LU05c - Die Asymmetrische Verschlüsselung

Lernziele

- Den Begriff **Asymmetrische Verschlüsselung** in eigenen Worten erklären können.
- Die relevanten Komponenten einer asymmetrischen Verschlüsselung nennen und ihre Funktion erläutern können.
- Vor- und die Nachteile einer asymmetrischen Verschlüsselung erläutern können.
- Darlegen können auf welchen zwei Arten die Verteilung von Schlüsseln durchgeführt werden kann.

Einleitung

Bei der symmetrischen Verschlüsselung wird eine Nachricht mit einem unbekannten Key verschlüsselt und entschlüsselt. Dieser Key muss sorgfältig bewacht werden, da von diesem einem die gesamte Sicherheit der Geheimnachricht abhängt. Da nicht alle Sender einer Nachricht gleich sorgfältig mit den Keys umgehen, kann das zu Sicherheitslücken, und damit zu ungewollten Veröffentlichungen von Geheimnachrichten führen. Zudem ist die Schlüsselverwaltung recht kompliziert, zumal die Anzahl der Keys nahezu quadratisch wächst.

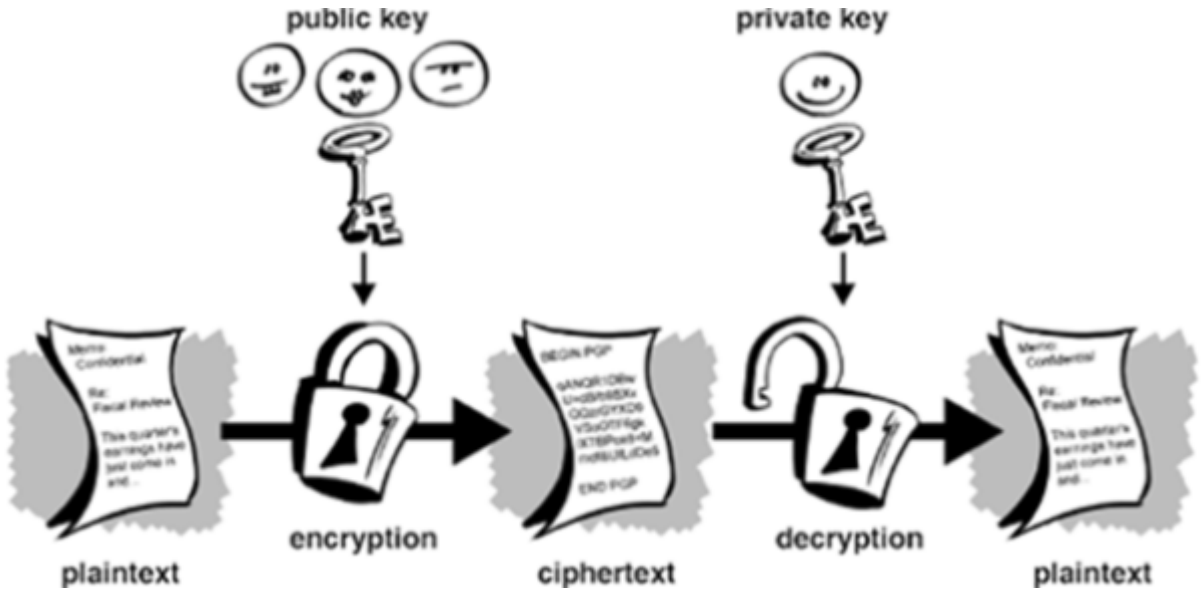
Es wäre doch schön, wenn wir einen Schlüssel hätten, der nur zum Verschlüsseln verwendet wird, da wir diesen dann öffentlich zugänglich machen könnten. Zudem wäre es doch noch besser, wenn nur wir als Empfänger einer Nachricht die Chiffretexte entschlüsseln könnten. Hier kommt die **Asymmetrische Verschlüsselung** ins Spiel.

1. Die Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass es immer zwei Schlüsseln gibt:

- Einen öffentlichen Schlüssel (public key): Dieser darf ungesichert verteilt oder auch auf dem Internet publiziert werden.
- Einen privaten Schlüssel (private key): Dieser ist nur dem Besitzer bekannt.

Das Besondere ist, dass Nachrichten, die mit einem dieser Schlüssel verschlüsselt werden, nur mit dem jeweils anderen aus dem Paar wieder entschlüsselt werden können.



Will man also einer Person eine verschlüsselte Nachricht zukommen lassen, dann verschlüsselt man diese Nachricht mit dem öffentlichen Schlüssel des Empfängers. Nur der Besitzer des zugehörigen privaten Schlüssels, also in dem Fall der Empfänger, ist dann in der Lage die Nachricht zu lesen. Auch der Absender selbst kann diese nach dem Verschlüsseln nicht mehr lesen!

Alle bekannten asymmetrischen Verschlüsselungsverfahren beruhen darauf, dass es sehr einfach ist, aus zwei Primfaktoren das entsprechend Produkt zu berechnen, während das Umgekehrte, die Primfaktorenzerlegung bei grossen Zahlen unmöglich ist.

Vorteil:

- Einfacheres Schlüsselmanagement

Nachteil:

- Rechenintensiver
- Ciphertext ist viel grösser als Plaintext

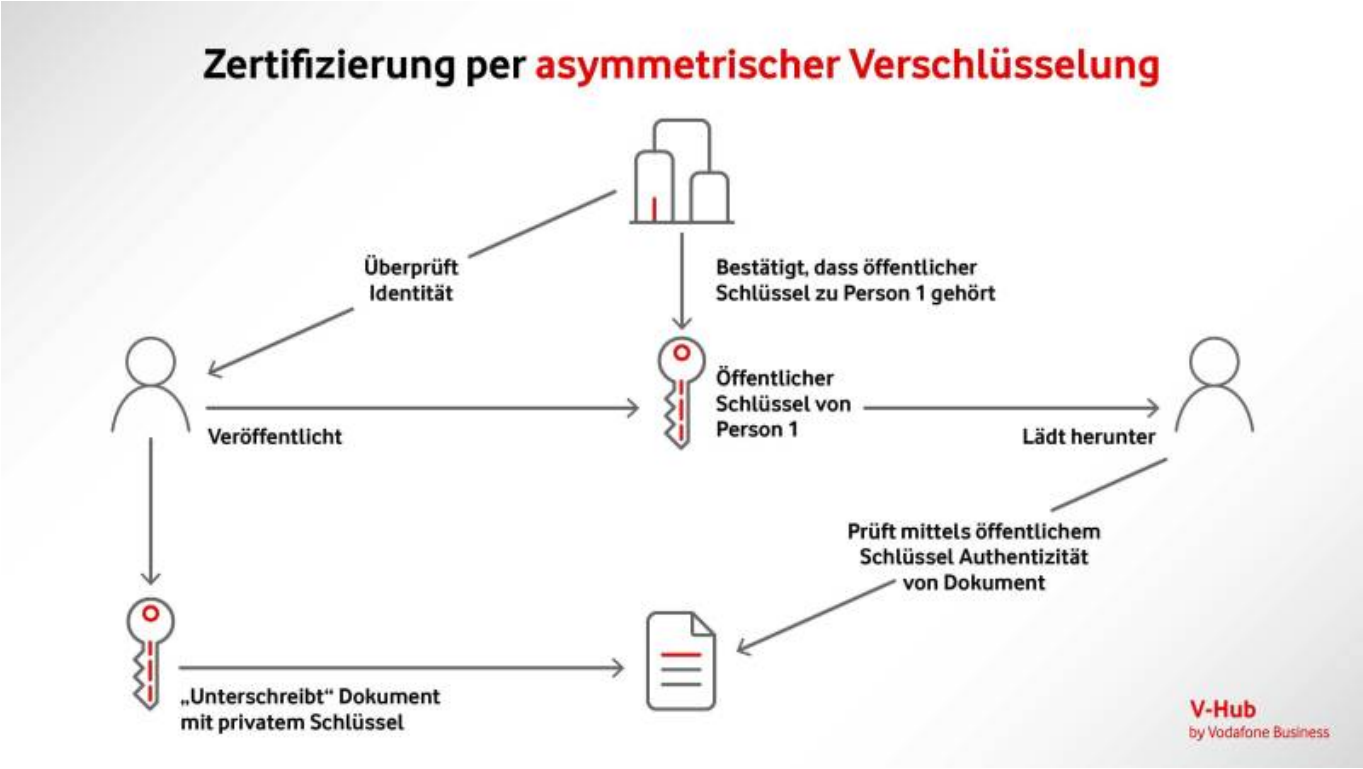
2. Schlüsselverteilung

Wenn man eine Nachricht für einen bestimmten Empfänger verschlüsseln will, dann ist das nur von Nutzen, wenn man 100% sicher ist, dass der verwendete Schlüssel auch tatsächlich der entsprechenden Person gehört. Es stellt sich also auch hier in einer gewissen Weise das Problem der Verteilung von Schlüsseln. Zwar nicht wegen der Geheimhaltung, aber wegen der Authentizität (Echtheit). Das Vertrauen in einen öffentlichen Schlüssel beruht darauf, dass man ihn von einer vertrauenswürdigen Quelle erhalten hat. Entweder direkt von der Inhaberin oder von einer anderen Person, der man vertraut und die mit ihrer digitalen Unterschrift (s.u.) die Echtheit des Schlüssels betätigt. Eine mögliche Lösung bietet das *Web Of Trust* oder auch *Ring OF Trust*.

2.1 Web Of Trust

Aus Wikipedia: Netz des Vertrauens bzw. Web of Trust (WOT) ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen),

kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“), zu sichern. Es stellt eine dezentrale Alternative zum hierarchischen PKI-System dar und basiert auf dem Prinzip *Der Freund meines Freundes ist auch mein Freund*.

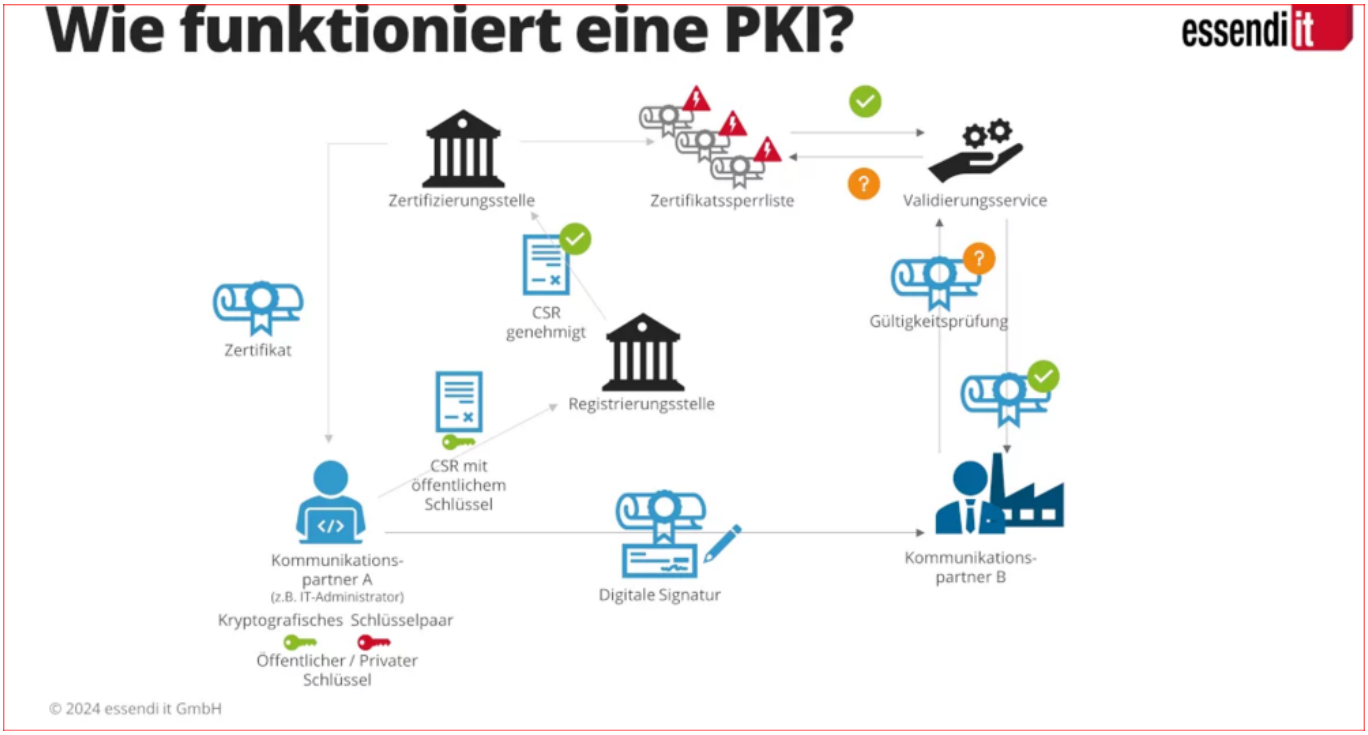


Ausprobieren: gnuPGP.org

PKI

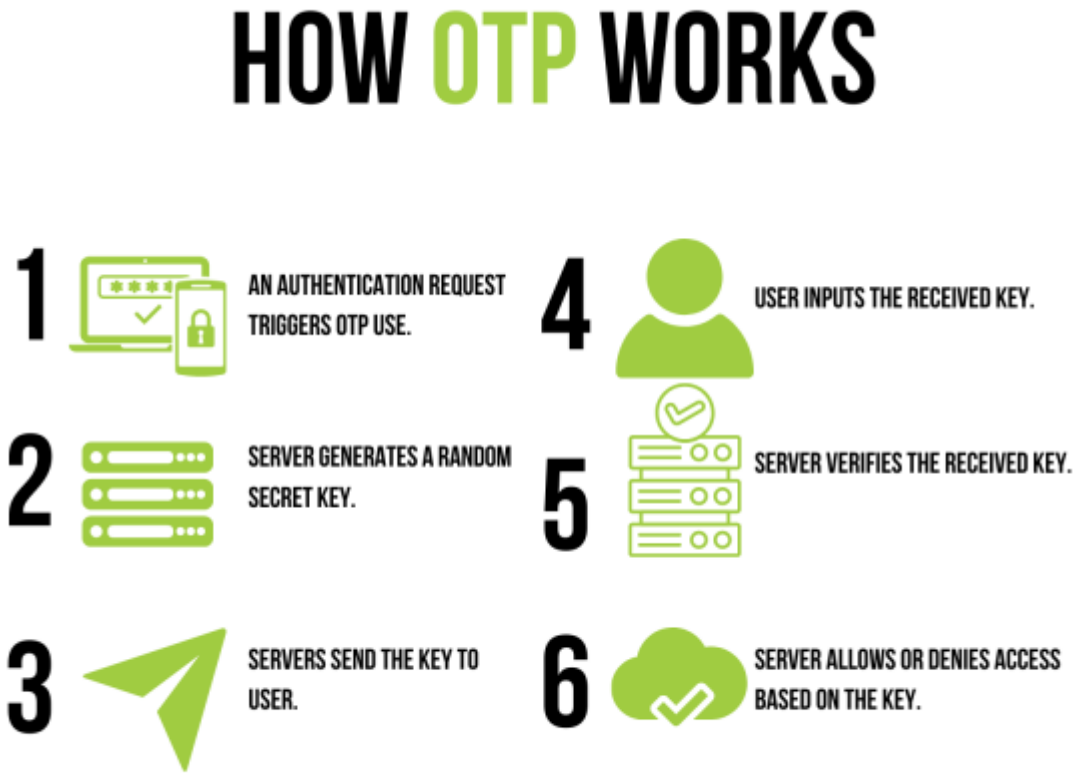
Aus Wikipedia: PKI steht für „Public Key Infrastructure. Mit Public-Key-Infrastruktur (PKI, englisch public key infrastructure) bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet

Es gibt Stellen, die die Aufgabe übernommen haben, die Zuordnung von Schlüsseln zu Personen zu überprüfen und dann mit ihrer Unterschrift zu bestätigen. Um einem so unterschriebenen Schlüssel zu vertrauen, muss man also der entsprechenden Zertifizierungsstelle trauen können. An diese Stellen werden denn auch hohe Anforderungen gestellt.



Einwegverschlüsselung (OTP)

Von Einweg-Verschlüsselungen spricht man, wenn ein Algorithmus zur Verschlüsselung verwendet wird, welcher nicht umkehrbar ist. Oft spricht man dann auch von Hash-Werten. Solche Verfahren werden oft angewandt, um die Unversehrtheit von Daten zu überprüfen. Ein guter Hash-Algorithmus ist so ausgelegt, dass bei der Änderung eines Bits in der Original-Meldung 50% der Bits im Hash-Wert ändern.

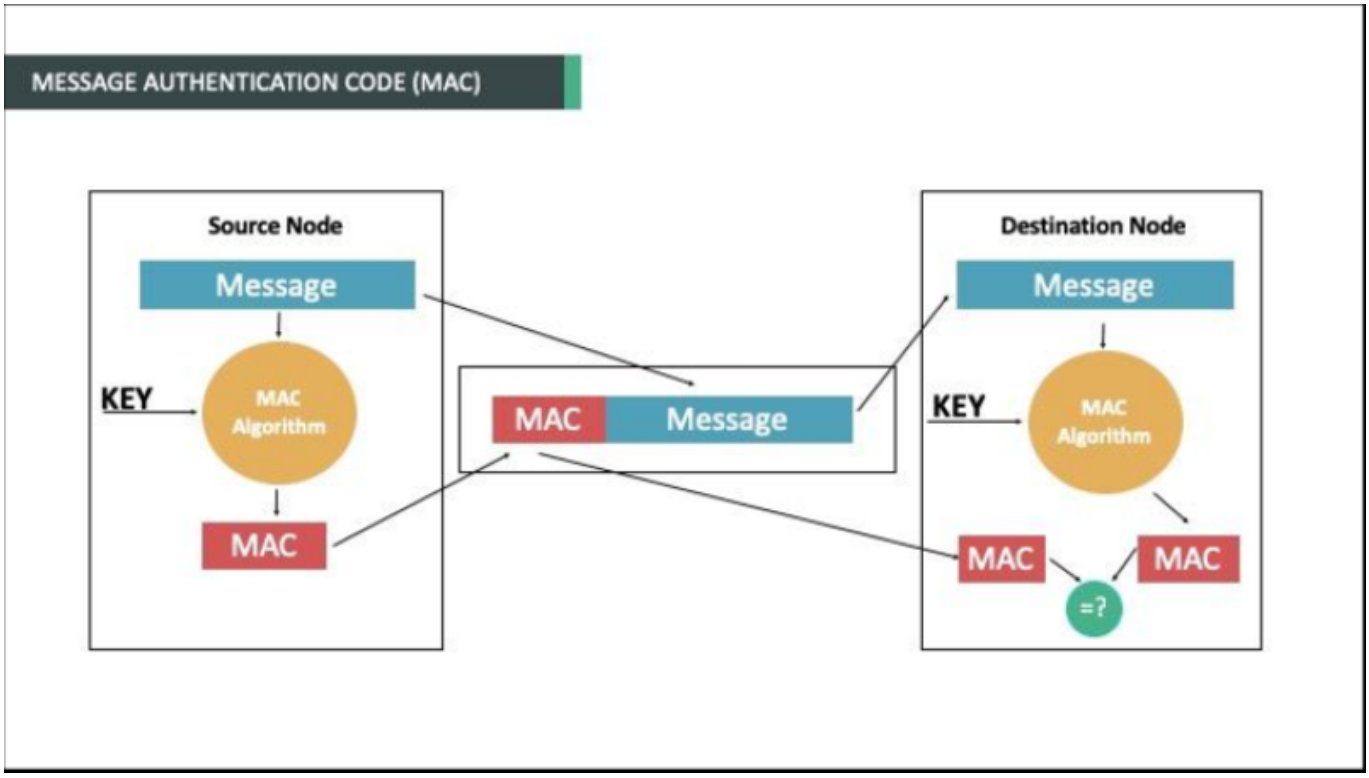


Digitale Signaturen/Message Authentication Codes (MACs)

Verschlüsselung allein garantiert noch nicht, dass eine Nachricht auf dem Weg vom einen zum anderen Kommunikationspartner nicht verfälscht wird. Um dies sicherzustellen, wird zusätzlich zur Verschlüsselung auch ein so genannter Hash-Wert der Nachricht berechnet und ebenfalls verschlüsselt. Wenn die entschlüsselte Nachricht dann wieder den gleichen Hash-Wert ergibt, dann kann man sicher sein, dass die Nachricht unversehrt geblieben ist.

Bei symmetrisch verschlüsselten Nachrichten nennt man diesen verschlüsselten Hash-Wert: Message Authentication Code (MAC).

Bei asymmetrischer Verschlüsselung kommt noch ein Aspekt dazu. Falls der Absender der Nachricht den Hash-Wert mit seinem privaten Schlüssel verschlüsselt hat und eine Entschlüsselung mit dem entsprechenden öffentlichen Schlüssel wieder den richtigen Wert ergibt, dann kann man nicht nur sicher sein, dass die Nachricht unverfälscht ist, sondern man kann auch beweisen, dass die Nachricht nur vom Absender stammen kann. Man spricht deshalb auch von digitaler Signatur.



Quellen

- https://de.wikipedia.org/wiki/Web_of_Trust
- https://de.wikipedia.org/wiki/Public-Key-Infrastruktur
- https://www.ssl.com/article/what-is-a-one-time-password-otp/
