

Asymmetrische Verschlüsselung

Aufgabe 1: Herr Schlaumeier muss seine Klasse für einige Zeit per Fernunterricht von zu Hause aus unterrichten. Um den Schülerinnen und Schülern die Noten der letzten Klassenarbeit mitzuteilen schlägt er folgendes Vorgehen vor:

Damit außer euch die Nachricht ganz sicher niemand lesen kann, verschlüssele ich die Nachricht mit dem Vigenère-Verfahren. Dazu schicke ich jedem von euch in einer ersten Mail ein individuelles Schlüsselwort. In einer zweiten Mail schicke ich jedem von euch eine mit dem Vigenère-Verfahren verschlüsselte Nachricht, die eure Noten enthält. Die Nachricht könnt ihr mit dem Schlüsselwort aus der ersten Mail entschlüsseln.

Diskutiert, ob das ein sinnvolles Vorgehen ist, um die Noten geheim zu halten.

Das Problem mit dem Schlüssel

Bei allen Verschlüsselungsverfahren, die ihr kennengelernt habt, besteht das Problem, dass sich die beiden Personen, die geheim kommunizieren möchten, zunächst auf einen gemeinsamen geheimen Schlüssel einigen müssen. Man spricht daher von **symmetrischer Verschlüsselung**. Sender und Empfänger verwenden den gleichen geheimen Schlüssel.

Damit niemand den Schlüssel mithören oder mitlesen kann, muss ein persönliches Treffen stattfinden oder es muss einen Boten geben, dem die beiden Personen vertrauen. Wir können aber nicht jede Person, mit der wir E-Mails oder Nachrichten über einen Messenger austauschen oder deren Webseite wir verwenden, vorher persönlich treffen.

Das Prinzip der asymmetrischen Verschlüsselung

Unsere sichere, geheime Kommunikation im Internet beruht daher auf einer Idee aus dem Jahr 1976: die **asymmetrische Verschlüsselung**. Dabei verwenden Sender und Empfänger unterschiedliche Schlüssel. Jeder, der geheim kommunizieren möchte, benötigt nur ein solches Schlüsselpaar. Das Schlüsselpaar ist so konstruiert, dass einer der Schlüssel an beliebig viele Personen verteilt werden kann und nicht geheim gehalten werden muss. Mit diesem Schlüssel kann man eine Nachricht nämlich nur verschlüsseln. Um die Nachricht wieder zu entschlüsseln, benötigt man den zweiten Schlüssel, den nur der Empfänger besitzt. Den Schlüssel, der an die Sender verteilt wird, nennt man **öffentlichen Schlüssel**. Den Schlüssel, den der Empfänger für sich behält, nennt man **privaten Schlüssel**. Mit dem öffentlichen Schlüssel kann man eine Nachricht weder entschlüsseln noch auf den privaten Schlüssel schließen. Deshalb kann der öffentliche Schlüssel für jeden sichtbar ins Internet gestellt oder per E-Mail verschickt und für beliebig viele Kommunikationspartner verwendet werden.

Wir können uns den öffentlichen und den privaten Schlüssel wie ein Vorhängeschloss mit einem Schlüssel vorstellen. Stell dir vor, du besitzt ganz viele Vorhängeschlösser, die du alle mit dem gleichen Schlüssel öffnen kannst und diesen Schlüssel besitzt nur du. Dann könntest du allen deinen Freunden so ein Vorhängeschloss schicken. Wenn deine Freunde dir eine geheime Nachricht übermitteln möchten, legen sie diese in eine Kiste und verschließen sie mit dem Vorhängeschloss. Dieses Vorhängeschloss kann dein Freund nun nicht mehr öffnen. Und auch ein Bote, der dir die Kiste bringt, kann das Schloss nicht öffnen. Der Einzige, der das Schloss öffnen und die Nachricht lesen kann, bist du, da nur du den Schlüssel für das Vorhängeschloss besitzt. Natürlich müssen Kiste und Schloss so stabil sein, dass sie sich wirklich nur mit dem Schlüssel öffnen lassen!

Die Abbildungen 1 bis 3 stellen den Austausch geheimer Nachrichten mithilfe eines öffentlichen und eines privaten Schlüssels schematisch dar.

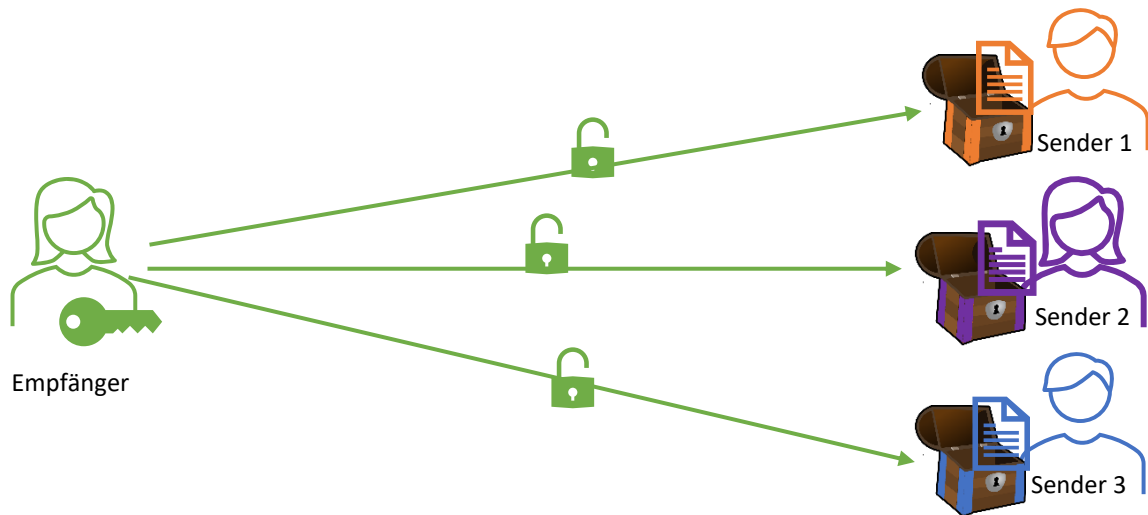


Abbildung 1: Empfänger verteilt öffentliche Schlüssel (hier Vorhängeschloss)

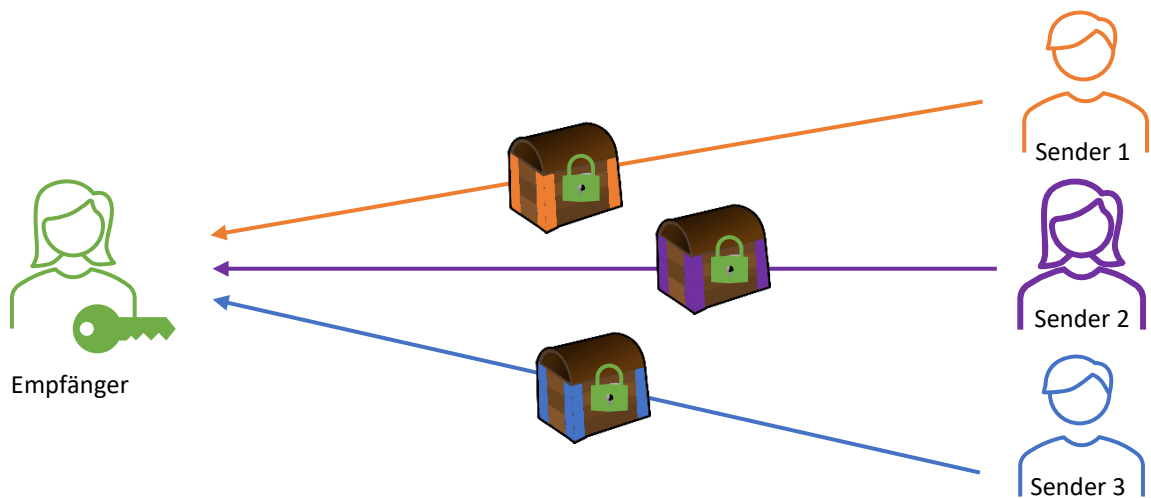


Abbildung 2: Versand der geheimen Nachrichten

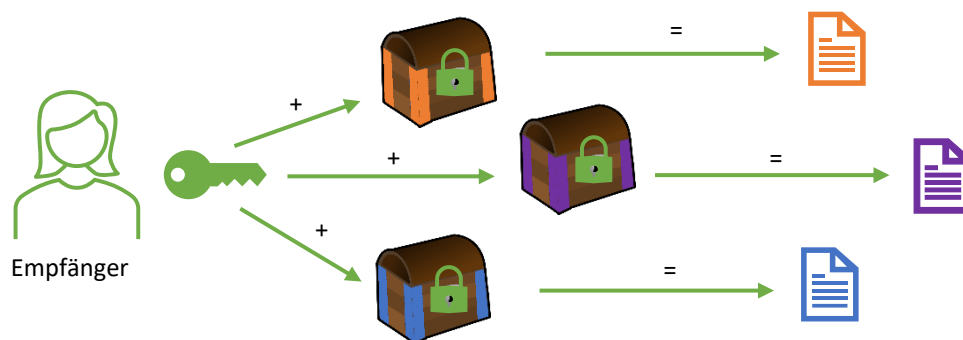


Abbildung 3: Entschlüsseln der geheimen Nachrichten mithilfe des privaten Schlüssels

Aufgabe 2: Skizziere, wie die Abbildungen 1 bis 3 erweitert werden müssten, damit Sender 1 eine geheime Antwort der Empfängerin erhalten kann.

Aufgabe 3: In Abbildung 4 siehst du vier Personen. Jeder soll mit jedem geheime Nachrichten austauschen können, ohne dass die anderen beiden mitlesen können. Zeichne in der Abbildung ein, welche Schlüssel die Personen dazu benötigen. Stelle private Schlüssel als Schlüssel oder *P* und öffentliche Schlüssel als Schloss oder *Ö* dar. Wähle jeweils die passende Farbe, um die Schlüssel einer Person zuzuordnen.

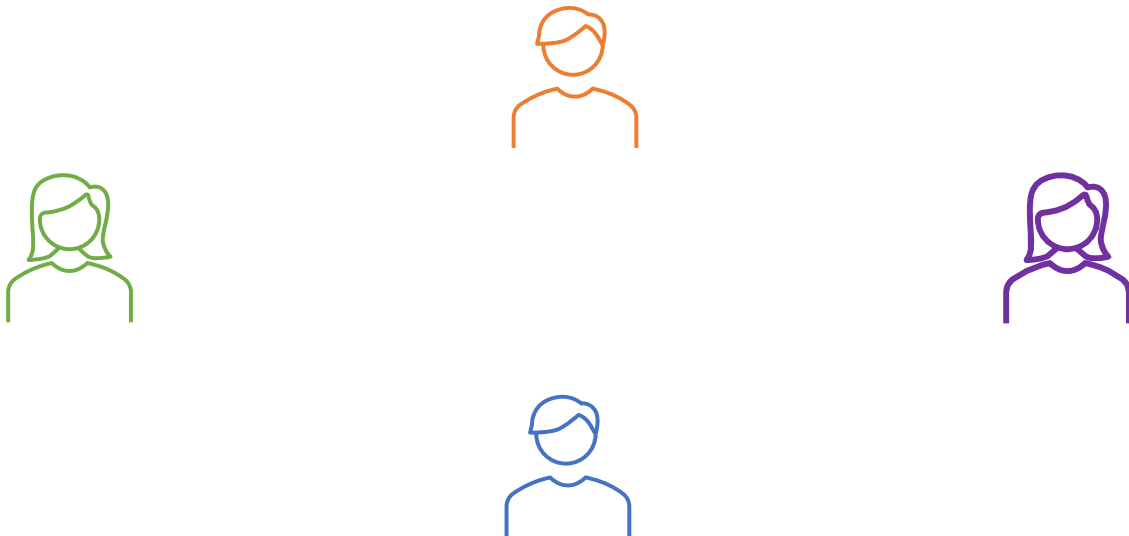


Abbildung 4: Vier Personen, die in jeder Zweierkombination geheim kommunizieren möchten.

Aufgabe 4:

- a) Erläutere, wie ein asymmetrisches Verschlüsselungsverfahren verwendet werden kann, um das Problem aus Aufgabe 1 zu lösen.
- b) Frau Neunmalklug hat ihrer Klasse eine Aufgabe gestellt. Die Lösungen sollen in einen gemeinsamen Klassenordner hochgeladen werden. Um zu verhindern, dass jemand einfach eine vorhandene Abgabe kopiert und seinen Namen darunterschreibt, möchte Frau Neunmalklug, dass die Schülerinnen und Schüler ihren Text vor dem Hochladen verschlüsseln. Erläutere, wie hier ein asymmetrisches Verschlüsselungsverfahren eingesetzt werden kann.

Asymmetrische Verschlüsselung in der Praxis

Asymmetrische Verschlüsselungsverfahren, die bei der Kommunikation im Internet eingesetzt werden, können wir uns als Rechenverfahren vorstellen. Die Zeichen, aus denen eine Nachricht besteht, werden zunächst mit Zahlen codiert, z. B. mithilfe des ASCII-Codes. Auf diese Zahlen wird dann die Rechenvorschrift, der Verschlüsselungsalgorithmus, angewendet. Der öffentliche und der private Schlüssel sind ebenfalls Zahlen, die in die Rechnung mit einfließen. Die Rechenvorschrift muss dabei so konstruiert sein, dass man die Rechnung, die mithilfe des öffentlichen Schlüssels durchgeführt wurde, nicht einfach umkehren und rückgängig machen kann. Sonst könnte ja jeder die Nachricht rekonstruieren. Stattdessen gelingt es nur mithilfe des privaten Schlüssels aus der geheimen Nachricht den Klartext zu berechnen. Außerdem darf es nicht möglich sein oder nur mit

sehr, sehr großem Zeitaufwand, aus dem öffentlichen Schlüssel den privaten zu berechnen, obwohl die beiden Schlüssel zusammenhängen.

Das können wir uns an einem Beispiel klar machen: Das Produkt der Primzahlen 37 und 113 lässt sich leicht berechnen: $37 \cdot 113 = 4181$. Es dürfte jedoch deutlich länger dauern, bis du herausgefunden hast, welche Primzahlen für die Zahl 4853 multipliziert wurden. Denn hier hilft nur ausprobieren. Wenn wir Primzahlen mit 100 Stellen und mehr multiplizieren und nur das Produkt weitergeben, würde es sogar Jahre dauern, bis man die richtigen Primfaktoren findet.

Asymmetrische Verschlüsselungsverfahren verwenden daher häufig große Primzahlen zum Erzeugen der Schlüssel. Da die genauen Rechenvorschriften zum Erzeugen eines Schlüsselpaares und zum Ver- und Entschlüsseln ziemlich kompliziert sind, überlassen wir das Rechnen an dieser Stelle dem Rechner.

Wir schauen uns das Vorgehen bei der asymmetrischen Verschlüsselung stattdessen aus der Anwendersicht noch ein wenig genauer an. Ein Softwarepaket, das es jedem ermöglicht ein asymmetrisches Schlüsselpaar zu erstellen und zu verwenden, ist *GnuPG4Win*. Mit deinem Schlüsselpaar kannst du z. B. den Text deiner E-Mails verschlüsseln.

Aufgabe 5: Das Softwarepaket *GnuPG4Win* enthält die Schlüsselverwaltungsprogramme *Kleopatra* und *GPA*. Erstelle dir mithilfe von einem dieser Programme dein persönliches asymmetrisches Schlüsselpaar. Tauscht anschließend eure öffentlichen Schlüssel untereinander aus.

Eine genaue Anleitung dazu findest du in den Dateien *Anleitung_SchlüsselErzeugen_Kleopatra* bzw. *Anleitung_SchlüsselErzeugen_GPA*.

Aufgabe 6: In der Datei *Anleitung_Ver_Entschlüsseln_Kleopatra* bzw. *Anleitung_Ver_Entschlüsseln_GPA* findest du eine Anleitung zum Ver- und Entschlüsseln von Texten. Tauscht mithilfe des Programms geheime Nachrichten aus. Jeder sollte dabei mindestens einmal der Sender und einmal der Empfänger sein. Fertigt dabei ein kurzes Protokoll an, in dem ihr festhaltet, wer welchen Schlüssel verwendet hat.

Beispiel: Hannah kommuniziert mit Bernhard:

1. Hannah schreibt eine Nachricht und verschlüsselt sie mit dem öffentlichen Schlüssel von Bernhard.
2. Bernhard erhält die Nachricht von Hannah und entschlüsselt sie mit ...
3. ...
4. ...

Das Problem mit dem Vertrauen

Kommen wir noch einmal zurück zu Frau Neunmalklug. Sie findet in dem Klassenordner für die Hausaufgabenabgabe die zwei verschiedenen Texte in Abbildung 5, unter denen jeweils von Hannah Hübsch steht. Frau Neunmalklug stellt Hannah zur Rede. Sie behauptet, sie habe den linken Text nicht hochgeladen. Frau Neunmalklug ist unsicher, ob sie Hannah glauben soll.

Mathehausaufgabe

Ich habe heute keine Lust zu rechnen, rechnen Sie doch selbst!

von Hannah Hübsch

Mathehausaufgabe

Aufgabe 1:

$$3x + 7 = 14x - 4 \quad | -3x$$

$$7 = 11x - 4 \quad | +4$$

$$11 = 11x \quad | :11$$

$$1 = x$$

von Hannah Hübsch

Abbildung 5: Hausaufgaben unterzeichnet mit Hannah Hübsch

Aufgabe 7:

- Diskutiert, ob Frau Neunmalklug Hannah glauben sollte. Warum wäre es einfacher Hannah zu glauben, wenn Frau Neunmalklug die Hausaufgaben in der Schule eingesammelt hätte.
- Erstellt eine Liste mit Verfahren, die ihr kennt, um die Echtheit einer Nachricht bzw. des Absenders in der analogen Welt zu garantieren.

Die digitale Unterschrift

Wenn es darum geht, die Echtheit des Absenders sicherzustellen, spricht man von **Authentifikation**. Auch hier kann die asymmetrische Verschlüsselung helfen. Du hast bereits gelernt, dass es sich bei dem privaten und dem öffentlichen Schlüssel um Zahlen handelt, die zusammen mit der Nachricht in eine Rechnung einfließen. Beim Verschlüsseln führt zuerst der Sender die Rechnung mit dem öffentlichen Schlüssel durch. Anschließend führt der Empfänger die Rechnung mit dem privaten Schlüssel durch, um die Nachricht zu entschlüsseln. Die Reihenfolge der Rechnungen lässt sich aber auch umdrehen. Das heißt, die Nachricht wird zuerst mithilfe des privaten Schlüssels des Senders codiert und anschließend mithilfe des öffentlichen Schlüssels decodiert, so dass man wieder die ursprüngliche Nachricht erhält.

Aufgabe 8: Begründe die folgenden Aussagen:

Wenn der Absender zuerst seinen privaten Schlüssel zur Codierung der Nachricht verwendet und dann der Empfänger diese mit dem öffentlichen Schlüssel des Absenders decodiert, ...

- ... handelt es sich nicht um eine Verschlüsselung, mit der die Nachricht geheim gehalten werden kann.
- ... kann der Empfänger sicher sein, von wem die Nachricht stammt.

Das Codieren einer Nachricht mit dem privaten Schlüssel bezeichnet man auch als **Signieren** oder als **digitale Unterschrift**. Da nur der Absender im Besitz seines privaten Schlüssels ist, kann nur er diesen Code für die Nachricht erzeugt haben. Überprüfen kann ihn hingegen jeder, der den öffentlichen Schlüssel des Absenders besitzt. Auch das Vorgehen beim Signieren einer Nachricht schauen wir uns anhand des Programms *Kleopatra* bzw. *GPA* etwas genauer an.

Aufgabe 9: Eine Anleitung zum Signieren von Nachrichten findest du in der Datei *Anleitung_Signieren_Kleopatra* bzw. *Anleitung_Signieren_GPA*.

- a) Schreibe in einem Editor eine kurze Antwort zu der Frage „Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Verschlüsselungsverfahren?“.
- b) Signiere deine Antwort und lade sie anschließend in einen gemeinsamen Klassenordner hoch.
- c) Diskutiert, ob es möglich ist ...
 - (1) ... von jemandem abzuschreiben
 - (2) ... eine Antwort unter einem falschen Namen einzureichen.
 - (3) ... eine Abgabe von jemand anderem zu verändern.
- d) Bearbeite deinen Antworttext jetzt so, dass ihn nur dein Lehrer/deine Lehrerin lesen kann und dass deine Lehrerin sicher sein kann, dass die Antwort von dir ist.
- e) Halte fest ...
 - (1) ... was man unter einer Signatur versteht
 - (2) ... worin sich das Signieren vom Verschlüsseln unterscheidet

Bei der Bearbeitung von Aufgabe 9 ist dir sicherlich aufgefallen, dass die Nachricht nach dem Erstellen der digitalen Unterschrift immer noch lesbar war. Das Programm hat lediglich einen Code an die Nachricht angehängt. Diesen Code, der die digitale Unterschrift darstellt, kannst du dir bei Interesse im folgenden Abschnitt noch etwas genauer anschauen. Du kannst aber auch gleich mit dem Kapitel *Vertrauen ist gut, Kontrolle ist besser* weiter machen.

Für Interessierte

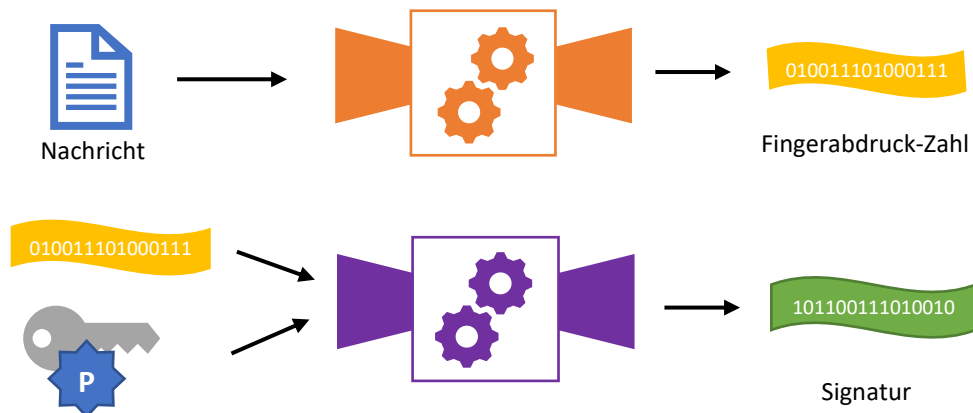
Aufgabe 10: Erstelle zwei verschiedene Nachrichten: eine kurze Nachricht (zwei Wörter oder ein kurzer Satz) und eine lange Nachricht (mindestens zwei Seiten Text). Du musst die lange Nachricht nicht selbst schreiben, sondern kannst einen beliebigen Text kopieren.

- a) Erstelle sowohl für die kurze als auch für die lange Nachricht eine Signatur und vergleiche das Ergebnis. Was fällt dir auf?
- b) Führe sowohl für die kurze als auch für die lange Nachricht eine Verschlüsselung durch und vergleiche das Ergebnis. Gibt es Unterschiede zu den Beobachtungen in a)

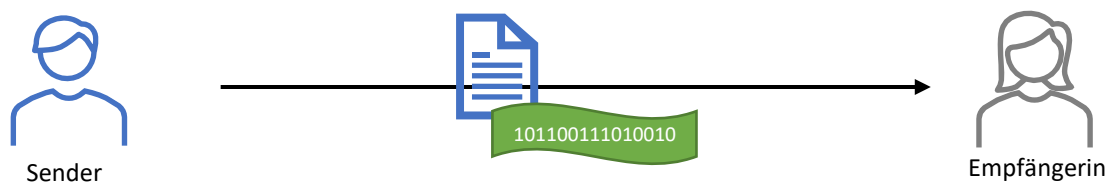
Offensichtlich hat die Signatur eine feste Länge unabhängig vom Umfang der Nachricht. Wie kann das sein? Anders als bei der Verschlüsselung wird nicht die Nachricht selbst codiert. Stattdessen wird die Nachricht mithilfe einer mathematischen Funktion auf eine eindeutige Zahl fester Länge zusammengeschrumpft. Diese Zahl ist wie eine Art **Fingerabdruck** der Nachricht. Die Codierung mit dem privaten Schlüssel wird dann für diese Zahl durchgeführt und der Code an die Nachricht angehängt.

Beim Überprüfen der Signatur decodiert der Empfänger die angehängte digitale Unterschrift mit dem öffentlichen Schlüssel des Senders. Heraus kommt eine Zahl, aber nicht die Nachricht selbst. Woher weiß der Empfänger nun, dass diese Zahl zu der Nachricht passt und die Unterschrift gültig ist? Nun der Algorithmus zum Berechnen der Fingerabdruck-Zahl einer Nachricht ist allgemein bekannt. Den können Programme wie Kleopatra und GPA ausführen. Der Empfänger berechnet also selbst die Fingerabdruck-Zahl der Nachricht und wenn diese der Zahl entspricht, die beim Decodieren der digitalen Unterschrift herausgekommen ist, dann war die Unterschrift gültig. Abbildung 6 veranschaulicht das Erstellen und Überprüfen einer digitalen Signatur.

Sender: Erstellen der Signatur



Übertragen der signierten Nachricht



Empfänger: Überprüfen der Signatur

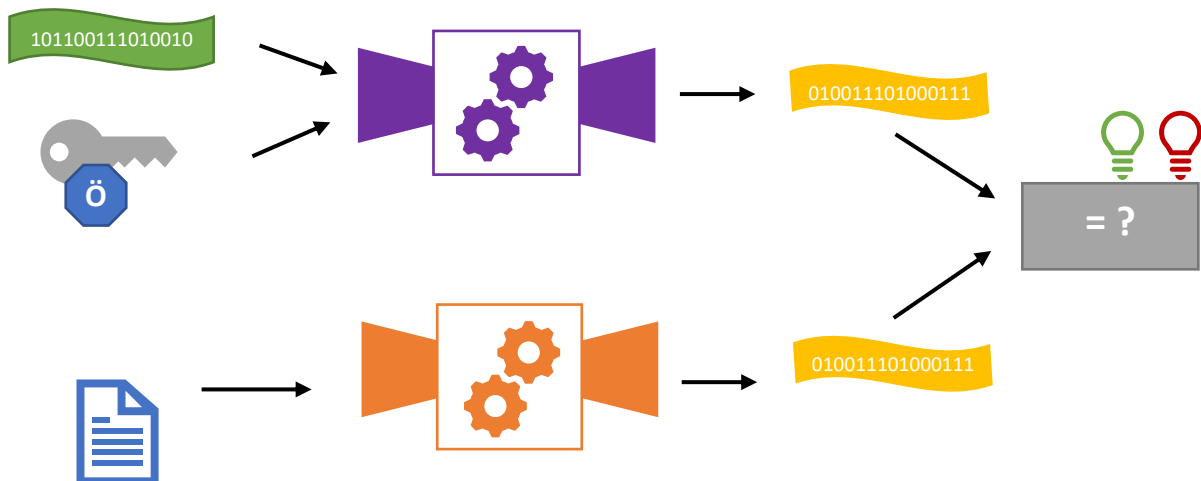


Abbildung 6: Erstellen und Überprüfen einer digitalen Signatur

Aufgabe 11: Erläutere die Vorgänge beim Erstellen und Überprüfen einer Signatur anhand von Abbildung 6.

Vertrauen ist gut, Kontrolle ist besser

Aufgabe 12:

- Tausche mit deinem Nachbarn/deiner Nachbarin eine signierte Nachricht aus.
- Überprüfe die Signatur der Nachricht, die du erhalten hast.
Fällt die Rückmeldung des Programms zur Gültigkeit der Signatur so aus, wie du es erwartet hast? Versuche die Rückmeldung zu erklären.
- In der Datei *nachricht_aufgabe12* findest du eine signierte Nachricht. Kopiere die Nachricht und überprüfe die Signatur. Versuche wieder die Rückmeldung zu erklären.
- Importiere den öffentlichen Schlüssel *Beste Stimme-Team_0xD5F953F1_public.asc*. Wie ändert sich die Rückmeldung, wenn du die Signatur der *nachricht_aufgabe12* noch einmal überprüfst?

Beim Austausch der öffentlichen Schlüssel besteht das Problem, dass ich mir sicher sein muss, welcher Person dieser Schlüssel gehört, also welche Person den passenden privaten Schlüssel dazu besitzt. Eine Signatur wird nur als gültig eingestuft, wenn der zugehörige öffentliche Schlüssel als vertrauenswürdig eingestuft wurde.

Aufgabe 13:

- Suche in deinem Programm nach Möglichkeiten, dich von der Echtheit eines Schlüssels zu überzeugen. Bei *Kleopatra* erhältst du z. B. entsprechende Hinweise, wenn du einen Schlüssel importierst. Du kannst dir auch die Informationen (Details), die zusammen mit dem Schlüssel gespeichert werden, einmal genauer anschauen.
- Suche in deinem Programm nach der Möglichkeit, einen Schlüssel als vertrauenswürdig einzustufen.
- Welche der öffentlichen Schlüssel, die du bereits gesammelt hast, hältst du für vertrauenswürdig? Nimm entsprechende Einstellungen für die Schlüssel im Programm vor.
- Lass dir eine signierte Nachricht von einem Mitschüler / einer Mitschülerin geben, von dem/der du einen vertrauenswürdigen öffentlichen Schlüssel besitzt. Wie fällt die Rückmeldung zur Gültigkeit der Signatur diesmal aus?

Aufgabe 14: Es soll online eine geheime Wahl durchgeführt werden.

- Sammelt Kriterien, die eine gerechte Wahl erfüllen sollte.
- Diskutiert ob und ggf. wie diese Kriterien mithilfe asymmetrischer Verschlüsselung sichergestellt werden können.
- Führt nach den Regeln, die ihr in a) und b) erarbeitet habt, eine geheime Wahl in eurer Klasse durch. Ihr könnt eine Klassensprecherwahl simulieren, den größten Klassenclown wählen oder das Wunschziel für die nächste Klassenfahrt.

Asymmetrische Verschlüsselung im WWW

Die Programme GPA und Kleopatra kannst du verwenden, um z. B. den Text einer E-Mail zu verschlüsseln. Die asymmetrische Verschlüsselung kommt aber auch zum Einsatz, wenn du Webseiten im World Wide Web aufrufst. Webseiten bzw. Webserver, die eine Verschlüsselung verwenden, erkennst du daran, dass im Browser vor der Adresse **https** und ein kleines Schlosssymbol stehen. Das **s** in **https** steht für sicher.

Möglicherweise hast du dich zu Beginn der Einheit zur Kryptologie bereits mit der verschlüsselten Übertragung von Webseiten beschäftigt. Nachdem du nun einiges über Verschlüsselungsverfahren gelernt hast, kannst du die Abläufe, die dabei eine Rolle spielen, besser einordnen. Deshalb greifen wir das Thema hier noch einmal auf.

Aufgabe 15:

- a) Öffne einen Browser und überprüfe welche der Webseiten, die du häufig besuchst, das https-Protokoll verwenden.
- b) Klicke einmal auf das kleine Schloss-Symbol in der Adresszeile einer Webseite, die das https-Protokoll verwendet. Welche Informationen findest du hier, die dir für die sichere Kommunikation mit dem Webserver wichtig erscheinen?

Du fragst dich jetzt vielleicht, warum du bislang gar nicht gemerkt hast, dass die Webseiten, die du häufig aufrufst, verschlüsselt übertragen werden. Vermutlich kennst du auch keinen der öffentlichen Schlüssel deiner Lieblingsseiten. Das liegt daran, dass den Schlüsselaustausch und das Ver- und Entschlüsseln in diesem Fall der Browser und andere Komponenten, die für die Kommunikation mit dem Webserver zuständig sind, für dich übernehmen. Wenn du eine Webseite, die das https-Protokoll verwendet, aufrufst, sendet der Webserver zuerst seinen öffentlichen Schlüssel. Diesen öffentlichen Schlüssel nutzt dein Rechner, um mit dem Webserver einen geheimen Schlüssel zu vereinbaren. Danach können der Webserver und dein Rechner alle Nachrichten, die sie austauschen, ver- und entschlüsseln.

Aufgabe 16: Welche der folgenden Aussagen hältst du für einen Online-Shop, der das https-Protokoll verwendet, für wahr? Begründe.

- a) Wenn ich bei dem Online-Shop meinen Namen und meine Kontonummer angebe, kann die Daten niemand anderes lesen.
- b) Die Identität des Betreibers des Online-Shops wurde überprüft.
- c) Der Online-Shop ist auf jeden Fall seriös.
- d) Wenn ich etwas in das Suchfeld des Online-Shops eingebe, weiß der Betreiber nicht, wonach ich gesucht habe, da die Daten verschlüsselt übertragen werden.
- e) Wenn ich eine Bestellung abschicke, kann niemand die Nachricht abfangen und z. B. meine gegen seine Adresse austauschen.

Aufgabe 17: Gelegentlich kann es passieren, dass beim Aufruf einer Webseite, die das https-Protokoll verwendet, eine Warnung wie in Abbildung 7 erscheint.

Diskutiert, wie ihr euch in diesem Fall verhalten solltet.

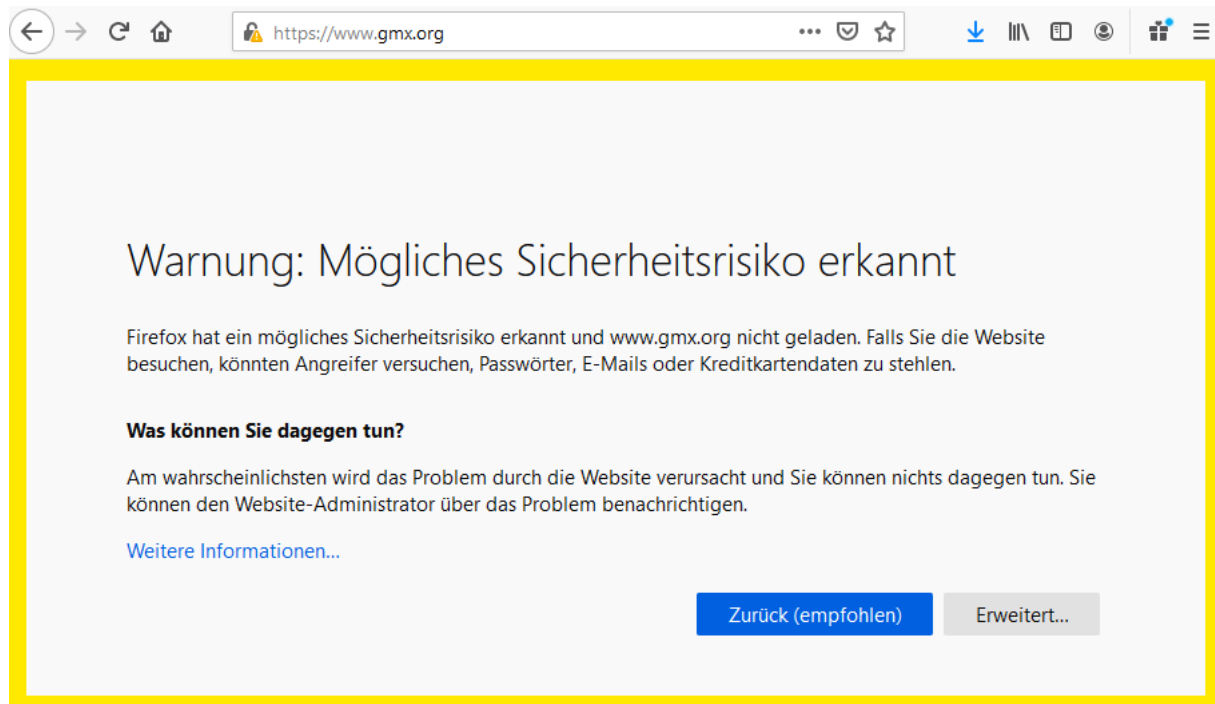


Abbildung 8: Warnung beim Aufruf einer Webseite über das https-Protokoll

Zusammenfassung

Bei der sicheren Kommunikation unterscheidet man zwischen Vertraulichkeit, Integrität und Authentizität. **Vertraulichkeit** bedeutet, dass die Nachricht geheim ist und nicht von einem Dritten mitgelesen werden kann. **Integrität** bedeutet, dass die Nachricht auf ihrem Weg vom Sender zum Empfänger nicht von einem Dritten verändert werden kann. Die **Authentizität** bezieht sich darauf, dass die Nachricht tatsächlich vom angegebenen Absender stammt.

Aufgabe 18: Erläutere, wie alle drei Anforderungen, Vertraulichkeit, Integrität und Authentizität, mithilfe der asymmetrischen Verschlüsselung sichergestellt werden können.

Ein Problem der asymmetrischen Verschlüsselung ist, dass das Ver- und Entschlüsseln sehr viel aufwändiger zu berechnen sind als bei symmetrischen Verfahren. Deshalb werden die asymmetrischen und die symmetrischen Verfahren häufig kombiniert.

Aufgabe 19: Diskutiert, welche Sicherheitsaspekte sich bei der Kommunikation über das Internet nur mit einem asymmetrischen Verfahren umsetzen lassen und wann auch ein symmetrisches Verfahren zum Einsatz kommen kann.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.

Bildnachweis: Mit Ausnahme der Abbildung 8 wurden die Abbildungen mithilfe der Formen und Piktogramme von Microsoft Word 2016 erstellt. In Abbildung 1 bis 3 ergänzt um eine Grafik von Ckcr-Free-Vector-Images auf Pixabay zur freien kommerziellen Nutzung.

Abbildung 8: Screenshot des Browsers Mozilla Firefox

