8.2 Grundbegriffe

Die Wörter stammen aus dem Griechischen: *kryptós* (verborgen), *gráphein* (schreiben), *lógos* (Wort, Lehre).

- **Kryptographie** ist die Lehre vom Entwurf von Verschlüsselungsverfahren.
- **Kryptoanalyse** ist die Lehre vom Brechen dieser Verfahren.
- **Kryptologie** ist der Oberbegriff für beides. Wer gute Verfahren bauen will, muss angreifen können – beide Seiten gehören untrennbar zusammen.

Der **Klartext** ist die lesbare Nachricht, der **Geheimtext** (auch: Chiffrat) ihre verschlüsselte Form. Der Vorgang heißt **Chiffrierung** bzw. **Dechiffrierung**, das zugrunde liegende Verfahren **Chiffre**. Die Information, die Sender und Empfänger geheim halten, ist der **Schlüssel**.

Benutzen beide Seiten denselben Schlüssel, heißt das Verfahren **symmetrisch**. Gibt es getrennte Schlüssel zum Ver- und Entschlüsseln, heißt es **asymmetrisch** (Abschnitt 8.9).

8.2.1 Das Prinzip von Kerckhoffs

Ein Anfängerfehler ist es, die Sicherheit auf die Geheimhaltung des Verfahrens zu gründen. Auguste Kerckhoffs formulierte 1883 die bis heute gültige Gegenregel.

Merke: Prinzip von Kerckhoffs

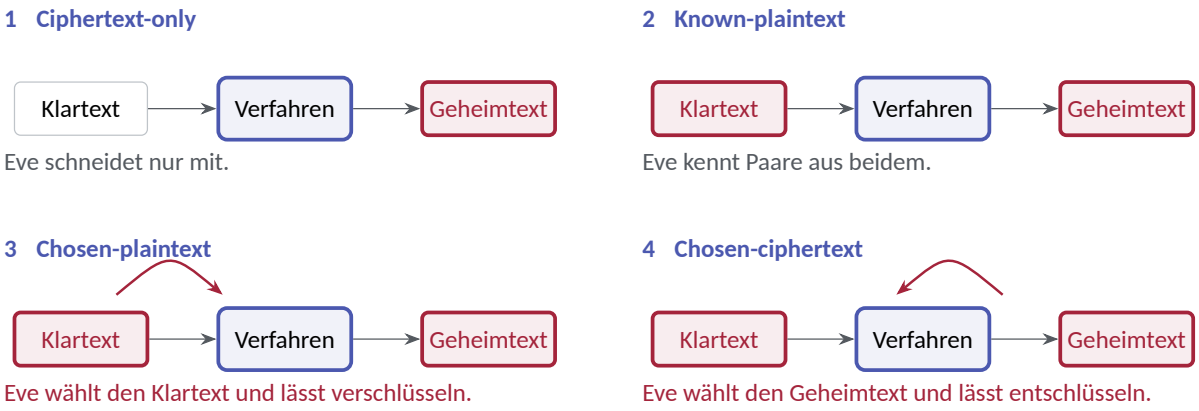
Die Sicherheit eines Verschlüsselungsverfahrens darf allein auf der Geheimhaltung des Schlüssels beruhen, nicht auf der Geheimhaltung des Algorithmus.

Das klingt paradox, ist aber praktisch begründet: Algorithmen werden implementiert, verteilt, disassembliert, von Mitarbeitern weitergetragen. Ein Verfahren, das nur geheim funktioniert, ist genau einmal sicher – bis zum ersten Leck. Ein Schlüssel dagegen lässt sich austauschen, ohne dass alles Übrige neu gebaut werden muss. Moderne Verfahren wie AES sind vollständig veröffentlicht und werden weltweit öffentlich angegriffen; dass sie das aushalten, ist ihr Sicherheitsnachweis.

8.2.2 Angriffsmodelle

Nach Kerckhoffs kennt der Angreifer das Verfahren. Unterschieden wird danach, welches Material ihm darüber hinaus vorliegt.

Gymnasium Ottweiler



Rot = liegt Eve vor. Das *Verfahren* kennt sie nach Kerckhoffs immer, den *Schlüssel* nie.

Die vier Angriffsmodelle. Von oben links nach unten rechts wird Eves Ausgangslage immer besser.

Modell	Der Angreifer hat …	Realistisch, wenn …
Ciphertext-only	nur Geheimtexte	er Datenverkehr mitschneidet
Known-plaintext	Geheimtexte und zugehörige Klartexte	Formulierungen vorhersehbar sind (Briefköpfe, Protokolle)
Chosen-plaintext	er darf Klartexte seiner Wahl verschlüsseln lassen	er Zugang zum Verschlüsselungsgerät hat
Chosen-ciphertext	er darf Geheimtexte seiner Wahl entschlüsseln lassen	ein Server jede Anfrage beantwortet

ZUSATZ

Beide Lehrpläne nennen als Angriffsarten nur Brute-Force, Known-Plaintext und Häufigkeitsanalyse. Die beiden unteren Zeilen der Tabelle — *chosen plaintext* und *chosen ciphertext* — gehen darüber hinaus. Sie stehen hier, weil ohne sie unklar bleibt, woran moderne Verfahren eigentlich gemessen werden.

Ein Verfahren gilt als gut, wenn es selbst im stärksten Modell standhält. Die Verfahren dieses Kapitels scheitern der Reihe nach immer früher, je weiter wir zurückgehen.

Arbeitsauftrag 2

4. Erklären Sie, warum das Prinzip von Kerckhoffs für Open-Source-Software besonders gut passt.
5. Der Klassiker unter den Known-plaintext-Angriffen: Im Zweiten Weltkrieg enthielten viele deutsche Funksprüche das Wort „Wetter“. Erläutern Sie, welchen Vorteil das einem Angreifer verschafft.