D_KRYPTOGRAFIE_ASYM

Asymmetrische Verschlüsselung

Die Nachteile bei der symmetrischen Verschlüsselung ist der sichere Schlüsseltausch und die Schlüsselanzahl die quadratisch zur Anzahl Teilnehmer wächst. Diese Nachteile sollen mit einem neuen Ansatz behoben werden: Mit der asymmetrischen Verschlüsselungstechnik!

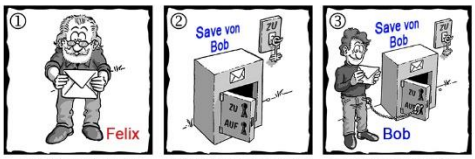
Das Schlüsselkonzept bei der asymmetrischen Verschlüsselung

Der andere Ansatz: Zweiteiliger Schlüssel Man nennt dies asymmetrische Verschlüsselung

Das heisst: Der öffentliche Schlüssel einer Person (Public-Key) kann von allen eingesehen werden

Wobei der private Schlüssel dieser Person (Private-Key) von ihr geheim gehalten wird

Das Verfahren bei der asymmetrischen Verschlüsselung



Eine Botschaft zu übermitteln funktioniert also so: Jederman kann mir eine Botschaft hinterlegen

Damit diese Botschaft auch geheim bleibt, schliesst der Absender den Safe mit meinem öffentlichen Schlüssel zu

Nur ich, mit meinem privaten (geheimen) Schlüssel, kann den Safe öffnen und die Botschaft lesen

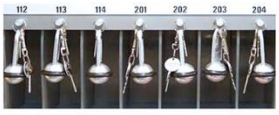
Die Verteilung des öffentlichen Schlüssels bei der asymmetrischen Verschlüsselung

Wo erhalte ich den Public-Key einer Person, die nicht grad um die Ecke wohnt?

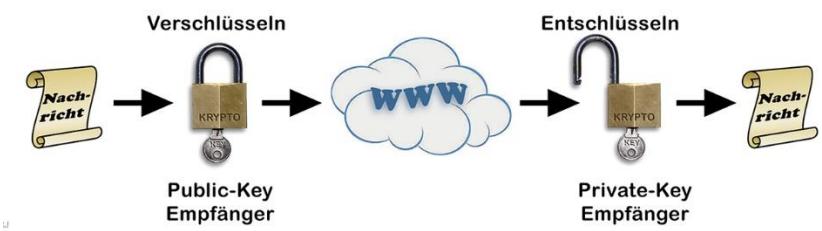
Nicht am Kiosk gegenüber sondern von global vernetzten Keyservern

Wer garantiert mir die Echtheit von auf Key-Servern hinterlegten Public-Keys?
- X.509-CA's
- Web-of-Trust
- PGP-CA's

Schlüsselpaar erzeugen



Public-Key veröffentlichen
Private-Key geheim halten



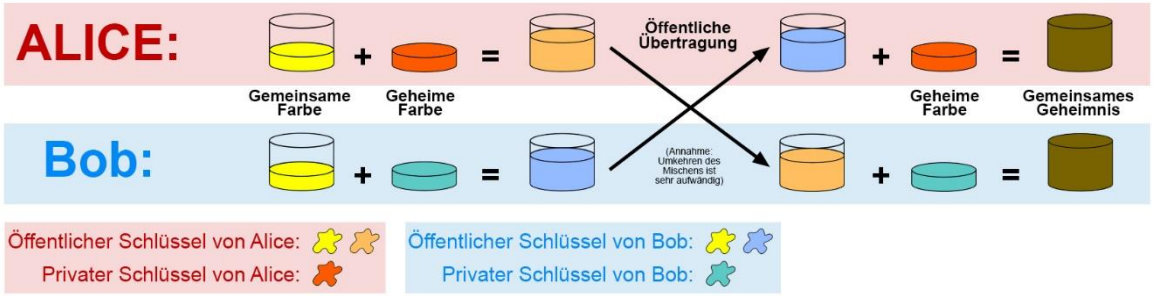
Public-Key Empfänger

Private-Key Empfänger

Wie sicher ist das Verfahren wie z.B. Diffie-Hellman grundsätzlich?

Der Einstieg in die asymmetrische Verschlüsselung erfolgte um das Jahr 1976 durch die Entwicklung eines Protokolls für eine sichere Schlüsselvereinbarung durch die beiden Kryptologen Whitfield Diffie und Martin Hellman. Zwei Kommunikationspartner konnten nun über eine öffentliche, abhörbare Leitung einen gemeinsamen, geheimen und von Drittpersonen nicht berechenbaren Schlüssel in Form einer Zahl vereinbaren. Dieser gemeinsame Schlüssel konnte anschliessend für eine symmetrische Datenverschlüsselung verwendet werden (z.B. DES Data Encryption Standard oder AES Advanced Encryption Standard).

Die Grundidee dieses Diffie-Hellman-Schlüsseltauschs soll nun anhand einer Farb-Analogie bzw. mittels Farbmischung erklärt werden. Das Farbenmischen wird hier als eine Einwegfunktion aufgefasst. Damit meint man, dass es einfach ist, zwei oder mehrere verschiedene Farben zusammenzuschütten. Wesentlich schwieriger ist es allerdings, die erhaltene Farbmischung wieder in ihre ursprünglichen Komponenten aufzuteilen. (Umkehrung)



- Alice und Bob einigen sich öffentlich auf eine gemeinsame Farbe (Gelb).
- Jeder wählt für sich eine eigene, geheime Farbe (Alice: Orange, Bob; Türkis).
- Bob und Alice mischen nun jeweils die gemeinsame Farbe (Gelb) mit ihrer geheimen Farbe (Orange/Türkis). Alice erhält die Farbe Beige und Bob Graublau.
- Diese Farbmischungen tauschen Alice und Bob nun aus. Da darf jeder zuschauen. Diese beiden Farbmischungen sind nämlich nicht geheim. Für einen Aussenstehenden ist es nicht effizient möglich, aus den «öffentlichen» Farben (Gelb, Beige, Graublau) auf die geheimen Farben von Alice und Bob zu schliessen.
- Nun mischen Alice und Bob die Farbmischung ihres Gegenübers mit ihrer eigenen geheimen Farbe. Daraus entsteht wiederum eine neue Farbe (Ockerbraun), die für beide Kommunikationspartner gleich ist (Gelb + Orange + Türkis = Gelb + Türkis + Orange = Ockerbraun). Somit haben Alice und Bob eine gemeinsame geheime Farbe. Einer Drittperson ist es nicht möglich, die geheimen Farben von Alice und Bob herauszufinden, da diese Alices und Bobs geheime Farbzutaten nicht kennt.

Obwohl das mathematische Verfahren sicher ist und eine Brute-Force-Attacke an der Verarbeitungsgeschwindigkeit heutiger Prozessoren scheitert, bleiben zwei Gefahren:

- Unsichere, leicht erratbare Passwörter
- Der unbewusste Einsatz von gefälschten Public-Keys. Damit ist ein Public-Key gemeint, der vorgibt, der Person Bob zu gehören, tatsächlich aber von Mallory kreiert wurde. Die vermeintlich an Bob verschlüsselt verschickte Datei kann nun von Mallory problemlos geöffnet werden. Abhilfe schafft hier eine möglichst zentrale und vertrauenswürdige Public-Key-Verwaltung (PKI) oder ein Vertrauensnetzwerk.

Hybride Verfahren

Symmetrische Verschlüsselungsverfahren haben das bereits besprochene Problem des Schlüsseltauschs und Schlüsselmanagements, das bei den asymmetrischen Verfahren so nicht besteht. Allerdings benötigen symmetrische Verfahren weniger Rechenzeit zur Erstellung des Chiffretexts als rein asymmetrische Verfahren. Darum liegt es auf der Hand, dass in einem hybriden Verfahren die Vorteile der beiden Verfahren genutzt werden:

- **Asymmetrisches** oder Public-Key-Verfahren für **Schlüsselmanagement**, z.B. RSA
- **Symmetrisches** Verfahren zum Versenden der eigentlichen **Nachricht**, z.B. RC4, DES, AES

Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.

Digitale Signatur

Nicht immer ist es das Ziel, eine Nachricht zu verschlüsseln. Oftmals besteht auch das Bedürfnis, die Authentizität, Integrität, Verbindlichkeit etc. einer Nachricht zu erfahren:

- Wer hat in meinem E-Shop bestellt?
- wer hat mir diese oder jene E-Mail zugestellt?
- Hat wirklich der Absender das geschrieben hat, was ich da nun lese?
- Woher stammt das Applet, das ich gerade auf meinen PC lade?
- Handelt es sich bei dem Update wirklich um das richtige und unmanipulierte Original?
- Wohin wird meine Kreditkartennummer übermittelt?
- Wer hat bei einer Wahlveranstaltung gerade seine Stimme abgegeben?
- Stammt der Inhalt von www.admin.ch wirklich von unserer Regierung?

Ausgehend von seinem Grundprinzip ist das Internet nicht sicher. Die Gefahren:

- Mitlesen von Daten (Sniffing)
- Vortäuschen falscher Identitäten (Spoofing)
- Angriffe auf die Verfügbarkeit (Denial-of-Service)
- Übertragen von Programmen mit Schadfunktion (Viren, Würmer...)
- Menschliches Fehlverhalten (Preisgabe von geheimen Daten)

Das möchte man erreichen:

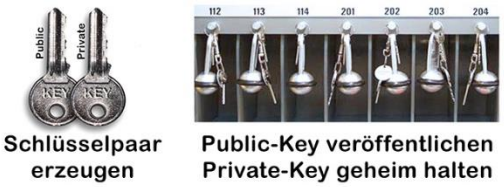
- **Authentisierung** - Sicherstellung der Identität eines Kommunikationspartners
- **Vertraulichkeit** - Zugänglichkeit der Nachricht nur für bestimmten Empfängerkreis
- **Integrität** - Schutz vor Verfälschung von Nachrichten bei der Übermittlung
- **Autorisierung** - Prüfung der Zugriffsberechtigung auf Ressourcen
- **Verfügbarkeit** - Schutz vor Datenverlust, Sicherstellung des laufenden Betriebs
- **Verbindlichkeit** - Sicherer Nachweis der Absendung bzw. des Empfangs

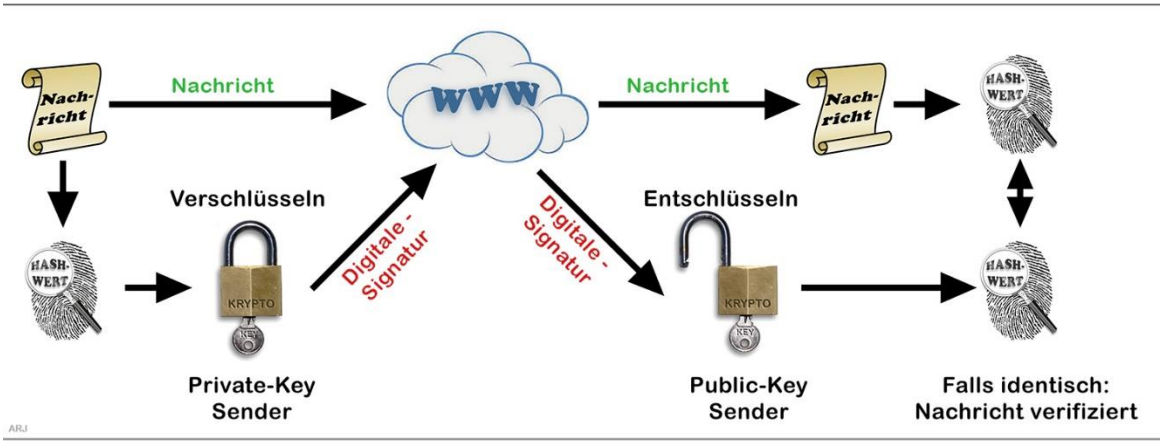
Und da kommt die digitale Signatur ins Spiel, weil diese folgendes bieten kann:

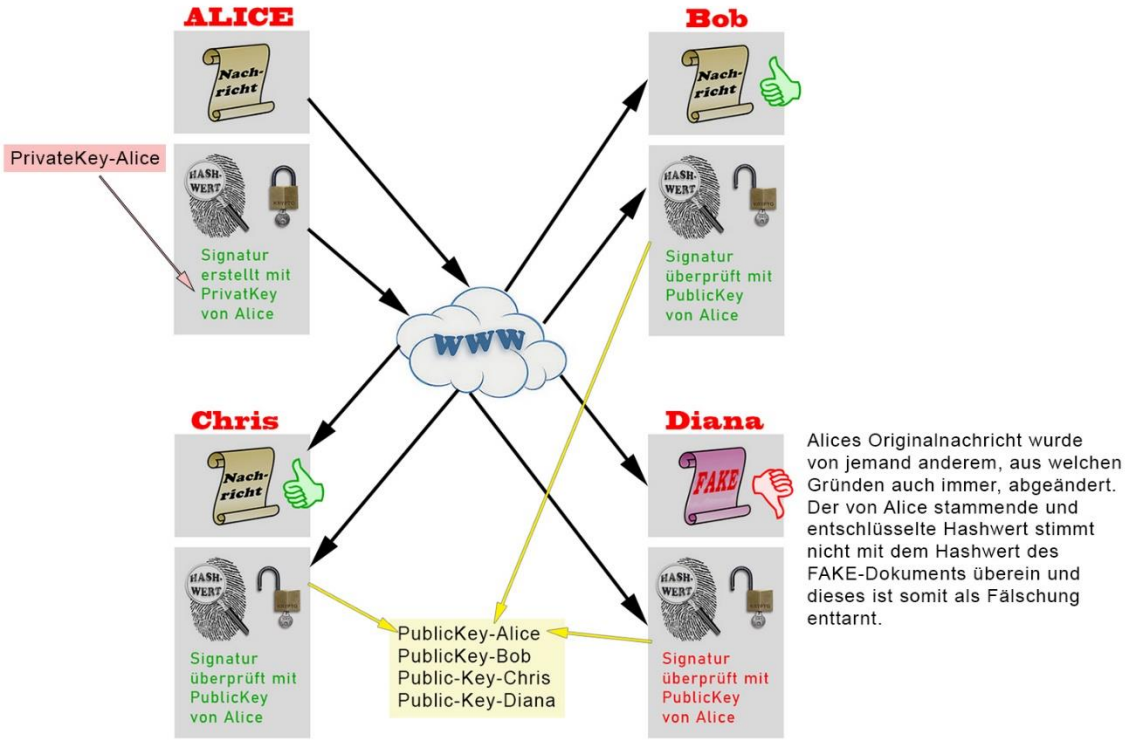
- Sichere **Identifizierung** des Absenders eines Dokumentes
- Sicherheit vor nachträglichen **Manipulationen** des Dokumentes
- Elektronisch signierte Dokumente sind mit unterschriebenen Papierdokumenten gleichgesetzt
- Ist ein Prüfwert einer Information
- Die Digitale Signatur hat die Aufgabe einer Unterschrift und eines Siegels

Technisch kommt **dasselbe Verfahren** zur Anwendung, wie bei der **asymmetrischen Verschlüsselung**. Bis auf einen kleinen, aber nicht unwesentlichen Unterschied, nämlich der Verwendung der Schlüssel:

- Der Inhalt der Nachricht wird auf eine eindeutige Kenngrösse abgebildet. Dazu bedient man sich eines **Hash-Algorithmus**
- Der **Hash-Wert** wird mit dem **privaten Schlüssel** verschlüsselt und zur Nachricht hinzugefügt
- Der Empfänger kann mit Hilfe des **öffentlichen Schlüssels** des Senders **prüfen**, ob die Information wirklich vom Absender stammt und nicht verändert wurde







Wie wird der Hash-Wert gebildet? (Hash-Algorithmus)

- Der Hashwert ist eine Art **Fingerabdruck** (Fingerprint) eines Dokuments.
- Der Hashwert bildet einen beliebig langen Nachrichtentext auf einen Wert vorgegebener, kurzer Länge an. (Hashwert, Prüfsumme)
- Aus dem Hashwert kann die ursprüngliche Nachricht **nicht errechnet** werden. (Irreversibilität)
- Die Konstruktion von Nachrichten mit identischem Hashwert muss praktisch unmöglich sein.
- Die zufällige Übereinstimmung von Hashwerten beliebiger Nachrichten ist sehr unwahrscheinlich. (Kollisionsresistenz, Integrität prüfbar)

Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.
