8.13 Zusammenfassung

- Verschlüsselung schützt die Vertraulichkeit; Integrität und Authentizität brauchen Hashfunktionen und Signaturen.
- Nach Kerckhoffs darf nur der Schlüssel geheim sein, nie das Verfahren.
- Klassische Verfahren kombinieren Transposition und Substitution. Monoalphabetische Substitution fällt der Häufigkeitsanalyse zum Opfer, polyalphabetische dem Kasiski-Test.
- Ein großer Schlüsselraum schützt nur vor Brute Force.
- Das One-Time-Pad ist beweisbar sicher, aber praktisch kaum einsetzbar.
- Symmetrische Verfahren (AES) sind schnell, haben aber das Schlüsselverteilungsproblem.
- Der Schlüsseltausch von Diffie und Hellman löst es ohne jedes Geheimnis auf der Leitung: Beide Seiten potenzieren modular, und das Potenzgesetz sorgt dafür, dass dasselbe herauskommt. Rückwärts steht der diskrete Logarithmus im Weg.
- Asymmetrische Verfahren (RSA) gehen einen Schritt weiter und lösen es über Einweg- und Falltürfunktionen.
- Kein Schlüsselaustausch sichert, *mit wem* man spricht — das ist die Lücke, in die sich ein Man-in-the-Middle setzt und die erst Zertifikate schließen.
- Die Praxis kombiniert beides: asymmetrischer Schlüsselaustausch, symmetrische Datenverschlüsselung, Signaturen und Zertifikate für die Echtheit.

Wiederholungsaufgaben

52. Erläutern Sie an einem selbst gewählten Beispiel den Unterschied zwischen einem passiven und einem aktiven Angriff.
53. Vergleichen Sie Cäsar-, Vigenère- und One-Time-Pad-Chiffre in einer Tabelle nach Schlüssellänge, Schlüsselraum und bekanntem Angriff.
54. Ein Mitschüler behauptet: „Ein Verfahren mit 10^{26} Schlüsseln kann niemand knacken.“ Nehmen Sie begründet Stellung.
55. Skizzieren Sie den Ablauf einer HTTPS-Verbindung und markieren Sie, an welcher Stelle symmetrisch und an welcher asymmetrisch gearbeitet wird.
56. Erklären Sie, warum RSA mit $n = 91$ zwar rechenbar, aber vollkommen unsicher ist.

Gymnasium Ottweiler