Kryptografie und -analyse, Prüfungsprotokoll SS 2022

Prüferin: Dr.-Ing. Elke Franz

Wir haben die Schlüsselverteilung in symmetrisch und asymmetrisch unterteilt. Was bedeutet das und was sind die Vorteile?

Was ist informationstheoretisch perfekte Sicherheit? Geben Sie ein Beispielverfahren an! Wird das Verfahren praktisch angewendet?

Schutzziele der Kryptographie, Warum benutzen wir nicht das informationstheoretisch perfekt sichere Verfahren in Bezug auf die Schutzziele?

Was sind Betriebsarten? Was kann man damit erreichen?

Was ist Electronic Code Book und was ist daran das Problem?

Wie funktioniert Cipher Block Chaining?

Wie funktioniert RSA? Schlüsselgenerierung (Bedingungen, $\Phi(n)$, ...), Ver- und Entschlüsselung?

Ist das gerade eben skizzierte RSA-System sicher?

Was besagt das Prinzip von Kerkhoff?