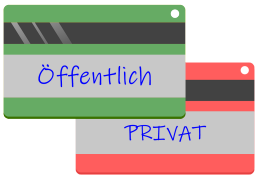
# 4. Die Gruft – Asymmetrische Verschlüsselungsverfahren und digitale Signaturen

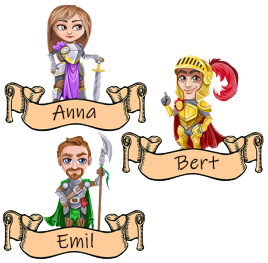
In der Gruft lernst du das Grundprinzip von **asymmetrischen Verschlüsselungsverfahren** kennen, und wie diese Verfahren angewendet werden können, um die Sicherheitsziele **Vertraulichkeit**, **Authentizität**, **Verbindlichkeit** und **Integrität** zu erreichen.




Anders als bei den symmetrischen Verschlüsselungsverfahren wird bei den asymmetrischen Verfahren für die Ver- und Entschlüsselung nicht der gleiche Schlüssel verwendet. Es kommen hier Schlüsselpaare bestehend aus einem **öffentlichen Schlüssel** und einem zugehörigen **privaten Schlüssel** zum Einsatz.

Bevor es allerdings an das Knacken der verschiedenen Rätsel geht, um das dritte Teilfragmente für den Zugang zum sagenumwobenen Schatz der Burgruine zu erhalten, gibt es einen kurzen Einblick in die Geschichte des Crypto-Castle.

**Crypto-Castle unter der Regentschaft von Königin Anna und König Bert...**
In der Glanzzeit des Crypto-Castle wurde dieses von Königin Anna und König Bert regiert. Beide waren sehr geschäftstüchtig und deshalb viel auf Reisen. Um trotzdem die Geschicke des Crypto-Castle lenken zu können, mussten sie viele Nachrichten austauschen. Dies geschah über ihren listigen Boten Emil. Dieser wollte selbst über Crypto-Castle regieren und versuchte den beiden zu schaden, wo es nur ging[1].




**Überblick (Öffentlicher und Privater Schlüssel - Teil 1)**

Jeder Kommunikationspartner besitzt ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel.

Auf den **öffentlichen Schlüssel** (public key) einer Person hat jeder Zugriff. Dieser Schlüssel kann genutzt werden, um eine Nachricht zu verschlüsseln. Eine Entschlüsselung der Nachricht ist nur mit dem zugehörigen privaten Schlüssel möglich.


Der **private Schlüssel** (private key) einer Person verbleibt bei seinem Besitzer. Dieser muss sicherstellen, dass *niemand außer ihm selbst* Zugriff auf diesen Schlüssel hat. Nur mit dem privaten Schlüssel ist es möglich, eine mit dem zugehörigen öffentlichen Schlüssel verschlüsselte Nachricht wieder zu entschlüsseln.


[1] Inspiriert von Gallenbacher, Jens (2017b). Abenteuer Informatik: Kapitel 12 „Mit Sicherheit“.

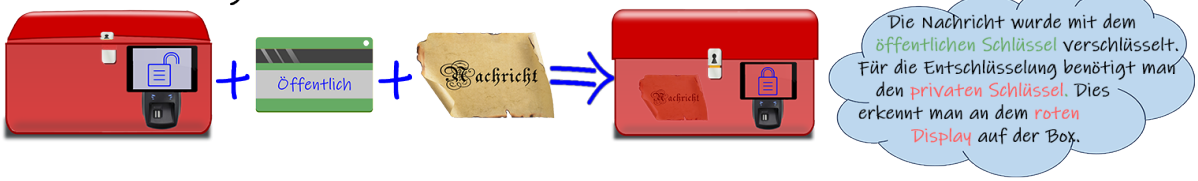
## Überblick (Ver- und Entschlüsseln mit öffentlichen und privaten Schlüsseln)

Ziel ist es, eine Nachricht sicher / verschlüsselt zu übertragen.

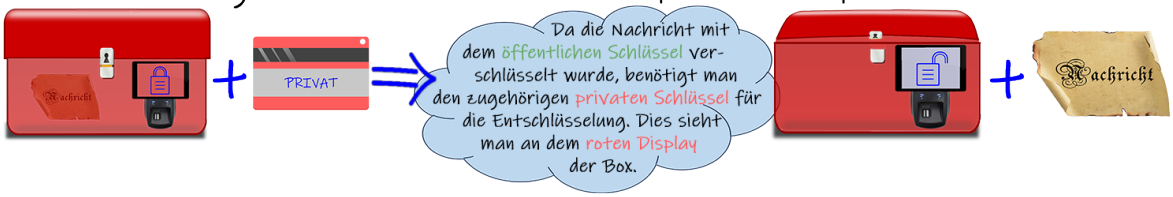
Das Verschlüsseln wird bei uns durch das Deponieren der Nachricht in einer verschließbaren Box symbolisiert. Das Verschließen und Öffnen der Box stellt das Ver- und Entschlüsseln der Nachricht dar. Wird die Box mit dem öffentlichen Schlüssel verschlossen (verschlüsselt), so kann sie nur mit Hilfe des zugehörigen privaten Schlüssels wieder geöffnet (entschlüsselt) werden.


Es ergeben sich folgende Möglichkeiten:

Verschlüsselung der Nachricht mit dem öffentlichen Schlüssel:




Entschlüsselung der Nachricht mit dem passenden privaten Schlüssel:




## Exkurs (Einwegfunktion mit Falltür („Hintertür"))

In unserer symbolhaften Darstellung wird das Ver- und Entschlüsseln einer Nachricht durch das Deponieren und Verschließen in bzw. das Aufschließen und Entnehmen der Nachricht aus der Box dargestellt. In der Realität verwendet man für das Ver- und Entschlüsseln eine sogenannte **Einwegfunktion mit Falltür** (Falltürfunktion) zusammen mit dem öffentlichen bzw. privaten Schlüssel.

Eigenschaften einer Falltürfunktion:

- Die Eingabe lässt sich mit wenig Aufwand mit Hilfe der Funktion verschlüsseln
- Aus der verschlüsselten Ausgabe lässt sich die Eingabe nicht oder nur mit unverhältnismäßig großem Aufwand zurückrechnen
- Mit Hilfe eines passenden Schlüssels (*Falltür/Hintertür*) lässt sich die Umkehrung (Entschlüsselung) sehr einfach berechnen

*Beispiel:*
Betrachten wir die beiden Primzahlen 2333 und 4243. Als Funktion verwenden wir die *Multiplikation*. Die *Ausgabe*, also das Produkt, lässt sich einfach berechnen:

$$2333 \cdot 4243 = 9898919$$

Die *Umkehrung der Funktion* ist die *Faktorisierung in Primfaktoren* (Finden der Teiler). Ausgehend von der Zahl 9898919 lassen sich die beiden Teiler 2333 und 4243 nur mit sehr großem Aufwand finden.

Kennt man allerdings die Ausgabe und zusätzlich eine der beiden Zahlen, z.B. 2333 (*Schlüssel/Falltür/Hintertür*), so findet man den zweiten Teiler sehr einfach.

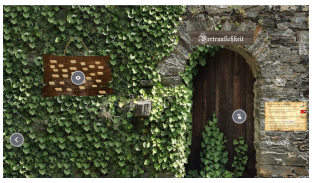
$$9898919 : 2333 = 4243$$

## Überblick (Sicherheitsziel Vertraulichkeit)

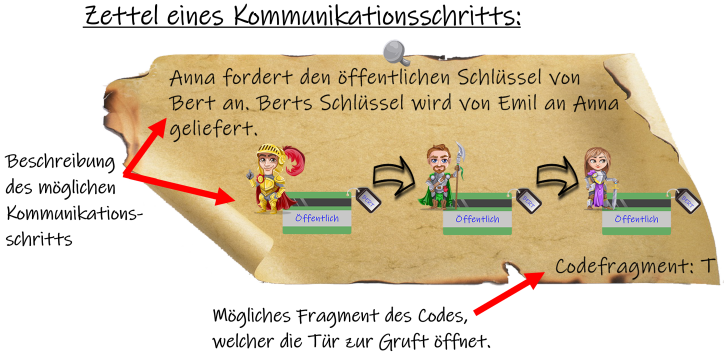
**Vertraulichkeit** ist dann hergestellt, wenn nur die Adressaten einer Nachricht deren Information erschließen können.

Anders ausgedrückt: Eine vertrauliche Nachricht kann nicht von Dritten gelesen werden.

## Arbeitsauftrag 11: Zugang zur Gruft - Eingang Vertraulichkeit



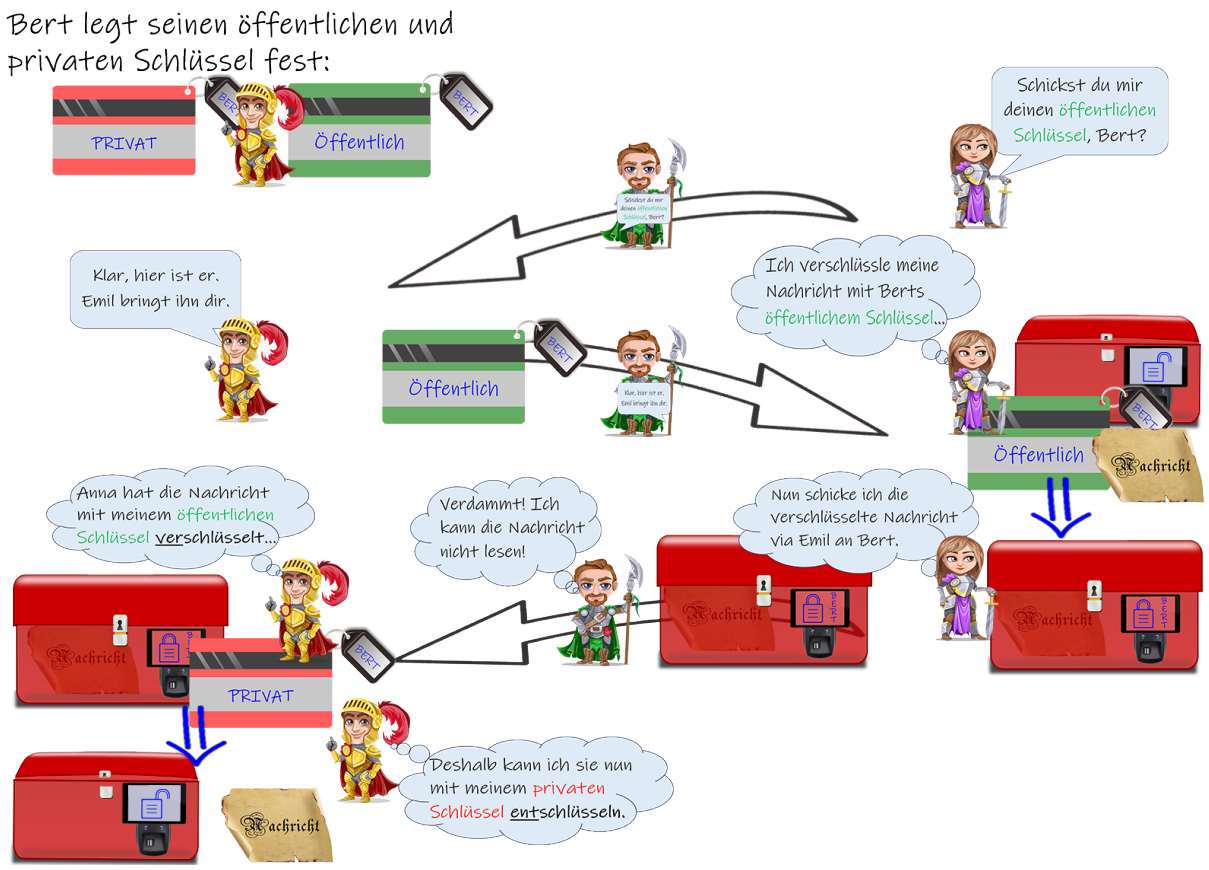
Es soll eine Nachricht von Anna an Bert geschickt werden, sodass das Sicherheitsziel Vertraulichkeit erfüllt ist. Muss etwas zwischen Anna und Bert ausgetauscht werden, so funktioniert das nur über Emil.
Zu Beginn gibt es nur „Blanko"-Schlüsselpaare und es wurden keine Schlüssel ausgetauscht.
Deine Aufgabe ist es, die richtigen fünf Kommunikationsschritte unter allen Zetteln auf der Holztafel zu finden und in die richtige Reihenfolge zu bringen. Die Codefragmente auf den gefundenen fünf Zetteln öffnen dir den Zugang zur Gruft.




*Der fünfstellige Code lautet:*


**Blättere erst um, wenn Du dir Zugang zur Gruft verschafft hast!**

## Überblick (Kommunikationsablauf Sicherheitsziel Vertraulichkeit)




Bisher hat sich Emil zurückgehalten und hat seine Aufgabe, die Nachrichten von Anna und Bert zu übermitteln, erledigt. Emil will nun die Kommunikation von Anna und Bert mitlesen und ggf. für seine Zwecke manipulieren. Er hat eine Möglichkeit gefunden, wie er die zuvor beschriebene Kommunikation beliebig manipulieren kann, ohne dass die beiden es mitbekommen. Dafür will Emil seine Position *in der Mitte der Kommunikation* von Anna und Bert ausnutzen. Nun ist deine kriminelle Energie gefragt.

## Arbeitsauftrag 12: Weg zur Gruft – Man-in-the-middle-Angriff

Es soll eine Nachricht von Anna an Bert geschickt werden. Ziel ist es, dass Emil unbemerkt diese Nachricht mitlesen oder manipulieren kann.


Zu Beginn besitzen Anna, Bert und Emil jeweils ihr eigenes Schlüsselpaar[2] bestehend aus einem öffentlichen und einem privaten Schlüssel.
Es wurden noch keine Schlüssel ausgetauscht.

[2] Die Anhänger an den Schlüsselkarten dienen nur uns zur Orientierung und sind für die Kommunikationspartner nicht sichtbar.

*Hinweis:*
Emil weiß, sobald Anna ihre Nachricht mit Berts öffentlichen Schlüssel verschlüsselt hat, hat er keine Chance mehr, die Nachricht zu lesen oder in seinem Sinne zu verändern. Deshalb muss er unter anderem bereits beim Tauschen der Schlüssel aktiv werden.

Deine Aufgabe ist es, die richtigen sieben Kommunikationsschritte unter allen Zetteln auf der Holztafel zu finden und in die richtige Reihenfolge zu bringen. Die Codefragmente auf den gefundenen sieben Zetteln öffnen dir die nächste Tür zur Gruft.

*Der siebenstellige Code lautet:*

*Hinweis:*
Sollte dir die kriminelle Energie fehlen, kannst du auch den folgenden Merkkasten zum *Man-in-the-middle-Angriff* lesen und dich inspirieren lassen. Aber noch nicht umblättern!

**Überblick (Man-in-the-middle-Angriff)**

Ziel bei einem **Man-in-the-middle-Angriff** ist es, sich unbemerkt in eine Kommunikation zwischen zwei Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich *gegenüber dem Sender als Empfänger* und *gegenüber dem Empfänger als Sender* ausgibt.

In unserem Beispiel ist Emil dieser Angreifer. Da er für den Nachrichtentransport verantwortlich ist, steht er in der Mitte von Anna und Bert. Der Angriff besteht aus zwei Teilen:

1. Abfangen der jeweiligen öffentlichen Schlüssel beim Schlüsseltausch und Ersetzen dieser durch den eigenen (Emils) öffentlichen Schlüssel
2. Entschlüsselung und Mitlesen der gesendeten Nachrichten. Da Emil allen Kommunikationsteilnehmern seinen öffentlichen Schlüssel gibt, kann er alle Nachrichten entschlüsseln, lesen und im Anschluss die Nachricht mit dem richtigen öffentlichen Schlüssel des Empfängers wieder verschlüsseln.


**Blättere erst um, wenn Du den Code zum Öffnen der Türe ermittelt hast!**

## Überblick (Überblick Kommunikation mit Man-in-the-middle-Angriff)

### Voraussetzung:

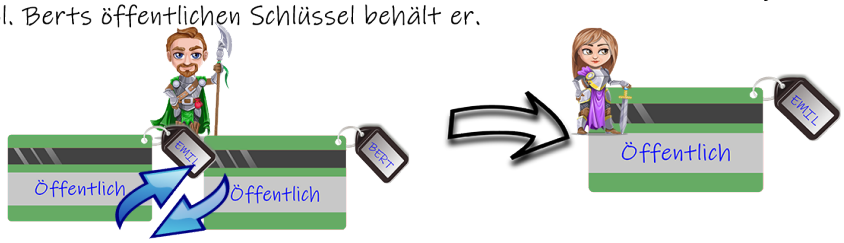
Jeder Kommunikationsteilnehmer besitzt ein eigenes Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel.


### Kommunikation:

1. Anna fordert den öffentlichen Schlüssel von Bert über Emil an.

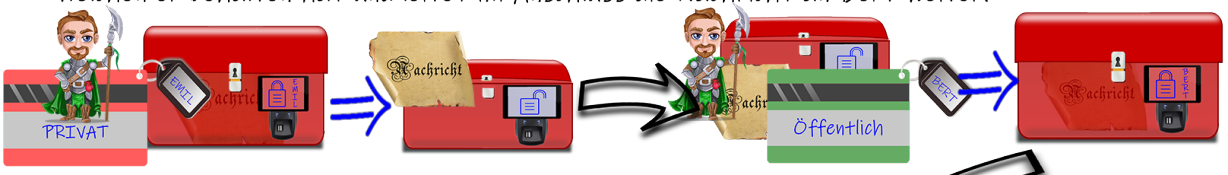

2. Bert gibt seinen öffentlichen Schlüssel an Emil. Dieser soll ihn zu Anna bringen.


3. Emil liefert nicht Berts öffentlichen Schlüssel an Anna, sondern seinen <u>eigenen</u> öffentlichen Schlüssel. Berts öffentlichen Schlüssel behält er.

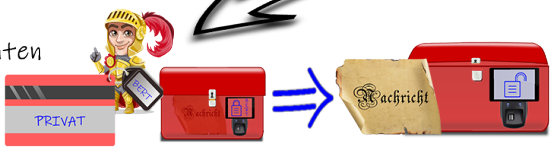



4. Anna verschlüsselt ihre Nachricht an Bert mit dem öffentlichen Schlüssel, welchen sie von Emil erhalten hat. Sie denkt, dass es sich dabei um Berts öffentlichen Schlüssel handelt. Die verschlüsselte Nachricht gibt sie an Emil, damit dieser die Nachricht an Bert liefert.


5. Emil entschlüsselt die Nachricht mit seinem privaten Schlüssel. Das ist möglich, da er statt Berts öffentlichen Schlüssel seinen öffentlichen Schlüssel an Anna weitergegeben hat. Nachdem er die Nachricht gelesen hat, verschlüsselt er diese mit Berts öffentlichem Schlüssel, welchen er behalten hat und leitet im Anschluss die Nachricht an Bert weiter.




6. Bert entschlüsselt die Nachricht mit seinem privaten Schlüssel und weiß nicht, dass Emil auch Zugriff auf die Nachricht hatte.



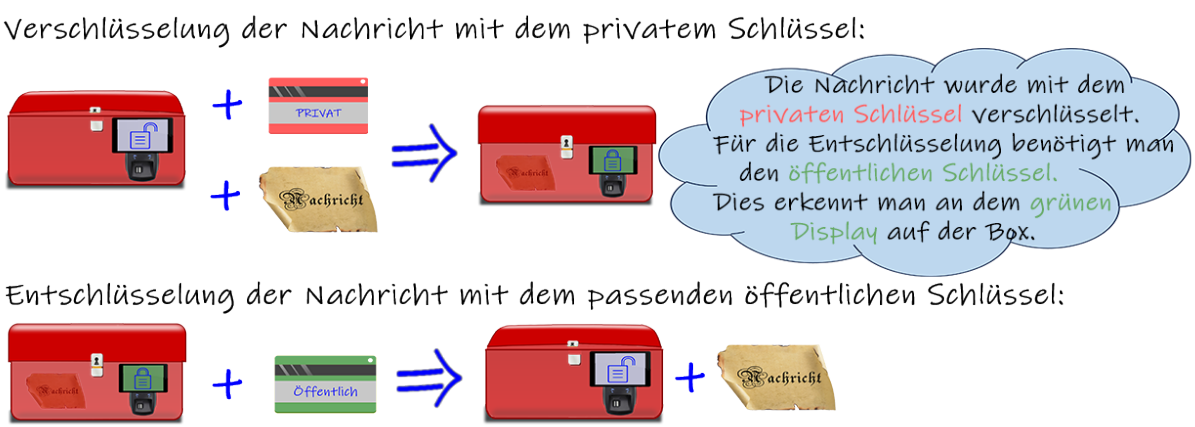
## Überblick (Öffentlicher und privater Schlüssel - Teil 2 und digitales Unterschreiben)

Wir wissen bereits, dass man mit Hilfe des *öffentlichen* Schlüssels eine Nachricht `VER`schlüsseln kann. Diese kann dann ausschließlich mit dem zugehörigen *privaten* Schlüssel des Schlüsselpaars wieder `ENT`schlüsselt werden.

Beim digitalen Unterschreiben geht man **genau umgekehrt** vor.

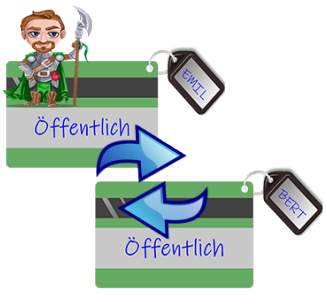

Der **private Schlüssel** wird genutzt, um eine Nachricht zu `VER`schlüsseln. Da *nur der Besitzer* des privaten Schlüssels diesen besitzt, kann das Verschlüsseln damit als „*Unterschrift*“ angesehen werden.


Der **öffentliche Schlüssel** wird genutzt, um die Nachricht, welche mit dem privaten Schlüssel des Schlüsselpaars verschlüsselt wurde, wieder zu `ENT`schlüsseln. Die Entschlüsselung mit dem öffentlichen Schlüssel kann als „*Überprüfung der Unterschrift*“ angesehen werden, da mit dem öffentlichen Schlüssel nur etwas entschlüsselt werden kann, das vorher mit dem privaten Schlüssel verschlüsselt („*Unterschrift*“) wurde.




Zusammenfassend kann man also sagen, dass für die Ver- und Entschlüsselung immer ein zusammengehörendes Schlüsselpaar benötigt wird. Wird mit dem einen Schlüssel des Paars verschlüsselt, kann eine Entschlüsselung nur mit dem anderen Schlüssel des Paars stattfinden.

Wir haben gesehen, dass es Emil nur möglich ist, die Nachrichten von Anna an Bert zu lesen und ggf. zu manipulieren, wenn er beim Übertragen des Schlüssels den eigentlich angeforderten Schlüssel durch seinen öffentlichen Schlüssel austauscht. Man müsste also sicherstellen, dass es sich bei dem gelieferten öffentlichen Schlüssel auch wirklich um den öffentlichen Schlüssel des Kommunikationspartners handelt, den man angefordert hat (*Authentizität des Schlüssels*). Konkret meint das, dass man auch wirklich Berts öffentlichen Schlüssel bekommt, wenn man diesen anfordert.

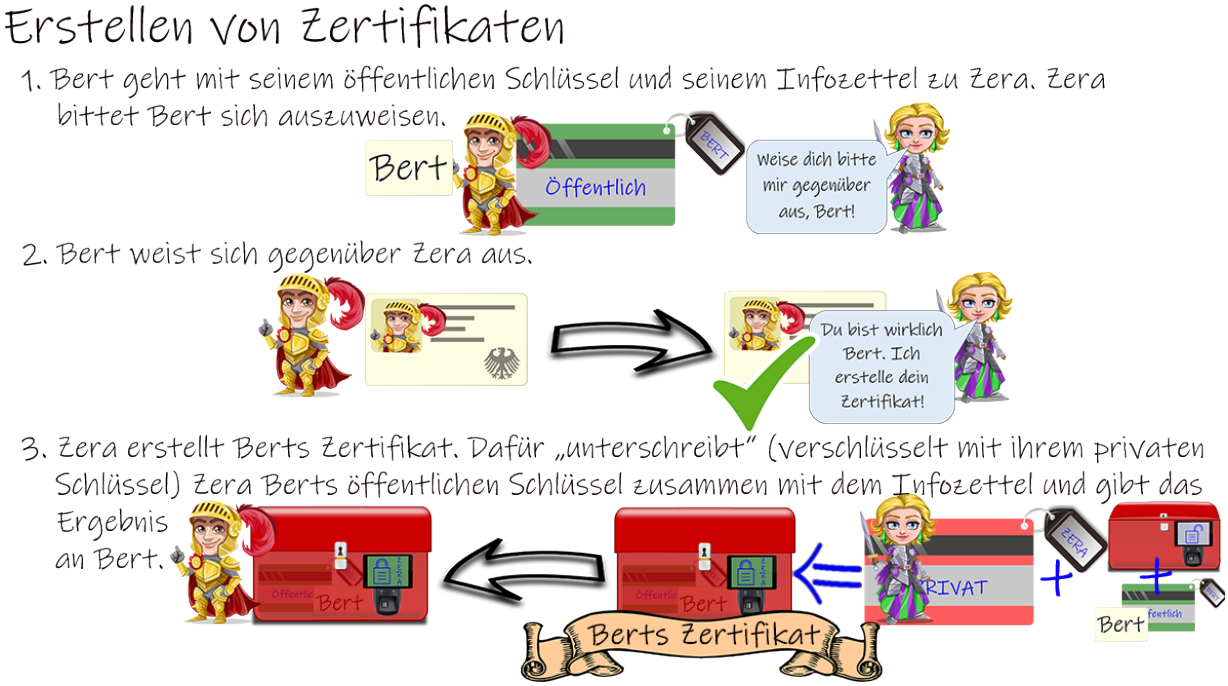


## Überblick (Die Zertifizierungsstelle (Certification Authority))

Zum Verschlüsseln von Dokumenten bzw. zum Überprüfen digitaler Signaturen benötigt man den öffentlichen Schlüssel des Kommunikationspartners. Diesen besitzt man aber in der Regel nicht. Damit man sicher sein kann, den korrekten Schlüssel des gewünschten Kommunikationspartners zu erhalten, gibt es Zertifizierungsstellen.

In unserem Fall ist die vertrauenswürdige Zera diese Zertifizierungsstelle. Ihre Aufgabe ist die Erstellung von sog. **Zertifikaten**, mit welchen man sicherstellen kann, dass ein erhaltener Schlüssel wirklich zu einer Person gehört (*Authentizität des Schlüssels*). Ein Zertifikat enthält u.a. den öffentlichen Schlüssel einer Person, Informationen zum Besitzer des öffentlichen Schlüssels („Infozettel“), die Gültigkeitsdauer des Zertifikats, etc.


Zera erstellt das Zertifikat nicht einfach so. Man muss sich dafür bei ihr ausweisen. Dann übergibt man ihr den eigenen öffentlichen Schlüssel sowie Informationen zur eigenen Person. Zera erstellt daraus das Zertifikat, indem sie den erhaltenen Schlüssel, die Personeninformationen („Infozettel“),... digital „unterschreibt“.




## Exkurs (Wieso braucht man die zusätzliche Information im Zertifikat?)

Wenn Anna das Zertifikat von Bert anfordert, benötigt sie nur den darin enthaltenen öffentlichen Schlüssel. Es stellt sich also die Frage, weshalb auch noch unter anderem Informationen zum Besitzer des öffentlichen Schlüssels („Infozettel“) enthalten sein müssen.

Nehmen wir an, dass Zera **nur** den öffentlichen Schlüssel für Berts Zertifikat „unterschreibt“, ohne die zusätzlichen Informationen zum Besitzer.

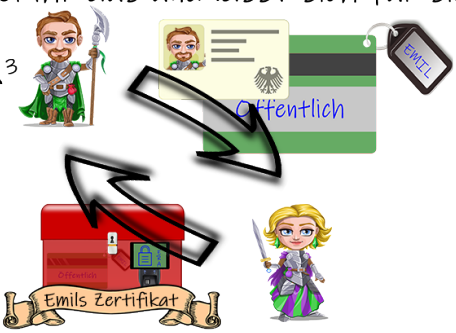
Wir versetzen uns in die Position von Emil, welcher die Kommunikation unbemerkt mitlesen will. Emil weiß, sobald Anna Berts öffentlichen Schlüssel besitzt, hat er keine Chance mehr.
Lassen wir nun unserer kriminellen Energie freien Lauf. So könnte Emil vorgehen, dass Anna trotz der Anforderung von Berts Zertifikat nicht Berts öffentlichen Schlüssel, sondern Emils öffentlichen Schlüssel erhält.

**Mögliches Vorgehen von Emil:**

1. Anna fordert Berts Zertifikat an.


2. Bert gibt sein Zertifikat an Emil, damit dieser es an Anna liefert


3. Emil geht zu Zera, weist sich bei ihr aus und lässt sich für sich selbst ein Zertifikat mit seinem (Emils) öffentlichen Schlüssel erstellen.[3]




4. Emil bringt sein Zertifikat statt Berts Zertifikat zu Anna.


5. Anna entschlüsselt das erhaltene Zertifikat mit Zeras öffentlichem Schlüssel. Da dies funktioniert, geht sie davon aus, dass darin auch wirklich Berts öffentlicher Schlüssel war. In Wahrheit hat sie aber Emils öffentlichen Schlüssel erhalten, ohne dass sie das weiß.

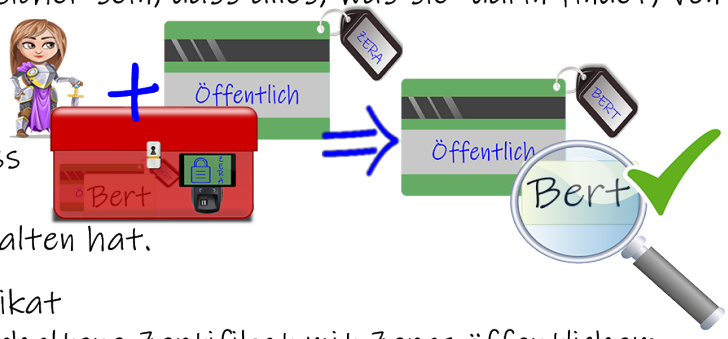

[3] Emil besorgt sich das Zertifikat schon vor dem Kommunikationsvorgang, um gut gerüstet zu sein.

Bei der Erstellung des Zertifikats packt nun Zera nicht nur den öffentlichen Schlüssel der Person in das Zertifikat, sondern unter anderem auch Informationen zum Besitzer des Schlüssels. Das ist bei uns durch den „Infozettel“ dargestellt. Entschlüsselt man das Zertifikat, kann man über den Infozettel leicht prüfen, wem der Schlüssel gehört, denn Zera packt nur den korrekten Namen in das Zertifikat.


Erhält Anna nun ein Zertifikat, gibt es folgende zwei Möglichkeiten:

Fall 1: Anna erhält Berts Zertifikat

Anna entschlüsselt das erhaltene Zertifikat mit Zeras öffentlichem Schlüssel. Sie kann somit sicher sein, dass alles, was sie darin findet, von Zera eingepackt wurde. Anna prüft den Infozettel und da dort Berts Name steht, weiß sie, dass sie wirklich Berts öffentlichen Schlüssel erhalten hat.




Fall 2: Anna erhält Emils Zertifikat

Anna entschlüsselt das erhaltene Zertifikat mit Zeras öffentlichem Schlüssel. Sie kann somit sicher sein, dass alles, was sie darin findet, von Zera eingepackt wurde. Anna prüft den Infozettel. Sie findet dort Emils Namen. Somit weiß sie, dass sie mit dem Zertifikat nicht Berts öffentlichen Schlüssel erhalten hat.


## Exkurs (Zertifikate im Browser)

Viele Webbrowser und Betriebssysteme beinhalten bereits eine Reihe an vertrauenswürdigen Zertifizierungsstellen mit deren öffentlichen Schlüsseln geprüft werden kann, ob ein erhaltener öffentlicher Schlüssel wirklich der angeforderte Schlüssel ist.

Kommuniziert man im Internet gesichert mit Webservern, kommen auch dort Zertifikate zum Einsatz. Diese lassen sich im Normalfall im Browser anzeigen. Nach Aufruf einer Webseite klickt man dazu auf das „Schloss“-Symbol in der Adresszeile des Browsers.


Hier kann man die Details des Zertifikats, wie etwa die ausstellende Zertifizierungsstelle, den Besitzer des Zertifikats, die Gültigkeitsdauer und den enthaltenen öffentlichen Schlüssel einsehen.
Nachfolgend ist ein Musterzertifikat abgebildet.

Zertifikat: *.meineWebseite.de

Ausgestellt für

| | |
|---|---|
| Allgemeiner Name | *.meineWebseite.de |
| Organisation | Firma MeineWebseite |

Ausgestellt von

| | |
|---|---|
| Allgemeiner Name | ZERA |
| Organisation | ZERA Zertifizierungsstelle |

Gültigkeitsdauer

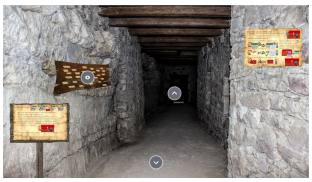
| | |
|---|---|
| Ausgestellt am | 22.09.2023 um 01:00:00 |
| Gültig bis | 22.09.2025 um 00:59:59 |

Public Key Info

| | |
|---|---|
| Algorithmus | RSA |
| Schlüsselgröße | 2048 |
| Modulus | F1 BB 23 FC 19 A4 C7 6C 70 49 76 53 D3 09 23<br>65 B2 48 7B B6 1C AA 07 1A E2 79 1A F9 7A 5E<br>79 BE E8 87 F1 88 C5 B4 49 9B 10 BB CA AF EA<br>AF BE 54 0C 78 43 7F CA 7B 4E 45 5B 0B 24 29<br>… |

## Arbeitsauftrag 13: Weg zur Gruft - Zertifikate

Es soll eine Nachricht von Anna an Bert via Emil geschickt werden.
Ziel ist es, dass Emil diese Nachricht **nicht** mitlesen oder manipulieren kann.




- Zu Beginn besitzen Anna, Bert und Emil jeweils ihr eigenes Schlüsselpaar (öffentlicher und privater Schlüssel)
- Zera hat bereits ein Zertifikat für Berts öffentlichen Schlüssel erstellt und dieses an Bert gesendet
- Alle haben Zugriff auf den öffentlichen Schlüssel von Zera
- Es wurden noch keine Schlüssel ausgetauscht

Deine Aufgabe ist es, die richtigen vier Kommunikationsschritte unter allen Zetteln auf der Holztafel zu finden und in die richtige Reihenfolge zu bringen. Die Codefragmente auf den gefundenen vier Zetteln öffnen dir die nächste Tür zur Gruft.

*Der vierstellige Code lautet:*


**Blättere erst um, wenn Du den Code zum Öffnen der Türe ermittelt hast!**

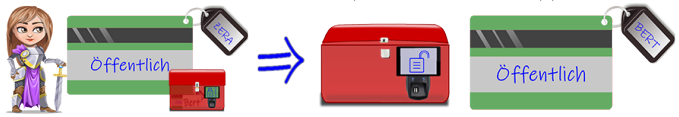
## Überblick (Kommunikation mit Zertifikat)

### Voraussetzung:


### Kommunikation:

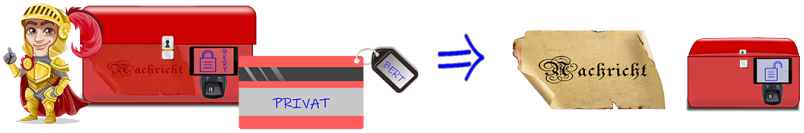
1. Anna fordert das Zertifikat von Bert über Emil an. Bert schickt sein Zertifikat via Emil an Anna.


2. Anna entschlüsselt das von Bert erhaltene Zertifikat mit dem öffentlichen Schlüssel von Zera.




3. Anna verschlüsselt ihre Nachricht an Bert mit Berts öffentlichem Schlüssel und schickt diese via Emil an Bert.


4. Bert nutzt seinen privaten Schlüssel, um die von Anna mit Berts öffentlichen Schlüssel verschlüsselte Nachricht zu entschlüsseln.




Bisher haben wir uns hauptsächlich mit dem Sicherheitsziel *Vertraulichkeit* beschäftigt. Dabei hast du gelernt, dass bei der asymmetrischen Verschlüsselung der **öffentliche** Schlüssel verwendet wird, um eine Nachricht zu **VER**schlüsseln. Diese verschlüsselte Nachricht kann dann nur mit dem zugehörigen **privaten** Schlüssel wieder **ENT**schlüsselt werden.


Aber es geht auch in umgekehrter Form, also **VER**schlüsseln mit dem **privaten** Schlüssel und **ENT**schlüsseln mit dem zugehörigen **öffentlichen** Schlüssel. Das kennst du bereits von der Erstellung der Zertifikate. Dort wurde der öffentliche Schlüssel einer Person von der Zertifizierungsstelle mit dem privaten Schlüssel dieser Stelle verschlüsselt („unterschrieben“). Dieses Vorgehen kann man nun auch auf *Nachrichten* übertragen.

Damit kann man die verbleibenden Sicherheitsziele *Authentizität*, *Verbindlichkeit* und *Integrität* erreichen. Kümmern wir uns zuerst um die *Authentizität* und die *Verbindlichkeit*, die sich hauptsächlich in der Betrachtungsperspektive (*Authentizität*: Empfänger, *Verbindlichkeit*: unbeteiligte Dritte) unterscheiden.

**Überblick (Sicherheitsziele Authentizität und Verbindlichkeit)**

**Authentizität** ist dann hergestellt, wenn sichergestellt ist, dass eine Nachricht tatsächlich von dem angegebenen Absender stammt.
Anders ausgedrückt: Es kann niemand unbefugt unter meinem Namen eine Nachricht verschicken.

**Verbindlichkeit** ist dann hergestellt, wenn sichergestellt ist, dass der Absender einer Nachricht im Nachhinein nicht abstreiten kann, dass er die Nachricht verfasst hat.

**Exkurs (Beispiel - Authentisch, aber nicht verbindlich)**

Übergibt der Sender seine Nachricht persönlich an den Empfänger, so weiß dieser, von wem er die Nachricht erhalten hat. Das Sicherheitsziel *Authentizität* ist erfüllt. In der Regel kann der Empfänger das in diesem Szenario aber gegenüber einem Dritten nicht nachweisen, weshalb die *Verbindlichkeit* nicht erfüllt ist.

**Arbeitsauftrag 14: Weg zur Gruft - Digitale Signatur**

Bert will nun Anna antworten, dass er ihre Nachricht erhalten hat. Anna soll sicher sein können, dass die Nachricht von Bert ist. Bert soll also die Nachricht „unterschreiben“. Der Inhalt der Nachricht ist nicht geheim. Es ist also kein Problem, wenn Emil diese liest.

Da Bert antwortet, wird die Nachricht diesmal **von Bert an Anna** via Emil geschickt.


- Zu Beginn besitzen Anna, Bert und Emil jeweils ihr eigenes Schlüsselpaar (öffentlicher und privater Schlüssel)
- Zera hat bereits ein Zertifikat für Berts öffentlichen Schlüssel erstellt und dieses an Bert gesendet
- Alle haben Zugriff auf den öffentlichen Schlüssel von Zera
- Es wurden noch keine Schlüssel ausgetauscht

Deine Aufgabe ist es, die richtigen vier Kommunikationsschritte unter allen Zetteln auf der Holztafel zu finden und in die richtige Reihenfolge zu bringen. Die Codefragmente auf den gefundenen vier Zetteln öffnen dir die nächste Tür zur Gruft.

*Hinweis:* Anna soll zuerst den Schlüssel in Händen halten. Berts Antwort, ... kommt danach.

*Der vierstellige Code lautet:* _____

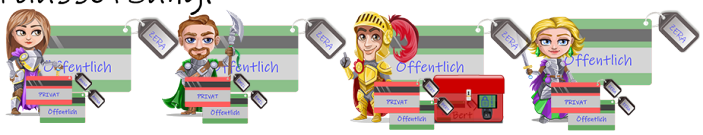

**Blättere erst um, wenn Du den Code zum Öffnen der Türe ermittelt hast!**

## Überblick (Digitale Signaturen: Wie Verschlüsseln - nur anders herum)

Bei einer **digitalen Signatur** wird der private Schlüssel zur *VER*schlüsselung und der zugehörige öffentlichen Schlüssel zur *ENT*schlüsselung verwendet. Ziel ist hier nicht die Geheimhaltung der Nachricht. Diese kann prinzipiell von allen gelesen werden. Die digitale Unterschrift verfolgt ein ganz anderes Ziel. Sie stellt sicher, dass die Nachricht tatsächlich so vom angegebenen Absender stammt. So ist auch eine nachträgliche Manipulation von Dritten nicht möglich.

Sicherheitsziele *Authentizität und Verbindlichkeit*:
Die zu unterschreibende Nachricht wird mit dem privaten Schlüssel des Absenders verschlüsselt (**signiert**) und zusammen mit der Nachricht übertragen. Der Empfänger entschlüsselt die verschlüsselte Nachricht mit dem öffentlichen Schlüssel des Absenders und vergleicht die entschlüsselte Nachricht mit der unverschlüsselt erhaltenen Nachricht. Stimmen beide überein, kann sich der Empfänger sicher sein, dass die Nachricht vom gewünschten Absender ist, da nur der Absender den privaten Schlüssel besitzt, um die Nachricht passend zu verschlüsseln.

Voraussetzung:




Kommunikation:

1. Anna fordert das Zertifikat von Bert über Emil an. Bert schickt sein Zertifikat via Emil an Anna.


2. Anna entschlüsselt das von Bert erhaltene Zertifikat mit dem öffentlichen Schlüssel von Zera.

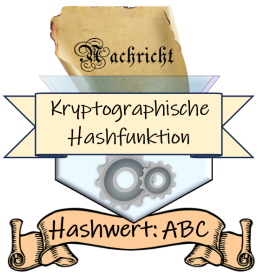

3. Bert nutzt seinen privaten Schlüssel um seine Nachricht an Anna zu verschlüsseln (signieren). Die verschlüsselte Nachricht schickt er zusammen mit der Nachricht via Emil an Anna.


4. Anna nutzt Berts öffentlichen Schlüssel um die von Bert erhaltene Nachricht zu entschlüsseln. Diese vergleicht sie mit der unverschlüsselten mitgeschickten Nachricht. Da die beiden Nachrichten übereinstimmen, kann sie sicher sein, dass die Nachricht von Bert kommt.


Für die Überprüfung, ob die Entschlüsselung mit Berts öffentlichen Schlüssel *erfolgreich* ist, wird die entschlüsselte Nachricht noch mit der Orginalnachricht verglichen. Wird für die Entschlüsselung nicht Berts öffentlicher Schlüssel verwendet, ist deren Ergebnis „Kauderwelsch“, welches nicht mit der Orginalnachricht übereinstimmt. Stimmt die Orginalnachricht also mit der entschlüsselten Nachricht überein, kann man sicher sein, dass diese mit Berts privatem Schlüssel verschlüsselt wurde.

Um die digitale Signatur klein zu halten, wird in der Realität nicht wie oben die komplette Nachricht verschlüsselt, sondern lediglich eine eindeutige, verkürzte Darstellung der Nachricht. Diese Darstellung erhält man mit Hilfe von **kryptographischen Hashfunktionen**.

## Exkurs (Kryptographische Hashfunktion)




Eine **kryptographische Hashfunktion** ist ein Verfahren, welches lange Zeichenketten auf kürzere Zeichenketten abbildet. Die resultierenden Zeichenketten nennt man *Hashwerte*.
Kennzeichnend für kryptographische Hashfunktionen ist, dass es praktisch unmöglich ist, aus einer Nachricht und dem zugehörigen Hashwert eine zweite Nachricht zu finden, welche den identischen Hashwert besitzt.
Deshalb ist es möglich, den Hashwert als „Repräsentant“ der zugehörigen Nachricht anzusehen.

Der Hashwert zu dem Gedicht „Erlkönig“ von Johann Wolfgang von Goethe lautet beispielsweise *eed57212c3c2c8be412c03eb0decb9e2*. Das Gedicht an sich besteht aus *226 Wörtern*.

Kommen wir nun zum letzten Sicherheitsziel, der *Integrität*. Und das Schöne dabei ist, diese haben wir mit unserem bisherigen Vorgehen bereits erfüllt!
Im vorherigen Schritt haben wir am Ende die Orginalnachricht mit der entschlüsselten Nachricht verglichen. Stimmen die beiden Nachrichten überein, können wir automatisch auch sagen, dass die Nachricht nicht manipuliert wurde. Die Integrität ist also erfüllt, aber wir haben umständlich zweimal die gleiche (ggf. große) Nachricht übermittelt. Mit Hilfe der kryptographischen Hashfunktionen bekommen wir das auch effizienter hin.

## Überblick (Sicherheitsziel Integrität)

**Integrität** ist dann hergestellt, wenn sichergestellt ist, dass eine Nachricht nicht manipuliert wurde.

Um die Integrität einer Nachricht sicherzustellen, übermittelt der Absender neben der Nachricht auch den zur Nachricht berechneten Hashwert. Der Empfänger berechnet den Hashwert der erhaltenen Nachricht erneut und vergleicht diesen mit dem übermittelten Hashwert. Sind die beiden Hashwerte identisch, so ist es sehr unwahrscheinlich, dass die Nachricht manipuliert wurde.

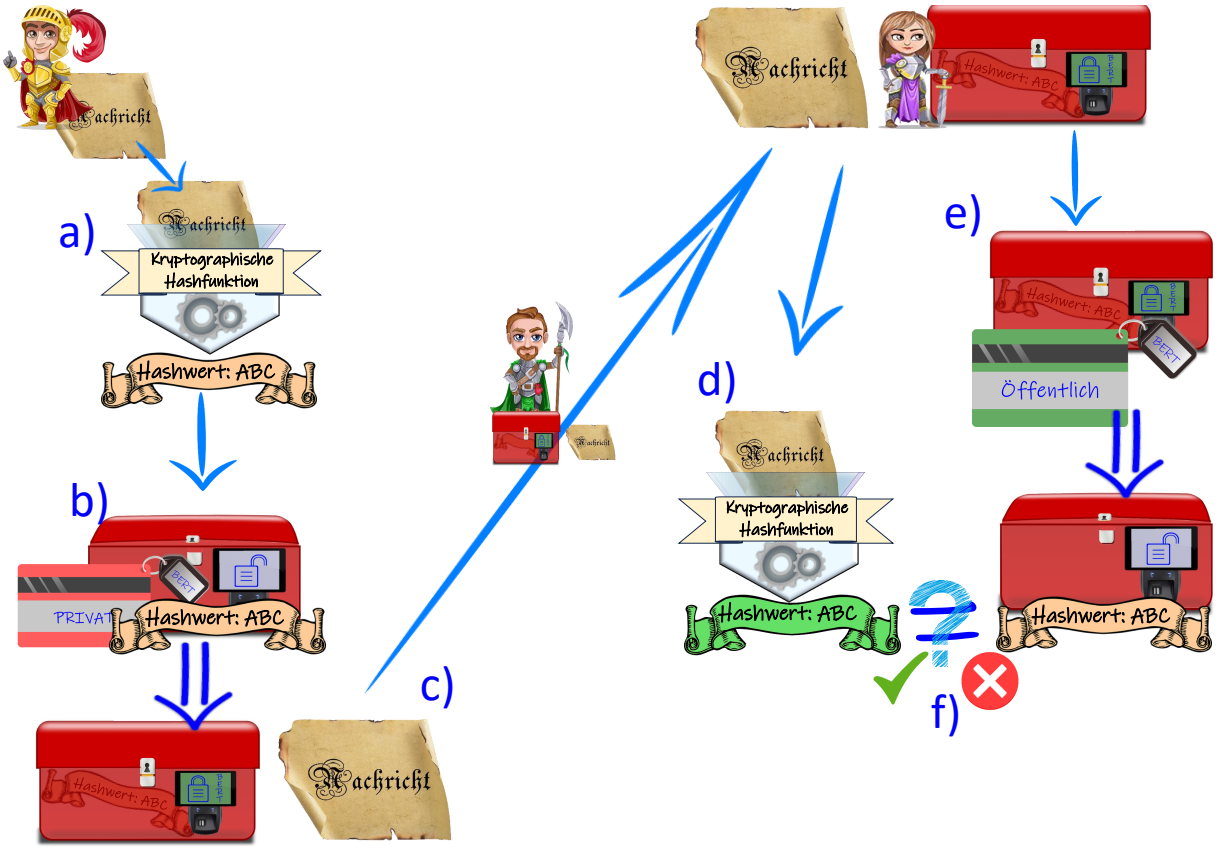

Fassen wir also zusammen...

## Überblick (Digitale Signaturen - Alles zusammen...)

Mit Hilfe von digitalen Signaturen lassen sich die Sicherheitsziele *Authentizität*, *Verbindlichkeit* und *Integrität* gleichzeitig erfüllen. Der prinzipielle Ablauf der Kommunikation ist im Folgenden dargestellt.

**Ablauf:**

Bert möchte eine Nachricht via Emil an Anna schicken, wobei der Inhalt der Nachricht nicht geheim ist. Allerdings soll Anna sicher sein können, dass die Nachricht von Bert ist und nicht manipuliert wurde.




a) Bert berechnet mit einer kryptographischen Hashfunktion den Hashwert seiner Nachricht an Anna

b) Den Hashwert der Nachricht verschlüsselt (*signiert*) Bert mit seinem *privaten Schlüssel*

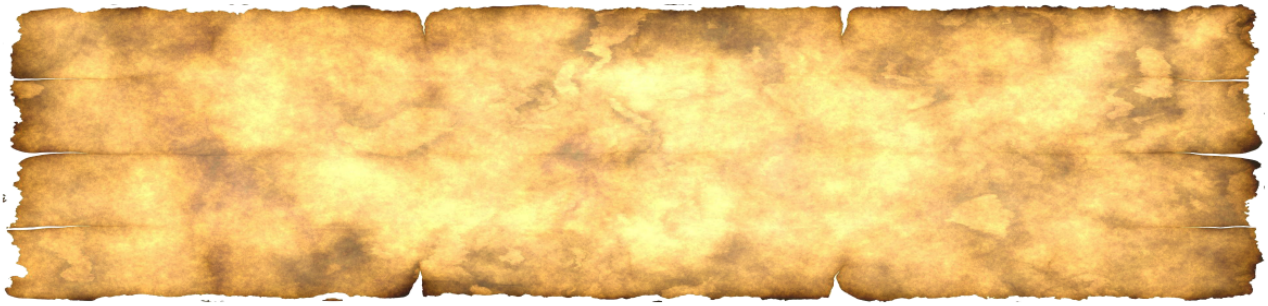
c) Die Nachricht und den verschlüsselten (*signierten*) Hashwert sendet Bert via Emil an Anna

d) Anna berechnet den Hashwert (grün) der Nachricht, die sie von Bert erhalten hat

e) Anna entschlüsselt den verschlüsselten Hashwert mit Hilfe von Berts *öffentlichen Schlüssel*.
*Hinweis:* Um sicher zu gehen, dass es sich bei dem öffentlichen Schlüssel um Berts öffentlichen Schlüssel handelt, kann ein Zertifikat verwendet werden. Dies ist nicht in der Grafik dargestellt.

f) Anna vergleicht den berechneten Hashwert der Nachricht (grün) mit dem entschlüsselten Hashwert (ocker). Stimmen sie überein, wurde die Nachricht nicht manipuliert. (Integrität ✓)
Außerdem besitzt nur Bert den privaten Schlüssel, der zu dem öffentlichen Schlüssel passt, welchen Anna zur Entschlüsselung des Hashwerts verwendet hat. Damit weiß Anna zudem, dass die Nachricht von Bert kommt, und Bert kann auch nicht leugnen, der Absender zu sein. (Authentizität und Verbindlichkeit ✓)

**Geschafft!!** Du hast alle Rätsel auf den Weg in die Gruft erfolgreich gemeistert und das dritte Teil-Fragment erhalten. Notiere dieses hier im Heft und mach dich auf den Weg zur Höhle im Burgfelsen. Falls du nun im Besitzt aller drei Teil-Fragmente bist, kannst du dort alle drei Portale aktivieren und dir Zugang zum Schatz verschaffen!



*Platz für zusätzliche Notizen:*