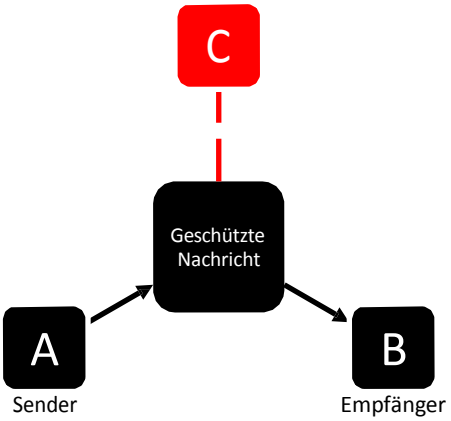
Wie funktioniert Verschlüsselung?

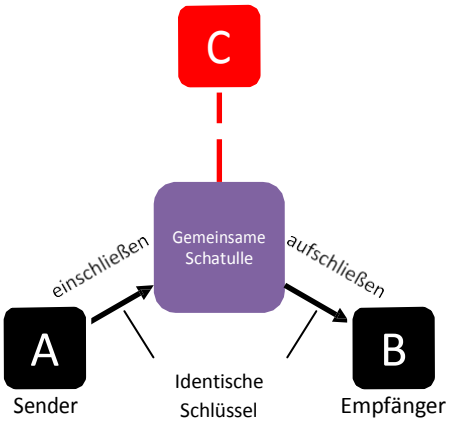
Nachdem Sie im Fokusthema „Verschlüsselt durch den Tag“ kennengelernt haben, wo Sie überall im Alltag mit Verschlüsselung in Berührung kommen und was Sie damit machen können, wollen wir Ihnen in diesem Artikel erklären, wie Verschlüsselung genau funktioniert. Dabei geht es uns weder um konkrete Verschlüsselungsanwendungen/-tools, noch um den mathematischen Hintergrund, sondern um die grundlegende Funktionsweise.[1]

Alle gängigen Verschlüsselungsverfahren beruhen im Großen und Ganzen auf dem gleichen Prinzip. Damit Sie sich dieses Prinzip gut vorstellen können, möchten wir dieses anhand einer Metapher erläutern: Stellen Sie sich einfach einmal reale, analoge Schlösser und Schlüssel vor, wie Sie Ihnen täglich begegnen: Nehmen wir an, Person A (Sender) möchte Person B (Empfänger) eine Nachricht so schicken, dass Person C die Nachricht nicht mitlesen kann, selbst wenn es ihm gelingt, diese auf ihrem Weg von A nach B abzufangen.



Symmetrische Verschlüsselung

A und B kaufen sich eine Schatulle mit einem Schloss, um ihre Nachrichten in Zukunft sicher vor fremden Blicken zu transportieren. Für das Schloss der Schatulle gibt es nur zwei Schlüssel. Nun können sich A und B sichere Nachrichten schicken, indem A die Nachricht vor dem Versand in die Schatulle einschließt (verschlüsselt) und B die Schatulle nach dem Empfang wieder öffnet (entschlüsselt), um die Nachricht zu lesen. Selbst wenn C die Schatulle in die Hände bekäme, bliebe die enthaltene Nachricht geschützt, da C keinen Schlüssel für das Schloss hat.



In diesem Fall spricht man von symmetrischer Verschlüsselung, da der gleiche Schlüssel sowohl für das Verschlüsseln als auch das Entschlüsseln verwendet wird. Dementsprechend verfügen auch Sender und Empfänger über den gleichen Schlüssel.

Symmetrische Verschlüsselung wird beispielsweise bei verschlüsseltem WLAN verwendet und hat den Vorteil, dass sie besonders schnell ist. Ein Nachteil symmetrischer Verschlüsselung: Der Schlüssel muss unbedingt geheim gehalten werden. Örtlich voneinander entfernte Kommunikationspartner – nehmen wir an, A und B leben weit auseinander – stehen beispielsweise vor der Herausforderung, dass beide den gleichen Schlüssel brauchen, sie diesen aber nicht einfach über das Internet austauschen können: Der Schlüssel könnte unterwegs einfach von C abgefangen und kopiert werden und die Verschlüsselung wäre nicht mehr sicher.

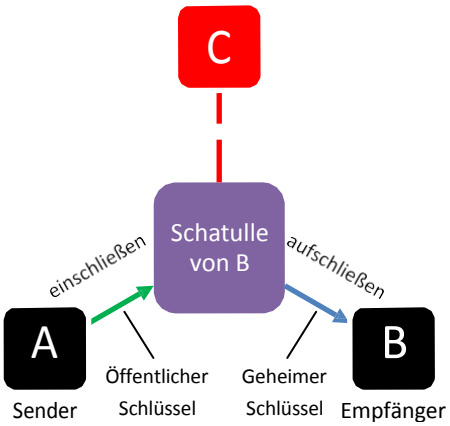
[1] Auf den mathematischen Hintergrund wird an dieser Stelle nicht eingegangen.

Asymmetrische Verschlüsselung

Ein Verfahren, das dieses Problem löst, ist die asymmetrische Verschlüsselung. Das Verfahren ist zwar komplizierter und langsamer, dafür müssen aber grundsätzlich keine geheimen Schlüssel ausgetauscht werden. In unserem Beispiel aus dem realen Leben kaufen sich A und B jeweils eine eigene Schatulle. Diese sind jeweils mit zwei Schlössern versehen: Mit dem einen Schloss kann man die Schatulle öffnen (entschlüsseln) und mit dem anderen verschließen (verschlüsseln).

Den Schlüssel zum ersten Schloss behalten A und B jeweils für sich (man nennt ihn den „privaten Schlüssel“). Diesen dürfen und müssen sie auch mit niemanden austauschen. Den Schlüssel für das zweite Schloss schicken sie – ähnlich wie in der symmetrischen Verschlüsselung – dem jeweils anderen. Nur ist es jetzt egal, wenn C den verschickten Schlüssel abfängt und kopiert, da er mit diesem Schlüssel allein nichts anfangen kann. Aus diesem Grund nennt man diesen Schlüssel den „öffentlichen Schlüssel“.

Nun kann beispielsweise A eine Nachricht vertraulich an B schicken, in dem die Nachricht von A mit dem öffentlichen Schlüssel von B in der Schatulle eingeschlossen wird. Mit dem privaten Schlüssel kann B die Schatulle öffnen und die Nachricht lesen. Genauso kann B eine vertrauliche Nachricht an A schicken. C bleibt außen vor, da ihm die privaten Schlüssel fehlen, die zum Öffnen der Schatullen bräuchte.



Der große Vorteil dieses Verfahrens: Der öffentliche Schlüssel kann allen geschickt werden, die verschlüsselt mit einem Empfänger kommunizieren möchten. Es gibt im Internet sogar Datenbanken, in denen man wie in einem Telefonbuch öffentliche Schlüssel hinterlegen kann, sodass andere sie dort finden. Asymmetrische Verschlüsselung wird deshalb beispielsweise gerne bei der Ende-zu-Ende-Verschlüsselung von E-Mails verwendet.

Hybride Verschlüsselung

In der Praxis gibt es neben den Anwendungsszenarien, die ausschließlich symmetrische oder asymmetrische Verschlüsselung verwenden, viele, die beide Arten kombinieren. Ein Beispiel hierfür ist die verschlüsselte Kommunikation zwischen Browser und Webseite via SSL: Die eigentliche Kommunikation wird über symmetrische Verschlüsselung erledigt, da diese schnell und effizient ist. Um den Schlüssel für die symmetrische Verschlüsselung auszutauschen, wird hingegen beim Aufbau der SSL- Verbindung eine asymmetrische Verschlüsselung verwendet: Der Browser nutzt den öffentlichen Schlüssel der Webseite, um eine verschlüsselte Nachricht an die Webseite zu schicken und die Kommunikation so zu initiieren.