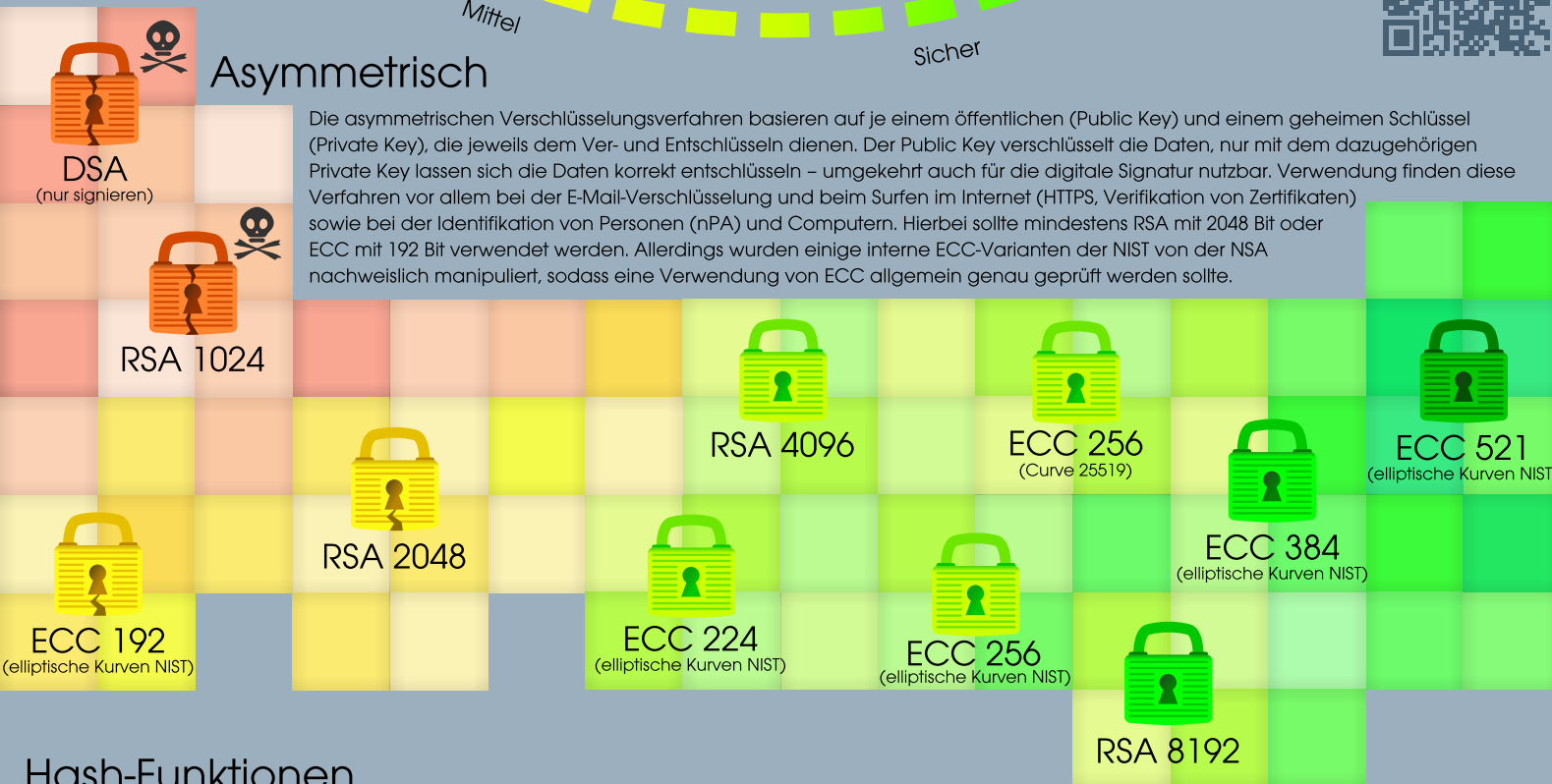
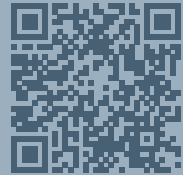
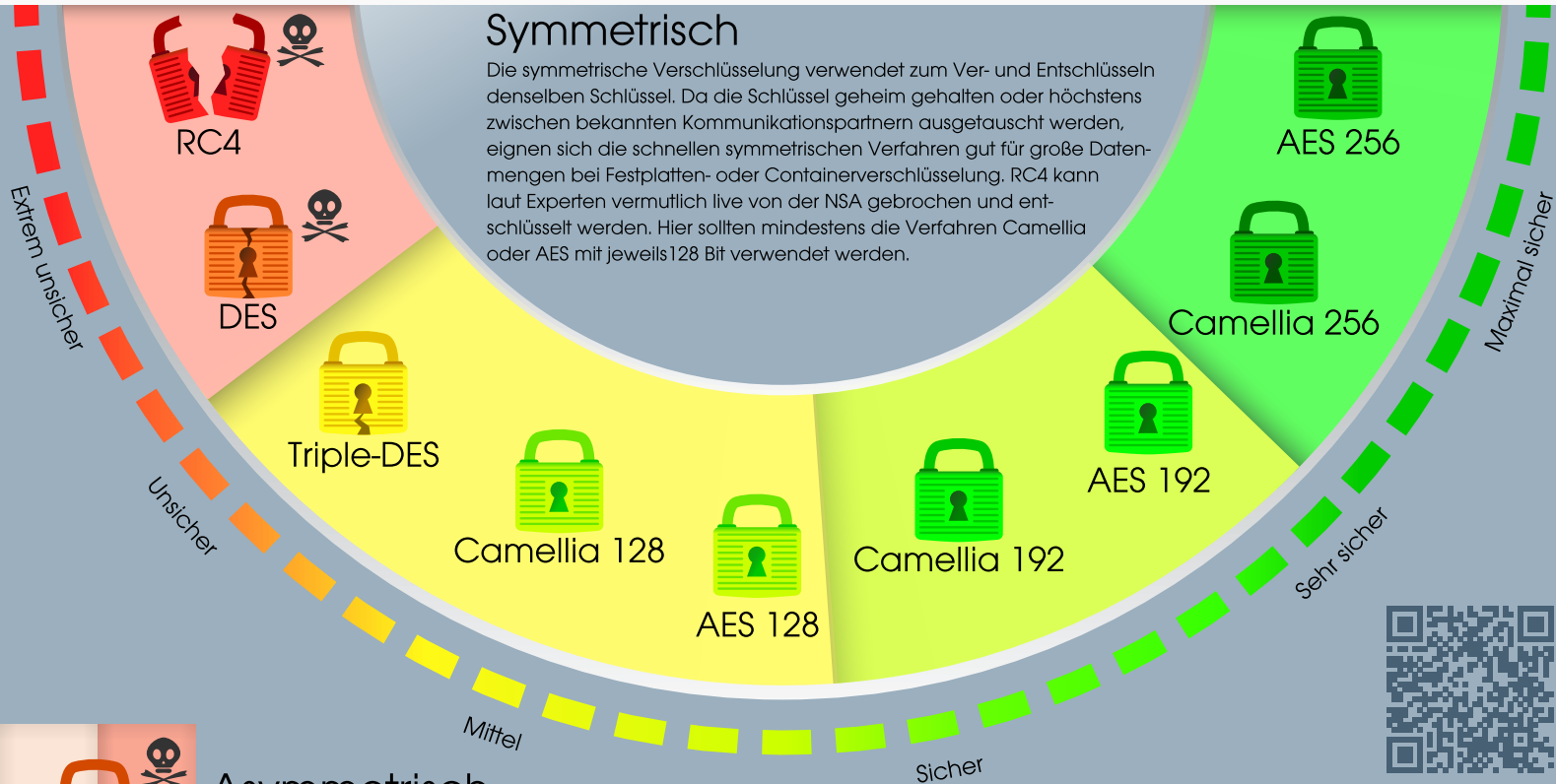


<https://www.internet-sicherheit.de/crypto-poster/>



Hash-Funktionen

Hash-Funktionen reduzieren eine beliebige Menge von Daten auf eine Zahl bestimmter Länge (sog. Fingerabdruck, z.B. 160 Bit). Als Einwegfunktionen bieten sie keine praktikable Möglichkeit auf die ursprünglichen Daten zu schließen. Asymmetrische Verfahren sind deutlich langsamer und nicht für größere Datenmengen geeignet, daher sind Hash-Funktionen von zentraler Bedeutung. Beim Verschlüsseln des damit erzeugten Fingerabdrucks mit dem Private Key kann jeder Empfänger mithilfe des Public Keys prüfen, ob die Nachricht tatsächlich vom Absender stammt und nicht durch einen Dritten manipuliert wurde. Werden allerdings gebrochene Verfahren wie MD5 verwendet, können nahezu beliebige manipulierte Nachrichten untergeschoben werden. Daher sollte mindestens ein Verfahren aus der RIPE-MD- und SHA2/3-Familie mit mindestens 256 Bit gewählt werden.

