

Konzepte und Anwendungen der asymmetrischen 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 Note 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 von Whitfield Diffie und Martin Hellman 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 werden und für beliebig viele Kommunikationspartner verwendet werden.

Wir können uns den öffentlichen und den privaten Schlüssel wie ein Vorhängeschloss mit einem Schlüssel vorstellen. Stellen Sie sich vor, Sie besitzen ganz viele Vorhängeschlösser, die Sie alle mit dem gleichen Schlüssel öffnen können und diesen Schlüssel besitzen nur Sie. Dann könnten Sie all Ihren Freunden so ein Vorhängeschloss schicken. Wenn Ihr Freund Ihnen eine geheime Nachricht übermitteln möchte, legt er diese in eine Kiste und verschließt sie mit dem Vorhängeschloss. Dieses Vorhängeschloss kann Ihr Freund nun nicht mehr öffnen. Und auch ein Bote, der Ihnen die Kiste bringt, kann das Schloss nicht öffnen. Der Einzige, der das Schloss öffnen und die Nachricht lesen kann, sind Sie, da nur Sie den Schlüssel für das Vorhängeschloss besitzen. 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.

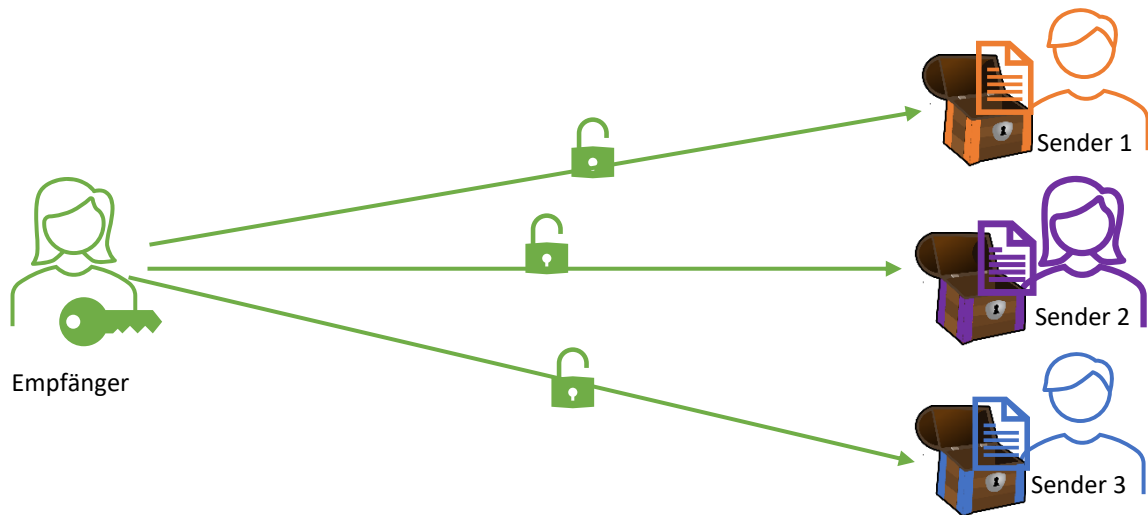


Abbildung 1: Empfänger verteilt öffentliche Schlüssel (hier Vorhängeschloss)

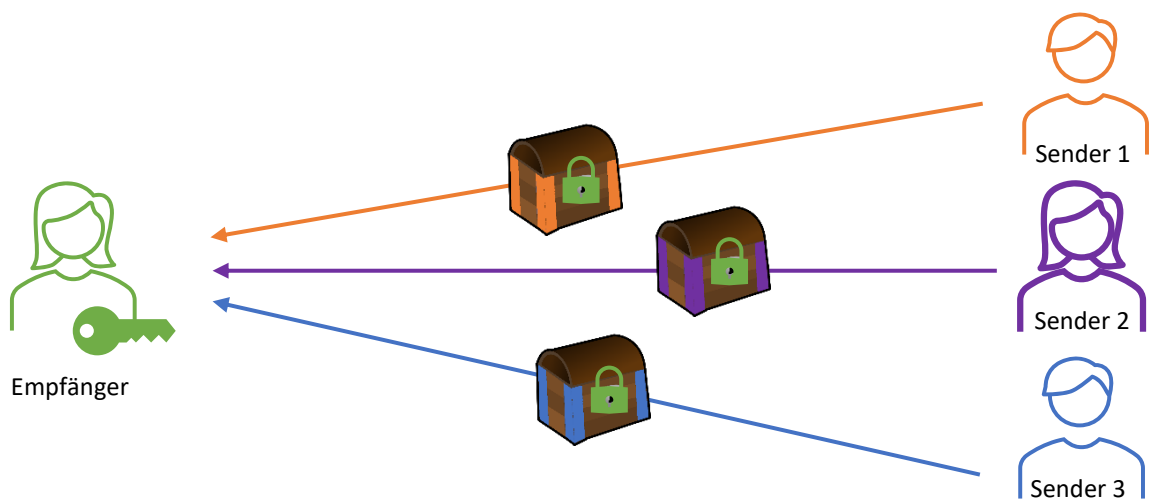


Abbildung 2: Versand der geheimen Nachrichten

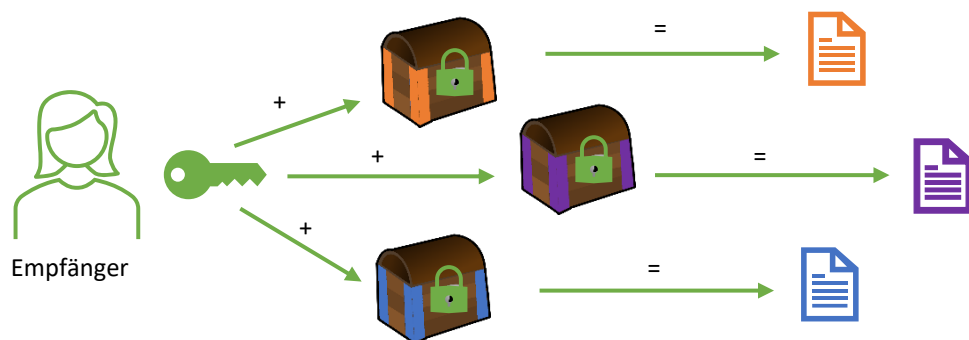


Abbildung 3: Entschlüsseln der geheimen Nachrichten mithilfe des privaten Schlüssels

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

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

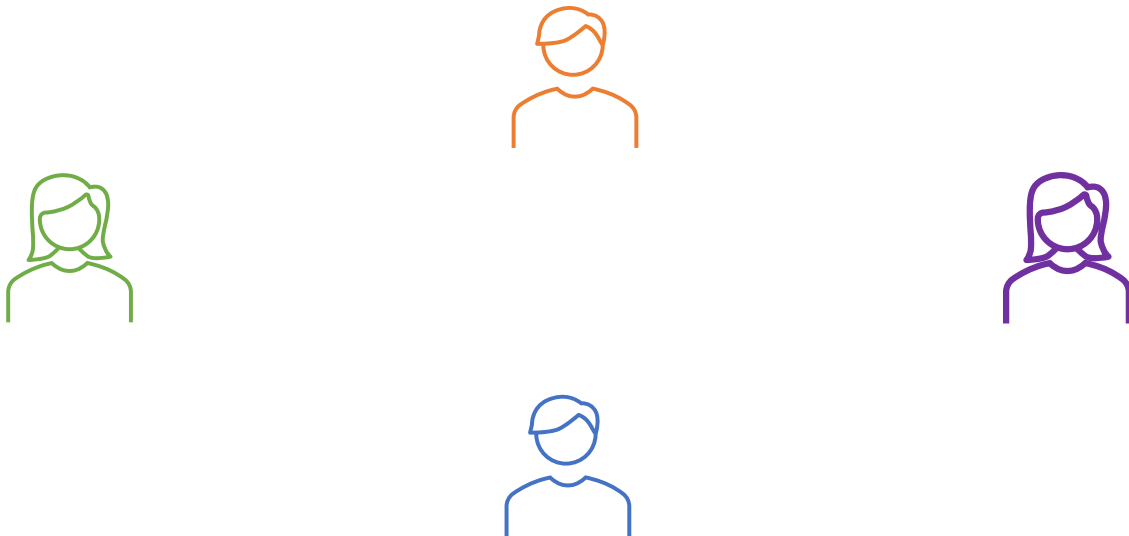


Abbildung 4: Vier Personen, die in jeder Zweierkombination geheim kommunizieren möchten.

Aufgabe 4:

- a) Erläutern Sie, 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.
Erläutern Sie, 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 Sie herausgefunden haben, welche Primzahlen für die Zahl 4853 multipliziert wurden. Denn hier hilft nur ausprobieren. Wenn wir sehr große Primzahlen multiplizieren, so dass das Produkt aus über fünfhundert Ziffern besteht, würde es sogar Millionen Jahre dauern, bis man die richtigen Primfaktoren findet¹.

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 Rechner².

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*³. Mit Ihrem Schlüsselpaar können Sie z. B. E-Mails verschlüsseln.

Aufgabe 5: Das Softwarepaket *GnuPG4Win* enthält die Schlüsselverwaltungsprogramme *Kleopatra* und *GPA*. Erstellen Sie mithilfe von einem dieser Programme Ihr persönliches asymmetrisches Schlüsselpaar. Tauschen Sie anschließend Ihre öffentlichen Schlüssel untereinander aus.

Eine genaue Anleitung dazu finden Sie in den Dateien *Anleitung_SchlüsselErzeugen_Kleopatra* bzw. *Anleitung_SchlüsselErzeugen_GPA*.

Aufgabe 6: In der Datei *Anleitung_Ver_Entschlüsseln_Kleopatra* bzw. *Anleitung_Ver_Entschlüsseln_GPA* finden Sie eine Anleitung zum Ver- und Entschlüsseln von Texten. Tauschen Sie mithilfe des Programms geheime Nachrichten aus. Jeder sollte dabei mindestens einmal der Sender und einmal der Empfänger sein. Fertigen Sie dabei ein kurzes Protokoll an, in dem Sie festhalten, 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. ...

¹ Man bezeichnet das Multiplizieren von Primzahlen daher auch als Einwegfunktion. Eine genaue Erläuterung der Einweg-Funktionen finden Sie hier: Reischuk & Hinkelmann (2006). 17. *Algorithmus der Woche Einweg-Funktionen Vorsicht Falle - Rückweg nur für Eingeweihte!* <https://algo.rwth-aachen.de/~algorithmus/algo17.php> [Datum des Zugriffs: 10.02.2021]

² Wenn Sie sich für die Rechenverfahren, z. B. das RSA-Verfahren interessieren, können Sie sich diese z. B. mithilfe des Werkzeugs Cryptool erarbeiten: <https://www.cryptool.org/de/> [Datum des Zugriffs: 10.02.2021]

³ Ein äquivalentes Softwarepaket für MacOS finden Sie unter <https://gpgtools.org/> [Datum des Zugriffs: 10.02.2021]

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:

- Diskutieren Sie, ob Frau Neunmalklug Hannah glauben sollte. Warum wäre es einfacher Hannah zu glauben, wenn Frau Neunmalklug die Hausaufgaben in der Schule eingesammelt hätte.
- Erstellen Sie eine Liste mit Verfahren, die Sie kennen, 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. Sie haben 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: Begründen Sie 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.
- ... kann der Empfänger sicher sein, von wem die Nachricht stammt.
- Wenn die Nachricht auch geheim gehalten werden soll, muss sie zusätzlich mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden.

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 finden Sie in den Dateien

Anleitung_Signieren_Kleopatra bzw. *Anleitung_Signieren_GPA*.

- a) Schreiben Sie in einem Editor eine kurze Antwort zu der Frage „Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Verschlüsselungsverfahren?“.
- b) Signieren Sie Ihre Antwort und laden Sie sie anschließend in einen gemeinsamen Ordner Ihrer Lerngruppe hoch.
- c) Diskutieren Sie, 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) Bearbeiten Sie Ihren Antworttext jetzt so, dass ihn nur Ihr Lehrer/Ihre Lehrerin lesen kann und dass er bzw. sie sicher sein kann, dass die Antwort von Ihnen stammt.
- e) Halten Sie schriftlich fest,
 - (1) was man unter einer Signatur versteht.
 - (2) worin sich das Signieren vom Verschlüsseln unterscheidet.

Bei der Bearbeitung von Aufgabe 9 ist Ihnen 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, können wir uns noch etwas genauer anschauen.

Aufgabe 10: Erstellen Sie zwei verschiedene Nachrichten: eine kurze Nachricht (zwei Wörter oder ein kurzer Satz) und eine lange Nachricht (mindestens zwei Seiten Text). Sie müssen die lange Nachricht nicht selbst schreiben, sondern können einen beliebigen Text kopieren.

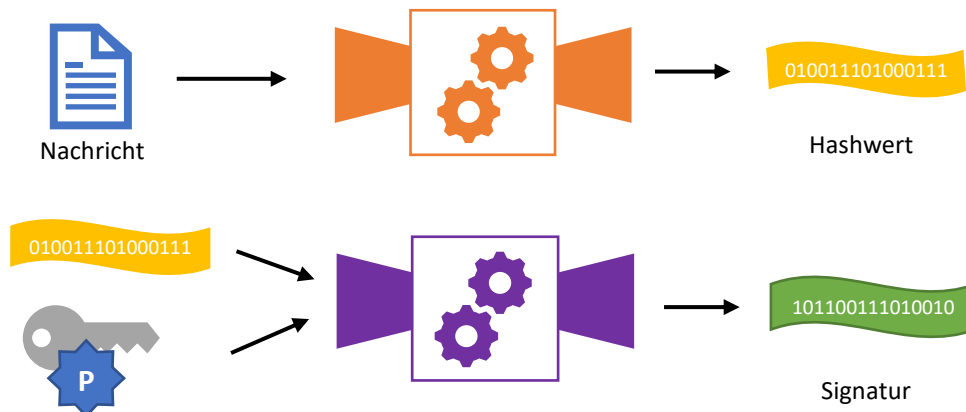
- a) Erstellen Sie sowohl für die kurze als auch für die lange Nachricht eine Signatur und vergleichen Sie das Ergebnis. Was fällt Ihnen auf?
- b) Führen Sie sowohl für die kurze als auch für die lange Nachricht eine Verschlüsselung durch und vergleichen Sie das Ergebnis. Gibt es Unterschiede zu den 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. Eine solche Zahl bezeichnet man als **Hashwert**. Die Codierung mit dem privaten Schlüssel wird dann für diesen Hashwert 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 des Hashwertes einer Nachricht ist allgemein bekannt. Den können

Programme wie Kleopatra und GPA ausführen. Der Empfänger berechnet also selbst den Hashwert 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

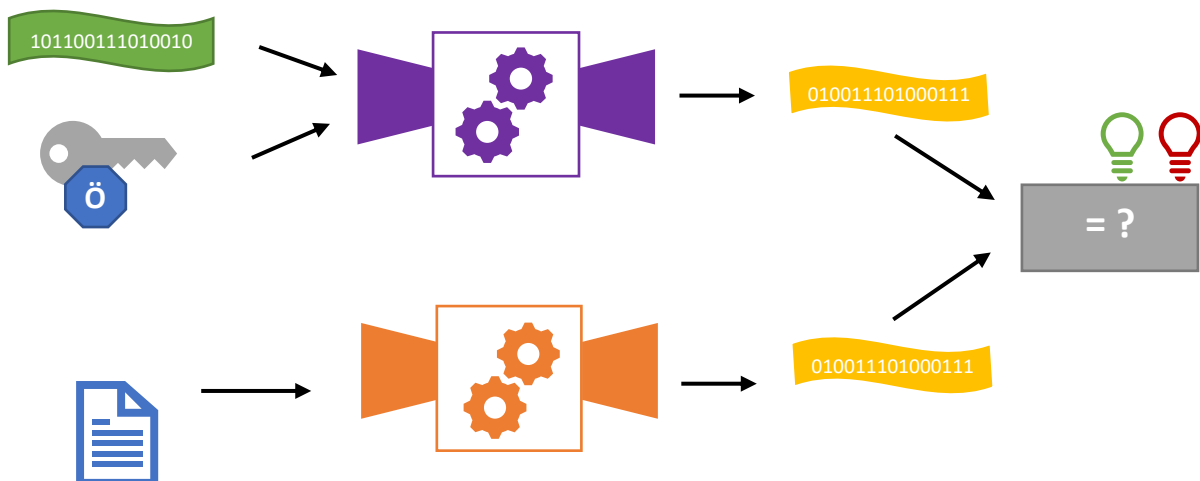


Abbildung 6: Erstellen und Überprüfen einer digitalen Signatur

Aufgabe 11:

- a) An eine Funktion zur Berechnung eines Hashwerts für die Authentifikation einer Nachricht werden die folgenden Anforderungen gestellt. Begründen Sie, warum es wichtig ist, dass die Funktion diese Anforderungen erfüllt.
- (1) Der Hashwert muss von jedem Zeichen der Nachricht abhängen. Ändert sich ein Zeichen, ändert sich auch der Hashwert. (Als Gegenbeispiel können Sie sich überlegen, warum es eine schlechte Idee wäre, als Hashwert immer die ersten zehn Zeichen der Nachricht zu nehmen.)
 - (2) Es muss sehr schwer sein, zu einer signierten Nachricht eine zweite Nachricht zu erzeugen, welche den gleichen Hashwert hat.
- b) Man bezeichnet einen Hashwert, der die Anforderungen aus Aufgabenteil a) erfüllt auch als **Fingerabdruck** einer Nachricht. Begründen Sie.

Wenn Sie mehr über solche Funktionen zum Erzeugen eines Hashwerts bzw. Fingerabdrucks wissen möchten, können Sie hier weiterlesen:

- Christian Schindelbauer (2006). 34. *Algorithmus der Woche: Hashing*. <https://algo.rwth-aachen.de/~algorithmus/algo34.php> [Datum des Zugriffs: 04.02.2021]
- Martin Dietzfelbinger (2006). 37. *Algorithmus der Woche: Fingerprinting*. <https://algo.rwth-aachen.de/~algorithmus/algo37.php> [Datum des Zugriffs: 16.04.2021]

Vertrauen ist gut, Kontrolle ist besser

Aufgabe 12:

- a) Tauschen Sie mit Ihrem Nachbarn / Ihrer Nachbarin eine signierte Nachricht aus.
- b) Überprüfen Sie die Signatur der Nachricht, die Sie erhalten haben.
Fällt die Rückmeldung des Programms zur Gültigkeit der Signatur so aus, wie Sie es erwartet haben? Versuchen Sie die Rückmeldung zu erklären.
- c) In der Datei *nachricht_aufgabe12* finden Sie eine signierte Nachricht. Kopieren Sie die Nachricht und überprüfen Sie die Signatur. Versuchen Sie wieder die Rückmeldung zu erklären.
- d) Importieren Sie den öffentlichen Schlüssel *Beste Stimme-Team_0xD5F953F1_public.asc*. Wie ändert sich die Rückmeldung, wenn Sie die Signatur für die Nachricht in der Datei *nachricht_aufgabe12* noch einmal überprüfen?

Beim Austausch der öffentlichen Schlüssel besteht das Problem, dass Sie sich sicher sein müssen, welcher Person ein Schlüssel gehört, also welche Person den passenden privaten Schlüssel dazu besitzt. Eine Signatur wird nur als gültig eingestuft, wenn Sie den zugehörigen öffentlichen Schlüssel als vertrauenswürdig eingestuft haben.

Aufgabe 13:

- a) Suchen Sie in Ihrem Programm (Kleopatra oder GPA) nach Möglichkeiten, sich von der Echtheit eines Schlüssels zu überzeugen. Bei *Kleopatra* erhalten Sie z. B. entsprechende Hinweise, wenn Sie einen Schlüssel importieren. Sie können sich auch die Informationen (Details), die zusammen mit dem Schlüssel gespeichert werden, einmal genauer anschauen.
- b) Suchen Sie in Ihrem Programm nach der Möglichkeit, einen Schlüssel als vertrauenswürdig einzustufen.
- c) Welche der öffentlichen Schlüssel, die Sie bereits gesammelt haben, halten Sie für vertrauenswürdig? Nehmen Sie entsprechende Einstellungen für die Schlüssel vor.

- d) Lassen Sie sich eine signierte Nachricht von einem Mitschüler / einer Mitschülerin geben, von dem/der Sie einen vertrauenswürdigen öffentlichen Schlüssel besitzen. Wie fällt die Rückmeldung zur Gültigkeit der Signatur diesmal aus?

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

- Sammeln Sie Kriterien, die eine gerechte, geheime Wahl erfüllen sollte.
- Diskutieren Sie ob und ggf. wie diese Kriterien mithilfe eines asymmetrischen Verschlüsselungsverfahrens sichergestellt werden können.
- Führen Sie nach den Regeln, die Sie in a) und b) erarbeitet haben, eine geheime Wahl in Ihrer Lerngruppe durch. Sie können z. B. eine Kursprecherwahl simulieren.

Zertifikate

Bislang haben Sie öffentliche Schlüssel mit Personen ausgetauscht, die Sie kennen. Um sich von der Echtheit des Schlüssels zu überzeugen, konnten Sie z. B. mit der Person sprechen und den Fingerabdruck des öffentlichen Schlüssels vergleichen. Aber wie können wir uns von der Echtheit eines Schlüssels überzeugen, wenn wir den Besitzer nicht persönlich kennen. Diese Situation entsteht z. B. immer dann, wenn Sie eine Webseite aufrufen, die das https-Protokoll verwendet. Das **s** in https steht für sicher. Das heißt, die Daten werden verschlüsselt übertragen und die Identität des Besitzers dieser Webseite wurde überprüft. Aber wer hat die Identität überprüft? Sie wahrscheinlich nicht.

Aufgabe 15: Bei Webseiten, die das https-Protokoll verwenden, erscheint ein kleines Schloss-Symbol in der Adresszeile.

- Öffnen Sie einen Browser und überprüfen Sie, welche der Webseiten, die Sie häufig besuchen, das https-Protokoll verwenden.
- Klicken Sie einmal auf das Schloss. Finden Sie einen Hinweis darauf, wer die Identität des Besitzers der Seite geprüft hat? Welche Informationen finden Sie hier noch, die für die sichere Kommunikation mit dem Webserver wichtig erscheinen?

Vielleicht sind Sie bei Ihrer Recherche auf den Begriff **Zertifikat** gestoßen. Zertifikate bezeugen die Echtheit eines öffentlichen Schlüssels bzw. die Identität seines Besitzers. Da wir nicht mit jedem Betreiber einer Webseite persönlich in Kontakt treten können, übernehmen das **Zertifizierungsstellen** für uns. Das sind Unternehmen oder Organisationen, die als vertrauenswürdig gelten und deren öffentliche Schlüssel in allen Browsern hinterlegt sind. Ein Beispiel für ein solches Unternehmen in Deutschland ist die Telekom AG (www.telesec.de). Wenn wir von einer Zertifizierungsstelle eine Nachricht erhalten, die digital signiert ist, können wir bzw. unser Browser die digitale Signatur überprüfen, da wir den öffentlichen Schlüssel besitzen. Wenn in dieser Nachricht steht, dass der öffentliche Schlüssel \tilde{O}_X einer Person X^4 gehört, dann können wir darauf vertrauen, dass das stimmt, da die Zertifizierungsstelle diese Nachricht unterschrieben hat. Damit Person X für ihren Schlüssel \tilde{O}_X eine solche signierte Nachricht der Zertifizierungsstelle erhält, muss sie sich dort persönlich mit ihrem Schlüssel vorstellen und die Zertifizierungsstelle überprüft die Identität der Person. Ist alles in Ordnung, erstellt sie eine Nachricht mit dem Namen der Person, dem öffentlichen Schlüssel und einigen anderen Informationen und signiert diese Nachricht mit ihrem privaten Schlüssel. Einen auf diese Weise signierten öffentlichen Schlüssel bezeichnet man als **Zertifikat**.

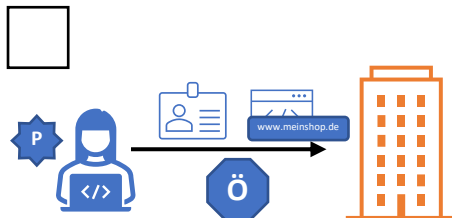
⁴ Alternativ kann ein Öffentlicher Schlüssel z. B. auch einem Unternehmen zugeordnet werden.

Person X kann nun dieses Zertifikat verbreiten und anhand der digitalen Unterschrift der Zertifizierungsstelle, sieht jeder, dass die Informationen in dem Zertifikat vertrauenswürdig sind.

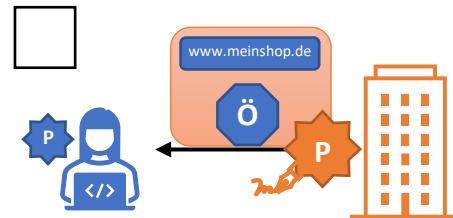
Aufgabe 16:

- Klicken Sie noch einmal auf das Schloss vor der Adresse einer Webseite, die das https-Protokoll verwendet. Suchen Sie nach der Option *Zertifikat anzeigen*. Wählen Sie fünf Informationen aus, die das Zertifikat zusätzlich zum öffentlichen Schlüssel und dem Namen des Besitzers enthält und die Ihnen wichtig erscheinen.
- Suchen Sie in den Einstellungen Ihres Browsers nach einer Liste aller gespeicherten Zertifizierungsstellen.

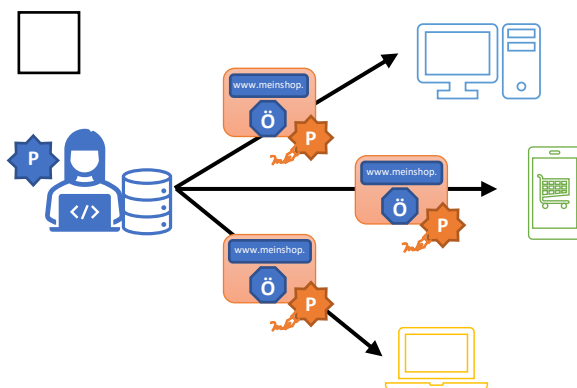
Aufgabe 17: Abbildung 7 stellt die einzelnen Schritte beim Erstellen eines Zertifikats schematisch dar. Bringen Sie die Abbildungen in die richtige Reihenfolge.



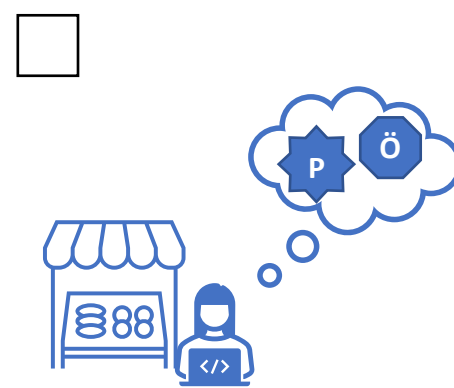
Die Betreiberin des online-Shops bringt ihren öffentlichen Schlüssel, die Adresse ihrer Webseite und einen Identitätsnachweis zur Zertifizierungsstelle.



Die Zertifizierungsstelle erstellt das Zertifikat: Sie signiert den öffentlichen Schlüssel und die Adresse der Webseite mit ihrem privaten Schlüssel.



Der Webserver der Betreiberin kann das Zertifikat an jeden im Internet verteilen.



Die Betreiberin eines online-Shops erstellt ein asymmetrisches Schlüsselpaar.

Abbildung 7: schematische Darstellung der Schritte beim Erstellen eines Zertifikats

Aufgabe 18:

- a) Gelegentlich kann es passieren, dass beim Aufruf einer Webseite, die das https-Protokoll verwendet, eine Warnung wie in Abbildung 8 erscheint.
Diskutieren Sie, wie Sie sich in diesem Fall verhalten sollten.

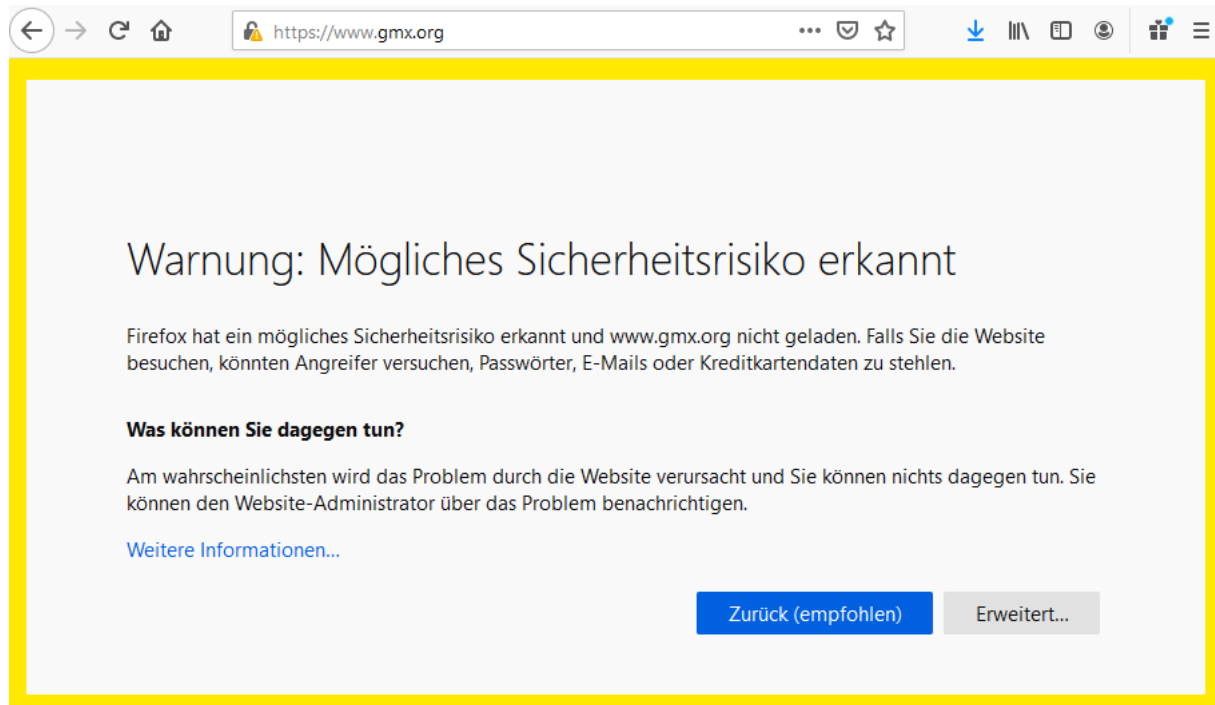
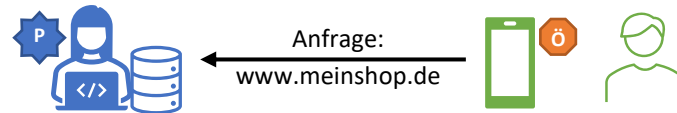


Abbildung 8: Warnung beim Aufruf einer Webseite über das https-Protokoll

- b) Begründen Sie, ob die folgenden Aussagen für einen Online-Shop, der das https-Protokoll verwendet, wahr oder falsch sind.
- (1) Wenn ich bei dem Online-Shop meinen Namen und meine Kontonummer angebe, kann die Daten niemand anderes lesen.
 - (2) Die Identität des Betreibers des Online-Shops wurde überprüft.
 - (3) Der Online-Shop ist auf jeden Fall seriös.
 - (4) Wenn ich etwas in das Suchfeld des Online-Shops eingebe, weiß der Betreiber nicht, wonach ich gesucht habe, da die Daten verschlüsselt übertragen werden.
 - (5) Wenn ich eine Bestellung abschicke, kann niemand die Nachricht abfangen und z. B. meine gegen seine Adresse austauschen.

Aufgabe 19: Abbildung 9 stellt den Ablauf bei der Authentifikation eines Webservers schematisch dar. Die Abbildung setzt das Beispiel aus Abbildung 7 fort. Schreiben Sie zu jedem Schritt eine kurze Erläuterung.

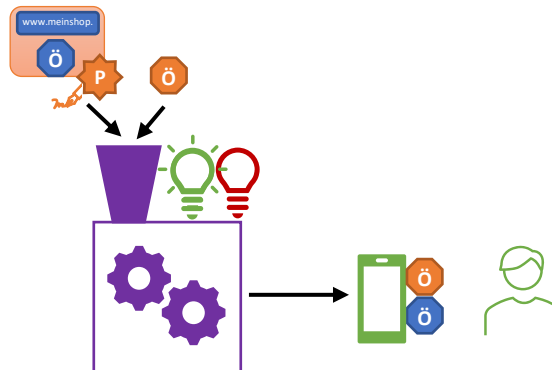
Schritt 1:



Schritt 2:



Schritt 3:



Schritt 4:



Abbildung 9: schematischer Ablauf bei der Authentifikation eines Webservers

Web of Trust

Neben den Zertifizierungsstellen als Vertrauensinstanzen im Internet wurde die Idee eines **Web of Trust** entwickelt. Im *Web of Trust* sind alle Teilnehmer*innen gleichberechtigt und können die öffentlichen Schlüssel anderer Teilnehmer*innen signieren. Wie nun Vertrauen in die Schlüssel aufgebaut wird, schauen wir uns am Beispiel einer Person A an. Person A kennt einige Personen, die sich am *Web of Trust* beteiligen, persönlich. Wir nennen sie Person B, C und D. Den öffentlichen Schlüssel von B, C und D vertraut Person A, da sie den Schlüssel direkt von diesen Personen erhalten hat. Außerdem vertraut Person A darauf, dass Person B nur Schlüssel signieren würde, die echt sind, bei denen sich Person B also von der Identität des Besitzers überzeugt hat. Person B kennt eine Person Y persönlich und signiert ihren öffentlichen Schlüssel. Person A kennt diese Person Y nicht persönlich. Da der öffentliche Schlüssel, den Person A von Person Y erhält, aber von Person B unterschrieben wurde, vertraut sie auf die Echtheit des öffentlichen Schlüssels von Person Y.

Abbildung 10 zeigt eine schematische Darstellung eines *Web of Trust*.

Aufgabe 20:

- Welche Personen in Abbildung 10 könnten Person A, Person B bzw. Person Y aus der Erläuterung zugeordnet werden. Geben Sie unterschiedliche Beispiele an.
- Erläutern Sie, warum Ingo die Echtheit des öffentlichen Schlüssels von Manfred nicht einschätzen kann.
- Erläutern Sie, weshalb man beim *Web of Trust* von einem dezentralen System spricht, während die Zertifizierungsstellen ein zentrales System bilden.

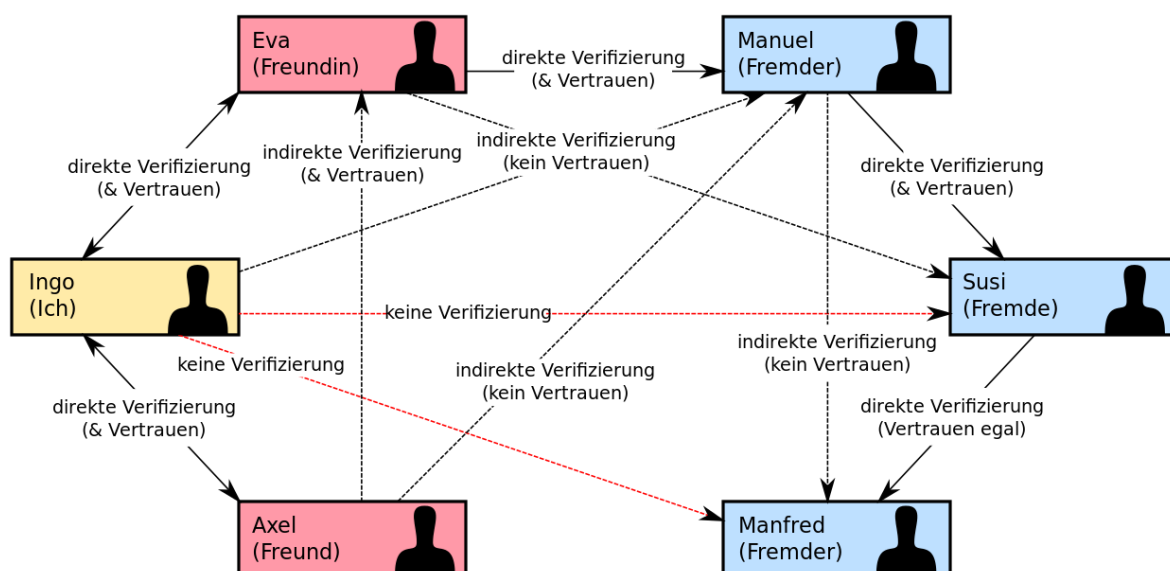


Abbildung 10: Schematische Darstellung eines Web of Trust von User:Ogmios - Diese Datei wurde von diesem Werk abgeleitet: Web of Trust.svg, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=30127548>

Aufgabe 21: Auch mit den Programmen Kleopatra oder GPA haben Sie die Möglichkeit den öffentlichen Schlüssel einer anderen Person zu signieren. Nutzen Sie diese Möglichkeit, um in Ihrer Lerngruppe ein *Web of Trust* aufzubauen. Diskutieren Sie zunächst, wie Sie Vorgehen wollen.

Hybride Verschlüsselung

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.

Mit der asymmetrischen Verschlüsselung haben wir ein Verfahren kennengelernt, das alle drei Kriterien für eine sichere Kommunikation erfüllen kann. Außerdem löst die asymmetrische Verschlüsselung das Problem der Schlüsselverteilung. Somit stellt sich die Frage, ob wir symmetrische Verschlüsselungsverfahren überhaupt noch benötigen. Die Antwort ist ja!

Ein Nachteil der asymmetrischen Verschlüsselung ist, dass die Berechnungen sehr komplex sind und das Verschlüsseln einer Nachricht viel länger dauert als mit einem symmetrischen Verfahren. Bei langen Nachrichten verlangsamt das die Kommunikation. Wenn die Programme Kleopatra oder GPA eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln, passiert daher Folgendes: Es wird zunächst ein Schlüssel für ein sicheres symmetrisches Verfahren erstellt. Die Nachricht wird mit dem symmetrischen Schlüssel verschlüsselt. Nur der symmetrische Schlüssel selbst wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und an die Nachricht angehängt. Der Empfänger kann den symmetrischen Schlüssel mit seinem privaten Schlüssel entschlüsseln. Er kennt nun den symmetrischen Schlüssel und kann damit die Nachricht entschlüsseln. Diese Kombination aus asymmetrischer und symmetrischer Verschlüsselung nennt man **hybride Verschlüsselung**.

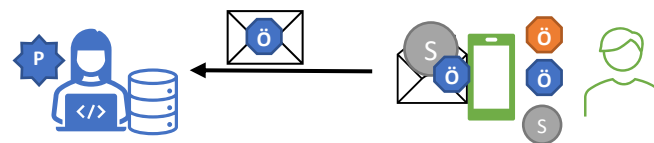
Auch das https-Protokoll verwendet eine hybride Verschlüsselung. Nachdem der Webserver sein Zertifikat an den Client gesendet und dieser das Zertifikat überprüft hat, erzeugt der Client einen zufälligen symmetrischen Schlüssel und verschlüsselt diesen mit dem öffentlichen Schlüssel des Webserver. Der symmetrische Schlüssel kann nun geheim an den Webserver übermittelt werden. Client und Server besitzen somit einen gemeinsamen symmetrischen Schlüssel, der Ihnen eine geheime Kommunikation erlaubt.

Aufgabe 22: Abbildung 11 zeigt eine vereinfachte, schematische Darstellung der geheimen Kommunikation über das https-Protokoll mittels hybrider Verschlüsselung. Die Abbildung knüpft an das Beispiel aus Abbildung 7 und 9 an.
Erläutern Sie die einzelnen Schritte kurz.

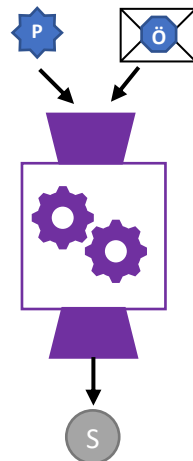
Schritt 1:



Schritt 2:



Schritt 3:



Schritt 4:

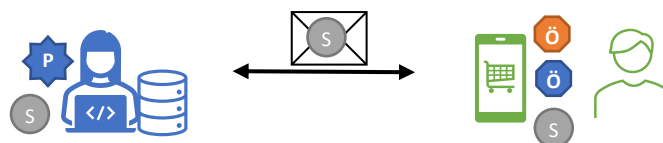


Abbildung 11: schematische Darstellung des Nachrichtenaustauschs mit hybrider Verschlüsselung

Bei der sicheren Kommunikation spielt manchmal auch die **Nicht-Anfechtbarkeit** einer Nachricht eine Rolle. Das heißt, dass Sender und Empfänger die Übertragung der Nachricht nicht leugnen können. Der Empfänger kann z. B. belegen, dass er die Nachricht nicht selbst geschrieben, sondern tatsächlich vom Absender erhalten hat.

Aufgabe 23:

- Nennen Sie Beispiele, in denen die Nicht-Anfechtbarkeit einer Nachricht wichtig ist.
- Beurteilen Sie, für die Nicht-Anfechtbarkeit und die Authentizität einer Nachricht jeweils, ob diese mithilfe eines symmetrischen Verfahrens sichergestellt werden können, wenn die Kommunikationspartner zuvor einen entsprechenden Schlüssel vereinbart haben.

Hinweis

Die Materialien erheben keinen Anspruch auf Vollständigkeit hinsichtlich der für die Abiturprüfung erwarteten Kompetenzen. Verbindlich für das Abitur in Niedersachsen sind allein das niedersächsische Kerncurriculum für die gymnasiale Oberstufe sowie die ergänzenden Hinweise in der jeweils aktuellen Fassung.

Lizenz

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 Abbildungen 8 und 10 wurden die Abbildungen mithilfe der Formen und Piktogramme von Microsoft Word 2016 erstellt. In Abbildung 1 bis 3 ergänzt um eine Grafik von Clker-Free-Vector-Images auf Pixabay zur freien kommerziellen Nutzung.

Abbildung 8: Screenshot des Browsers Mozilla Firefox

Abbildung 10: User: Ogmios - Diese Datei wurde von diesem Werk abgeleitet: Web of Trust.svg, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=30127548>