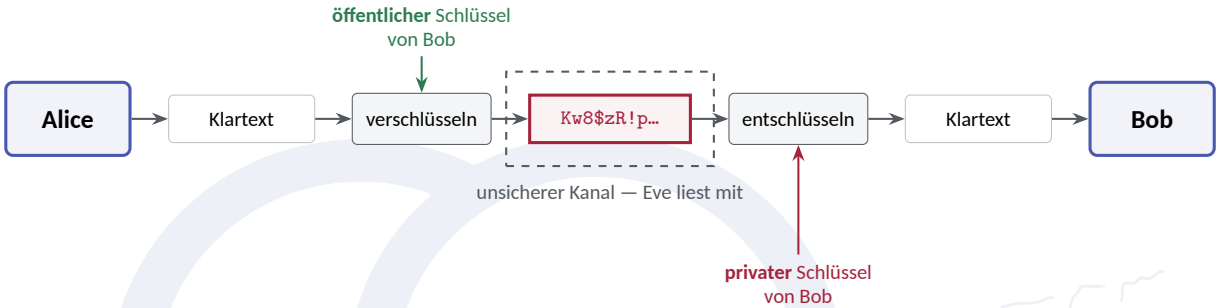
8.9 Asymmetrische Verfahren

1976 schlugen Whitfield Diffie und Martin Hellman eine Lösung vor, die zunächst unmöglich klingt: Jeder Teilnehmer besitzt **zwei** Schlüssel.

- Der **öffentliche Schlüssel** (public key) wird veröffentlicht. Mit ihm kann jeder eine Nachricht an den Besitzer verschlüsseln.
- Der **private Schlüssel** (private key) bleibt geheim und verlässt den Besitzer nie. Nur mit ihm lässt sich wieder entschlüsseln.

Damit verschwindet das Schlüsselverteilungsproblem: Es muss nie ein Geheimnis übertragen werden. Bei n Teilnehmern genügen n Schlüsselpaare.

Die Metapher dazu ist ein Briefkasten: Den Einwurfschlitz kann jeder benutzen, herausholen kann nur, wer den Schlüssel hat.



Bob veröffentlicht den grünen Schlüssel. Jeder darf damit *ver*schlüsseln — *ent*schlüsseln kann nur er, mit dem roten. Ein Geheimnis wird nie übertragen.

Asymmetrische Verschlüsselung. Verschlüsselt wird mit dem Schlüssel des *Empfängers*, nicht des Absenders.

Mathematisch braucht man dafür **Einwegfunktionen**: Berechnungen, die in eine Richtung leicht, in die andere praktisch unmöglich sind. Das Standardbeispiel ist die Multiplikation von Primzahlen.

$$\underbrace{7919 \cdot 6841 = 54\,173\,879}_{\text{leicht}} \qquad \underbrace{54\,173\,879 = ? \cdot ?}_{\text{schwer}}$$

Für die Verschlüsselung braucht man etwas mehr, nämlich eine **Falltürfunktion**: eine Einwegfunktion, die sich doch umkehren lässt, wenn man eine Zusatzinformation besitzt – die Falltür ist der private Schlüssel.

Merke

Asymmetrische Verfahren beruhen nicht darauf, dass ein Angreifer den privaten Schlüssel nicht berechnen *kann*, sondern darauf, dass die Berechnung zu lange dauert. Sicherheit ist hier eine Frage des Aufwands, nicht der Unmöglichkeit.

8.9.1 Der Haken: Man-in-the-Middle

LK

LK

Den Man-in-the-Middle-Angriff verlangt ausdrücklich nur der LK-Lehrplan („beschreiben den Man-in-the-middle-Angriff auf das Diffie-Hellman-Verfahren"). Dass die Lücke existiert, sollte aber auch im Grundkurs gesagt werden — sonst bleibt der falsche Eindruck zurück, Verschlüsselung allein genüge.

Oben stand, das Schlüsselverteilungsproblem verschwinde. Das stimmt nur halb. Übertragen wird zwar kein Geheimnis mehr — aber Alice muss immer noch wissen, dass der Schlüssel, den sie für Bobs öffentlichen hält, wirklich Bob gehört.

Genau hier setzt der **Man-in-the-Middle-Angriff** an (auch *Mittelsmann*-Angriff). Der Angreifer — traditionell **Mallory** genannt, von *malicious* — stellt sich nicht neben die Leitung, sondern **hinein**.



Beide Verbindungen sind einwandfrei verschlüsselt. Nur verschlüsseln sie zu *Mallory* statt zueinander. Die Mathematik ist in Ordnung — die Zuordnung von Schlüssel zu Person ist es nicht.

Man-in-the-Middle. Mallory führt zwei einwandfrei verschlüsselte Gespräche und übersetzt dazwischen.

Der Ablauf:

1. Alice fragt nach Bobs öffentlichem Schlüssel. Mallory fängt die Antwort ab und schickt stattdessen **seinen eigenen**.
2. Alice verschlüsselt mit diesem Schlüssel und schickt los. Mallory kann entschlüsseln — es ist ja sein Schlüssel.
3. Mallory liest mit, ändert nach Belieben, verschlüsselt mit **Bobs echtem** Schlüssel neu und schickt weiter.
4. Bob antwortet, und dasselbe geschieht in der Gegenrichtung.

Beide merken nichts. Beide Verbindungen sind kryptographisch einwandfrei.

Merke

Ein Man-in-the-Middle bricht die Verschlüsselung nicht — er unterläuft sie. Die Mathematik bleibt unangetastet; was fehlt, ist die Zuordnung von **Schlüssel zu Person**.

Deshalb löst Kryptographie allein das Problem nie ganz. Es braucht einen zweiten Weg, über den sich ein Schlüssel überprüfen lässt: persönliche Übergabe, ein Fingerabdruck über das Telefon — oder eine dritte Stelle, der beide trauen. Das sind die **Zertifikate** aus Abschnitt 8.11.

Stolperstein

Es ist derselbe Angriff, den Sie in Abschnitt 8.8 schon am Schlüsseltausch gesehen haben, und er hat denselben Grund: Beide Verfahren stellen sicher, dass am Ende *zwei* Partner einen Schlüssel teilen — aber nicht, **wer** diese beiden sind. Die Mathematik kann diese Lücke nicht schließen; dafür braucht es die Zertifikate aus Abschnitt 8.11.

Arbeitsauftrag 8

32. Erklären Sie, warum ein Man-in-the-Middle-Angriff kein Widerspruch zu der Aussage ist, RSA sei sicher.
33. Sie bekommen den öffentlichen Schlüssel einer Mitschülerin per E-Mail. Nennen Sie zwei Wege, auf denen Sie prüfen können, ob er wirklich von ihr stammt.
34. Begründen Sie, warum der Angriff auf einem Flughafen-WLAN leichter ist als im Schulnetz.

Gymnasium Ottweiler