INFORMATIONSGESELLSCHAFT UND DATENSICHERHEIT:

ASYMMETRISCHE VERSCHLÜSSELUNG

Dieses Werk ist unter einem **Creative Commons 3.0 Deutschland Lizenzvertrag** lizenziert:

- Namensnennung
- Keine kommerzielle Nutzung
- Weitergabe unter gleichen Bedingungen

Um die Lizenz anzusehen, gehen Sie bitte zu http://creativecommons.org/licenses/by-nc-sa/3.0/de oder schicken Sie einen Brief an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Miriam Klein – E-Mail: miriam.klein@lmg-bzk.de – Januar 2020

Inhaltsverzeichnis

Hinweis zur Verzahnung mit Mathematik:

Das Konzept der asymmetrischen Verschlüsselung ist Basis sowohl für den Informatik Unterricht *Informationsgesellschaft und Datensicherheit* als auch für den Mathematikunterricht *mathematische Grundlagen der Kryptologie*. Eine enge Abstimmung mit dem Kollegen, der IMP-Mathematik unterrichtet, ist notwendig.

Fall 1 : Im Mathematikunterricht wurde noch nicht mit *mathematische Grundlagen der Kryptologie* begonnen: Dann wird im Informatikunterricht diese Einheit ‚normal' am Stück unterrichtet.

Fall 2: Der Mathematikunterricht beginnt mit *mathematischen Grundlagen der Kryptologie* bevor der Informatikunterricht mit *Informationsgesellschaft und Datensicherheit (IuD)* beginnt: Dann werden die beiden Kapitel

IuD - Wiederholung Kryptologie Klasse 8 und

IuD - Asymmetrische Verschlüsselung

im Mathematikunterricht als Einstieg unterrichtet und später im Informatikunterricht weggelassen. Der Informatikunterricht beginnt dann mit dem Kapitel *Man-in-the-middle*.

Das Thema *(9) die behandelten Verschlüsselungsverfahren vergleichend beurteilen* des Bildungsplans Mathematik (Mathem. Grundl. der Kryptologie) wurde in den Bereich Informatik übernommen, weil es thematisch sehr gut im Anschluss an die Asymmetrische Verschlüsselung unterrichtet werden kann. (*06_iud_ab_vergleich_verfahren.odt*)

Ergänzung: Mit dem Arbeitsblatt 0e*_iud_ab_Caesar-mod.odt* kann eine Verknüpfung zwischen der (neuen) Modulo-Rechnung und dem (bekannten) Cäsarverfahren hergestellt werden – sofern das noch nicht in Mathematik erfolgt ist.

Wiederholung Kryptologie Klasse 8

Material: *01_iud_ab_wdh.odt*
00_iud_krypto.odp (Folie 3-10)

Aus Klasse 7 und 8 kennen die SuS bereits Transpositions- sowie Substitutionsverfahren (Cäsar, Vigenère, One-Time-Pad) und wissen, dass moderne symmetrische Verschlüsselungsverfahren auf elementaren Verschlüsselungsverfahren basieren und einen Kompromiss zwischen Sicherheit und Praktikabilität sind.

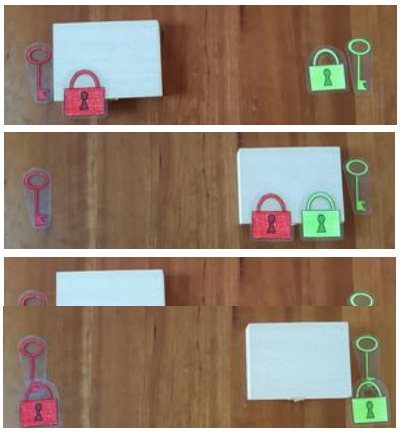
Auf dem ersten Arbeitsblatt werden die Verschlüsselungsverfahren mit ihren Vor-und Nachteilen werden wiederholt. Es werden die Gefahren bei einer Kommunikation über einen unsicheren Kanal sowie die daraus resultierenden Kryptoziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit behandelt. Auf Verbindlichkeit wird im Folgenden nicht weiter eingegangen.

Der Schlüsseltausch ist bei symmetrischen Verfahren ein zentrales Problem, das nur mit einem persönlichen Treffen gelöst werden kann. Allerdings gibt ein interessantes Verfahren, Merkles Puzzle, bei dem dieses Problem auch ohne persönliches Treffen gelöst wird[1]. Das geht aber weit über den Bildungsplan hinaus und sei hier als Hintergrundinformation erwähnt.

1*https://de.wikipedia.org/wiki/Merkles_Puzzle (abgerufen 27.4.20)*

Asymmetrische Verschlüsselung

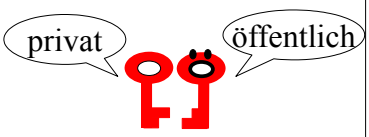
Material: *02_iud_ab_asym.odt*
02_iud_mat_schluessel.odt
00_iud_krypto.odp (Folie 12-20)



Als erste Idee, dass das Schlüsselproblem gelöst werden könnte eignet sich folgende Analogie:

Alice verschlüsselt die Nachricht mit ihren Schloss und schickt sie zu Bob (Bild 1). Bob verschlüsselt die Nachricht zusätzlich mit seinem Schloss und schickt sie zurück zu Alice (Bild 2). Alice entfernt ihr Schloss (Bild 3). Nun kann Bob sein Schloss entfernen und die Nachricht lesen (Bild 4).

Diese Veranschaulichung ist für die SuS sofort verständlich: Das Schloss als Einwegfunktion ist sehr einleuchtend. Um allerdings eine korrekte Analogie zu öffentlichem und privatem Schlüssel zu erhalten, müsste Alice eher ein geöffnetes Schloss verschicken, das Bob zu „klickt“ und damit seine Nachricht an Alice verschlüsselt. Nur Alice hat den Schlüssel zum Öffnen des Schlosses. Weiterhin hinkt der Vergleich (Schloss = privater Schlüssel, Schlüssel = öffentlicher Schlüssel) beim Signieren von Nachrichten. Trotzdem kann man das Prinzip den SuS vorstellen, um grundsätzlich zur Idee der asymmetrischen Verschlüsselung zu gelangen.



Verschlüsselungsverfahren, bei denen Sender und Empfänger einer verschlüsselten Nachricht verschiedene Schlüssel haben, nennt man asymmetrische Verfahren. Hierbei wird ein Schlüsselpaar erzeugt. Den privaten Schlüssel behält man, den öffentlichen Schlüssel kopiert man und verteilt ihn an jeden, der mit einem kommunizieren möchte.

Wird eine Text mit dem privaten Schlüssel verschlüsselt, kann man ihn nur mit dem öffentlichen Schlüssel entschlüsseln. Wird ein Text mit dem öffentlichen Schlüssel verschlüsselt, kann man ihn nur mit dem privatem Schlüssel entschlüsseln.

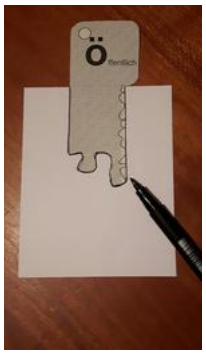
Zur schematischen Darstellung: Im Folgenden wird ein Schlüsselpaar immer in derselben Farbe dargestellt. Der Schlüssel mit dem **Ö** im Ring ist der öffentliche, der Schlüssel ohne ein **Ö** ist der private.

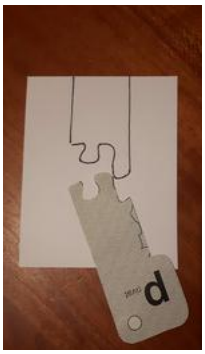
Die SuS spielen auf dem AB *02_iud_ab_asym_rsa.odt* das Ver- und Entschlüsseln händisch mit den Schlüsselpaaren des Materials durch (Aufgabe 2-3).

Vorbereitung: Die bunten Schlüssel (*02_iud_mat_schluessel.odt)* werden ausgeschnitten und laminiert. Für jede Gruppe wird ein privater Schlüssel und zwei bis drei öffentliche Schlüssel benötigt. (Das Material kann wiederverwendet werden, jedoch ist die Herstellung aufwendiger.)

Einfache Variante (ohne Wiederverwendung):
Die schwarzweiße Seite wird kopiert und in Streifen geschnitten. Zusätzlich schneidet man so viele

leere Streifen, wie Gruppen vorhanden sind. Jede Gruppe erhält ein Schlüsselpaar, welches von den SuS noch auseinander geschnitten werden muss. Weiterhin muss jede Gruppe aus dem leeren Streifen 1-2 Kopien des öffentlichen Schlüssels anfertigen.





Durchführung: Die SuS teilen sich in Dreier- oder Vierergruppen auf. Alice erhält ein Schlüsselpaar, sowie die Kopien ihres öffentlichen Schlüssels. Die öffentlichen Schlüssel gibt sie ihren beiden Freunden Bob und Charlie. Will man eine Nachricht verschlüsseln, so schreibt man die Nachricht auf einen DIN-A-6-Blatt, faltet ihn in der Mitte, legt den öffentlichen Schlüssel des Empfängers darauf und zeichnet die Schnittlinie ab. Der Empfänger legt seinen privaten Schlüssel an die Schnittlinie. Passt er, kann er die Nachricht entschlüsseln und darf den Zettel öffnen und lesen.

Die SuS erkennen folgende Zusammenhänge:

Wird mit dem öffentlichen Schlüssel verschlüsselt und mit dem privaten Schlüsselt entschlüsselt, dann kann die Nachricht nicht mitgelesen werden (Kryptoziel: Vertraulichkeit).

Wird mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüsselt entschlüsselt, dann ist die Nachricht nicht vertraulich, weil jeder den öffentlichen Schlüssel zum Entschlüsseln haben und anwenden kann. Aber es ist gesichert, dass die Nachricht tatsächlich vom Absender stammt. Die Verschlüsselung mit dem privaten Schlüssel ist vergleichbar mit einer Unterschrift, die unter ein Dokument gesetzt wird. Gemäß dieser Parallele nennt man das Anwenden des privaten Schlüssels *signieren* und das darauffolgende Anwenden des öffentlichen Schlüssels *verifizieren*. (Kryptoziel: Authentizität)

Beim eigentlichen Verfahren der „digitalen Signatur“ wird aus einem Text ein Hashwert (Fingerprint) generiert und nur auf diesen wird der private Schlüssel angewendet. Die eigentliche Nachricht wird nicht notwendigerweise verschlüsselt. Die digitale Signatur wird erst später betrachtet.

Anmerkung: Im Zusammenhang mit Vertraulichkeit werden die Begriffe *verschlüsseln* und *entschlüsseln* verwendet. Im Zusammenhang mit Authentizität hingegen werden die Begriffe s*ignieren* und v*erifizieren* verwendet. Das Verfahren ist in beiden Fällen das Gleiche: Der Schlüssel wird *angewendet:*

- Verschlüsseln: Der öffentliche Schlüssel wird auf einen Text angewendet, um Vertraulichkeit sicherzustellen. Durch Entschlüsseln (mit dem privaten Schlüssel) wird der Klartext wieder hergestellt.
- Signieren: Der private Schlüssel wird auf einen Text angewendet, um Authentizität sicherzustellen, der Text wird signiert. Die Authentizität wird geprüft, indem der öffentliche Schlüssel angewendet wird (= verifizieren).

Bis Klasse 10 wurden die Begriffe „einen Schlüssel *anwenden*“ und „*ver-* bzw. *entschlüsseln“* im Unterricht synonym verwendet. Nachdem an dieser Stelle die neue Möglichkeit des Signierens eingeführt wird, sollte darauf geachtet werden, im Zusammenhang mit Authentizität nicht die Begriffe *ver-* und *entschlüsseln* zu verwenden, sondern „einen Schlüssel *anwenden*“. Damit wird unterstrichen, dass es hierbei nicht um Geheimhaltung geht.

In Aufgabe 5 wird das Erlernte eingeübt - diesmal nicht händisch, sondern mit einem Chat-Tool. Dazu bilden die SuS Dreiergruppen. Je Gruppe wird ein Server gestartet und jeder Schüler startet einen Client und meldet sich am Server an. (siehe Aufgabe)

In Aufgabe 4 werden symmetrische und asymmetrische Verfahren verglichen hinsichtlich der benötigten Anzahl an Schlüsseln.

Nachteil asymmetrischer Verschlüsselung:

In der praktischen Anwendung eignen sich asymmetrische Verfahren, wie das RSA-Verfahren nicht zur Verschlüsselung längerer Texte. Je länger der zu verschlüsselnde Text, desto länger der Schlüssel und desto länger dauert das Verschlüsseln. Das erkennt man auch im Chat-Tool, wo zwischen verschieden langen Schlüsselpaaren gewählt werden kann. (Auspobieren!) Eine Verschlüsselung mit RSA dauert ca. 100 mal so lang wie mit dem symmetrischen AES-Verfahren.

Hinweis: Falls dieser Einstig innerhalb IMP-Mathematik unterrichtet wird, geht es an dieser Stelle weiter mit den mathematischen Grundlagen der Kryptologie. Der IMP-Informatikunterricht beginnt in diesem Fall erst an dieser Stelle.

Aufgabe auf dem AB	**zugehörige Folie in der Präsentation**
Nr. 2	15 - 16
Nr. 3	17
Nr. 4	18 - 19
Nr. 5	20

Man-in-the-middle-Angriff

Material: 03_iud_ab_man-in-the-middle.*odt*
00_iud_krypto.odp (Folie 21-29)

Nachdem die SuS das Prinzip der asymmetrischen Verschlüsselung verstanden haben, wird die Frage aufgeworfen, ob es bei dieser Art der Kommunikation wirklich keinen Angriffspunkt gibt.

Beim symmetrischen Verfahren ist der Schlüsseltausch das zentrale Problem. Das Verteilen des öffentlichen Schlüssels sollte beim asymmetrischen Verfahren kein Problem darstellen, da der öffentliche Schlüssel (wie der Name schon sagt) kein Geheimnis darstellt. Dennoch gibt es genau hier eine Schwachstelle, die die SuS finden sollen.

Die SuS spielen in Aufgabe 1 das Szenario durch, das beginnt, bevor Alice ihren öffentlichen Schlüssel verteilt hat und erstellen dazu das Sequenzdiagramm.

Gearbeitet wird wieder in Dreiergruppen. Jede Dreiergruppe erhält drei Schlüsselpaare (für Alice, Bob, Mal). Alternativ kann man zuerst nur Alice ein Schlüsselpaar (mit zwei öffentlichen Schlüsseln) geben. Das zusätzliche Schlüsselpaar für Mal erhält die Gruppe erst wenn die SuS die Notwendigkeit erkennen, dass Mal auch ein eigenes Schlüsselpaar benötigt. Oder sie erhalten Mals Schlüsselpaar bei Bedarf als Tipp.

Für Mal ist es leicht, die Nachricht mit dem öffentlichen Schlüssel von Alice zu lesen und eine Kopie des öffentlichen Schlüssels für sich zu erstellen. Allerdings stellt das kein Problem da, da Alice Schlüssel ohnehin öffentlich ist. Problematisch ist allerdings, wenn Mal die Nachricht abfängt, den Schlüssel von Alice entfernt und durch seinen eigenen öffentlichen Schlüssel ersetzt. Bob erhält scheinbar eine Nachricht von Alice mit einem Schlüssel. Er geht davon aus, dass dies Alice Schlüssel ist und verschlüsselt damit vertrauliche Nachrichten an Alice. Diese kann Mal lesen, weil er ja den passenden privaten Schlüssel hat. Leitet er die Nachricht weiter an Alice (unverändert oder manipuliert) verschlüsselt er sie zuvor mit Alice öffentlichem Schlüssel. Alice denkt nun, die verschlüsselte Nachricht käme von Bob.

Das zentrale Problem (siehe Aufgabe 2) ist also, dass nicht sichergestellt werden kann, ob der erhaltene öffentliche Schlüssel tatsächlich vom scheinbaren Absender stammt. Die Lösung könnte in einem persönlichen Treffen liegen oder in einer Person, der beide Kommunikationspartner vertrauen und deren öffentlichen Schlüssel sie bereits auf sicherem Weg erhalten haben. Sie wird im Folgenden CAty genannt, von Certification Authority. Zentraler Punkt ist, dass Alice und Bob Caty vertrauen, es ist hingegen nicht notwendig, dass Caty jemandem vertraut.

Auf dem Arbeitsblatt wird in Aufgabe 3 die man-in-the-middle-Problematik mit dem bereits bekannten Chat-Tool praktisch umgesetzt.

Aufgabe 4 führt hin zur Idee und Notwendigkeit eines Zertifikats. Diese Aufgabe ist nicht zwingend notwendig und man kann stattdessen auch gleich zu den Zertifikaten übergehen. Es soll nicht der Eindruck erweckt werden, dass CAty eine Art Schlüsseldatenbank ist, an die alle ihre Schlüsselanfragen stellen. Tatsächlich prüft die CA die Identität der Antragsteller und stellt ihnen das Zertifikat aus. Für die Verteilung sind die Zertifikat-Eigentümer selber verantwortlich.

Bob fragt in Aufgabe 4 Alice nach ihrem öffentlichen Schlüssel. Alice bittet CAty zu bestätigen, dass es sich um Alice Schlüssel handelt. CAty wendet auf die Nachricht mit Alice Schlüssel ihren eigenen privaten Schlüssel an und schickt sie zu Bob. Bob wendet Catys öffentlichen Schlüssel an, verifiziert also die Nachricht und hat Alice öffentlichen Schlüssel. Mal kann Alice Nachricht

mit der Bitte um Bestätigung nicht lesen, weil Alice sie mit CAtys öffentlichen Schlüssel verschlüsselt hat. Die Vertraulichkeit der Nachricht ist sichergestellt. Die Nachricht, die Alice Schlüssel beinhaltet, kann Mal lesen, weil er CAtys öffentlichen Schlüssel hat. Das ist aber nicht problematisch, da es sich um den öffentlichen Schlüssel von Alice handelt, den jeder haben darf. Weil CAty auf die Nachricht, die Alice Schlüssel beinhaltet, ihrem eigenen privaten Schlüssel anwendet, kann Bob sicher sein, dass die Nachricht von CAty stammt.

Eine Schwachstelle (siehe Aufgabe 4 d) liegt z.B. darin, dass Mal eine verschlüsselte Nachricht von Alice an CAty sieht und vermutet, dass dies eine Schlüsselanfrage sein könnte (weil CAty ja als vertrauenswürdige Person bekannt ist). Spätestens mit diesem Hinweis können die SuS erkennen, dass Mal Bobs Nachricht abfängt und statt dessen eine eigene Schlüsselanfrage nach seinem, Mals, Schlüssel an CAty schickt. CAty kennt Mals öffentlichen Schlüssel, wendet auf die Nachricht mit Mals Schlüssel ihrem eigenen privaten Schlüssel an (Authentifizierung) und schickt sie zurück. Mal braucht nichts weiter zu tun, als diese Nachricht an Bob weiterzuleiten. Da die Nachricht als Antwort auf seine Schlüsselanfrage kommt und zudem von CAty signiert ist, geht er fälschlicherweise davon aus, dass es sich um Alice Schlüssel handelt. Nun kann Mal Bobs Nachrichten an Alice lesen und ändern. Weiterhin kann Mal in Bobs Namen Nachrichten an Alice schicken.

Die Lösung dieses Dilemmas (siehe Aufgabe 4 e) besteht darin, dass CAty nicht nur den Schlüssel von Alice signiert, sondern zusätzlich Alice Namen. Nun würde es sofort auffallen, wenn die Nachricht nicht Alice sondern Mals Schlüssel (und auch seinen Namen) beinhaltet.

Aufgabe auf dem AB	zugehörige Folie in der Präsentation
Nr. 1	21 - 23
Nr. 2	24 - 25
Nr. 4 a-c, d, e	26, 27, 28 (- 29)

Zertifikate

Material: *04_iud_ab_zertifikat.odt*
00_iud_krypto.odp (Folie 29-31)

Eine Einheit aus dem Namen und dem öffentlichem Schlüssel, die mit dem privaten Schlüssel einer Zertifizierungsinstanz (also einer vertrauenswürdigen CAty) verschlüsselt ist, nennt man Zertifikat. Eine Zertifizierungsinstanz (Zertifizierungsstelle, Certification Authority (CA)) ist (wie CAty) eine vertrauenswürdige Instanz, die die Zertifikate sicher verwaltet.

Tatsächlich beantwortet die Zertifizierungsstelle nicht jede einzelne Schlüsselanfrage, sondern stellt für Alice ein Zertifikat aus, verschlüsselt dieses mit dem privaten Schlüssel der Zertifizierungsstelle und übergibt es Alice. Alice schickt dieses verschlüsselte Zertifikat an ihre Kunden. Um sicher zu sein, dass Alice wirklich Alice ist, muss Alice persönlich bei der Zertifizierungsstelle erscheinen und sich ausweisen.

Damit nicht alle Kunden bei der Zertifizierungsstelle nach deren öffentlichem Schlüssel anfragen müssen, ist der öffentliche Schlüssel der Zertifizierungsstelle direkt im Browser eingetragen.

Es gibt nicht nur eine einzelne CA für die ganze Welt, sondern mehrere, die hierarchisch gegliedert sind und sich gegenseitig vertrauen.

Es sollte die Problematik thematisiert werden, dass Zertifizierung auf dem Vertrauen gegenüber der gesamten Hierarchie der Zertifizierungsstellen beruht. Ein Fehler bzw. Betrug bei einer der Instanzen hätte Folgen für jeden Nutzer des Zertifikats.

In Aufgabe 1 verwenden die SuS das Chat-Tool unter Einbeziehung von Zertifikaten.

Digitale Signatur

Material: *05_iud_ab_digit_signatur.odt*
00_iud_krypto.odp (Folie 32 - 39)

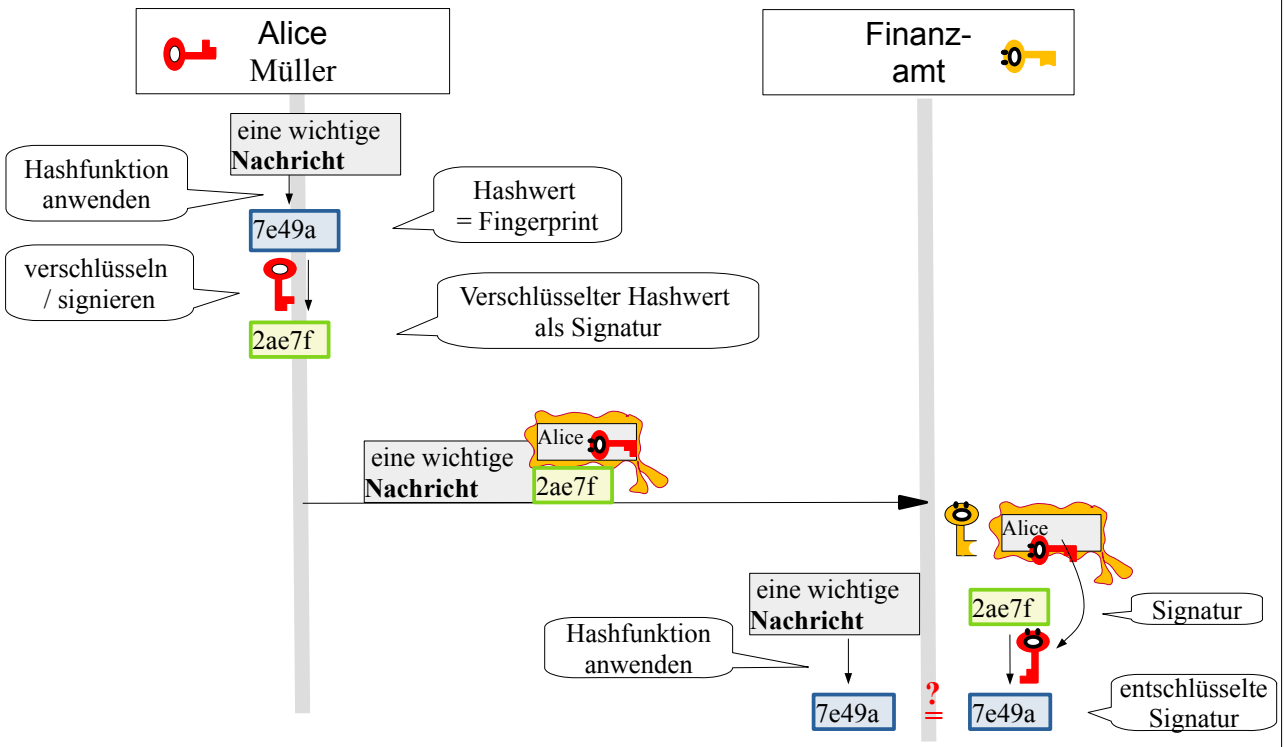
Mit einem Zertifikat kann man seinen öffentlichen Schlüssel ‚fälschungssicher' an Personen verteilen, die einem damit vertrauliche Nachrichten schicken können.

Ein Zertifikat bietet aber noch mehr Möglichkeiten:

Immer, wenn eine elektronische Unterschrift eine Unterschrift auf Papier ersetzen soll, kann eine digitale Signatur eingesetzt werden. (Anträge bei Behörden, Steuererklärung beim Finanzamt, Firmen, die anderen Firmen Rechnungen stellen,…)

So verschlüsselt Frau Müller zum Beispiel ihre Steuererklärung mit dem öffentlichen Schlüssel des Finanzamts, dessen Zertifikat sie erhalten hat. Damit ist die Nachricht vertraulich und kann nicht mitgelesen werden. Aber wie kann das Finanzamt sicher sein, dass die Steuererklärung tatsächlich von Frau Müller stammt? Dazu benötigt Frau Müller ein eigenes Zertifikat.

Ablauf:



Um Zeit zu sparen, wird nicht die komplette Nachricht signiert, sondern nur ein kleiner Teil, der Fingerabdruck der Nachricht. Dazu wird mit einer Hash-Funktion ein Hash-Wert berechnet. Das ist der Fingerabdruck der Nachricht. Nur auf diesen (viel kleineren) Hash-Wert wird der private Schlüssel angewendet. Das Ergebnis ist die Signatur. Die Signatur wird zusammen mit der Nachricht an den Empfänger geschickt. Das Zertifikat ihres öffentlichen Schlüssels schickt Alice gleich mit. Der Empfänger trennt die Nachricht von der Signatur. Auf die Nachricht wendet er die Hash-Funktion an und erzeugt den Fingerabdruck der Nachricht. Parallel dazu wendet er den

öffentlichen Schlüssel aus dem Zertifikat auf die Signatur an und erhält den Fingerabdruck der Nachricht. Diese beiden Fingerabdrücke vergleicht er. Sind sie gleich, stammt die Nachricht tatsächlich von Alice.

Die Hashfunktion erzeugt eine Art Fingerabdruck der eigentlichen Nachricht. Also einen Text, der viel kürzer ist als die Nachricht und aus dem man die ursprüngliche Nachricht nicht wieder herleiten kann. Weiterhin ist es nicht möglich, die Nachricht so zu verändern, dass der Hash wieder gleich ist. (Diese Genauigkeit genügt in Klasse 10.)

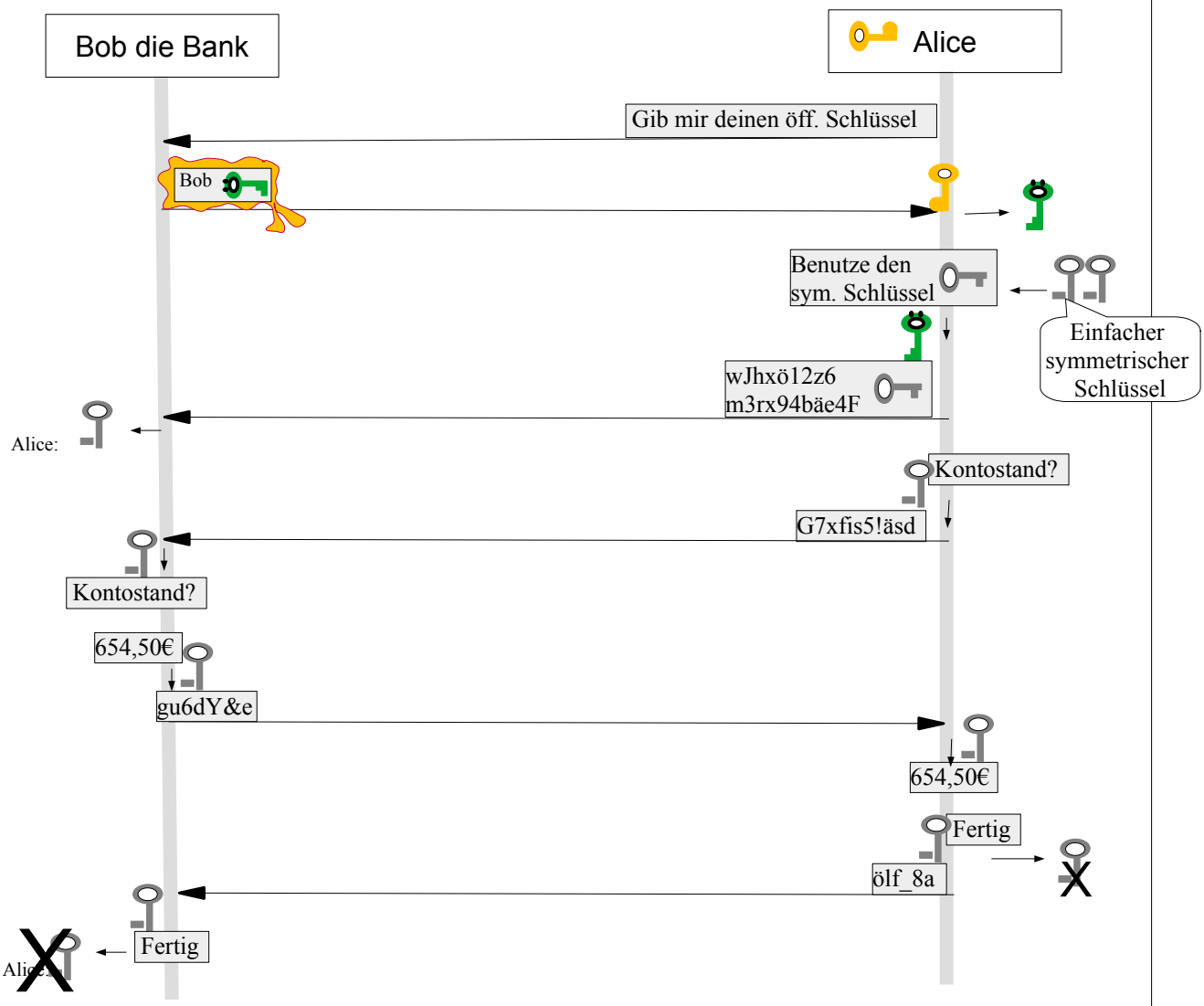
In Aufgabe 1 analysieren die SuS den im Diagramm dargestellten Ablauf und bringen ihn mit der Definition aus Wikipedia in Zusammenhang. In Teilaufgabe (d) wird das Szenario dahingehend erweitert, dass die eigentliche Nachricht zusätzlich verschlüsselt wird. Damit sind dann Authentizität und Vertraulichkeit gewährleistet.

In den Aufgaben 2-4 spielen die SuS die Szenarien des Signierens und Verschlüsselns mit den Chat-Tool durch. Zunächst ohne Zertifikat (Aufgabe 2-3), dann mit Zertifikat Aufgabe 4).

In Aufgabe 5 wird eine asymmetrisch-symmetrische Browserkommunikation analysiert, bei der nur der Austausch eines (symmetrischen) Schlüssels asymmetrisch erfolgt (siehe Diagramm). Alice schickt dazu eine Anfrage an Bobs Internetseite, und teilt mit, dass sie kommunizieren will. Bob sendet ihr sein Zertifikat. Alice Browser entschlüsselt das und merkt sich Bobs öffentlichen Schlüssel. Es wird eine Nachricht an Bob geschickt mit einem symmetrischen Schlüssel. Die folgende Kommunikation findet mit diesem symmetrischen Schlüssel statt. Wenn die Seite verlassen wird, wird der Schlüssel wieder gelöscht.

Hintergrund: Hybride Verschlüsselung:

> In der praktischen Anwendung wird das RSA-Verfahren verwendet, um einen symmetrischen Schlüssel sicher auszutauschen. Die eigentliche Verschlüsselung erfolgt dann mit einem symmetrischen Verfahren, z.B. AES.
>
> Solche hybride Verschlüsselungsverfahren kombinieren symmetrische und asymmetrische Verschlüsselungsverfahren und nutzen so die jeweiligen Vorteile:
>
> Symmetrische Verschlüsselungsverfahren sind sehr schnell und eignen sich auch für große Datenmengen. Asymmetrische Verschlüsselungsverfahren sind hingegen sehr langsam und nur für kleine Datenmengen geeignet, also z.B. um einen Schlüssel für ein symmetrisches Verfahren zu verschlüsseln. Dafür löst asymmetrische RSA-Verfahren das Problem des Schlüsseltauschs, das bei symmetrischen Verfahren ein Angriffspunkt ist. Der symmetrische Schlüssel wird nur für die Dauer einer Sitzung verwendet.



Asymmetrisch-symmetrische Browserkommunikation

In Aufgabe 6 informieren sich die SuS, wie ein echtes Zertifikat aussieht und recherchieren nach den einzelnen Bestandteilen. Dazu kann man sich im Browser z.B. Zertifikate anzeigen lassen, die der Browserhersteller direkt in den Browser integriert hat.

Firefox:	Chrome:	Internet Explorer:
Einstellungen → Datenschutz & Sicherheit → Sicherheit → Zertifikate → Zertifikate anzeigen.	Je nach Version: *kleines grünes Schloss links der Adresszeile.* Oder: *rechts der Adresszeile die drei Punkte anklicken → weitere Tools → Entwicklertools (oder F12) → Sicherheit → Zertifikat anzeigen → Details.*	*Menü: Datei → Eigenschaften → Zertifikate → Zertifizierungspfad → Zertifikat anzeigen → Details.*

Mögliche Probleme werden in Aufgabe 7 und 8 betrachtet.

In Aufgabe 9 wird im Chat-Tool mit der Hashfunktion experimentiert und die SuS gelangen zu folgenden Erkenntnissen:

- Der Hashwert ist immer gleich lang, unabhängig von der Länge des Ursprungstextes. (Bei der MD2(128 bits)-Variante ist er 128 Bit bzw. 16 HexZahlen lang)
- Selbst wenn nur ein einzelnes Zeichen geändert wird, ändert sich der Hashwert wesentlich. (um mindestens fast 50%)
- Weil der Hashwert kürzer ist als der Ursprungstext, muss es zu einem Hashwert mehrere Ausgangstexte geben.
- Es ist quasi unmöglich, zu einem Hashwert den Ausgangstext zu rekonstruieren.

Ergänzung/Differenzierung:

Alternativ oder zur Differenzierung können die SuS mit Cryptool experimentieren und Hashwerte erzeugen. Eine Anleitung sowie Aufgaben findet man auf inf-schule.de[2]

Ebenfalls als Differenzierung recherchieren die SuS in Aufgabe 9 gängige Hashfunktionen und deren Algorithmen.

In Aufgabe 11 und 12 recherchieren die SuS PGP-Systeme (pretty good privacy) und Web-of-Trust, das auf transitiven Vertrauensbeziehungen der Teilnehmer beruht. Ausgehend davon können Vor- und Nachteile analysiert und diskutiert werden.

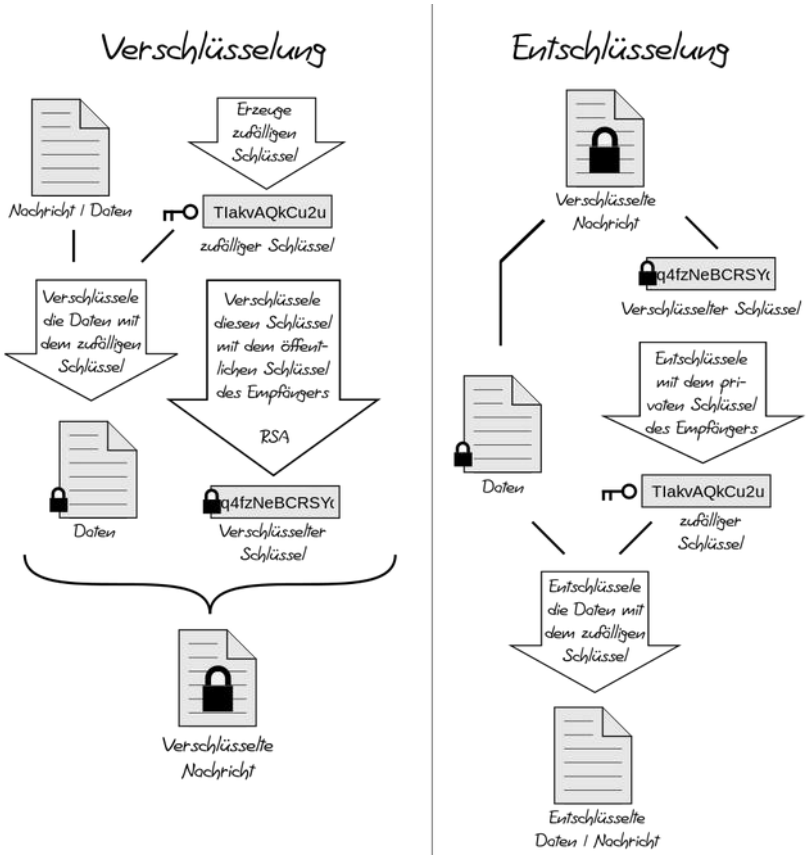
Hintergrund:

Pretty Good Privacy (PGP)

Um Zeit und Rechenkapazität zu sparen, wird nicht die ganze Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Vielmehr wird ein zufälliger symmetrischer Schlüssel erzeugt, womit die Nachricht verschlüsselt wird. Nur der symmetrische Schlüssel wird mit dem öffentlichen Schlüssel verschlüsselt. Vorteile:

- benötigt weniger Zeit
- weniger Rechenkapazität
- geht dieselbe Nachricht an mehrere Empfänger, muss nur einmal verschlüsselt werden.

Mit PGP kann man eine Nachricht nur signieren, nur verschlüsseln oder sowohl signieren als auch verschlüsseln.

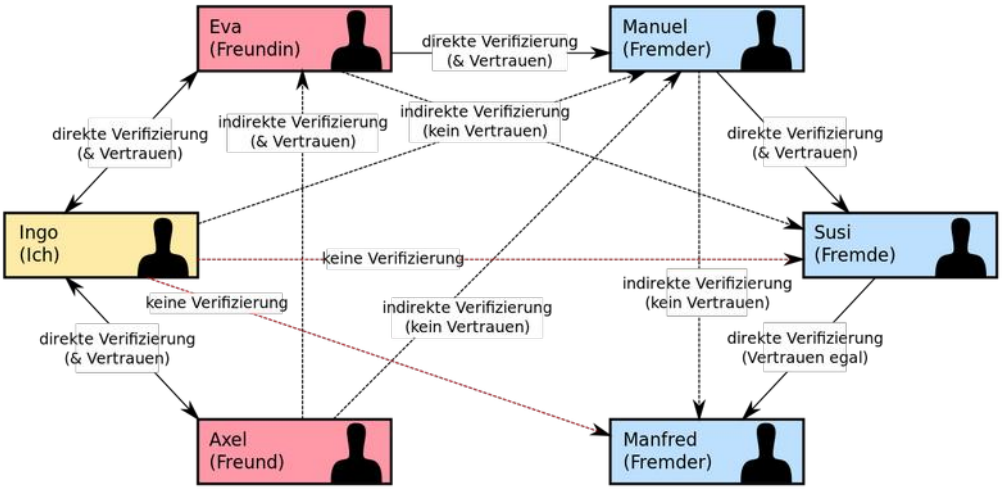


https://commons.wikimedia.org/wiki/File:PGP_diagram_de.svg (16.5.20)
Gregorerhardt / CC BY-SA (https://creativecommons.org/licenses/by-sa/4.0)

2 *https://www.inf-schule.de/kommunik*
(abgerufen: 30.3.20)

PGP wurde 1991 von Phil Zimmermann entwickelt und basiert auf dem Web of Trust.

Web of Trust (WOT)



https://commons.wikimedia.org/wiki/File:Web_of_Trust_2.svghttps://upload.wikimedia.org/wikipedia/commons/4/49 Web_of_Trust_2.svgUser:Ogmios / CC BY-SA (https://creativecommons.org/licenses/by-sa/3.0) (16.5.20)

Das WOT ist eine Alternative zum Prinzip der hierarchisch gegliederten Zertifizierungsinstanzen. Die Echtheit der Schlüssel wird durch ein Netz von gegenseitigen Vertrauensbeziehungen gewährleistet: Alice vertraut Bob, ich vertraue Alice, also vertraue ich auch Bob.

Siehe dazu auch Wikipedia [3] [4] sowie inf-schule.de[5]

Aufgabe auf dem AB	zugehörige Folie in der Präsentation
Nr. 1 (1 d)	32, 33 (34)
5	35
6	36
9	37
11, 12	38, 39

3 *https://de.wikipedia.org/wiki/Pretty_Good_Privacy (28.3.20)*
4 *https://de.wikipedia.org/wiki/Web_of_Trust (28.3.20)*
5 *https://www.inf-schule.de/kommunikation/kryptologie/sicherheitsinfrastruktur/konzept_weboftrust (28.3.20)*

Vergleich der Verfahren

Material: *06_iud_ab_vergleich_verfahren.odt,*
*00_iud_krypto.odp (*Folie 40-42)

Hinweis: Das Thema ist im Bildungsplan Mathematik – Mathematische Grundlagen der Kryptologie enthalten, passt aber thematisch besser an diese Stelle.

Im AB *06_iud_ab_vergleich_verfahren.odt* werden alle bisher kennengelernten Verschlüsselungsverfahren gegenübergestellt und bezüglich ihrer Sicherheit bewertet.

Weitere Hinweise:

Ein Tool, mit dem Sequenzdiagramme erstellt werden können (auch von SuS):
http://www.umletino.com [6]

6 *zuletzt abgerufen 3.6.20*