Übung 3

1.) **Assume you shall develop an embedded product that processes life-critical (medical) data. Describe whether you would employ crypto hardware or software. Why?**
    a. Es sollte ein Hardware kryptografisches System verwendet werden
    b. Da Gesundheitsdaten gesichert werden sollten, und diese sehr persönlichen Informationen nicht für jeden zugänglich gemacht werden sollten, wäre ein HW-System besser, da diese Systeme schwerer zu knacken/hacken sind.
        i. HW ist signifikant unempfindlicher in Bezug auf Schadsoftware als eine vergleichbare SW-Lösung
        ii. HW ist standardmäßig schnelle, was vor allem beim angesprochenen life-critical Requirement gefordert wird
        iii. Schlüssel können in HW so gestaltet werden, dass sie das HW-Modul nie verlassen, was HW noch einmal sicherere gegenüber Angriffen macht
        iv. Attacken sind allgemein schwieriger als bei einer SW-Lösung
2.) **What about a high-volume sensor (for the mass market) that delivers safety-critical data? Describe whether you would employ crypto hardware or software. Why?**
    a. Es sollte ein Software System verwendet werden
    b. Da es sich um ein Massenprodukt handelt, ist die Lösung über SW empfehlenswert, da diese günstiger ist als eine vergleichsweise HW Lösung
        i. Nachträgliche Sicherheitsupdates sind möglich
        ii. Symmetrische Algorithmen bieten bei SW Lösungen eine hohe Leistung
        iii. Bugs können einfacher gelöst werden
        iv. Umsetzung ist einfacher und darum günstiger
    c. Es handelt sich zwar um sicherheitskritische Daten, wodurch ein HW Lösung die bessere Wahl wäre, allerdings können durch eine gute Wartung Softwareupdates für die nötige Sicherheit bei der SW Variante sorgen.