch ist rege. Das Internet ist weltumspannend. Die TeilnehmerInnen am Internet sind beliebig, sie kennen sich in der Regel nicht.
- **E-Mail** (Electronic Mail) ist der am häufigsten benutzte Dienst zum Informationsaustausch im Internet. E-Mail funktioniert ganz analog zur normalen Post. Das heisst: Eine E-Mail wird mit der Zieladresse versehen und losgeschickt. Optimal wäre natürlich, wenn die Studierenden selbst schon E-Mails verfasst und verschickt hätten.

- Sobald mehrere BenutzerInnen an einem Computer oder in einem Netzwerk arbeiten, erhalten die einzelnen Personen jeweils ein **Konto** (Account). Dadurch werden ein gewisser Anteil an Speicherplatz und bestimmte Rechte zur Verfügung gestellt. Alle BenutzerInnen erhalten einen Namen (User-Namen) und ein Passwort, mit welchem sie sich am Computer oder im betreffenden Netzwerk anmelden können.

Unterrichtsvorbereitung

Beschreibung des Unterrichts – Sequenz

	Inhalt	*Methode*	*Dauer*
1	Der Informierende Unterrichtseinstieg führt in die Lektion ein. Zu dieser Einleitung gehören die vier Folien (Abschnitt "Folienvorschau").	Vortrag der Lehrperson	3'
2	In einem kurzen Vortrag geht die Lehrperson auf den Zweck von herkömmlichen Unterschriften und die Probleme bei digitalen Dokumenten ein (Abschnitt "Sinn und Zweck von Unterschriften").	Vortrag der Lehrperson	8'
3	Anschliessend bearbeiten die Studierenden die Lernaufgabe. Dabei lernen sie, wie eine digitale Unterschrift auszusehen hat und wie die Public Key Technik zum Unterzeichnen von Dokumenten verwendet werden kann. Sämtliches Material für die Lernaufgabe befindet sich im Kapitel "Die Lernaufabe".	Lernaufgabe, selbständig	20'
4	Die Lösungen zur Lernaufgabe erhalten die Studierenden ebenfalls schriftlich. Das Material studieren die Lernenden selbständig.	Selbststudium	8'
5	Abschliessend bleibt Zeit für allfällige Fragen oder eine Diskussion.	Klasse	6'

Informierender Unterrichtseinstieg

Heute geht es darum: (An dieser Stelle wird die erste Folie mit der Unterschrift aufgelegt.)
Das ist (m)eine Unterschrift. "Normale" Unterschriften auf Papier kennen Sie zur genüge. Sie alle haben Ihre Unterschrift schon unzählige Male auf Verträge, Formulare, Ausweise, Cheques, Briefe und ähnliches gesetzt.
Unterdessen leben wir aber bekanntlich im Digitalen Zeitalter. Deshalb befassen wir uns heute mit der Frage: Wie werden digitale Dokumente unterschrieben? Also zum Beispiel: Wie unterschreibt man eine E-Mail? Wie setzt man einen digitalen Vertrag auf und unterzeichnet diesen?

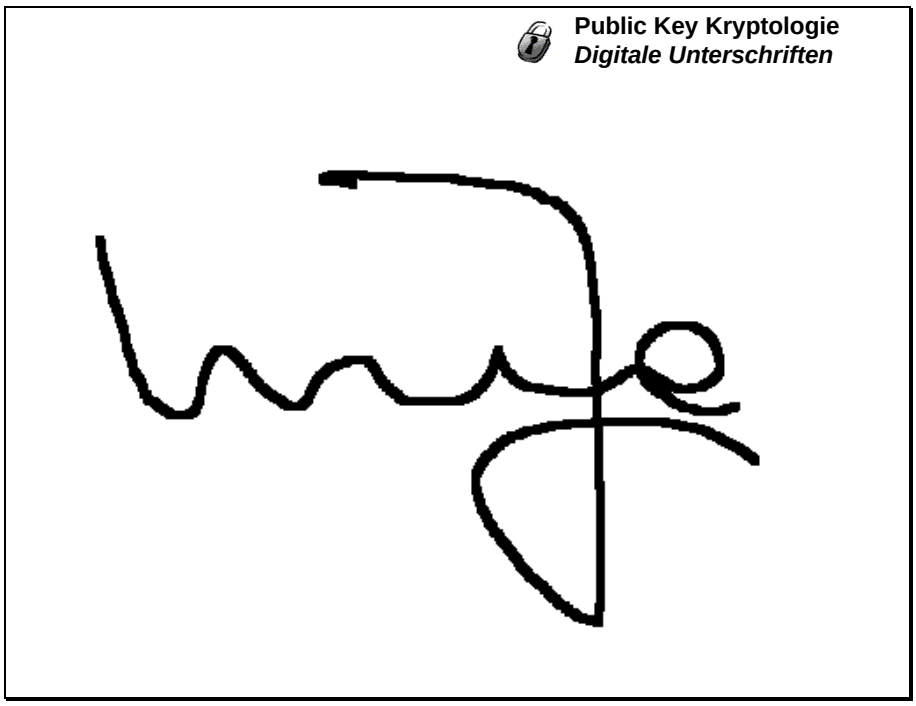
Welches sind die **Ziele** für diese Lektion?

- Sie wissen, welchen Zweck Unterschriften – ob digital oder auf Papier – zu erfüllen haben. Sie können erklären, wie dieses Ziel für digitale Dokumente mit Hilfe der Public Key Technologien erreicht wird.
- Sie wissen, welches die Probleme bei digitalen Unterschriften sind. Das heisst, wofür eine digitale Unterschrift genau garantiert.

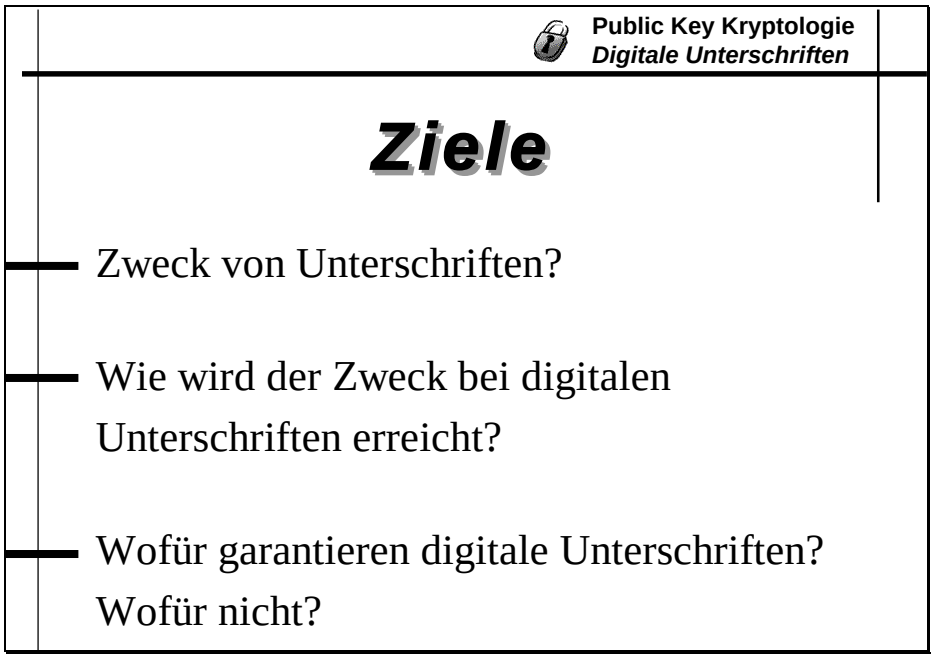
Und **wieso** das ganze? Digitale Dokumente werden immer verbreiteter und deshalb auch immer wichtiger. Diese Dokumente müssen natürlich häufig auch unterschrieben sein. Denken Sie zum Beispiel an Verträge, die über das Internet aufgesetzt werden. Oder: Sie schicken Ihrer Bank einen Zahlungsauftrag per E-Mail. Woher weiss die Bank, dass die Mail wirklich von Ihnen stammt? Was hat die Bank in der Hand? Um die Technik der digitalen Unterschriften anwenden zu können, sollten Sie offensichtlich eine Ahnung davon haben. Dazu gehören auch Problembereiche.

Zum **Ablauf** dieser Stunde. Die Einleitung haben wir fast schon hinter uns gebracht. Eine Frage: Haben Sie sich jemals überlegt, was eigentlich der Sinn und Zweck einer Unterschrift ist? Auf diese Frage werde ich in einem kurzen Vortrag eingehen. Dabei will ich auch erläutern, wo die Unterschiede zwischen Unterschriften auf Papier und digitalen Unterschriften liegen. Im folgenden Teil finden Sie selbständig heraus, wie Dokumente digital unterzeichnet werden. Dazu benötigen Sie die Public Key Technik, die Sie bereits kennen. Im Anschluss an die Arbeit erhalten Sie schriftlich die Antworten sowie einige zusätzliche Informationen zum Thema. Diese Unterlagen werden Sie studieren. Abschliessend bleibt uns Zeit für allfällige Fragen oder eine Diskussion.

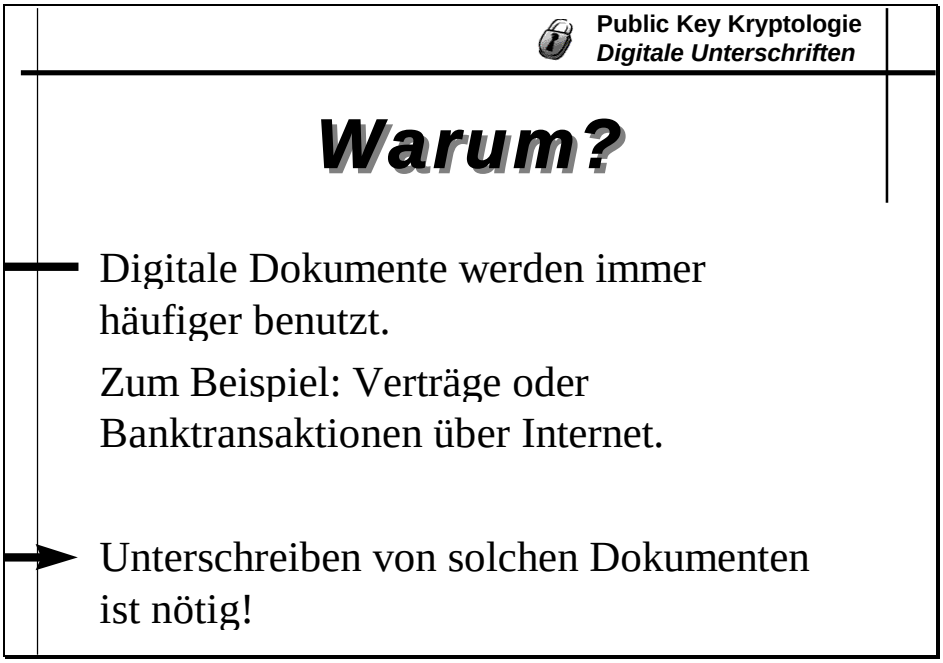
Folienvorschau



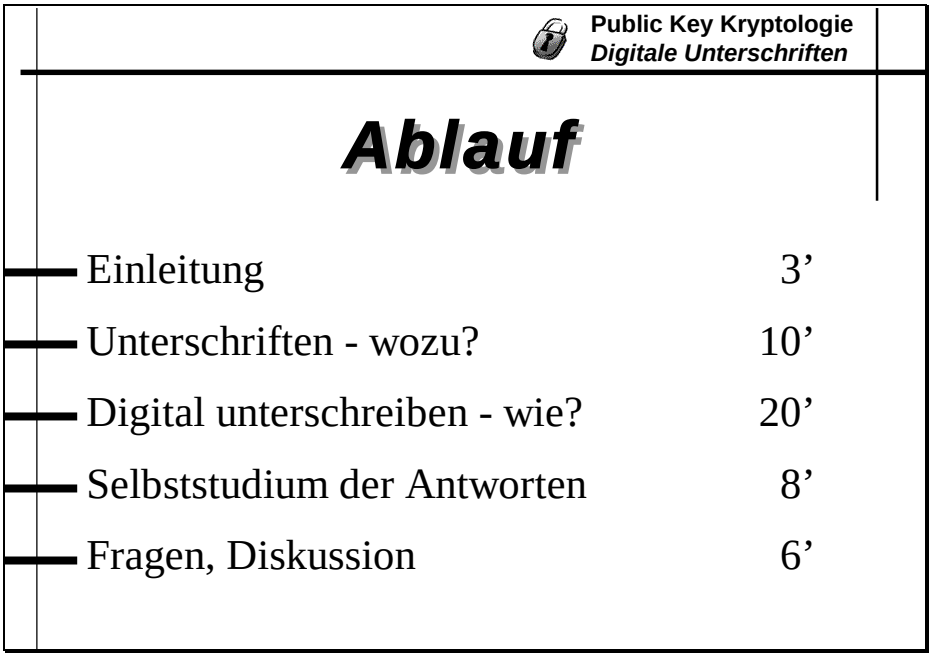
Folie 1 – Die Unterschrift der Lehrperson als Einführung in das Thema



Folie 2 – Ziele der Lektion



Folie 3 – Begründung der Lektion



Folie 4 – Ablauf der Lektion

Sinn und Zweck von Unterschriften

Bis jetzt hat sich der Unterricht mit dem Ver- und Entschlüsseln von Daten beschäftigt. Das Ziel: Niemand als der gewünschte Empfänger soll eine sensible Nachricht lesen können. Zu diesem Zweck wurde auch das Prinzip der Public Key Verfahren eingeführt.
Damit ist ein grosses Problem gelöst. Doch bleibt ein zweites bestehen. Woher weiss die Empfängerin, dass die Nachricht auch wirklich von der richtigen Person stammt? Man kann problemlos einen Brief an eine Person schicken und einen anderen Namen darunter setzen. Wenn es nicht eine ganz offensichtliche Lösung dazu gäbe: die **Unterschrift**! Im täglichen Leben garantiert die Unterschrift dafür, dass ein Dokument von einer ganz bestimmten Person stammt.

Wozu also dient die Unterschrift? Sie soll einen Text, einen Vertrag, eine schriftliche Aussage bestätigen und bekräftigen. Sie soll das Geschriebene mit einer bestimmten Person verbinden. Sie soll dafür garantieren, dass das Geschriebene von dieser Person stammt.

Wieviel wird durch die Unterschrift bestätigt? Die Unterschrift garantiert für alles, was auf demselben Stück Papier steht. Oder für alles im selben, zusammengehörenden Dokumentteil (zusammengeheftete Papiere). Demnach hält das Papier physisch den Text zusammen, der zu einer Unterschrift gehört. Das Papier *bindet* die Unterschrift an den Text.
Natürlich darf ein Text nach der Unterzeichnung nicht mehr verändert werden. Und es darf nichts hinzugefügt oder entfernt werden. Auch hier hilft das Papier, weil auf diesem Medium eine Änderung meistens Spuren hinterlässt und rasch auffällt.

Eigenschaften einer Unterschrift

"Normale", herkömmliche Unterschriften von Hand weisen einige Eigenschaften auf:

- Die Unterschrift ist **persönlich**. Sie verbindet die Unterschrift mit einer bestimmten Person.
- Das heisst auch: Die Unterschrift ist **eindeutig** und **verifizierbar** (überprüfbar). Jeder Mensch sollte eine eigene Unterschrift haben. Damit lässt sich feststellen, ob eine gewisse Unterschrift von einer ganz bestimmten Person stammt.
- Die Unterschrift sollte möglichst **nicht fälschbar** sein. Bei herkömmlichen Unterschriften ist diese Anforderung nicht immer erfüllt. Immerhin können Experten aber in den meisten Fällen eine Fälschung nachweisen.
- Unter den geschilderten Voraussetzungen **identifiziert** eine Unterschrift eine bestimmte Person.

Probleme bei digitalen Dokumenten

Eine herkömmliche Unterschrift wird ganz einfach zum betreffenden Dokument hinzugefügt. Wie oben beschrieben sorgt das Papier dafür, dass die Unterschrift mit dem Text in Verbindung gebracht wird. Nichts mehr und nichts weniger als der unterzeichnete Text!
Bei digitalen Dokumenten ist das nicht so einfach. Es genügt nicht, die Unterschrift dem Text mitzugeben. Auf diese Weise besteht keinerlei Beziehung zwischen dem Text und der Unterschrift. Digitale Dokumente können problemlos und vor allem spurlos verändert werden. Neue Textstellen können hinzugefügt und alte Stellen entfernt werden. Folglich geben digitale Dokumente Anlass zu einem eigenen Verfahren zur Unterzeichnung. Das Verfahren wird von den Studierenden im Rahmen der Lernaufgabe selbständig erarbeitet.

Die Lernaufgabe

Zugehöriges Schul-/Studienbuch

Die Lernaufgabe gehört zu keinem Schulbuch.

Das Neue

Die Studierenden erkennen, dass eine digitale Unterschrift den gesamten Inhalt des Dokumentes einbeziehen muss. Dokumentinhalt und Unterschrift müssen eine untrennbare Einheit bilden. Diese Einheit wird erreicht, indem der Inhalt des Dokuments verschlüsselt wird.
Weiter lernen die Studierenden, wie die Public Key Technik zur Unterzeichnung von Dokumenten benützt wird: Neu dient der Private Key zur Verschlüsselung (Unterzeichnung). Mit dem Public Key wird die Unterschrift überprüft, indem das Dokument entschlüsselt wird.
Zu guter letzt werden die Studierenden darauf aufmerksam gemacht, dass eine digitale Unterschrift nicht direkt für eine Person bürgt. Sondern lediglich für eine "digitale Identität".

Bewertung der Antworten

Für diese Lernaufgabe ist grundsätzlich keine Bewertung vorgesehen. Trotzdem soll an dieser Stelle ein mögliches Bewertungsschema vorgeschlagen werden. Die ausführlichen Antworten liegen als kopierfertige Unterlagen für die Studierenden vor.

Aufgabe 1

- Unterschrift muss gesamten Dokumentinhalt mit einbeziehen.

Oder: Unterschrift und Dokumentinhalt müssen eine untrennbare Einheit bilden. *2 Punkte*

- Lässt sich die Unterschrift leicht abtrennen, kann sie problemlos für andere Zwecke kopiert werden. *2 Punkte*

Aufgabe 2

- Nur eine Person soll Dokumente unterzeichnen können. Aber theoretisch die ganze Welt soll die Unterschrift überprüfen können. Das bedeutet: Umkehrung der Funktionen von Public und Private Key für Ver- und Entschlüsselung.

Oder: Private Key zum Verschlüsseln (=Unterzeichnen) des Dokuments. Public Key zum Entschlüsseln (=Verifizieren). *4 Punkte*

Aufgabe 3

- Fortsetzung des Szenarios: Eindringling hat Zugang zum Private Key und kann deshalb Dokumente mit dessen Unterschrift zeichnen. *2 Punkte*
- Digitale Unterschrift bürgt nicht direkt für eine Person. Sondern für den Zugang zu einem Computer oder eine E-Mail-Adresse. *2 Punkte*

Maximalpunktzahl = 12 Punkte

Materialien und Dokumentation

Die Studierenden benützen Schreibzeug und Papier für ihre Notizen während der Bearbeitung der Lernaufgabe. Ansonsten werden keine Materialien oder Dokumentationen benötigt.

Public Key Kryptologie

Digitale Unterschriften

Arbeitsanleitung

Ihre "handgefertigte" Unterschrift ist Ihnen in Fleisch und Blut übergegangen. Beinahe tagtäglich benutzen Sie sie ohne gross nachzudenken. Durch das Internet als neuartiges Kommunikationsmittel gewinnen Dokumente in digitaler Form immer mehr an Bedeutung. Normalerweise wird die Unterschrift am Textende angefügt. Bei digitalen Dokumenten genügt das leider nicht, weil der Text im Nachhinein problemlos und spurlos verändert werden kann. Ein neues Verfahren ist gesucht! Hier werden Sie es erarbeiten.

..... Ziele

Die Arbeit umfasst drei Aufgaben. Erwartet wird, dass Sie alle Aufgaben innerhalb der Zeit bearbeitet und eine Lösung notiert haben. Es genügt, wenn Sie Ihre Antworten stichwortartig festhalten. Aber Ihre Ausführungen sollen exakt sein! Sie brauchen nichts abzugeben.

..... Vorgehen

Sie arbeiten alleine. Ich stehe nur dann für Fragen zur Verfügung, wenn Sie eine Textstelle nicht verstehen. Insgesamt haben Sie 20 Minuten Zeit.

..... Aufgabe 1 *Die digitale Welt kennt kein Papier!*

Eine herkömmliche Unterschrift wird am Textende angefügt. Das Papier stellt die Verbindung zwischen Unterschrift und Text her. Nachträgliche Veränderungen am Text können meist einfach bemerkt werden. Anders sieht es bei digitalen Dokumenten aus – es gibt kein Papier.
Wie also müsste eine digitale Unterschrift aussehen, damit sie für den gesamten Dokumentinhalt garantieren kann? Überlegen Sie sich zusätzlich: Wieso darf sich eine digitale Unterschrift nicht vom zugehörigen Dokument trennen lassen?

..... Aufgabe 2 *Die Sache mit den Schlüsseln*

Die *Public Key Technik* zum Ver- und Entschlüsseln von Nachrichten kennen Sie bereits. Es gibt da zwei Schlüssel: Der *Public Key* dient zum Verschlüsseln von Nachrichten. Der *Private Key* macht die Entschlüsselung möglich. Der Public Key kann und soll veröffentlicht werden. Der Private Key hingegen muss unbedingt geheim bleiben.
Wie kann das System mit den beiden Schlüsseln verwendet werden, um Dokumente digital zu unterzeichnen? Skizzieren Sie die Idee stichwortartig.

Hinweis: Denken Sie daran: Der Public und der Private Key sind exakte Gegenstücke. Was mit dem Public Key verschlüsselt wird, kann mit dem Private Key entschlüsselt werden. Das gilt auch umgekehrt! Überlegen Sie sich ausserdem: Wer möchte ein Dokument unterzeichnen? Wer muss die Echtheit einer Unterschrift überprüfen können?

..... Aufgabe 3 *Sicher ist sicher?*

Ein konkretes Szenario: Sie besitzen ein Konto auf irgendeinem Computer. Für den Zugang zu diesem Computer benutzen Sie den User-Namen `ByteJuggler` und das Passwort `37Urabas`. Auf dem Computer ist Ihr persönlicher Private Key gespeichert. Wie Sie in Aufgabe 2 gesehen haben, unterzeichnen Sie mit dem Private Key Ihre Dokumente. Sie verfassen eine Zahlungsanweisung für Ihre Bank. Die Anweisung unterzeichnen Sie mit Hilfe des Private Key und schicken sie ab. Die Bank kann also sicher sein, dass die Anweisung von Ihnen stammt.
Oder ... Kann die Bank wirklich sicher sein? Führen Sie das Szenario weiter: Jemand findet Ihr Passwort `37Urabas` heraus. Problemlos kann er oder sie sich Zugang zu Ihrem Konto verschaffen. ... ...
Und als Zusatzfrage: Eine normale Unterschrift von Hand bürgt direkt für eine Person. Wofür bürgt eine digitale Unterschrift genau? Denken Sie an das Szenario!

Public Key Kryptologie

Digitale Unterschriften

Lösungen

..... Aufgabe 1

Eine Unterschrift gilt immer für einen ganz bestimmten Text (oder ein Bild, usw.). Die Unterschrift und das Geschriebene müssen also eine Einheit bilden. Diese Einheit darf nicht veränderbar sein. Bei herkömmlichen Unterschriften gewährleistet das Papier diese Einheit.
Bei digitalen Dokumenten hingegen genügt es keineswegs, die Unterschrift einfach nur dem Text beizufügen. Zwei Gründe:

- Dokumentinhalt und Unterschrift könnten problemlos getrennt werden. Anschliessend könnte man den Text abändern und die Unterschrift wieder hinzufügen. Das darf offensichtlich nicht möglich sein.
- Wenn sich Text und Unterschrift so leicht trennen lassen, kann jede und jeder die Unterschrift abtrennen. Mit der separaten Unterschrift kann dann ein anderes Dokument unterzeichnet werden. Auch das muss verhindert werden.

Konsequenz: Der Text und die Unterschrift müssen untrennbar miteinander verwoben werden. Nach dem Unterzeichnen darf nicht mehr erkenntlich sein, was Text und was Unterschrift ist. Konkret: Der Text selbst wird mit Hilfe der Unterschrift codiert. Näheres dazu bei der Antwort zur zweiten Aufgabe.

..... Aufgabe 2

Wie benützen Sie die Public Key Technik zum Ver- und Entschlüsseln? Den Public Key geben Sie weiter. Alle sollen ihn kennen. Jemand möchte Ihnen eine Nachricht verschlüsselt schicken. Also: Verschlüsseln mit Hilfe des Public Keys. Den Private Key behalten Sie geheim für sich und benützen ihn zum Entschlüsseln.

Wie sieht das Vorgehen für Unterschriften aus? Nur Sie selbst sollen ein Dokument unterzeichnen können. Auf der anderen Seite soll die ganze Welt überprüfen können, ob die Unterschrift von Ihnen stammt. Die Situation ist demnach dem Ver- und Entschlüsseln ganz ähnlich. Nur die Funktionen von Public und Private Key müssen umgekehrt werden.
Sie unterzeichnen Ihr Dokument, indem Sie es mit Ihrem Private Key verschlüsseln. Danach kann das Dokument nur noch mit dem zugehörigen Public Key entschlüsselt werden. Wie überprüft also zum Beispiel Ihre Bank, ob die Unterschrift gültig ist? Sie entschlüsselt das Dokument mit Hilfe Ihres Public Keys. Die Unterschrift ist echt, wenn dabei das ursprüngliche Dokument entsteht. In allen anderen Fällen würde beim Entschlüsseln ein Buchstaben-Wirrwarr entstehen.

..... Aufgabe 3

Die Bank kann nicht endgültig sicher sein, dass die Zahlungsanweisung von Ihnen stammt. Falls jemand Ihr Passwort `37Urabas` für Ihr Konto `ByteJuggler` herausfindet, hat er oder sie automatisch Zugang zu Ihrem Private Key. Mit Hilfe des Private Key kann der Eindringling beliebige Dokumente unterzeichnen. Das heisst: Die Zahlungsanweisung an die Bank würde zwar bestimmt von Ihrem Konto stammen und Ihre digitale Unterschrift tragen. Der Inhalt hätte aber der Eindringling aufgesetzt.
Sie können natürlich Ihren Private Key durch ein zusätzliches Passwort – getrennt vom Zugangspasswort `37Urabas` – schützen. Dadurch wird zwar das Leben des Eindringlings schwerer gemacht, doch lässt sich auch das spezielle Passwort für den Private Key theoretisch ausfindig machen.
Fazit: Eine digitale Unterschrift bürgt nicht direkt für eine Person. Die Unterschrift garantiert lediglich für eine "digitale Identität". Das kann zum Beispiel ein Konto auf einem Computer sein. So wie im beschriebenen Szenario. Oder die Unterschrift könnte für eine E-Mail-Adresse garantieren.
Wie kann eine digitale Unterschrift trotzdem mit einer Person aus Fleisch und Blut in Verbindung gebracht werden? Die Lösung heisst: **Zertifikate**. Ein Zertifikat wird durch eine Behörde ausgestellt. Es belegt, dass hinter einer gewissen Unterschrift eine ganz bestimmte Person steckt. Ein Zertifikat lässt sich mit einem Pass vergleichen. Im Pass steht Ihre Unterschrift zusammen mit Angaben zu Ihrer Person. Damit kann folglich belegt werden, dass Ihre Unterschrift zu Ihnen selbst gehört.

Quellenverzeichnis

Bücher / Artikel

Diffie W., Hellman M.: New directions in cryptography. In: IEEE Transactions on Information Theory. 22 (1976), 644-654.

Näf M.: Public Key Kryptologie – Die Idee mit den beiden Schlüsseln. Zürich 1997 (ETH Institut für Verhaltenswissenschaft, ETH Institut für Informatik). *Lernaufgabe innerhalb einer Semesterarbeit im Rahmen der Didaktikausbildung*.

Salomaa A.: Public-Key Cryptography. Berlin Heidelberg 1990 (Springer).

Welsh D.: Codes and Cryptography. New York 1988 (Oxford University Press).