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.

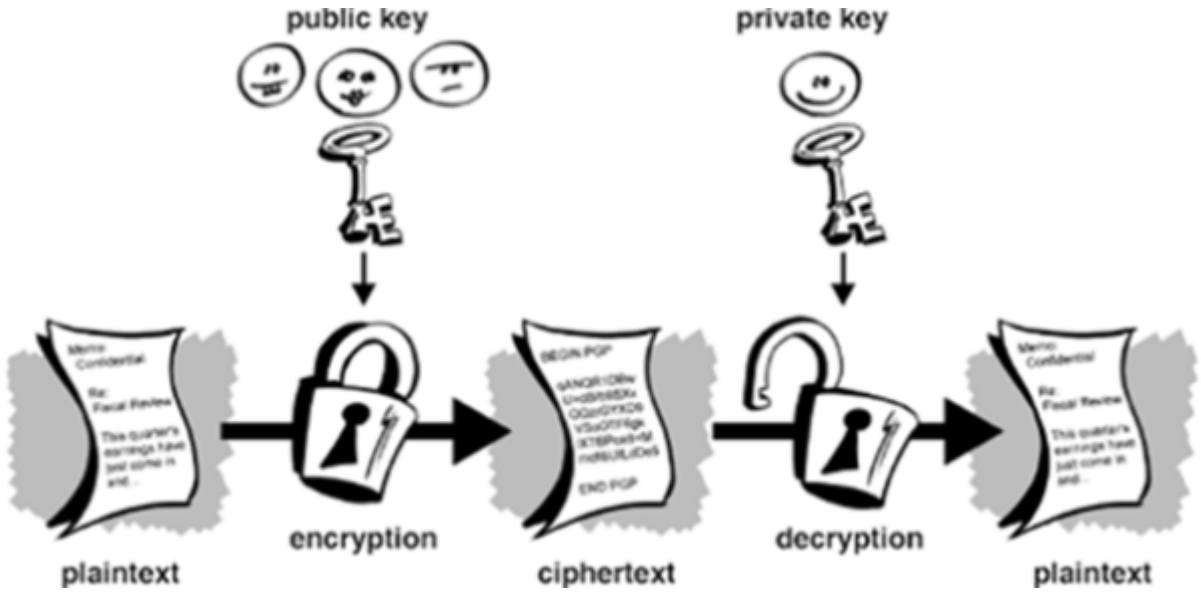
Es wäre doch schön, wenn wir einen Schlüssel hätten, der nur zum Verschlüsseln verwendet wird, da wir diesen dann öffentlich zugänglich machen könnten. Zudem wäre es doch noch besser, wenn nur wir als Empfänger einer Nachricht die Chiffretexte entschlüsseln könnten. Hier kommt die **Asymmetrische Verschlüsselung**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

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.
