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.

   Lösung: a. *Integrität*: Die empfangene Nachricht wurde von keiner dritten Person unbemerkt verändert (manipuliert).
   Verbindlichkeit: Der Urheber einer Nachricht kann nachträglich nicht bestreiten, sie verfasst zu haben.
   b. (1) Vertraulichkeit (2) Integrität (3) Authentizität (4) Verbindlichkeit

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

   Lösung:
   Bei der symmetrischen Verschlüsselung wird für das Ver- und Entschlüsseln nur ein Schlüssel verwendet. Der Schlüssel muss entweder persönlich oder mit Hilfe eines abhörsicheren Kanals vom Sender zum Empfänger übertragen werden. Bei der asymmetrischen Verschlüsselung gibt es zwei Schlüssel, einen privaten und einen öffentlichen Schlüssel, der letztere ist allen möglichen Kommunikationspartnern bekannt. Der private Schlüssel wird nie veröffentlicht, der öffentliche Schlüssel kann über alle zur Verfügung stehenden Publikationsmöglichkeiten veröffentlicht werden (E-Mail, WWW-Seiten, Public-Key-Server, ...). Um die Echtheit eines öffentlichen Schlüssels zu überprüfen, muss es ein Verfahren zur Herstellung von Schlüsselvertrauen geben. Das kann eine (zentrale) Zertifizierungsstelle sein oder ein dezentraler Web-of-Trust-Ansatz.

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.

   Lösung: Bei der Verschlüsselung einer Festplatte ist es wichtig, dass die verschlüsselten Daten schnell ausgelesen werden können, um die Arbeitsgeschwindigkeit nicht zu beeinträchtigen. Der Schlüsselaustausch ist nicht relevant, da sowohl der Empfänger als auch der Sender ein und dieselbe Person sind. Deshalb ist ein symmetrisches Verfahren vorzuziehen.

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.

Lösung: Der Webmaster veröffentlicht seinen eigenen öffentlichen Schlüssel an Stelle des öffentlichen Schlüssels des Vereins auf deren Homepage. Wenn ein Kunde mit Hilfe dieses Schlüssels eine Nachricht an den Verein schickt, fängt der Webmaster die Mail auf dem Mailserver ab, entschlüsselt sie mit Hilfe seines privaten Schlüssels, manipuliert die Nachricht und schickt sie dann mit Hilfe des öffentlichen Schlüssels des Vereins an den Verein weiter.

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.

Lösung:

Der erste Schlüssel *GEHEIM* ist 6 Buchstaben lang und damit ein Vielfaches der Länge des zweiten Schlüsselworts (3). Weil das zweite Schlüsselwort genau in das erste passt, ist es so, als hätte man nur mit einem einzelnen Schlüsselwort der Länge 6 *GFPEJU* verschlüsselt. Da die Sicherheit in erster Linie von der Schlüssellänge abhängt, gewinnt man damit nichts. Anders sähe es aus, wenn die Längen der Schlüssel teilerfremd wären, also z.B. ein Schlüsselwort der Länge 3 und eines der Länge 7. Dadurch entstünde ein neuer Schlüssel der Länge 21.

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?

Lösung: Öffentlich: A=2, B=10, p=11, g=7, Gemeinsamer Schlüssel: K=10
Berechnung: $A = 7^3$ in $\mathbb{Z}_{11}$, $B = 7^5$ in $\mathbb{Z}_{11}$ $K = 2^5 = 10^3$ in $\mathbb{Z}_{11}$

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?

Lösung:

p=7,q=13,e=11
m=p∗q=91
$\tilde{m} = (p-1)*(q-1) = 72$
e zulässig, da ggT(11,72) = 1
d = 1/e = 59 **in** $\mathbb{Z}_{72}$
oeffentlicher Schlüssel: (91,11)
privater Schlüssel: (91,59)
Berechnung von d mit dem erweiterten Euklidschen Algorithmus:

a	b	q	r	x	y
72	11	6	6	2	−13
11	6	1	5	−1	2
6	5	1	1	1	−1
5	1	5	0	0	1

$d = y = -13 = 59$ **in** $\mathbb{Z}_{72}$

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

Lösung:

Alice muss $56^{23} \bmod 143$ berechnen.
Berechnung mit dem Powermod–Verfahren:
Binärdarstellung von 23 = 10111
Potenzen von 56 werden für Potenzen von 2 berechnet:
In $\mathbb{Z}_{143}$:
$56^1 = 56$
$56^2 = -10$
$56^4 = -43$
$56^8 = -10$
$56^{16} = -43$

$56 * -10 * -43 * -43 = 23$ **in** $\mathbb{Z}_{143}$, 23 ist die verschlüsselte Nachricht.

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.

Lösung: a. Alice berechnet den Hashwert $h(n)$ der Nachricht und verschlüsselt diesen mit ihrem *privaten* Schlüssel. Das Ergebnis ist die Signatur s. Sie schickt n und s an Bob.
b. Bob entschlüsselt s mit dem *öffentlichen* Schlüssel von Alice und erhält so den von Alice gebildeten Hashwert. Er berechnet selbst $h(n)$ aus der empfangenen Nachricht und vergleicht beide Werte. Stimmen sie überein, ist die Signatur gültig.
c. Ändert der Angreifer n, so passt der neu berechnete Hashwert $h(n)$ nicht mehr zu dem in s verschlüsselten Hashwert (Integrität). Eine passende Signatur zu einer veränderten oder neuen Nachricht kann er nicht erzeugen, da er den privaten Schlüssel von Alice nicht kennt (Authentizität, Verbindlichkeit).

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).

Lösung: a. Eine Einwegfunktion lässt sich in einer Richtung leicht (mit vertretbarem Aufwand) berechnen, die Umkehrung ist aber praktisch nicht in vernünftiger Zeit möglich. Beim RSA-Verfahren ist das die Multiplikation zweier Primzahlen: $p \cdot q$ ist leicht, die Faktorzerlegung von m ist praktisch unmöglich.
b. Um d zu berechnen, benötigt man $\tilde{m} = (p-1)(q-1)$, also die Primfaktoren p und q von m. Für alle bekannten Faktorisierungsverfahren wächst der Aufwand exponentiell mit der Stellenzahl, sodass die Berechnung für große m nicht in praktisch nutzbarer Zeit gelingt.
c. $\frac{3 \cdot 10^{147}}{3 \cdot 10^{19}} = 10^{128}$ Jahre. Das ist etwa 10^{118}-mal so lang wie das Alter des Universums – der Angriff ist praktisch unmöglich.

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?

Lösung: a. Ein Zertifikat bestätigt die *Authentizität* eines öffentlichen Schlüssels, also die Zuordnung Schlüssel $\leftrightarrow$ Inhaber. Das Trust-Center prüft die Identität des Antragstellers und signiert dann dessen öffentlichen Schlüssel zusammen mit den Inhaberdaten mit seinem eigenen privaten Schlüssel. Wer dem Trust-Center vertraut und dessen öffentlichen Schlüssel kennt, kann das Zertifikat prüfen.
b. Zum Beispiel: Transportverschlüsselung im Web (HTTPS / TLS-Zertifikate), Mailverschlüsselung (S/MIME), digitaler Personalausweis, Signaturkarten.
c. Dann kann der Angreifer beliebige gefälschte Zertifikate ausstellen und sich als jede beliebige Stelle ausgeben (Man-in-the-Middle). Das Vertrauen in alle von diesem Trust-Center ausgestellten Zertifikate ist zerstört; sie müssen zurückgezogen werden.

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.

Lösung: a. Technisch z. B.: verschlüsselte Speicherung und verschlüsselte Übertragung (HTTPS), Zugriffskontrolle mit persönlichen Benutzerkonten und starken Passwörtern / Mehrfaktorauthentifizierung, regelmäßige Sicherungskopien (Backups), aktuelle Software / Sicherheitsupdates.
Organisatorisch z. B.: Rollen- und Rechtekonzept (Lehrkraft sieht nur die eigenen Klassen), Schulung der Mitarbeitenden, klare Regeln zur Weitergabe und Löschung von Daten, protokollierte Zugriffe.
b. *Datensicherheit*: Schutz der Daten vor Verlust, Manipulation und unbefugtem Zugriff (unabhängig davon, um welche Daten es sich handelt). *Datenschutz*: Schutz des Rechts der betroffenen Personen auf informationelle Selbstbestimmung – es dürfen nur die wirklich nötigen personenbezogenen Daten für einen festgelegten Zweck erhoben und verarbeitet werden.

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.

Lösung: a. *Datensicherheit* schützt **Daten** (alle Daten) vor Verlust, Manipulation und unbefugtem Zugriff – im Mittelpunkt stehen technische und organisatorische Maßnahmen. *Datenschutz* schützt **Menschen und ihre Persönlichkeitsrechte** und betrifft nur **personenbezogene** Daten – im Mittelpunkt steht die rechtmäßige Erhebung, Verarbeitung und Nutzung. Datensicherheit fragt „Sind die Daten geschützt?“, Datenschutz fragt „Dürfen diese Daten überhaupt erhoben und verwendet werden?“
b. Sind personenbezogene Daten nicht ausreichend gesichert, können sie abfließen oder manipuliert werden – Datenschutz ist dann nicht mehr gewährleistet. Umgekehrt kann eine perfekt gesicherte Datenbank trotzdem gegen den Datenschutz verstoßen, wenn die Daten ohne Rechtsgrundlage bzw. Einwilligung erhoben oder weitergegeben werden.
c. (1) nur Datensicherheit (keine personenbezogenen Daten). (2) beides (Schutz vor Hackern = Datensicherheit; Zweckbindung = Datenschutz). (3) Datensicherheit erfüllt, Datenschutz möglicherweise verletzt, da die Erhebung der Fingerabdrücke evtl. gar nicht zulässig ist.

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.

Lösung: a. Zum Beispiel: Aus den Bewegungsprofilen lassen sich Wohnort, Arbeitsplatz und Tagesablauf ableiten (Rückschlüsse auf einzelne Personen trotz „anonymer“ Speicherung). Gesundheitsdaten sind besonders sensibel und können bei Weitergabe an Dritte (Versicherungen, Arbeitgeber) oder bei einem Datenleck missbraucht werden. Die Daten können mit anderen Datenquellen zusammengeführt werden; eine spätere Zweckänderung ist für die Betroffenen kaum kontrollierbar.
b. Die Nutzung ist nur scheinbar kostenlos – bezahlt wird mit persönlichen Daten, deren Wert und spätere Verwendung die Nutzenden nicht überblicken. Datensparsamer wäre z. B.: nur die wirklich benötigten Daten erheben, Auswertung lokal auf dem Gerät statt zentral, frühzeitige Löschung bzw. Speicherung nur in aggregierter Form, echte Einwilligung mit klarer Zweckbindung.