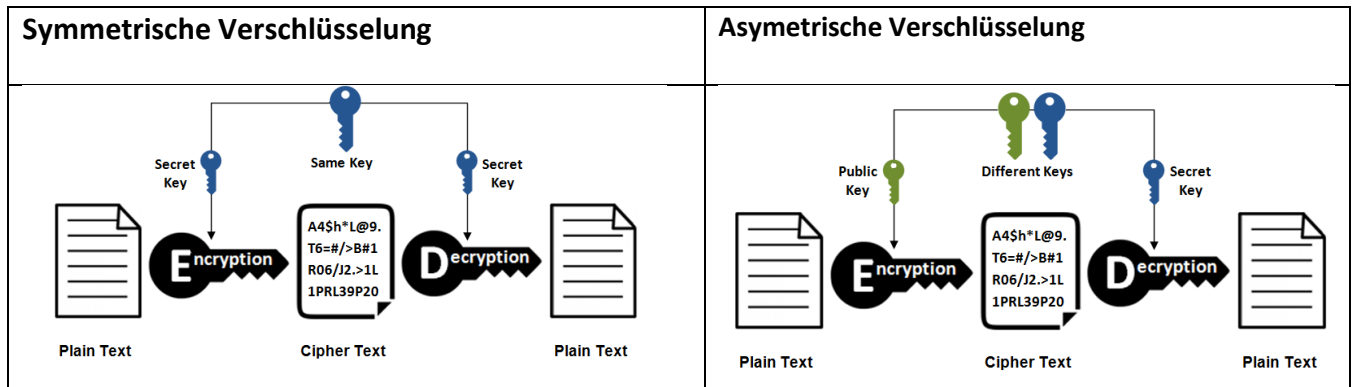


Lernzusammenfassung

Verschlüsselung

Verschlüsselung (auch: Chiffrierung oder Kryptierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffre“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.



Symmetrische Verschlüsselung

- Benutzt nur ein Kennwort zum ver- und entschlüsseln
- Wie: Zahlenkombination am Fahrradschloss. Jeder der sie kennt kann mit dem Rad fahren.
- Austausch des Schlüssels notwendig. (z.B. über das Internet unsicher)

Asymmetrische Verschlüsselung

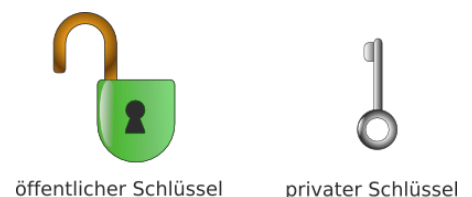
Hierbei kommen zwei verschiedene Schlüssel zum Einsatz: ein öffentlicher und ein geheimer (privater) Schlüssel. Das Prinzip der asymmetrischen Verschlüsselung beruht im Wesentlichen darauf, dass sich jeder Kommunikationspartner jeweils ein Schlüsselpaar erzeugt.

- Einer der Schlüssel wird **geheim gehalten**, der so genannte **private Schlüssel** und
- der andere, der so genannte **öffentliche Schlüssel** wird **jedem** kommunikationswilligen Wesen **zugänglich gemacht**.

Der große Vorteil dieses Verfahrens im Vergleich zur symmetrischen Verschlüsselung ist in der einfachen Verteilung des öffentlichen Schlüssels begründet. Dieser kann wirklich für jeden Menschen frei zugänglich sein, ohne dass dadurch das Verfahren unsicher wird.

Im folgenden Beispiel verwenden wir zur einfacheren Darstellung folgende Metapher: der **öffentliche Schlüssel** wird als Schloss betrachtet und der **private Schlüssel** als passender Schlüssel für dieses Schloss.

- Nehmen wir nun an, Bob möchte eine Nachricht an Alice schicken. Alice möchte aber nicht, dass ihr Vater lesen kann, was Bob ihr schreibt.
- Dazu wird sie also als Erstes einige Schlösser anfertigen, die nur von **einem** (ihrem) Schlüssel geöffnet werden können.



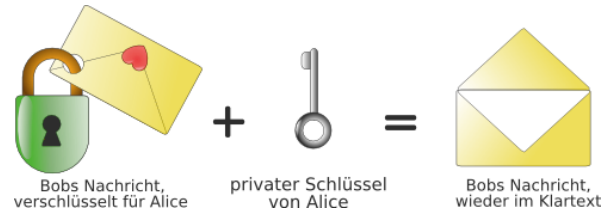
- Dann wird sie ihre (offenen!) Schlösser an ihre Freunde verteilen, also auch an Bob. Bob hat nun ein offenes Schloss von Alice, welches er zwar schließen kann, aber ohne passenden Schlüssel nicht wieder zu öffnen vermag (Alice wird ihren Schlüssel natürlich um keinen Preis der Welt rausrücken).



Lernzusammenfassung

Verschlüsselung

- Also fängt Bob an, seinen Brief zu schreiben, steckt ihn in eine Kiste und verschließt diese mit dem Schloss von Alice.
- Abgesehen von Alice ist nun niemand mehr in der Lage, die Kiste zu öffnen und den Brief zu lesen. Die Kiste macht sich nun auf die Reise und erreicht irgendwann Alice, welche mit ihrem Schlüssel das Schloss öffnet, den Brief der Kiste entnimmt, ihn liest und froh ist, dass ihr Vater Bobs Brief nicht lesen konnte.



Alice kann sich absolut sicher sein, dass niemand nach Verschließen der Kiste den Brief lesen konnte. Selbst Bob hatte nicht mehr die Möglichkeit, den Brief zu lesen, geschweige denn zu ändern, da nur Alice den passenden Schlüssel zum Schloss besitzt.

Der angesprochene Vorteil der öffentlichen Schlüsselübertragung besteht also darin, dass prinzipiell jeder ein Schloss von Alice benutzen kann um Kisten zu verschließen, aber nur sie in der Lage ist, diese wieder zu öffnen.

Hybride Verschlüsselung

Sie ist eigentlich sehr simpel und umso mehr genial. Sie verbindet die Vorteile der 2 anderen Systeme zu einem Neuen.

Hybride Verschlüsselung vereinigt die Vorteile und besitzt eigentlich keine Nachteile. Sie funktioniert nämlich in Kürze so:

mit Hilfe eines asymmetrischen Verfahrens (z.B. RSA) wird ein selbst generierter Schlüssel verschlüsselt ausgetauscht, welcher für eine symmetrische Verschlüsselung (z.B. AES) verwendet wird.

Das wars schon.

Schlüsselvereinbarung nach **Diffie-Hellmann**.

Ziel: Vereinbarung eines gemeinsam geheimen Schlüssels **ohne diesen auszutauschen**.

Achtung: Diffie-Hellman allein liefert keine Verschlüsselung und keine Authentisierung der Partner.

Verwendet wird dieses Verfahren z.B. bei SSH (Secure Shell) oder bei SSL/TLS (Secure Sockets Layer / Transport Layer Security).

Was ist ein Hash?

Ein Hashalgorithmus ist im Vergleich zu der Verschlüsselung dafür gemacht, dass man die Ausgabe nicht wieder in die Eingabe zurückführen kann. Ein Hash ist eine Prüfsumme. Es wird quasi eine (längere) Zahl mit fixer Länge für eine Eingabe mit beliebiger endlicher Länge berechnet. Dieses Ergebnis ist dann nicht mehr zuverlässig reversibel.

