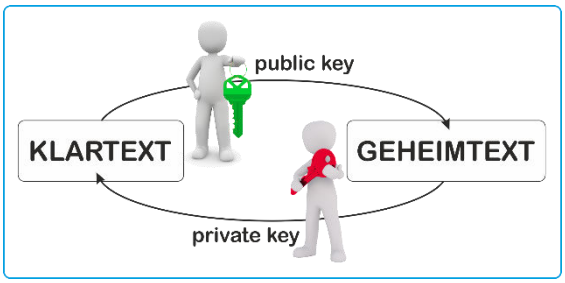
L3 1. Verschlüsselung und Datensicherheit

1.3 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung gibt es im Gegensatz zur symmetrischen Verschlüsselung immer zwei sich ergänzende Schlüssel. Ein Schlüssel

- der Public Key – dient für das Verschlüsseln einer Nachricht,
- ein anderer – der Private Key – für das Entschlüsseln.



Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Aus einem Schlüssel lässt sich der dazugehörige zweite Schlüssel nicht so leicht erraten oder berechnen. Dadurch kann man einen Schlüssel des Schlüsselpaares für jedermann öffentlich zugänglich machen. Daher auch die Bezeichnung Public Key.

Das Verfahren der asymmetrischen Verschlüsselung lässt sich leicht begreifen, wenn man an einen Tresor mit Schnappschloss denkt. Jeder kann etwas einschließen, weil der Tresor sich automatisch schließt, wenn die Tür ins Schloss fällt. Zum Öffnen ist allerdings ein Schlüssel nötig. Mit dem Public Key kann also jeder wie mit einem Schnappschloss etwas einschließen. Weil aber nur der Empfänger über den geheimen, den Private Key verfügt, kann nur er die Nachricht entziffern oder etwas aus dem Tresor holen.

Die asymmetrische Verschlüsselung beruht auf mathematischen Verfahren, die in einer Richtung einfach aber in der anderen Richtung schwierig durchzuführen sind. Multiplizieren ist so ein Beispiel:

Jeder kann einfach zwei Zahlen multiplizieren, zum Beispiel:

3 121 163 * 4 811 953 = 15 018 889 661 339

Zahlen in Faktoren zu zerlegen, ist dagegen sehr mühselig: Hat man erst einmal das Produkt, ist es sehr schwierig herauszufinden, aus welchen Faktoren dieses ursprünglich gebildet wurde. Verkürzt dargestellt, entspricht der Public Key dem Produkt. Dieses wird benötigt, um Informationen für den Empfänger zu verschlüsseln. Dessen Private Key enthält die beiden Zahlen, aus denen das Produkt gebildet wurde. Diese sind für das Entschlüsselungsprogramm nötig, um die verschlüsselte Botschaft zu entschlüsseln.

Das Problem des schwierigen Schlüsselaustausches ist daher elegant gelöst: Der öffentliche Teil kann jedem zugänglich gemacht werden, ohne dass die Sicherheit darunter leiden würde. Man benötigt ja immer noch den geheimen Schlüssel. Ein weiterer Vorteil des Verfahrens ist, dass sehr viel weniger Schlüssel benötigt werden als beim symmetrischen Verfahren, das schon für die Kommunikation von zwölf Menschen untereinander 66 Schlüssel erfordert. Bei der asymmetrischen Verschlüsselung benötigt jeder nur ein Schlüsselpaar.

Beispiel Signatur

Die digitale Signatur basiert auf der asymmetrischen Kryptografie, wobei das verwendete asymmetrische Verfahren umgekehrt wird. Bei der asymmetrischen Verschlüsselung dienen der öffentliche Schlüssel zum Verschlüsseln und der private Schlüssel zum Entschlüsseln. Bei der digitalen Signatur werden die Daten mit Kennzeichen versehen, die durch den privaten Schlüssel hinzugefügt werden.

Mit dem öffentlichen Schlüssel kann man feststellen, ob die Daten von demjenigen stammen, der mit seinem privaten Schlüssel signiert hat und ob die Daten unverändert sind.

Die Tatsache, dass der private Schlüssel durch seinen Besitzer geheim gehalten wird, erlaubt die Annahme, dass Daten, die mit dem privaten Schlüssel codiert sind, tatsächlich vom Schlüsselbesitzer stammen.
Ablauf:

1. Ein Teilnehmer "unterschreibt" eine Nachricht m, indem er sie mit seinem privaten Schlüssel d kodiert. Heraus kommt die Signatur s.
2. Er verschickt die Nachricht m zusammen mit der Signatur s.
3. Die Echtheit der Nachricht m und die Identität der Person kann durch die Signatur s und den öffentlichen Schlüssel von jedem überprüft werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Grundlagenwissen/AsymmetrischeVerschluesselung/asymmetrische_verschluesselung_node.html
heruntergeladen am 03.05.2018