1. (5 Punkte) Die Kryptologie unterscheidet die vier Sicherheitsziele *Vertraulichkeit*, *Integrität*, *Authentizität* und *Verbindlichkeit*.
   a. Erläutere kurz, was mit den Sicherheitszielen *Integrität* und *Verbindlichkeit* gemeint ist.
   b. Ordne den folgenden Situationen jeweils das verletzte Sicherheitsziel zu:
      (1) Eve liest eine unverschlüsselte E-Mail von Alice an Bob mit.
      (2) Mallory fängt eine Überweisung ab und ändert den Empfänger.
      (3) Mallory schickt Bob eine Bestellung, die scheinbar von Alice stammt.
      (4) Alice bestreitet nachträglich, einen von ihr verschickten Vertrag verfasst zu haben.

2. (3 Punkte) Erläutere den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung.

3. (2 Punkte) Du willst zur Sicherheit die Daten deiner Festplatte verschlüsseln. Gib an, ob du ein symmetrisches oder asymmetrisches Verschlüsselungsverfahren wählen würdest. Begründe deine Wahl.

4. (3 Punkte) Ein Verein möchte Nachrichten nur noch mit asymmetrischer Verschlüsselung per email empfangen. Deshalb soll der Webmaster, der Zugriff auf den Mailserver hat, den öffentlichen Schlüssel auf der Homepage des Vereins veröffentlichen. Erläutere, wie der Webmaster mit Hilfe eines sogenannten *Man-in-the-Middle-Angriffs* die Nachrichten manipulieren kann.

5. (4 Punkte) Jemand macht folgenden Verbesserungsvorschlag für das Vigenere-Verfahren. Der Klartext wird erst mit dem Schlüssel *GEHEIM* verschlüsselt, der verschlüsselte Text dann nochmal mit dem Schlüssel *ABI* verschlüsselt. Erhöht dieser Vorschlag die Sicherheit des Verfahrens? Begründe deine Antwort.

6. (4 Punkte) Für den Diffie-Hellman Schlüsselaustausch vereinbaren Alice und Bob die Primzahl p und die Primitivwurzel g. Alice wählt als geheime Zahl a, Bob wählt als geheime Zahl b. Die Werte sind: p = 11, g = 7, a = 3, b = 5.
a. Welche Zahlen sind öffentlich und wie werden diese berechnet?
b. Wie heißt der gemeinsame Schlüssel und wie wird er berechnet?

7. (4 Punkte) Für das RSA-Verfahren wählt Bob p und q als Primzahlen und den Verschlüsselungsexponent e.
Die Werte sind: p = 7, q = 13, e = 11.
Warum ist e ein zulässiger Verschlüsselungsexponent?
Wie heißen der öffentliche, wie der private Schlüssel von Bob? Wie werden diese Werte berechnet?

8. (4 Punkte) Bob hat den öffentlichen RSA-Schlüssel (143,23). Alice will Bob die Nachricht 56 schicken. Wie wird die verschlüsselte Nachricht berechnet?

9. (5 Punkte) Alice möchte Bob eine öffentlich lesbare Nachricht n schicken und diese so *signieren*, dass Bob sicher sein kann, dass die Nachricht wirklich von Alice stammt und unterwegs nicht verändert wurde. Alice und Bob besitzen jeweils ein RSA-Schlüsselpaar; zusätzlich ist eine kryptographische Hashfunktion h öffentlich bekannt.
a. Beschreibe, welche Schritte Alice ausführt, um zur Nachricht n die Signatur s zu erzeugen.
b. Beschreibe, wie Bob mit Hilfe von n und s prüft, ob die Signatur gültig ist.
c. Begründe, warum ein Angreifer die signierte Nachricht nicht unbemerkt ändern und warum er auch keine neue Nachricht im Namen von Alice signieren kann.

10. (4 Punkte) Die Sicherheit des RSA-Verfahrens beruht darauf, dass das Produkt $m = p \cdot q$ zweier großer Primzahlen zwar leicht zu berechnen, aber praktisch nicht wieder in seine Primfaktoren zu zerlegen ist.
a. Erkläre, was man unter einer *Einwegfunktion* versteht, und nenne, welche Einwegfunktion beim RSA-Verfahren genutzt wird.
b. Ein Angreifer kennt den öffentlichen Schlüssel (m, e). Erläutere, warum er daraus den privaten Schlüssel nicht praktisch bestimmen kann.
c. Für eine Zahl m mit 300 Dezimalstellen müssen etwa $3 \cdot 10^{147}$ Primzahlen als Teiler getestet werden. Ein Rechner schafft $3 \cdot 10^{19}$ Tests pro Jahr. Schätze die benötigte Zeit ab und vergleiche sie mit dem Alter des Universums (ca. 10^{10} Jahre).

11. (5 Punkte) Beim asymmetrischen Verfahren muss sichergestellt sein, dass ein öffentlicher Schlüssel wirklich zu der Person (oder dem Server) gehört, die ihn präsentiert. Dazu dient eine *Public-Key-Infrastruktur* (PKI) mit Zertifikaten, die von einem Trust-Center ausgestellt werden.
a. Erläutere, welches Problem ein Zertifikat löst und wie ein Trust-Center dabei vorgeht.
b. Nenne zwei Anwendungsbereiche von Public-Key-Infrastrukturen aus dem Alltag.
c. Bewerte einen Sicherheitsaspekt: Was passiert, wenn der private Schlüssel eines Trust-Centers in falsche Hände gerät?

12. (4 Punkte) Eine Schule setzt ein Informatiksystem ein, in dem Noten, Fehlzeiten und Kontaktdaten der Schülerinnen und Schüler gespeichert werden.
a. Erläutere je zwei technische und zwei organisatorische Maßnahmen, mit denen die Datensicherheit dieses Systems gewährleistet werden kann.
b. Erläutere den Unterschied zwischen *Datensicherheit* und *Datenschutz* an diesem Beispiel.

13. (5 Punkte) „Datensicherheit schützt Daten vor unbefugtem Zugriff – ist das dann nicht dasselbe wie Datenschutz?“
a. Erläutere den Kernunterschied zwischen *Datensicherheit* und *Datenschutz*. Gehe darauf ein, *was* jeweils geschützt wird und *welche Daten* jeweils betroffen sind.
b. Begründe die Aussage: „Datensicherheit ist eine Voraussetzung für Datenschutz, aber allein nicht ausreichend.“
c. Ordne jeder Situation zu, ob *Datensicherheit*, *Datenschutz* oder *beides* betroffen ist:
(1) Eine Firma sichert die Baupläne eines neuen Produkts gegen Diebstahl.
(2) Ein Online-Shop schützt die gespeicherten Namen und Adressen seiner Kunden vor Hackern und verwendet sie nur zur Bestellabwicklung.
(3) Eine Schule speichert die Fingerabdrücke aller Schülerinnen und Schüler in einer hervorragend abgesicherten Datenbank.

14. (4 Punkte) Ein Anbieter einer kostenlosen Fitness-App speichert dauerhaft Standort, Puls, Schlafzeiten und Bewegungsprofile aller Nutzerinnen und Nutzer und wertet diese zentral aus.
a. Nenne zwei Gründe, warum die massenhafte Erhebung und Speicherung dieser Daten für die Betroffenen problematisch sein kann.
b. Beurteile das Geschäftsmodell „kostenlose App gegen Daten“ und nenne zwei Maßnahmen, mit denen die Datenverarbeitung datensparsamer gestaltet werden könnte.