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.

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)

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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?