8.6 Das One-Time-Pad

ZUSATZ

Aus den bisherigen Angriffen lassen sich zwei Forderungen ableiten: Der Schlüssel darf sich nicht wiederholen, er muss also so lang sein wie die Nachricht, und er darf nur ein einziges Mal benutzt werden. Genau das leistet das **One-Time-Pad** (Vernam-Chiffre, 1917).

Der Schlüssel ist eine echt zufällige Buchstaben- oder Bitfolge, von der Sender und Empfänger je ein identisches Exemplar besitzen. Jedes Zeichen wird mit genau einem Schlüsselzeichen verknüpft, danach wird der verbrauchte Teil vernichtet.

Das One-Time-Pad ist das einzige Verfahren, dessen Sicherheit **bewiesen** ist (Shannon, 1949). Der Grund lässt sich mit den Werkzeugen dieses Kapitels formulieren: Zu einem gegebenen Geheimtext existiert für *jeden* denkbaren Klartext gleicher Länge ein passender Schlüssel. Der Kasiski-Test findet keine Periode, die Häufigkeitsanalyse keine Spalten. Der Geheimtext verrät über den Klartext nichts außer dessen Länge.

Warum benutzen wir es dann nicht überall? Wegen der Praxis:

- Der Schlüssel ist so lang wie alle Nachrichten zusammen und muss vorab sicher ausgetauscht werden. Wer das kann, könnte auch die Nachricht selbst sicher austauschen.
- Er muss echt zufällig sein; Pseudozufallszahlen aus einem Programm genügen nicht.
- Jede Wiederverwendung bricht das Verfahren sofort. Die sowjetischen Funksprüche des Venona-Projekts wurden genau deshalb entziffert: Schlüsselblöcke waren aus Zeitnot doppelt verwendet worden.

Arbeitsauftrag 5

21. Begründen Sie, warum aus einem One-Time-Pad-Geheimtext prinzipiell kein Klartext ableitbar ist, obwohl der Angreifer das Verfahren kennt.
22. Zwei Nachrichten wurden versehentlich mit demselben One-Time-Pad verschlüsselt. Zeigen Sie: Aus c_1 und c_2 lässt sich etwas berechnen, das den Schlüssel nicht mehr enthält. Was?
23. Erklären Sie, warum das One-Time-Pad für den Betrieb einer Webseite ungeeignet ist.

Gymnasium Ottweiler