1. (3 Punkte) a) Verschlüssele den Klartext `MORGENSTUNDE` mit der Cäsar-Chiffre und Schlüssel 4.
   b) Erläutere, wie ein Angreifer den Klartext wiederherstellen kann, wenn er den Schlüssel nicht kennt.

Lösung: a) `QSVKIRWXYRHI`
b) Es gibt nur 25 mögliche Schlüssel, die der Angreifer ausprobieren kann. Er kann also den Geheimtext mit allen 25 möglichen Schlüsseln entschlüsseln und dabei den Klartext erkennen.

2. (4 Punkte) Die folgenden beiden Zeilen zeigen den Ausgangspunkt für eine Vigenère-Verschlüsselung. Erläutere an dem Beispiel, wie die Verschlüsselung funktioniert, bestimme das Schlüsselwort und den resultierenden Geheimtext.

   `INFORMATIK` (Klartext)
   `CODECODECO` (Schlüssel)

Lösung:

Das Schlüsselwort ist `CODE`. Der Schüssel ist die Wiederholung des Schlüsselworts bis die Länge des Klartexts erreicht ist. Der Klartext wird zeichenweise mit dem Schlüssel `CODECODECO` verschlüsselt. Dabei wird jeder Buchstabe des Klartexts um die Position des entsprechenden Buchstabens im Schlüssel verschoben. Der resultierende Geheimtext ist `KBISTADXKY`.

3. (6 Punkte) Vergleiche die folgenden Verschlüsselungsverfahren:

   - Transpositionsverfahren (z. B. Skytale)
   - monoalphabetische Substitution (z. B. Caesar-Verfahren)
   - polyalphabetische Substitution (z. B. Vigenère-Verfahren)

   Erläutere jeweils, wie die Verschlüsselung erfolgt, und nenne einen Vor- bzw. Nachteil des Verfahrens.

Lösung:

Transposition: Die Buchstaben des Klartextes bleiben erhalten, ihre Reihenfolge wird verändert.
Monoalphabetische Substitution: Jeder Buchstabe wird im gesamten Text durch denselben Ersatzbuchstaben ersetzt.
Polyalphabetische Substitution: Die Ersetzung eines Buchstabens hängt von seiner Position bzw. vom Schlüssel ab.

Mögliche Vor- und Nachteile:
Transposition: einfache Durchführung, aber häufig leicht zu entschlüsseln.
Monoalphabetische Substitution: einfach anzuwenden, aber anfällig für Häufigkeitsanalysen.
Polyalphabetische Substitution: sicherer gegen Häufigkeitsanalysen, jedoch aufwendiger.

4. (4 Punkte) Das Vigenère-Verfahren galt lange Zeit als sicher. Dennoch kann es mit geeigneten Methoden angegriffen werden. Erläutere eine grundlegende Angriffsstrategie auf das Vigenère-Verfahren.

Lösung: Zunächst wird versucht, die Länge des Schlüsselworts zu bestimmen. Dazu können sich wiederholende Buchstabenfolgen im Geheimtext untersucht werden. Kennt man die Schlüssellänge, wird der Geheimtext in mehrere Teiltexte aufgeteilt. Jeder Teiltext wurde mit derselben Verschiebung verschlüsselt. Die einzelnen Teiltexte können danach mit einer Häufigkeitsanalyse untersucht werden.

5. (5 Punkte) Ein Geheimtext wurde mit dem Vigenère-Verfahren verschlüsselt. Die Schlüssellänge wurde bereits als 3 bestimmt.

   Der Geheimtext lautet:

   `OIGORXBKXX`

   Zur weiteren Analyse werden die Buchstaben entsprechend ihrer Position aufgeteilt:

1. Teiltext	2. Teiltext	3. Teiltext
O O B X	I R K	G X X

   Im ersten Teiltext tritt der Buchstabe `O` am häufigsten auf.

   a) Erkläre, warum der Geheimtext in Teiltexte zerlegt wird.

   b) Nimm an, dass `O` für den häufigen deutschen Buchstaben `E` steht. Bestimme die zugehörige Caesar-Verschiebung für den ersten Teiltext.

Lösung:

a) Alle Buchstaben eines Teiltexts wurden mit derselben Verschiebung verschlüsselt. Jeder Teiltext kann daher wie ein Caesar-Geheimtext untersucht werden.

b) E $\rightarrow$ O entspricht einer Verschiebung um 10 Stellen. Die vermutete Caesar-Verschiebung lautet daher 10.

6. (3 Punkte) Ein mit Vigenère verschlüsselter Geheimtext lautet:

   `HBWVHBWVHBWV`

   Man kennt weder den Klartext noch den Schlüssel. Erläutere die Grundidee des Kasiski-Tests und wende sie auf das obige Beispiel an, um eine wahrscheinliche Schlüssellänge zu bestimmen.

Lösung:

Der Kasiski-Test nutzt aus, dass sich Buchstabenfolgen im Klartext oft wiederholen (z. B. häufige Wörter oder Silben). Trifft eine solche Wiederholung im Klartext an zwei Stellen auf dieselbe Phase des periodisch wiederholten Schlüssels, entsteht an beiden Stellen dieselbe Geheimtextfolge. Der Abstand zwischen zwei gleichen Geheimtextfolgen ist dann ein Vielfaches der Schlüssellänge.

Im Beispiel wiederholt sich die Folge `HBWV` an den Positionen 1, 5 und 9. Die Abstände zwischen den Wiederholungen betragen 4 und 8 Zeichen. Der größte gemeinsame Teiler dieser Abstände ist 4. Die wahrscheinliche Schlüssellänge beträgt daher `4`.

7. (4 Punkte) Beim One-Time-Pad wird ein Klartext mit einem zufällig erzeugten Schlüssel verschlüsselt, der genauso lang wie der Klartext ist und nur ein einziges Mal verwendet wird.

   1. Erkläre kurz, wie die Ver- und Entschlüsselung beim One-Time-Pad grundsätzlich abläuft.
   2. Begründe, warum das One-Time-Pad als absolut sicheres Verschlüsselungsverfahren gilt, sofern der Schlüssel wirklich zufällig, geheim und nur einmal verwendet wird.
   3. Nenne einen Grund, warum das One-Time-Pad trotz seiner absoluten Sicherheit in der Praxis kaum eingesetzt wird.

Lösung:

1. Klartext und Schlüssel bestehen aus Zeichen gleicher Länge. Jedes Klartextzeichen wird mit dem an derselben Position stehenden Schlüsselzeichen verknüpft, wodurch das Geheimtextzeichen entsteht. Zur Entschlüsselung wird derselbe Schlüssel mit der Umkehroperation angewendet.

2. Da der Schlüssel echt zufällig, genauso lang wie der Klartext und nur ein einziges Mal verwendet wird, ist für jedes mögliche Geheimtextzeichen jedes Klartextzeichen gleich wahrscheinlich. Ein Angreifer, der nur den Geheimtext kennt, kann somit rein rechnerisch keinerlei Information über den Klartext gewinnen, egal wie viel Rechenleistung ihm zur Verfügung steht – selbst Ausprobieren aller Schlüssel liefert jeden denkbaren Klartext gleicher Länge als mögliches Ergebnis.

3. Der Schlüssel muss mindestens so lang wie der Klartext sein und darf nur ein einziges Mal benutzt werden. Für einen sicheren Nachrichtenaustausch müsste daher für jede Nachricht ein neuer, echt zufälliger Schlüssel erzeugt und auf einem sicheren Weg zwischen Sender und Empfänger ausgetauscht werden, was in der Praxis (großer Schlüsselaufwand, sichere Verteilung) meist unpraktikabel ist.

8. (4 Punkte) Ein Schüler behauptet: „Ein Verschlüsselungsverfahren ist nur dann sicher, wenn der Algorithmus, also die genaue Funktionsweise der Verschlüsselung, geheim bleibt. Kennt der Angreifer das Verfahren, ist die Verschlüsselung wertlos.“

   Erläutere das Kerckhoffs'sche Prinzip und nimm begründet Stellung zu der Aussage des Schülers.

Lösung:

Das Kerckhoffs'sche Prinzip besagt, dass die Sicherheit eines Verschlüsselungsverfahrens allein auf der Geheimhaltung des Schlüssels beruhen soll, nicht auf der Geheimhaltung des Algorithmus selbst. Der Algorithmus darf also öffentlich bekannt sein; ein Angreifer, der das Verfahren kennt, aber nicht den Schlüssel, soll den Klartext trotzdem nicht ermitteln können.

Die Aussage des Schülers ist daher nicht richtig. Ein Verfahren, dessen Sicherheit von der Geheimhaltung des Algorithmus abhängt, gilt als unsicher, denn sobald der Algorithmus bekannt wird – etwa durch Reverse Engineering, Spionage oder Veröffentlichung –, ist das gesamte Verfahren gebrochen und muss durch ein neues ersetzt werden. Zudem lässt sich ein geheimer Algorithmus in der Praxis kaum dauerhaft geheim halten und nicht von unabhängigen Fachleuten auf Schwachstellen überprüfen.

9. (4 Punkte) Ein Unternehmen entwickelt ein neues Verschlüsselungsverfahren. Die Entwickler sind der Meinung, dass das Verfahren sicher ist, weil der verwendete Algorithmus nicht veröffentlicht wird.

   Erläutere das Kerckhoffs'sche Prinzip und bewerte die Aussage der Entwickler. Gehe dabei darauf ein, wovon die Sicherheit eines modernen Verschlüsselungsverfahrens tatsächlich abhängen sollte.

Lösung: Nach dem Kerckhoffs'schen Prinzip darf die Sicherheit eines Verschlüsselungsverfahrens nicht von der Geheimhaltung des Algorithmus abhängen. Es wird angenommen, dass Angreifer den Algorithmus kennen, geheim bleiben soll lediglich der verwendete Schlüssel. Ein sicheres Verfahren muss auch dann sicher bleiben, wenn sein Aufbau öffentlich bekannt ist. Die Aussage der Entwickler ist daher nicht überzeugend und widerspricht dem Kerckhoffs'schen Prinzip.

10. (3 Punkte) Verschlüsselung begegnet uns im Alltag an vielen Stellen, auch wenn sie oft im Hintergrund abläuft und nicht bewusst wahrgenommen wird.

    Nenne **drei** unterschiedliche Anwendungsbereiche, in denen Verschlüsselung eingesetzt wird, und beschreibe jeweils kurz, welche Daten dabei geschützt werden und wovor.

Lösung:

- **Verschlüsselte Kommunikation (z. B. Messenger wie Signal oder WhatsApp):** Die Inhalte von Nachrichten werden verschlüsselt, sodass nur Sender und Empfänger sie lesen können. Geschützt wird der Inhalt der Kommunikation vor Mitlesen durch Dritte, etwa den Anbieter des Dienstes oder Angreifer im Netz.
- **Datenübertragung im Web (HTTPS):** Die Verbindung zwischen Browser und Webserver wird verschlüsselt (z. B. beim Online-Banking oder Onlineshopping). Geschützt werden dabei übertragene Daten wie Passwörter, Zahlungsinformationen oder persönliche Angaben vor dem Mitlesen oder Verändern durch Dritte während der Übertragung.
- **Verschlüsselte Speicherung von Daten (z. B. Festplattenverschlüsselung, Cloud-Speicher):** Dateien werden auf dem Gerät oder in der Cloud nur in verschlüsselter Form gespeichert. Geschützt werden die gespeicherten Daten vor unbefugtem Zugriff, etwa bei Diebstahl des Geräts oder Einbruch in den Cloud-Speicher.
- **WLAN-Verschlüsselung (z. B. WPA2/WPA3):** Der Datenverkehr zwischen Gerät und WLAN-Router wird verschlüsselt. Geschützt werden übertragene Daten vor dem Mitlesen durch andere Personen in Reichweite des Funknetzes.

11. (4 Punkte) Viele Apps auf dem Smartphone, z. B. Wetter-Apps, Navigations-Apps oder soziale Netzwerke, fragen bei der Installation nach der Berechtigung, auf den Standort (Geodaten) des Geräts zuzugreifen.

    1. Erkläre, wie Smartphones den eigenen Standort technisch bestimmen können.
    2. Nenne zwei legitime Gründe, warum eine App Geodaten benötigen könnte.
    3. Beschreibe ein Risiko, das entsteht, wenn Geodaten über einen längeren Zeitraum gesammelt und gespeichert werden.

Lösung:

1. Smartphones bestimmen ihren Standort meist über GPS (Satellitensignale), können ihn aber auch über die Position naher WLAN-Netze, die Entfernung zu Mobilfunkmasten oder eine Kombination dieser Verfahren ermitteln, wenn kein GPS-Signal verfügbar ist.

2. Beispiele: Eine Navigations-App benötigt den Standort, um eine Route berechnen zu können. Eine Wetter-App benötigt ihn, um das Wetter für den aktuellen Aufenthaltsort anzuzeigen. (Weitere gültige Beispiele: Standortmarkierung bei Fotos, Finden von Geschäften in der Nähe.)

3. Werden Geodaten über längere Zeit gesammelt, lässt sich aus den Bewegungsmustern ein detailliertes Profil erstellen, aus dem sich z. B. Wohnort, Arbeitsplatz, Tagesablauf oder besuchte Orte (etwa Arztpraxen) ablesen lassen. Gelangen diese Daten in falsche Hände oder werden sie mit anderen Daten verknüpft, können daraus sehr persönliche Rückschlüsse gezogen und die Betroffenen z. B. überwacht, erpresst oder gezielt beeinflusst werden (z. B. durch personalisierte Werbung).

12. (3 Punkte) Beim Besuch vieler Websites erscheint zunächst ein Cookie-Banner, das um Zustimmung zur Verwendung von Cookies bittet.

    1. Erkläre, was Cookies sind und welche personenbezogenen Daten mit ihrer Hilfe über Nutzerinnen und Nutzer gesammelt werden können.
    2. Erläutere den Unterschied zwischen notwendigen Cookies und Tracking-Cookies.

Lösung:

1. Cookies sind kleine Textdateien, die eine Website beim Besuch im Browser des Nutzers speichert und bei einem erneuten Besuch wieder ausliest. Über Cookies können unter anderem gespeichert werden: Login-Zustände, Spracheinstellungen, der Inhalt eines Warenkorbs, besuchte Seiten und Verweildauer, sowie eine eindeutige Kennung (ID), mit der ein Nutzer bei späteren Besuchen wiedererkannt werden kann. In Kombination lassen sich daraus Nutzungsprofile erstellen, etwa welche Interessen jemand hat oder welche Seiten regelmäßig besucht werden.

2. Notwendige Cookies sind für die Grundfunktion einer Website erforderlich, z. B. um einen Nutzer während einer Sitzung eingeloggt zu halten oder den Warenkorb zu speichern; sie dienen nicht der Datensammlung zu anderen Zwecken. Tracking-Cookies dagegen werden gezielt eingesetzt, um das Verhalten von Nutzern über mehrere Websites hinweg zu verfolgen, meist zu Zwecken der Werbung oder Marktanalyse. Sie stammen häufig von Drittanbietern (z. B. Werbenetzwerken), die auf vielen verschiedenen Websites eingebunden sind und so ein umfassenderes Bewegungsprofil im Web erstellen können.

13. (4 Punkte) Personenbezogene Daten werden bei der Nutzung von Webseiten und Apps häufig automatisch erfasst.

    Beschreibe vier Möglichkeiten, mit denen Nutzerinnen und Nutzer das Sammeln personenbezogener Daten einschränken können.

Lösung: Mögliche Antworten:

- Nicht notwendige Cookies ablehnen.
- Standortfreigaben deaktivieren oder nur bei Bedarf erlauben.
- App-Berechtigungen regelmäßig überprüfen und einschränken.
- Datenschutzfreundliche Suchmaschinen verwenden.
- Anonymes bzw. privates Surfen nutzen.
- Tracking-Schutz oder Werbeblocker einsetzen.
- Nur notwendige persönliche Angaben machen.

14. (4 Punkte) Beim Einrichten einer neuen App auf dem Smartphone fragt diese nach verschiedenen Berechtigungen, unter anderem nach Zugriff auf Kontakte, Kamera und Standort.

    1. Erkläre, was mit der „Rechteverwaltung“ (Berechtigungen) von Apps gemeint ist und wie sie dabei hilft, das Sammeln personenbezogener Daten einzuschränken.
    2. Eine Taschenlampen-App fordert bei der Installation Zugriff auf die Kontakte und den Standort des Geräts an. Bewerte diese Forderung und begründe, wie ein Nutzer in diesem Fall sinnvoll vorgehen sollte.
    3. Nenne eine weitere Einstellungsmöglichkeit (außer der App-Rechteverwaltung), mit der sich die Weitergabe des eigenen Standorts einschränken lässt.

Lösung:

1. Bei der Rechteverwaltung legt das Betriebssystem fest, dass Apps für den Zugriff auf bestimmte Funktionen oder Daten des Geräts (z. B. Kamera, Mikrofon, Kontakte, Standort) explizit die Erlaubnis der Nutzerin oder des Nutzers einholen müssen. Dadurch kann gezielt entschieden und jederzeit wieder geändert werden, welche App auf welche persönlichen Daten zugreifen darf, statt dass jede App automatisch uneingeschränkten Zugriff auf alle Daten des Geräts hat.

2. Der Zugriff auf Kontakte und Standort ist für die Funktion einer Taschenlampen-App nicht notwendig. Eine solche Berechtigungsanfrage ist daher als unangemessen zu bewerten und ein Hinweis darauf, dass die App möglicherweise personenbezogene Daten zu anderen Zwecken sammeln möchte (z. B. für Werbung oder Weiterverkauf der Daten). Ein Nutzer sollte diese Berechtigungen verweigern bzw. nicht erteilen; funktioniert die App danach nicht mehr wie erwartet oder verlangt sie die Rechte zwingend, sollte eine alternative App ohne diese Anforderungen gewählt werden.

3. Weitere Möglichkeiten, z. B.: Deaktivieren der Standortdienste (GPS) auf Betriebssystemebene, wenn sie nicht benötigt werden; Freigabe des Standorts nur „einmalig“ oder „nur während der Nutzung der App“ statt dauerhaft; Deaktivieren der WLAN- und Bluetooth-Standorterkennung.

15. (5 Punkte) Alice möchte Bob eine vertrauliche Nachricht senden. Bob besitzt ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel.

    Beschreibe den Ablauf der Verschlüsselung und Entschlüsselung.

    Gehe dabei auf die folgenden Fragen ein:

    a) Welchen Schlüssel verwendet Alice zur Verschlüsselung?

    b) Welchen Schlüssel verwendet Bob zur Entschlüsselung?

    c) Warum kann eine dritte Person die Nachricht nicht lesen, obwohl der öffentliche Schlüssel bekannt ist?

Lösung:

a) Alice verschlüsselt die Nachricht mit Bobs öffentlichem Schlüssel.

b) Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel.

c) Der öffentliche Schlüssel reicht nicht zum Entschlüsseln aus. Dazu wird der private Schlüssel benötigt, den nur Bob besitzt.