Übung 1

1.) **Find examples: where are random numbers used (excluding security applications)?**
    a. in der Statistik zur Auswahl von Stichproben aus einer Grundgesamtheit
    b. in der Statistik bei der Monte-Carlo Simulation
    c. für Glücksspielautomaten
    d. zum Testen von Software
    e. Simulationen von elektronischen Schaltungen für zufällige Bauteilwerten (Toleranzen)
2.) **Find examples: where are random numbers used in security applications?**
    a. Asymmetrische Kryptosysteme – Public-Key Kryptographie
        i. RSA
        ii. Elliptische Kurven
        iii. Digitale Signatur
    b. Symmetrische Kryptosysteme
        i. AES – Advanced Encryption Standard
    c. Verschlüsselung
        i. Data Encryption Standard DES – für Bankdienstleistungen
    d. Salt – Speicherung und Übermittlung von Passwörtern
    e. Sicherheitszertifikate
    f. Padding – zufällige padding bits
    g. Nonce
3.) **w/ and w/o security applications: For which applications is randomness more or less important? Which characteristic is most important?**
    a. Für echte und pseudoechte Zufallszahlengeneratoren
    b. Wichtig für kryptografische Verfahren, die auf Zufallszahlen basieren
    c. Wichtigste Eigenschaft von Zufallszahlen ist die Unvorhersagbarkeit. Es muss verhindert werden, dass Muster entstehen bzw. durch längeres Beobachten der Zufallszahlen ein Muster erkannt werden kann, mit dem die Arbeitsweise des Zufallszahlengenerators erkannt werden kann.